



Romel Cabling ▾



Home

Home > My courses > Seminars and Tours > O4 [Enter Module Title Here] > Lesson Proper for Week 4

# Lesson Proper for Week 4

When your computer is connected to the Internet, you are exposing your computer to a variety of potential threats. The Internet is structured so that if you can browse the Internet, all other computers on the Internet can communicate with your computer.

This leaves you extremely vulnerable to a variety of common attacks. This becomes especially troubling as several popular programs (such as Napster) open up services on your own computer that allow others to view files on your computer!

While this functionality is expected, the difficulty is that security flaws are discovered on a regular basis that allow hackers to attack your computer with the potential to view or destroy the sensitive data stored on your computer.

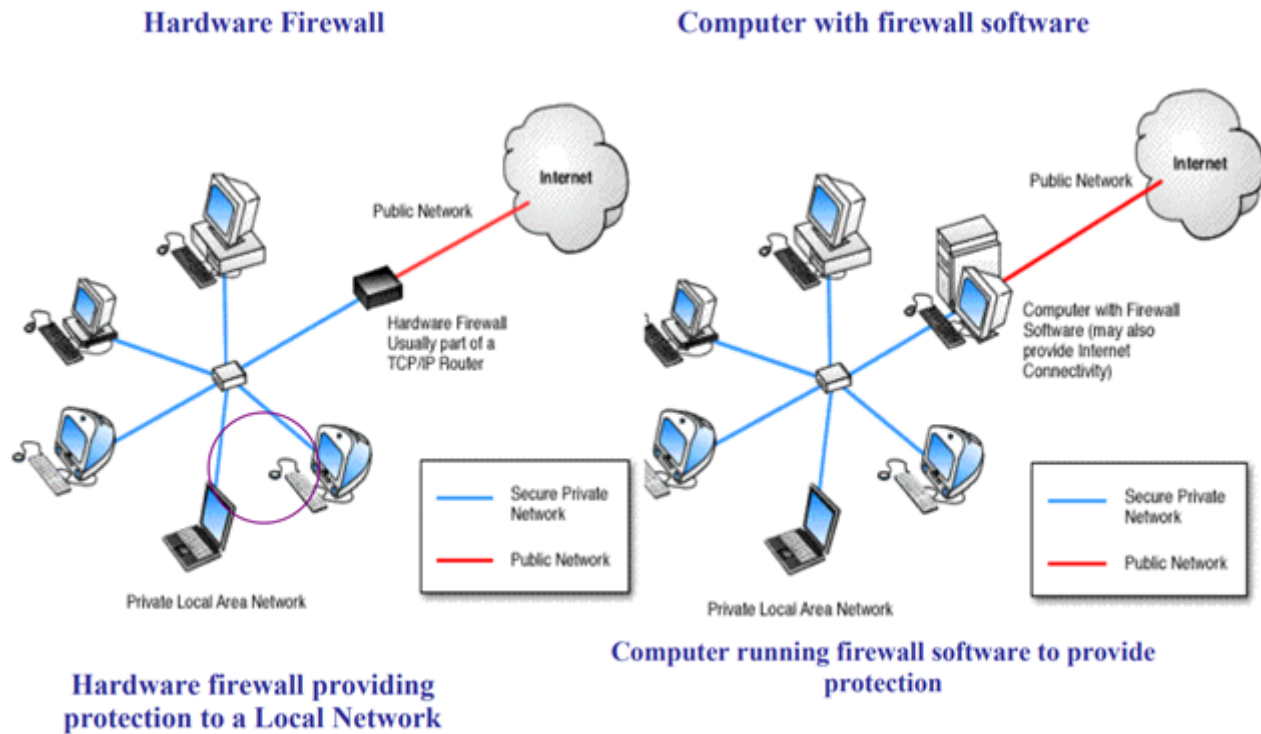
To secure your computer from such attacks you need to "teach" your computer to ignore or resist external connection attempts and probes. The generic term for such a program is a Firewall.

A Firewall protects a network by guarding the points of entry to it. The increasing complexity of networks, and the need to make them more open due to the growing emphasis on and attractiveness of the Internet as a medium for business transactions, mean that networks are becoming more and more exposed to attacks, both from without and from within. The search is on for mechanisms and techniques for the protection of internal networks from such attacks. One of the protective mechanisms under serious consideration is the Firewall. Firewalls are becoming more sophisticated by the day, and new features are constantly being added, so that, in spite of the criticisms made of them and developmental trends threatening them, they are still a powerful protective mechanism.

