PNS SCHOOL OF ENGINEERING & TECHNOLOGY

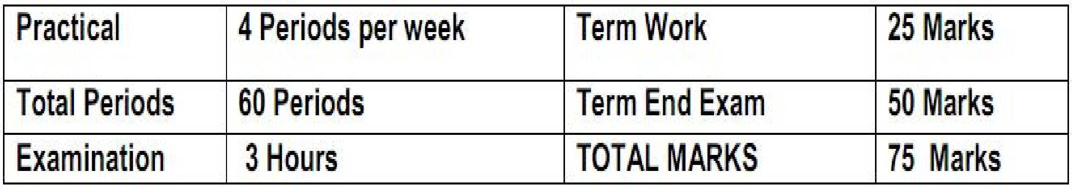
Nishamani Vihar, Marshaghai, Kendrapara

LAB MANUAL
for
NETWORK SECURITY LAB

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
6TH SEMESTER

PREPARED BY
MR. BISWARANJAN SWAIN
LECTURER IN COMPUTER SCIENCE & ENGINEERING

PR-1 NETWORK SECURITY LAB



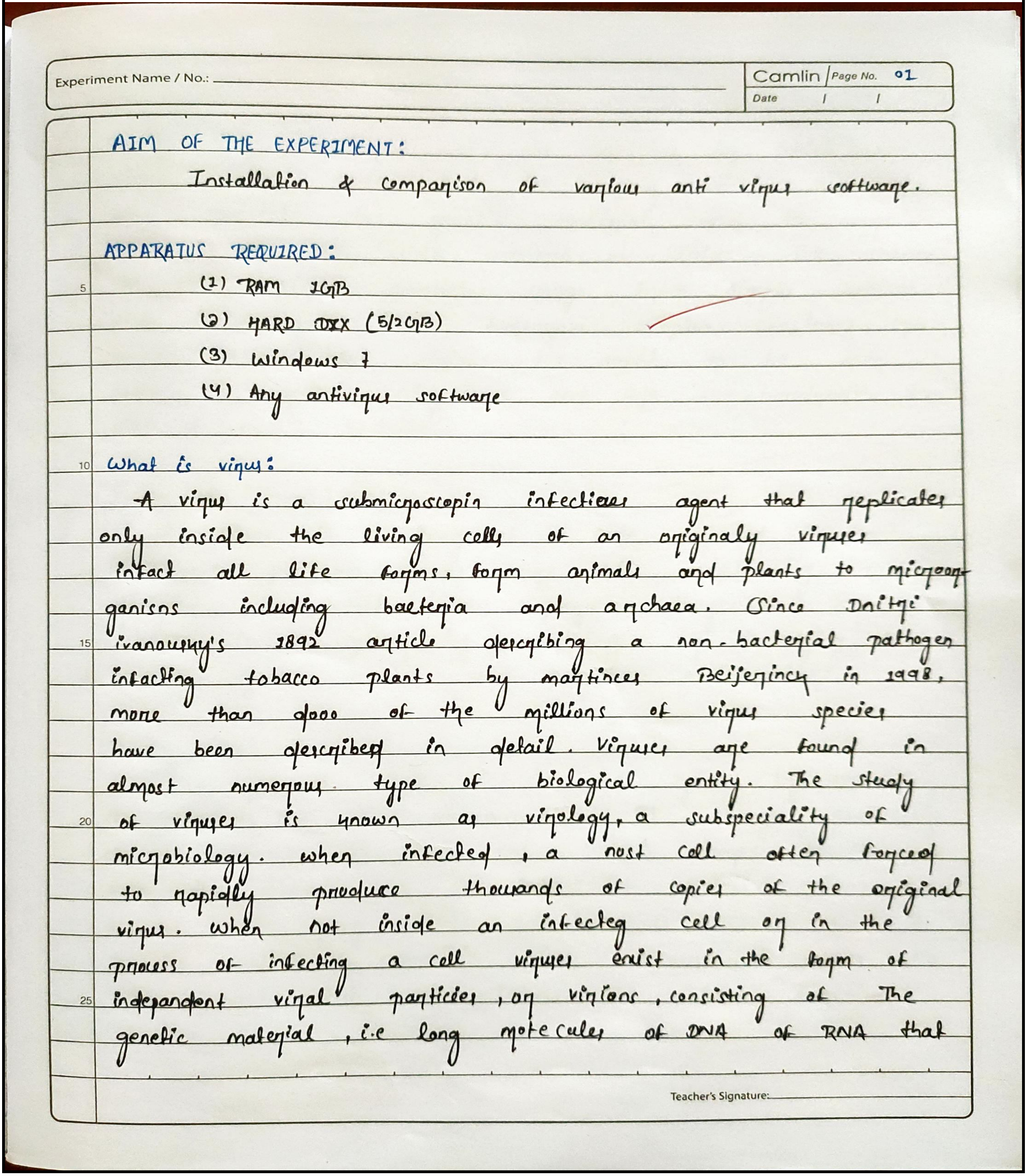
Practical	4 Periods per week	Term Work	25 Marks
Total Periods	60 Periods	Term End Exam	50 Marks
Examination	3 Hours	TOTAL MARKS	75 Marks

LIST OF PRACTICALS

1. Installation and comparison of various anti virus software
2. Installation and study of various parameters of firewall.
3. Writing program in C to Encrypt/Decrypt using XOR key.
4. Study of VPN.
5. Study of various hacking tools.
6. Practical applications of digital signature

Expt1.

Installation and comparison of various anti virus software



Experiment Name / No.:

Camlin Page No. 01

Date / /

AIM OF THE EXPERIMENT:

Installation & comparison of various anti virus software.

