

BCA SEMESTER- IV

Internet Security and Cyber laws

Paper Code- BCA SEC 402

By

Ms. Renu kumari


Assistant Professor

Dept. of Computer Science

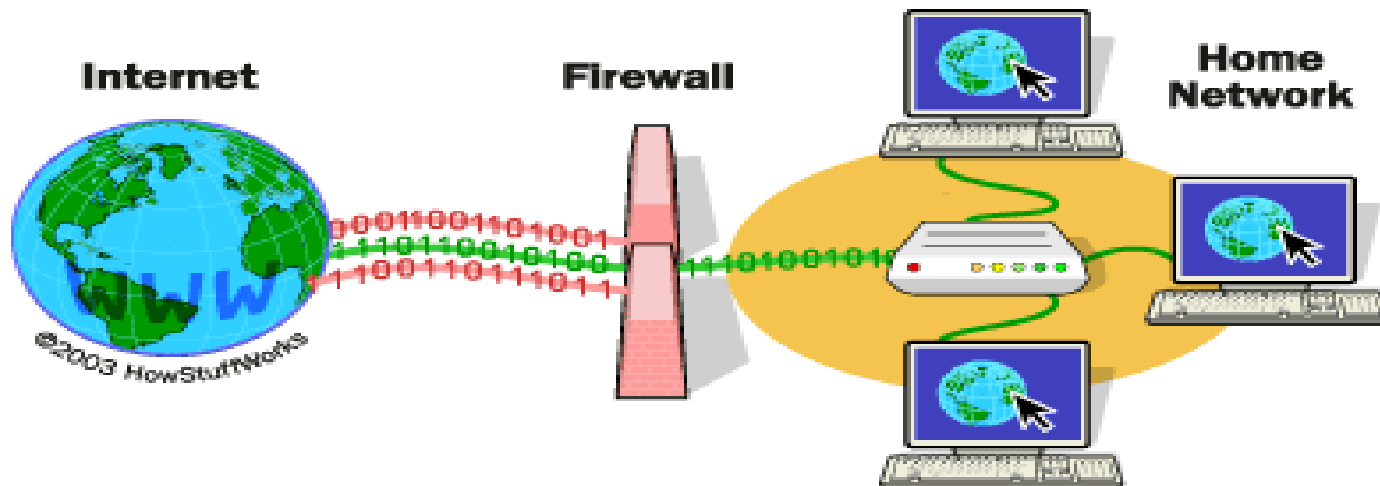
Patna Women's College

FIREWALLS

- A **firewall** is a system designed to prevent unauthorized access to or from a private network. You can implement a **firewall** in either hardware or software form, or a combination of both. **Firewalls** prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.
- It monitors incoming and outgoing packets. A **firewall** can be hardware, software, or both.
- A firewall is a software program or pieces of hardware that helps screen out hackers, virus, and worms that try to reach your computer over the internet.

- 
- If you use a computer at home the most effective and important first step you can take to help protect your computer is to turn on a firewall. Today's every window 7,8,vista and windows XP or higher have a firewall built in and tuned on by default.
 - If you have more than one computer connected in the home or if you have a small –office network it is important to protect every computer you should have a hardware firewall(such as a router) to protect your network ,but you should also use a software firewall on each computer to help prevent the spread of a virus in your network .

How it works



- **Firewalls work** like a filter between your computer/network and the Internet. You can program what you want to get out and what you want to get in. Everything else is not allowed. There are several different methods firewalls use to filter out information, and some are used in combination.

How do Firewalls protect our system

- Large corporations often have very complex firewalls in place to protect their extensive networks.
- On the outbound side, firewalls can be configured to prevent employees from sending certain types of emails or transmitting sensitive data outside of the network.
- On the inbound side, firewalls can be programmed to prevent access to certain websites (like social networking sites).
- Additionally, *firewalls* can prevent outside computers from accessing computers inside the network.
- A company might choose to designate a single computer on the network for file sharing and all other computers could be restricted.
- There is no limit to the variety of configurations that are possible when using firewalls.
- Extensive configurations typically need to be handle and maintained by highly trained IT specialists, however.

Firewall rules:

- Determine what traffic your firewall allows and what is blocked.
- Examine the control information in individual packets, and either block or allow them according to the criteria that you define.
- Control how the firewalls protect your network from malicious programs and unauthorized access.
- Managing your firewall rules across your devices and throughout your network is critical to network security.