## 1. What is Firewall?

- A *computer firewall* protects networked computers from intentional unauthorized interruption which are result in data corruption or denial of service.
- It is a network *firewall* sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.
- It may be a hardware device or a software program running on a secure host computer.

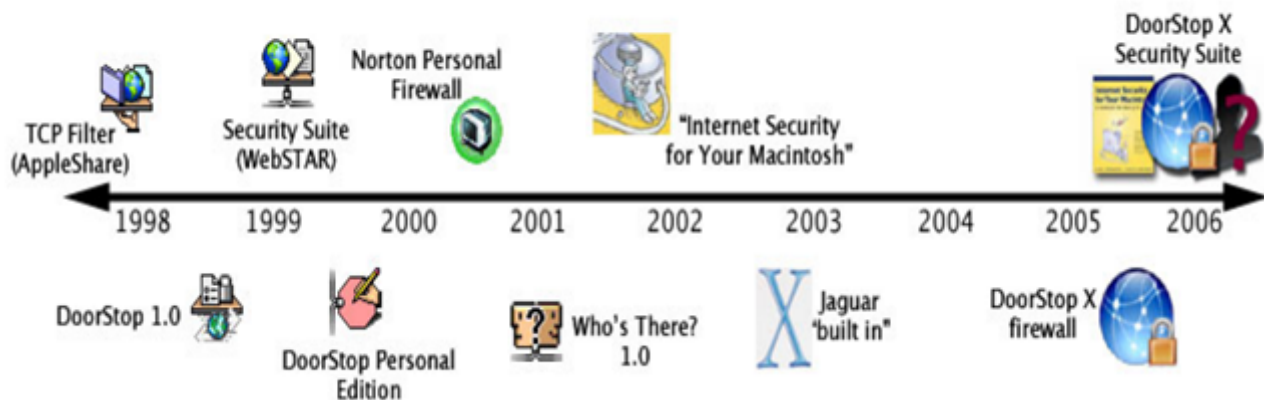
Both figures are shown in below



## 2. History of Firewall?

Open Door Networks shipped the first Macintosh firewall (for Mac OS 8.1) in 1998. With the DoorStop X Firewall and the DoorStop X Security Suite, Open Door has gotten back into the business that it helped get started.

### Macintosh firewall timeline



## 3. How does a firewall work?

### I. Components of a Secured System:

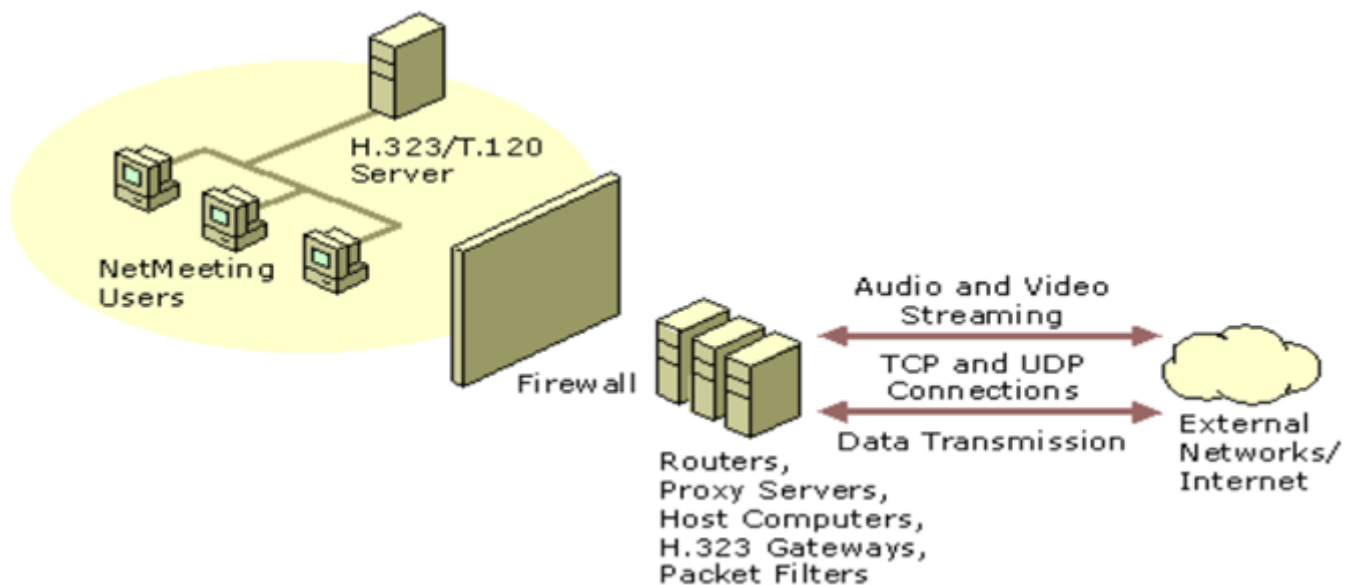
A Firewall is a set of security mechanisms that an organization implements both logically and physically, to prevent unsecured access to an internal network. Firewall configurations vary from organization to organization. Most often, the firewall consists of several components, which can include a combination of the following:

- Routers
- Proxy Servers

- Host Computers
- Gateways
- Networks with appropriate security software

Very rarely is a firewall a single component, although a number of newer commercial firewalls attempt to put all of the components into a single computer.

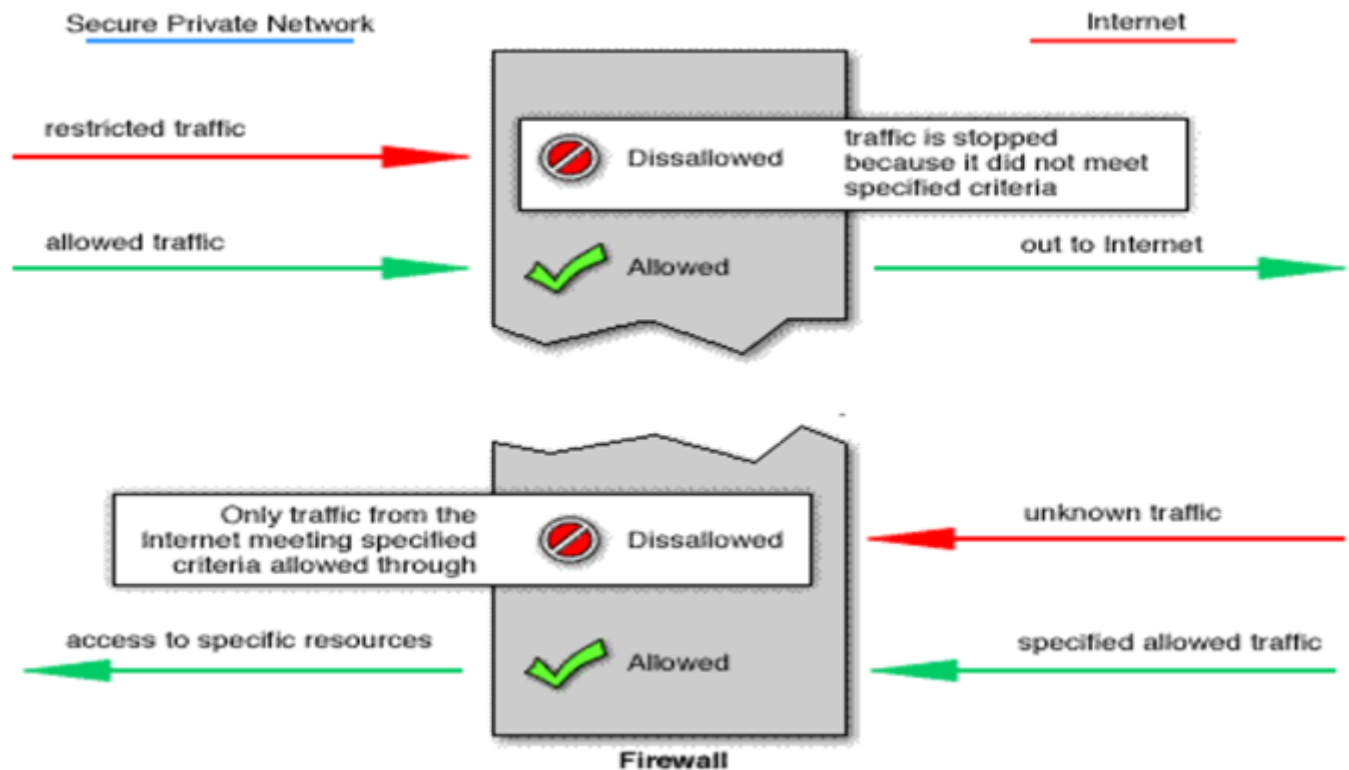
The following illustration shows a firewall configuration



The firewall might respond as a host, resulting in a virtual computer, or pass on packets bound for these hosts to assigned computers.