APPARATUS REQUIRED:

(1) RAM 1GB

(2) HARD DIX (512GB)

(3) Windows 7

(4) Any antivirus software

What is virus:

A virus is a submicroscopin infectious agent that replicates only inside the living cells of an originaly viruses infact all life forms, form animals and plants to microorganisms including bacteria and archaea. Since Dmitri ivanovsky's 1892 article describing a non-bacterial pathogen infacting tobacco plants by martinces Beijerinck in 1998, more than 6000 of the millions of virus species have been describeq in detail. Viruses are found in almost numerous type of biological entity. The study of viruses is known as virology, a subspeciality of microbiology. when infected, a nost cell often forced to rapidly produce thousands of copies of the original virus. when not inside an infecteg cell or in the process of infecting a cell viruses exist in the form of independent viral particles, or virions, consisting of The genetic material, i.e long molecules of DNA of RNA that

Teacher's Signature:

encode the structured of the proteins by which the viruses action proten coat the capsiq which surrounds and protects the genetic material and in same cases (III) an out side envelope of lipids. The shapes of these virus particles range from simple helical and icosanedral form tomorrow complex stactures. Must virus species have virions too small to be seen with an optical microscope and are one-hundredth the size of most bacteria.

Types of viruses:

A virus is a fragment of code embaded in a legitimate program. viruses are self replicating and designed to infelt other program they can wreay hovoc in a system by modifing or destroying files cousing system crashes and program malfcenctions.

(1) File virus:

This type of virus infects the system by appending it self to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code the control retuns back to the main program. Its execution is noteven noticed. It is also called a parasitic virus because it leaves no file intact but also leaves the host functions.

(2) Boot Sector virus:

It infects the boot sector of the system executing every time system is booted and before the operating system is loaded. It infects other bootable media like flopy disks. These are also known as memory viruses as they do not Infect the file systems.

(3) Macro Virus:

Unlike most viruses which are written in a low-level language (like or assembly language) these are written in a high level language like visal Basic. These viruses are triggered when a program capable of executing a macro is run for example the macro viruses can be contained in spreadsheet files.

(4) Source Code Virus:

It looks for source code and modifies it to include virus and to help spread it.

(5) Polymorphic Virus:

A virus signature is pattern that can identify a virus (a service of bytes that make up virus code) So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but it's signature is changed.

(6) Trojan horse:

A trojan horse (Trojan) is a type of malware that disgulses itself as legitimete code or software. Once inside the network attackers are able to carry out any action that a legitimade user could performs seen as ea porting files modifying data, delecting files or otherwise altering the contents of the device.

Antivirus:

Antivirus is a kind of software used to prevent scan detect and delete viruses form a computer. Once installed most antivirus software runs automatically in back ground to provide real time protection agaist virus attacks.

Comprehensive virus protection program helps protect help protect your files and hardware form malware such as worms to Jan horses and spyware and may also offer additional protection such as costomizable fire walls and website blacking.

Types of ANTIVIRUS:

AVG:-

AVG is one of the most popular antivirus program that can be obtained for free, and it's easy to download directly form the Internet. AVG didn't make it make it into our main list because their free version only includes virus and other malware blockage. Free antivirus software usually includes.

Avast Antivirus:

Avast antivirus definitely should be on any rundown of the best free antivirus programs. The antivirus form Avast is feature. filled antivirus.

Norton Antivirus:

Norton antivirus has proven it self to be one of the best antiviruses programs. one note worthy feature is its options mobile application which help users.

MCAfee:

- MCAfee multisystem compatibility malfee offer protection across all your device irrespective of the operting system. Realtime malware detection.
- It is world wide leader in online protection.

HOW TO INSTALL OF ANTI VIRUS:

To install an antivirus program anyone computer, follow the steps below.

1- If you purchered the antivirus program from a retail store, insert the CD or DVD into the computers disc driver. The installation process should start automatically.

with a window opening to help guide you through the install process.

2- If you downloaded the antivirus program on the internet, find the downloaded file on your computer. If the downloaded file is a zip file, unzip the file to extract & access the installation files. Look for a file named setup.exe, install.exe, or something similar, then double click that file. The installation process should start, with a window opening to help guide you through the install process.

3- In the installation process window, follow the steps provided to install the antivirus program. The install process provides recommended options so the antivirus program will function properly, which in most cases can be accepted as is the one for internet browsers or other helpful programs for your computer. If prompted to install other software with the antivirus program, uncheck all boxes or decline the install of those extra program, no additional programs should be needed for the antivirus program to install & run successfully on your computer.

4- When the install process is complete, close out of the install window.

5- If used, remove the CD or DVD from the computers Disc Drive.