TYPES OF FIREWALL

- Packet filtering Firewall
- Application level firewall(proxy firewall)
- Circuit level firewall
- Next generation /Hybrid Firewall

Packet filtering Firewall

- As the most “basic” and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.
- If the information packet doesn’t pass the inspection, it is dropped.
- The good thing about these firewalls is that they aren’t very resource-intensive. This means they don’t have a huge impact on system performance and are relatively simple. However, they’re also relatively easy to bypass compared to firewalls with more robust inspection capabilities

Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

- Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name “application-level gateway.” These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet. This check is similar to the stateful inspection firewall in that it looks at both the packet and at the TCP handshake protocol. However, proxy firewalls may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it contains no malware.
- Once the check is complete, and the packet is approved to connect to the destination, the proxy sends it off. This creates an extra layer of separation between the “client” (the system where the packet originated) and the individual devices on your network—obscuring them to create additional anonymity and protection for your network. If there’s one drawback to proxy firewalls, it’s that they can create significant slowdown because of the extra steps in the data packet transferal process.

Circuit level Firewall

- As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.
- While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuit-level gateways are not enough to protect your business by themselves.

Next Generation Firewall

- Many of the most recently-released firewall products are being touted as “next-generation” architectures. However, there is not as much consensus on what makes a firewall truly next-gen.
- Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.
- The issue is that there is no one definition of a next-generation firewall, so it’s important to verify what specific capabilities such firewalls have before investing in one.

MALWARE

- Malware is short for malicious software, computer programmes the designed to infiltrate and damage computers without the users consent “Malware is the general term covering all the different types of threats to your computer safety such as viruses, spyware,worms, trojans, rootkits and so on .These malicious programme can perform a variety of functions ,including stealing encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users’ computer activity without their permission.

Types of Malware

- Virus
- Worms
- Trojan
- Spyware
- Adware

VIRUS

A computer virus is a small program /software that gets loaded in the computer without the user's knowledge and replicates itself repeatedly or piece of code designed to damage your computer by corrupting system files, wasting resources, destroying data or otherwise being a nuisance.

A Virus is a type of malicious software that when executed ,replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be infected with computer virus. Some dangerous viruses may corrupt or delete files from the computer and may spread themselves to other computers by using the user's email program

WORMS

- Worms can replicate themselves and spread across a computer network .
- Unlike viruses, they do not interfere with the normal use of the computer and do not attach themselves to other programs
- Once installed, they steal confidential data
- They use the email program of the user to send a copy of themselves to everyone listed in his/her email address book
- Use so much network bandwidth and memory that they cause servers and individual computers to stop responding

Trojan

- A non-self-replicating type of malicious software that pretends to be harmless so that users can easily download it on the computer
- Usually contained inside a harmless program
- Once executed, it may slow down the computer, cause loss or theft of data, give unauthorized access to its controller, ruin the file allocation table (FAT), or install a virus

Spyware

- A malicious program that surreptitiously monitors the activity on a computer and reports that information to others without the user's knowledge
- Used for tracking and storing the user's Internet browsing patterns; gaining information about the user's bank login information; serving up pop-up advertisements to the Internet users; installing additional software; redirecting Web browsers to untrusted sites
- Bundled as a hidden piece of code in a freeware or shareware program, which can be difficult to remove

Adware

- A malicious program that surreptitiously monitors the activity on a computer and reports that information to others without the user's knowledge
- Used for tracking and storing the user's Internet browsing patterns; gaining information about the user's bank login information; serving up pop-up advertisements to the Internet users; installing additional software; redirecting Web browsers to untrusted sites
- Bundled as a hidden piece of code in a freeware or shareware program, which can be difficult to remove

Protect our system

- Downloading legal website
- Avoid Fake email attachment open
- Avoid Pirated software download
- Always used Licence antivirus software

Anti virus

- Antivirus software is a type of utility used for scanning and removing viruses from your computer. While many types of antivirus (or "anti-virus") programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found.
- Examples of common antivirus programs include Norton Antivirus, Kaspersky Anti-Virus, and ZoneAlarm Antivirus.

How to install antivirus

- If you purchased the **antivirus** program from a retail store, insert the **CD** or DVD into the computer's **disc drive**. The **installation** process should start automatically, with a window opening to help guide you through the **install** process
- Insert CD
- RIGHT Click on the my computer
- Right click on the cd drive click open
- Open window
- Click on set up file then startup file
- Open window click on next to go to the next step
- Click on next step “I accept the terms in the license agreement “ then click on next, now check the given option and click on next option
- Given two option we select first option and then click on” install”
- Open window and put here product activation key and click on activate
- Then message display on your system activation was successful then click on done

Without cd drive /Online install antivirus

Quick heal antivirus install

- firstly type in URL www.quickheal.com/installer
- open page
- then enter product key given on the inside the cd packaging, which is the main thing.
- click on submit option then open page and click on download software then open dialog box and asked path
- open path and click on file
- click on download then icon display on desktop screen and open dialog box
- click on installation then click on registered now
- enter product key click next
- user information click next
- ready to submit Check information click on next
- click on finish
- account successfully created