## II. Basic Firewall Operation:

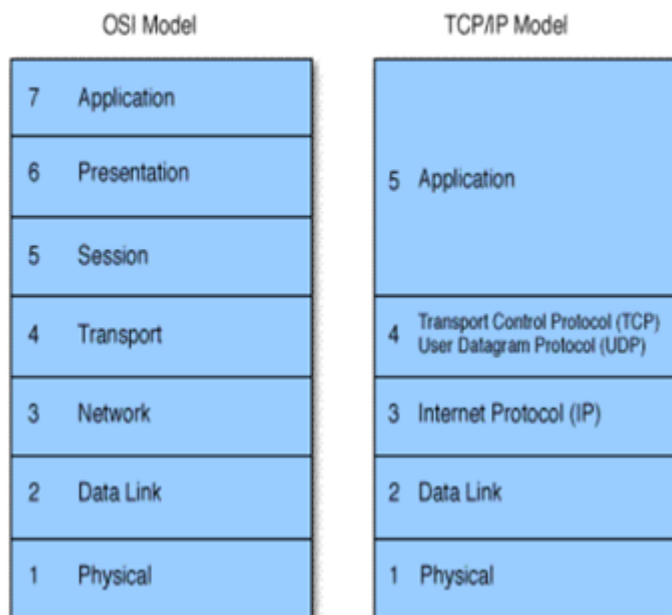
- There are two access denial methodologies used by computer firewalls. A Firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria.
- The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another.
- Computer Firewalls may be concerned with the type of traffic, or with source or destination addresses and ports.
- They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through. How a computer firewall determines what traffic to let through depends on which network layer it operates at.



### III. How does a network firewall interact with OSI and TCP/IP Network models?

- Network architecture is designed around a seven layer model. Each layer has its own set of responsibilities, and handles them in a well-defined manner. This enables networks to mix and match network protocols and physical supports.
- In a given network, a single protocol can travel over more than one physical support (layer one) because the physical layer has been dissociated from the protocol layers (layers three to seven).
- Similarly, a single physical cable can carry more than one protocol. The TCP/IP model is older than the OSI industry standard model which is why it does not comply in every respect. The first four layers are so closely analogous to OSI layers however that interoperability is a day to day reality.
- Network Firewalls operate at different layers to use different criteria to restrict traffic.
- *The lowest layer at which a firewall can work is layer three.* In the OSI model this is the network layer. In TCP/IP it is the Internet Protocol layer.
- This layer is concerned with routing packets to their destination. At this layer *a firewall can determine whether a packet is from a trusted source, but cannot be concerned with what it contains or what other packets it is associated with.*
- *Firewalls that operate at the transport layer know a little more about a packet, and are able to grant or deny access depending on more sophisticated criteria. At the application level, firewalls know a great deal about what is going on and can be very selective in granting access.*

## The OSI and TCP/IP models



➤ It would appear then, that firewalls functioning at a higher level in the stack must be superior in every respect. This is not necessarily the case, however.

➤ The lower in the stack the packet is intercepted, the more secure the firewall. If the intruder cannot get past level three, it is impossible to gain control of the operating system.

### 4. Types of Firewalls:

Firewalls fall into four broad categories:

- Packet filters*
- Circuit level gateway*
- Application level gateways*

#### a. Packet Filtering:

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP.
- They are usually part of a router firewall. A router is a device that receives packets from one network and forwards them to another.
- In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator.
- Filtering packets can limit or disable services such as NFS or telnet, restrict access to and from specific systems or domains, and hide information about subnets.