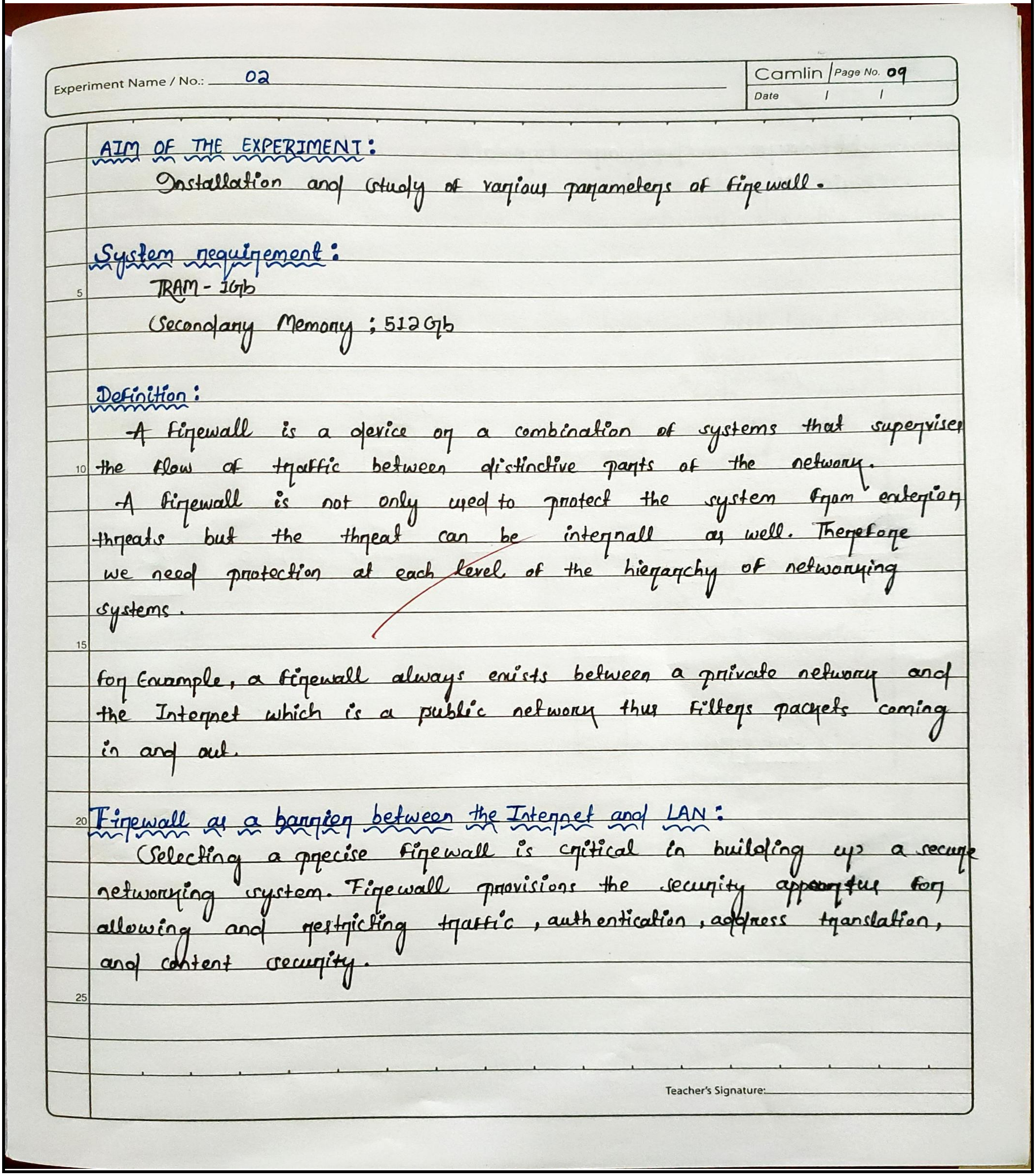
COMARISION OF VARIOUS ANTIVIRUS SOFTWARE :—

	McAfee	Norton	Bitdefender	Kaspersky
Rating	9.8	9.2	9.0	8.9
Detection Capability	Excellent	Excellent	Excellent	Good
System performance	Excellent	Good	Excellent	Good
PROTECTION				
Real-time protection	✓	✓	✓	✓
Remove Malware	✓	✓	✓	✓
Remove Adware	✓	✓	✓	✓
Remove spyware	✓	✓	✓	✓
Rescue Mode	✗	✗	✓	✗
FEATURE				
VPN	✗	✓	✓	✓
Safeline Banking	✗	✓	✓	✓
webcam protecting	✗	✓	✓	✓
Parental Advisor	✓	✓	✓	✓
Firewall	✓	✓	✓	✓
Quite mode	✓	✓	✓	✓
Live chat	✓	✓	✓	✓
Mac	✓	✓	✓	✓
Linux	✓	✓	✓	✓
Android	✓	✓	✓	✓
IOS	✓	✓	✓	✗
Windows	✓	✓	✓	✓

Conclusion:

From this above experiment we have successfully studied about how to install antivirus on our computer & comparision of various antivirus software.

Expt.2:
Installation and study of various parameters of firewall.



Experiment Name / No.: 02

Camlin Page No. 09

Date / /

AIM OF THE EXPERIMENT:

Installation and study of various parameters of firewall.

System requirement:

RAM - 1Gb

Secondary Memory : 512 Gb

Definition:

A firewall is a device or a combination of systems that supervises the flow of traffic between distinctive parts of the network.

A firewall is not only used to protect the system from exterior threats but the threat can be internall as well. Therefore we need protection at each level of the hierarchy of networking systems.

For Example, a firewall always exists between a private network and the Internet which is a public network thus filters packets coming in and out.

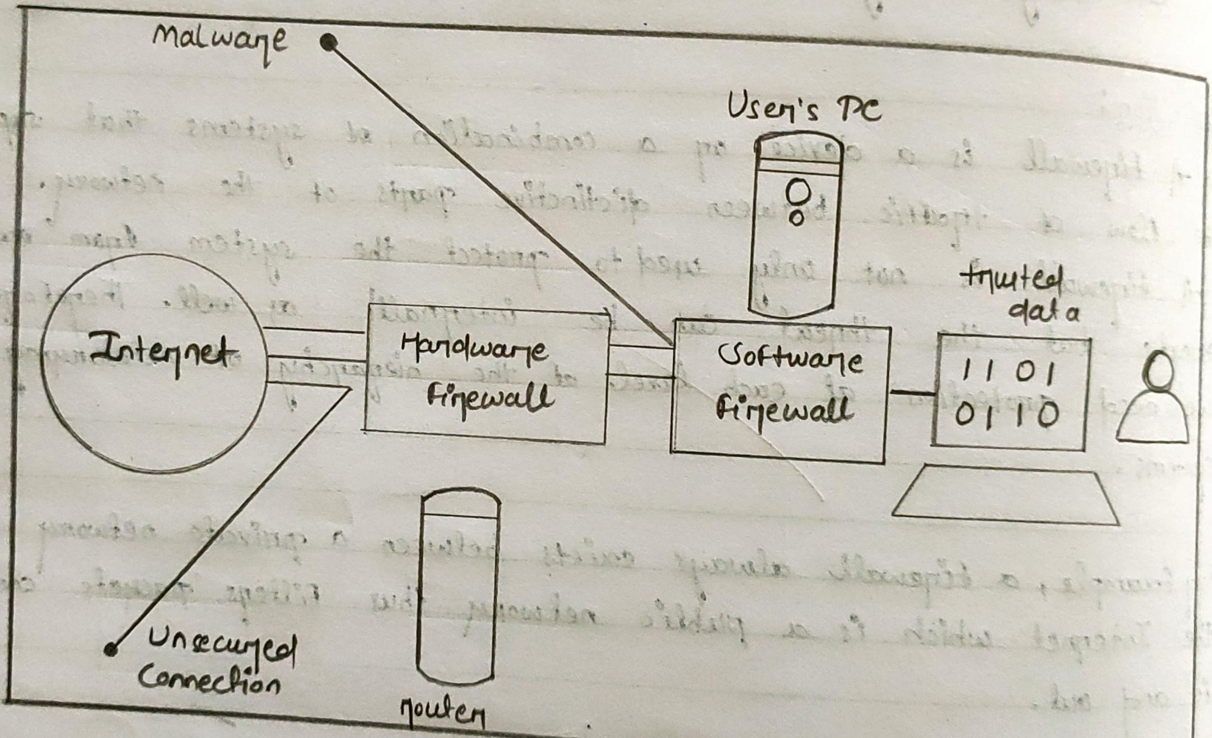
Firewall as a barrier between the Internet and LAN:

Selecting a precise firewall is critical in building up a secure networking system. Firewall provisions the security apparatus for allowing and restricting traffic, authentication, address translation, and content security.

Teacher's Signature:

Software vs Hardware Firewall

Basic Firewall Network Example



Hardware firewall protects the entire network of an organization using it from external threats only. In case, if an employee of the organization is connected to the network via his laptop then he can't avail the protection.

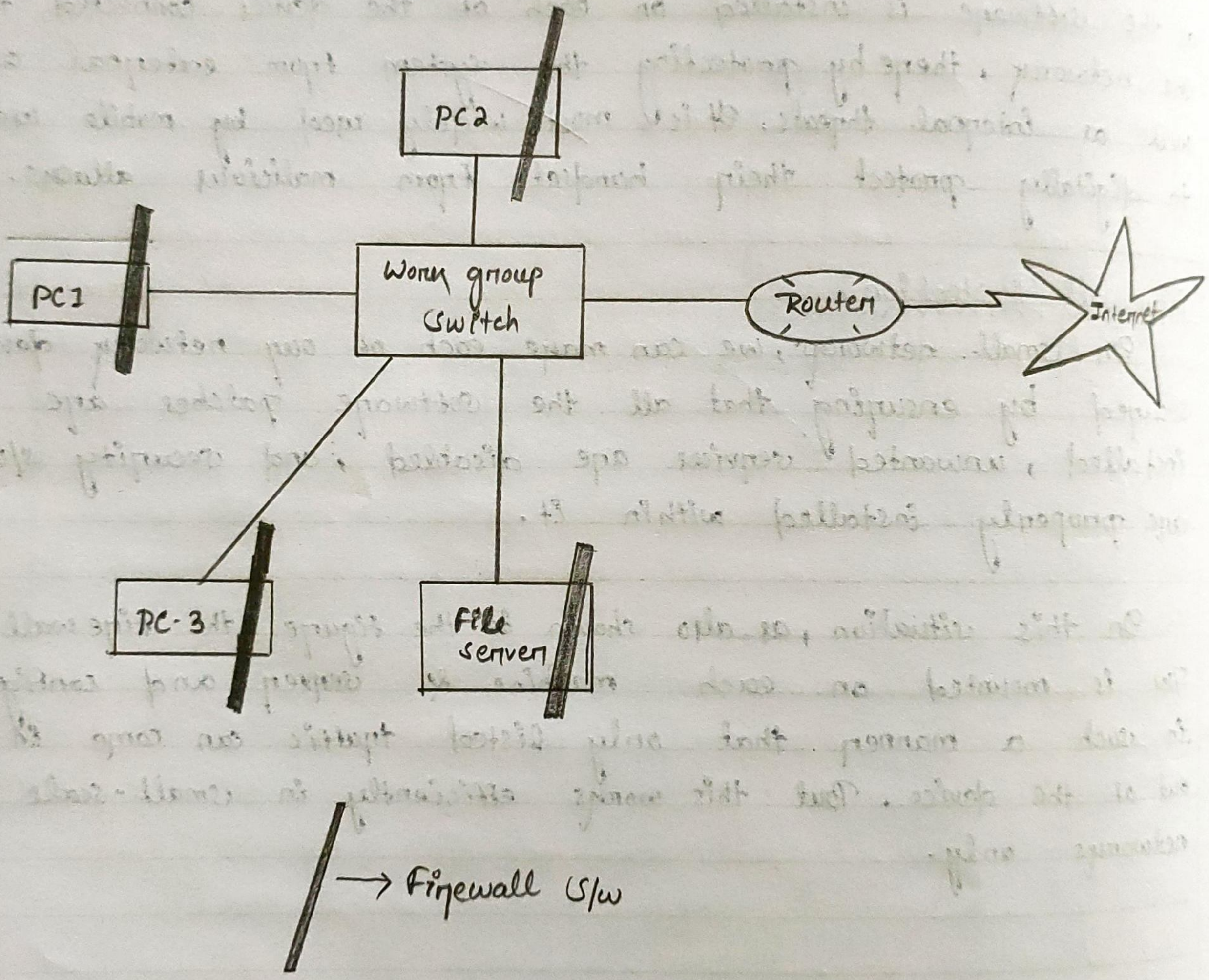
On the other hand, software firewall provision host-based security as the software is installed on each of the devices connected to the network, there by protecting the system from external as well as internal threats. It is most widely used by mobile users to digitally protect their handset from malicious attacks.

Firewall Protection:

In small networks, we can make each of our network device secured by ensuring that all the software patches are installed, unwanted services are disabled, and security s/w are properly installed within it.

In this situation, as also shown in the figure, the firewall s/w is mounted on each machine & server and configured in such a manner that only listed traffic can come in and out of the device. But this works efficiently in small-scale networks only.