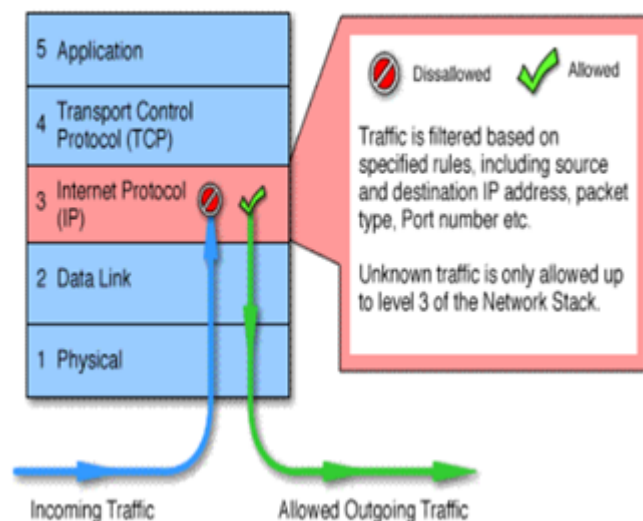
A firewall could filter the following fields within packets:

- packet type, such as IP, UDP, ICMP, or TCP;
- source IP address, the system from which the packet originated;
- destination IP address, the system for which the packet is destined;

- destination TCP/UDP port, a number designating a service such as telnet, ftp, smtp, nfs, etc., located on the destination host, and
- Source TCP/UDP port, the port number of the service on the host originating the connection.

→ The advantage of packet filtering firewalls is their low cost and low impact on network performance. Most routers support packet filtering.

### Packet Filtering Firewall



Usually, the following services are **blocked** at a firewall

➤ **tftp**, trivial ftp, used for booting diskless workstations, terminal servers and routers, can also be used to read any file on the system if set up incorrectly;

➤ **X Windows, Sun Open Windows**, can leak information from X window displays, such as all keystrokes;

→ SunRPC, including NIS and NFS, which can be used to steal system information such as passwords and read and write to files;

These services are inherently open to abuse and therefore should be blocked directly at the firewall. Other services, whether inherently dangerous or not, is usually filtered and possibly restricted to only those systems that need them.

These would include:

- **telnet, ftp** (often restricted to only certain systems);
- **SMTP** (Simple Mail Transfer Protocol) often restricted to a central e-mail server;
- **RIP** (Routing Information Protocol) which can be spoofed to redirect packet routing to the wrong place causing denial of service on the network, is often unnecessary if a single default route exists;
- **DNS** (Domain Names Service) zone transfers, contains names of hosts and information about hosts that could be helpful to attackers;

b. Circuit level Gateway:

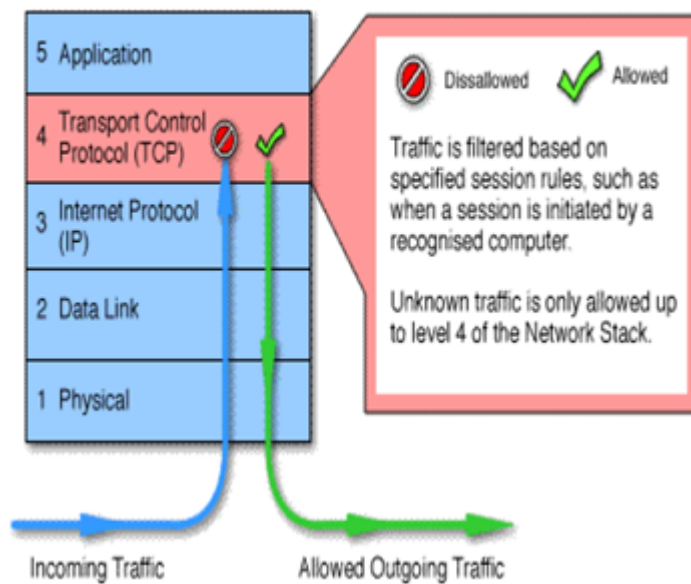
→ Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP.

→ They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit level gateway appears to have originated from the gateway.

→ The advantage of circuit level gateways is useful for hiding information about protected networks. Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect.

→ On the other hand, they do not filter individual packets.

## Circuit level gateway



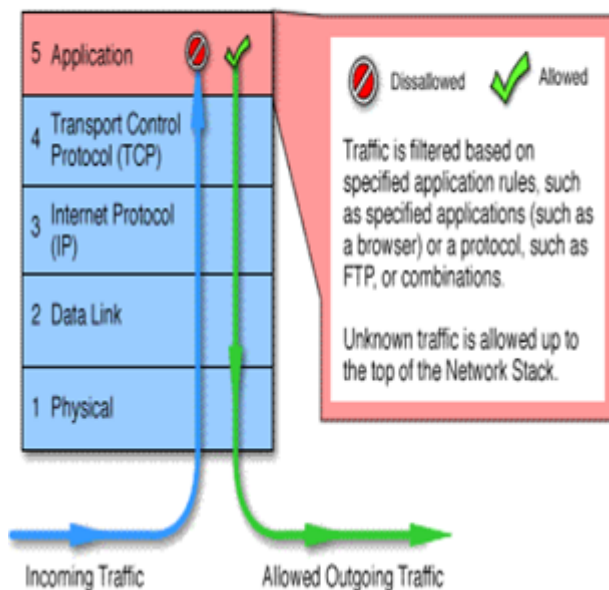
➤ A typical use of circuit-level gateways is situation in which the system administrator trusts the internal users.

### c) Application level Gateway:

➤ **Application level gateways**, also called **proxies**, are similar to circuit-level gateways except that they are application specific.

- They can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy.
- In plain terms, an application level gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through. Because they examine packets at application layer, they can filter application specific commands such as http: post and get, etc.
- This cannot be accomplished with either packet filtering firewalls or circuit level neither of which knows anything about the application level information.

## Application level Gateway



➤ *The advantage of Application level gateways is used to log user activity and logins. They offer a high level of security.*

➤ They have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer.

## 5. Functionalities of Firewall:

- Firewall can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.



→ Firewalls can filter packets based on their source, destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

The following four general techniques are used to control access and enforce the site's security policy.

#### Ä Service control:

- To determine which services on internal hosts are accessible for external access and to reject all other incoming service requests.
- Outgoing service requests and the responses to them may also be controlled.
- These filtering actions can be based on the contents of IP packets, TCP and UDP requests and port number.

**Ex:** incoming HTTP requests may be rejected unless they are directed to an official web server host.

#### Ä Behavior control:

- To prevent behavior that infringes the organization's policies, is anti-social or has no discernible legitimate purpose and is hence suspected of forming part of an attack.
- Some of these filtering actions may be applicable at the IP or TCP level, but others may require interpretation of messages at a higher level.

**Ex:** filtering of email 'spam' attacks may require examination of the sender's email address in message headers or even the message contents.

#### Ä Direction control:

Determines the direction in which particular service requests may be initiated and allowed the flow through the firewall.

#### Ä User control :

- The organization may wish to discriminate between its users, allowing some access to external services but inhibiting others from doing so.
- It is applied to local users, external users.

**Ex:** User control that is perhaps more socially acceptable than some is to prevent the acknowledging of software except to users who are members of the system administration team.

## 6. Example Implementation Of Firewall:

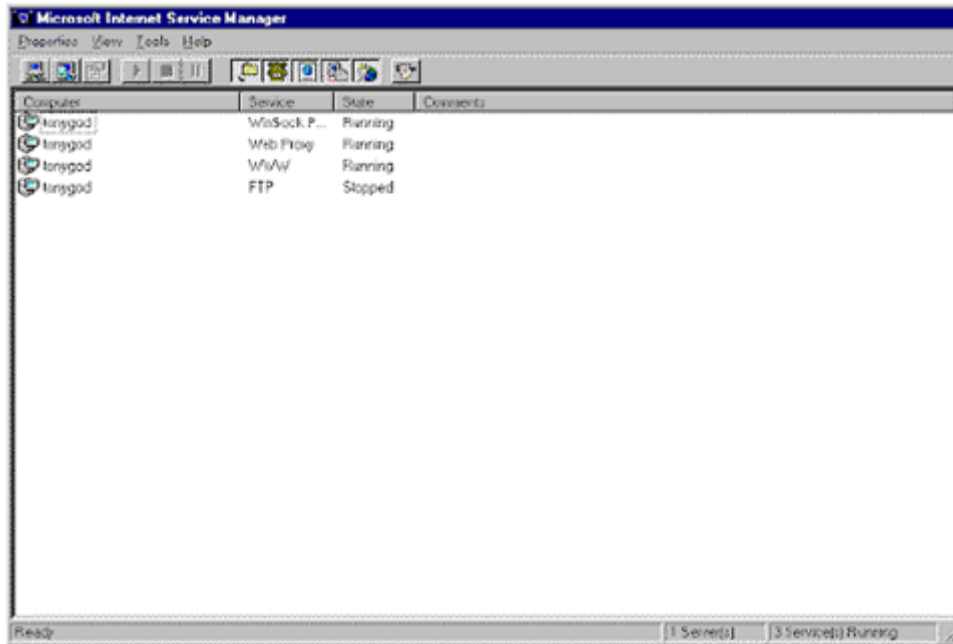


As we gave a figure of Firewall components for Net Meeting users. This section provides a guideline for setting up the Microsoft Proxy Server to enable the necessary ports for NetMeeting outbound calls.