Firewall Protection is Small Scale Network

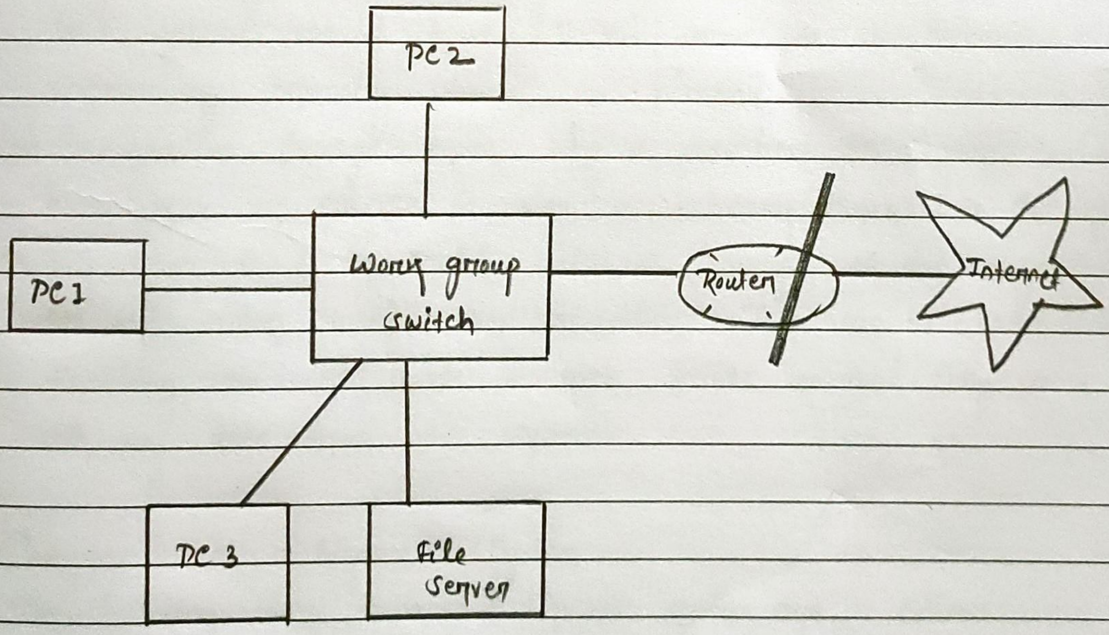


In a large-scale network, it is almost next to impossible to manually conifigure the firewall protection on each node.

The centralized security system is a solution to provide a secure network to big networks. With the help of an example, it is shown in the below figure that the firewall solution is imposed with the router itself, and it becomes simple to handle security policies. The policies of traffic come in and out into the device and can be handled solely by one device.

This makes the overall security system cost-effective.

Firewall Protection in Big Networks:



Dealing with Internal Threats

Most of the attacq on the networq occurs from inside the system so to deal with its firewall system should be capable of securing from internal threats also.

Few kinds of internal threats are described below:

(1) Malicious cyber-attacqs are the most common type of internal attacq. The system administrator or any employee from the IT department who is having access to the networq system can plant some viruses to steal crucial networq information or to damage the networqing system.

(2) Any of the host computers of the internal networq of the organization can download malicious internet content with a lacq of qnowledge of downloading the virus also with it. Thus the host systems should have limited access to the internet. All unnecessary browsing should be blocqed.

(3) Information leaqage from any of the host PC through pen drives, hard disq, or CD-ROM is also a networq threat to the system. This can lead to crcial database leaqage of the organization ~~to~~ the outer world or competitors. This can be controlled by disabling the USB ports of host devices so that they can't taqe out any data from the system.

Components of a Firewall System

The building blocqs of a good firewall system are as follows:

- Perimeter router
- Firewall
- VPN
- IDS.

Teacher's Signature:

● **Perimeter router :-**

The main reason for using it is to provide a link to a public networking system like the internet, or a distinctive organization. It performs the routing of data packets by following an appropriate routing protocol. It also provisions the filtering of packets and addresses translations.

● **Firewall :-**

As discussed earlier also its main task is to provision distinctive levels of security and supervises traffic among each level. Most of the firewall exists near the router to provide security from external threats but sometimes present in the internal network also to protect from internal attacks.

● **VPN :-**

Its function is to provisions a secured connection among two machines or network or a machine and a network. This consists of encryption, authentication, and packet-reliability assurance. It provisions the secure remote access of the network, there by connecting two WAN networks on the same platform while not being physically connected.

● **IDS :-**

Its function is to identify, preclude, investigate, and resolve unauthorized attacks. A hacker can attack the network in various ways. It can execute a DoS attack or an attack from the backside of the network through some unauthorized access. An IDS solution should be.

Firewall Categories

Based on the Filtering of traffic there are many categories of the firewall, some are explained below:

#1) Packet Filtering Firewall:

It is a kind of router which is having the ability to filter the few of the substance of the data packets. When using packet-filtering, the rules are classified on the firewall. These rules find out from the packets which traffic is permitted and which are not.

#2) Stateful Firewall:

It is also called as dynamic packet filtering, it inspects the status of active connections and uses that data to find out which of the packets should be permitted through the firewall and which are not.

The firewall inspects the packet down to the applications layer. By tracing the session data like IP address and port number of the data packet it can provide much strong security to the network.

It also inspects both incoming and outgoing traffic thus hackers found it difficult to interfere in the network using this firewall.

#3) Proxy Firewall:

These are also known as application gateway firewalls. The stateful firewall is unable to protect the system from HTTP based attacks. Therefore proxy firewall is introduced in the market.

Teacher's Signature:

It includes the features of stateful inspection plus having the capability of closely analyzing application layer protocals.

Thus it can monitor traffic from HTTP and FTP and find out the possibility of attacks. Thus Firewall behaves as a proxy means the client initiates a connection with the firewall and the firewall in return initiates a solo link with the server on the client's side.