Microsoft Proxy Server and Microsoft Internet Information Services are run on Windows NT 4.0.

### To configure the Microsoft Proxy Server for NetMeeting

Start the Microsoft Internet Service Manager, and then click **Winsock Proxy Service**.



1. Click the **Protocols** tab, and then click **Add**. The **Protocol Definition** dialog box appears.
2. Refer to the table in "**Establishing a NetMeeting Connection with a Firewall**" and add each port required for NetMeeting by typing or selecting values for the following fields:

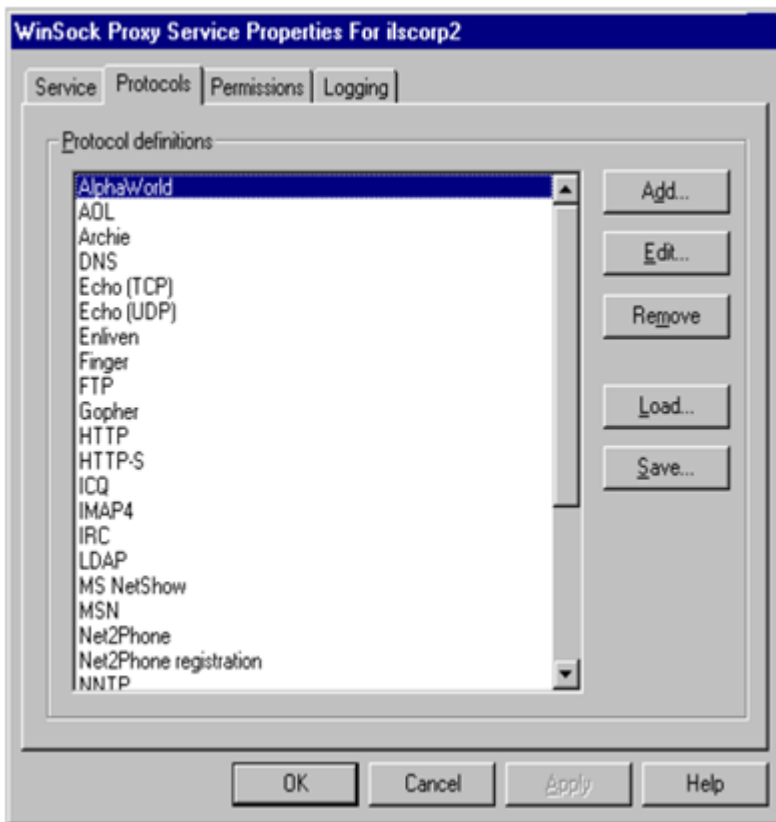
- Protocol name
- Port
- Type Direction

**Protocol name**    Type **LDAP**

**Port**                Type **389**

**Type**                Click **TCP** (default)

**Direction**        Click **Outbound**



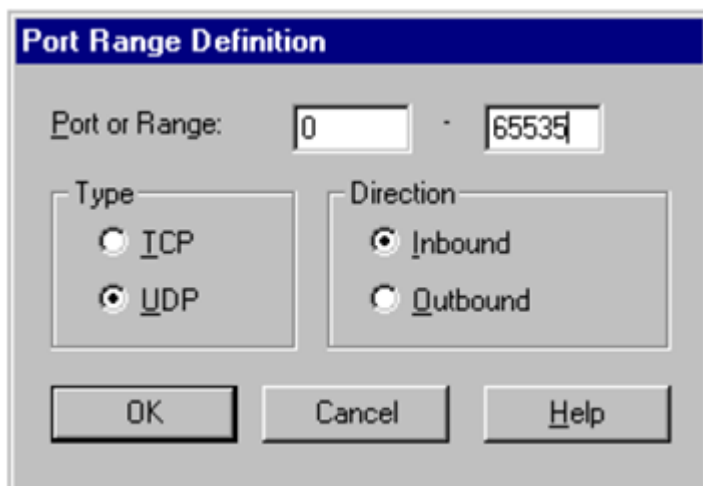
For example, if you want to add port 389, you would enter the following settings: In Do this

For TCP-only ports, click OK after adding information for each port and then continue to step 5. For ports that require UDP connections, continue with step 4.