Firewall in Windows 7 :-

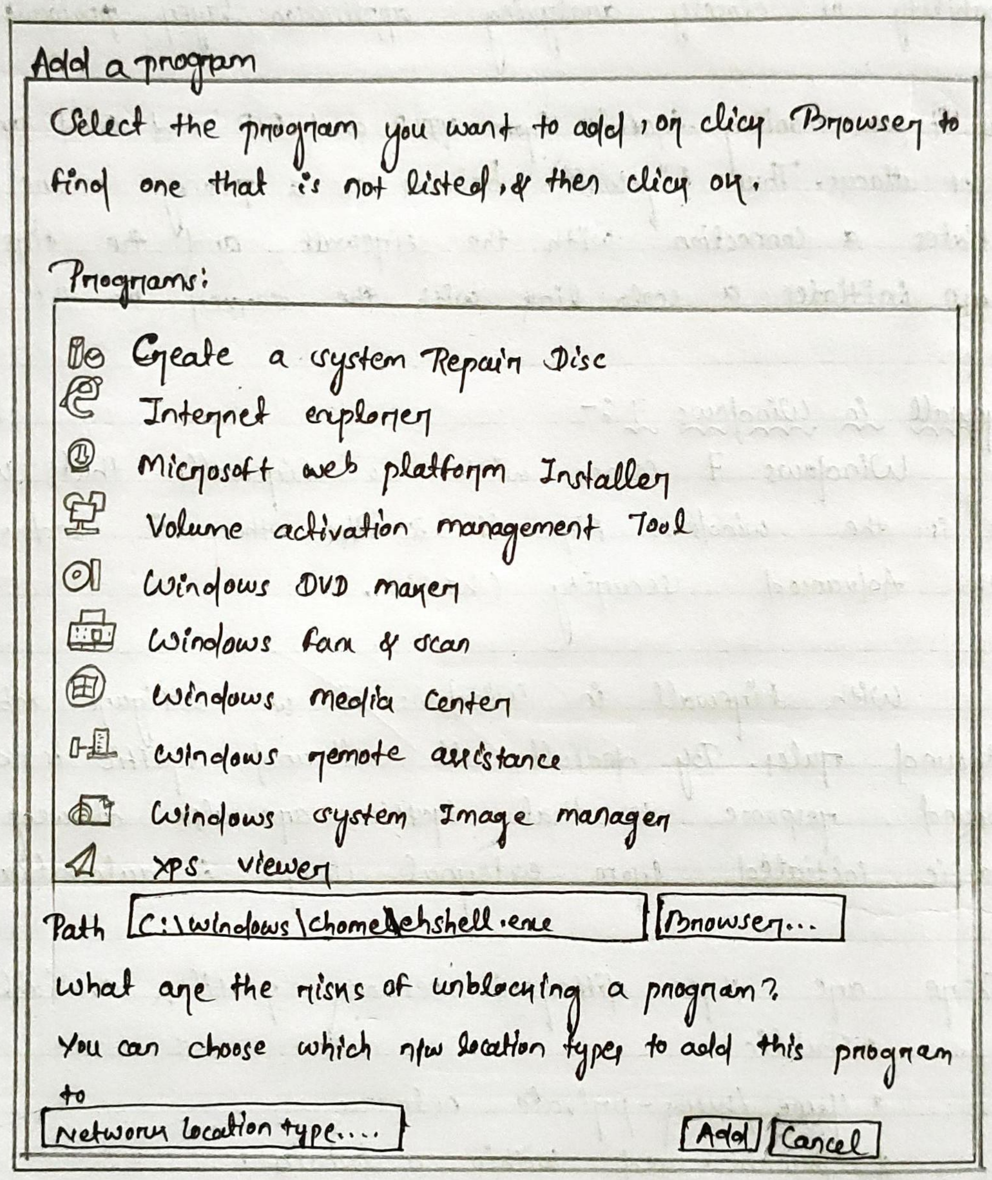
Windows 7 comes with two firewalls that work together One is the windows firewall & the other is windows firewall with Advanced Security (WFAS).

With Firewall in Windows 7 we configure inbound & outbound rules. By deafult. all outbound traffic is allowed. & inbound response to that traffic are also allowed. Inbound traffic initiated from external source is automatically blocked.

→ There are three different network profiles available.

* Public
* Home / work - private network
* Domain - used within a domain.

We choose those locations when we connect to a network. We can always change the location in the network & sharing center. In control panel. The Domain profile can be automatically



Add a program

Select the program you want to add, or click Browser to find one that is not listed, & then click ok.

Programs:

- Create a system Repair Disc
- Internet explorer
- Microsoft web platform Installer
- Volume activation management Tool
- Windows DVD maker
- Windows fax & scan
- Windows media center
- Windows remote assistance
- Windows system Image manager
- xps viewer

Path C:\windows\chome\ehshell.exe

What are the risks of unblocking a program?

You can choose which n/w location types to add this program to assigned by the NCA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in windows 7.

Configuring windows firewall :-

To open windows firewall we change to start > Control panel > windows firewall.

Exceptions :-

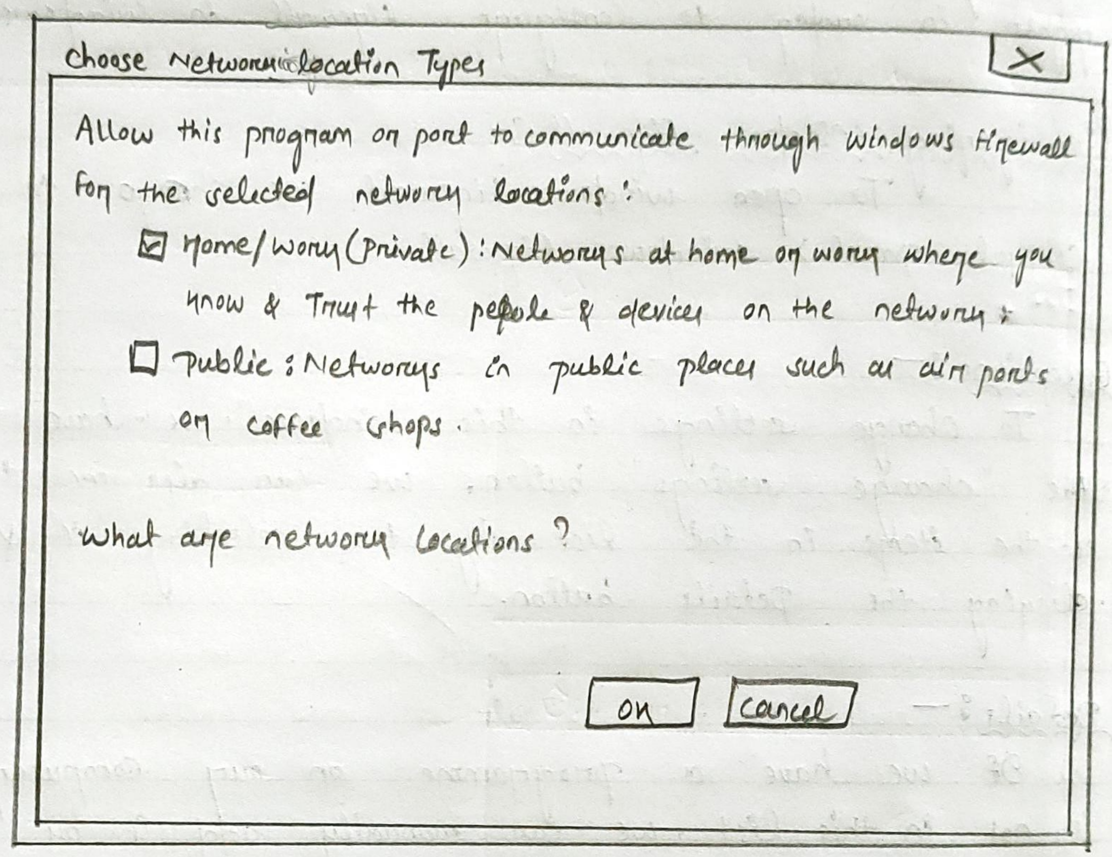
To change settings in this windows we have to click the "change settings" button. we can also see the details of the items in the list by the selecting it & then clicking the Details button.