3. For ports that require secondary UDP connections, click **Add** in the **Port Ranges for Subsequent Connections**

box, and then enter the following values:

<b>In</b>	<b>To this</b>
<b>Port or Range</b>	Type 0-65535
<b>Type</b>	Click <b>UDP</b> (default)
<b>Direction</b>	Click <b>Inbound</b> or <b>Outbound</b>



Click OK to add the UDP connection information. Repeat this process to add both Inbound and Outbound dynamic port ranges.

4. The following screen shot illustrates the setting for port 1720, configured for both TCP and UDP connections.

**Protocol Definition**

Protocol name: 1720 TCP Outbound (NetMeeting 3)

Initial connection

Port: 1720

Type: ☒ TCP ☐ UDP

Direction: ☐ Inbound ☒ Outbound

Port ranges for subsequent connections

Port	Type	Direction
0 - 65535	UDP	Inbound
0 - 65535	UDP	Outbound

Add... Edit... Remove

OK Cancel Help

After you have added all necessary connection information, click OK to add the protocol definition.

## 7. Benefits of Firewall Protection:

- Firewalls protect private local area networks (LANs) from hostile intrusion from the Internet.
- Consequently, firewall protection allows many LANs to be connected to the Internet where Internet connectivity would otherwise have been too great a risk.
- Firewalls allow network administrators to offer access to specific types of Internet services to selected LAN users. This selectivity is an essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what. Privileges can be granted according to job description and need rather than on an all-or-nothing basis.

## 8. Firewall Problems:

Is a firewall sufficient to secure my network?

- The firewall is an integral part of any security program, but it is not a security program in and of itself.
- Security involves data integrity (has it been modified?), service or application integrity (is the service available, and is it performing to spec?), data confidentiality (has anyone seen it?) and authentication (are they really who they say they are?).
- Firewall security only addresses the issues of data integrity, confidentiality and authentication of data that is behind the firewall.

→ Any data that transits outside the firewall is subject to factors out of the control of the firewall. It is therefore necessary for an organization to have a well-planned and strictly implemented security program that includes, but is not limited to, firewall protection.

#### 9. Limitations:

- Some firewalls cannot support an arbitrary number of virtual internal IP addresses, or cannot do so dynamically.
- With these firewalls, you can establish outbound NetMeeting connections from computers inside the firewall to computers outside the firewall, and you can use the audio and video features of NetMeeting. Other people, though, cannot establish inbound connections from outside the firewall to computers inside the firewall.
- Typically, this restriction is due to limitations in the network implementation of the firewall.

#### 10. Conclusion:

Firewall is against network intrusion, and despite development trends that threaten them, they are still a powerful protective mechanism, and will continue to play an important and central role in the maintenance of network security for some years yet, and any organization that ignores them does so at its peril.

They continue to change and develop, and new features are regularly added as the need arises. If developments follow the present trend, they will continue to combine configurable access control and authentication mechanisms with their traditional functions, thus providing more powerful and flexible protection for networks to make them secure.

#### 11. References:

- Network Security Essentials - (William Stallings)
- [www.microsoft.com/windows](http://www.microsoft.com/windows)
- [www.suse.de/mha/hypernews](http://www.suse.de/mha/hypernews)
- <https://www.seminarstopics.com>
- <http://projectstopics.com/>

◀ Preliminary Activity for Week 4

Jump to...



Go

Analysis, Application, and Exploration for Week 4 ▶



### Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 2

Participants

General


O2 [Enter Module Title Here]

O3 [Enter Module Title Here]


O4 [Enter Module Title Here]

 Preliminary Activity for Week 4

 **Lesson Proper for Week 4**

 Analysis, Application, and Exploration for Week 4

 Generalization for Week 4

 Evaluation for Week 4

 Assignment for Week 4

Courses

---

## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for *free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.*

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.


**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

---

## Activities

 Assignments

 Forums

 Quizzes

 Resources