Details :-

If we have a programme on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.

Add a program :-

Here we have to browse to the executable of our program & then click the add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



Choose Network location Types

Allow this program on port to communicate through windows firewall for the selected network locations:

☑ Home/work (Private): Networks at home or work where you know & Trust the people & devices on the network.

□ Public: Networks in public places such as air ports or coffee shops.

What are network locations?

Turn on or off windows firewall :-

Windows firewall can be turned off completely. To do that we can select the "Turn windows firewall on or off" option from the menu on the left.

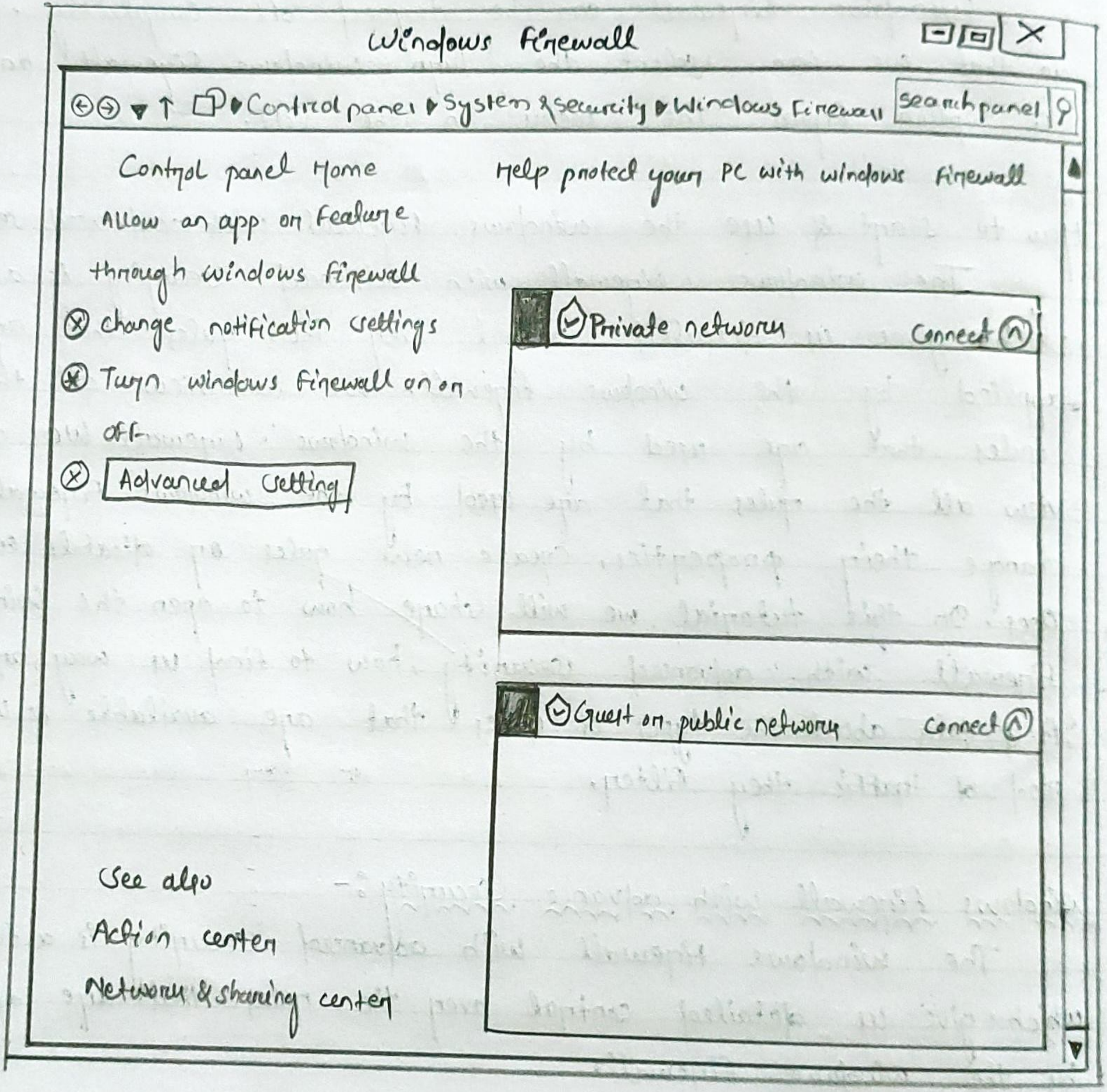
How to start & use the windows firewall with advanced security

The windows firewall with advanced security is a tool which gives us detailed control over the rules that are applied by the windows firewall. we can view all the rules that are used by the windows firewall. We can view all the rules that are used by the windows firewall. change their properties, create new rules or disable existing ones. In this tutorial we will share how to open the windows firewall with advanced security, how to find us way around it & talk about the types of rules that are available & what kind of traffic they filter.

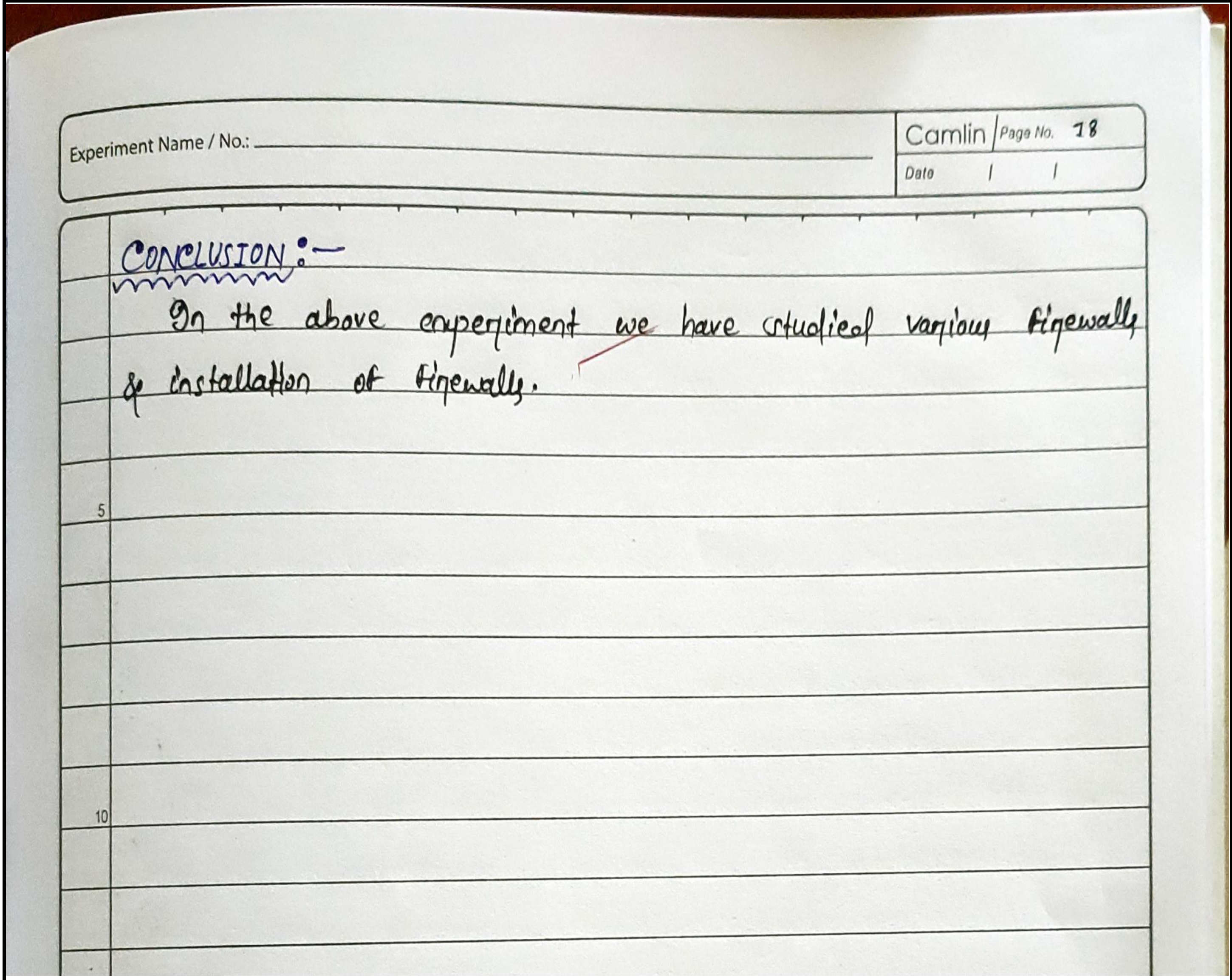
Windows firewall with advance security :-

The windows firewall with advanced security is a tool which give us detailed control over the rules that are applied by the windows firewall.

To open the standard windows firewall window by going to "control panel → system & security.
→ windows firewall then, click to tap advanced setting.


Windows Firewall
Control panel ▸ System & security ▸ Windows Firewall
search panel
Control panel Home
Allow an app on Feature through windows firewall
change notification settings
Turn windows firewall on on off
Advanced setting
Private networn
Connect
Guest on public networn
Connect
See also
Action center
Networn & sharing center

Help protect your PC with windows firewall



Experiment Name / No.:

Camlin Page No. 18

Date / /

CONCLUSION :-

In the above experiment we have studied various firewalls & installation of firewalls.

Expt.3:

Writing program in C to Encrypt/Decrypt using XOR key.

```
#include <stdio.h>
#include <string.h>
void encryptDecrypt(char *input, const char *key) {
    int inputLen = strlen(input);
    int keyLen = strlen(key);
    int i;

    for (i = 0; i < inputLen; i++) {
        input[i] = input[i] ^ key[i % keyLen]; // XOR operation with key
    }
}
int main() {
    char input[100];
    char key[100];
    int choice;

    printf("Enter input string: ");
    gets(input);
    printf("Enter key: ");
    gets(key);
    printf("Select operation:\n");

    printf("1. Encrypt\n");
    printf("2. Decrypt\n");
    printf("Enter your choice: ");
    scanf("%d", &choice);

    switch (choice) {
        case 1:
            encryptDecrypt(input, key);
            printf("Encrypted string: %s\n", input);
            break;
        case 2:
            encryptDecrypt(input, key);
            printf("Decrypted string: %s\n", input);
            break;
        default:
            printf("Invalid choice. Exiting...\n");
    }
    return 0;
}
```

Expt. 4:

Study of VPN

VPN

VPN stands for **"Virtual Private Network"** and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise online identity. This makes it more difficult for third parties to track the activities online and steal data. The encryption takes place in **real time**.

Working of VPN

A VPN hides the IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if we surf online with a VPN, the VPN server becomes the source of your data. This means our Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online.

The benefits of a VPN connection

A VPN connection disguises the data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can’t decipher this data.

Secure encryption: To read the data, there is a need of an *encryption key* . With the help of a VPN, our online activities are hidden even on public networks.

Disguising where-abouts : VPN servers essentially act as proxies on the internet. Because the demographic location data comes from a server in another country, the actual location of the user cannot be determined. In addition, most VPN services do not store logs of user activities. Some providers, on the other hand, record the user’s behavior, but do not pass this information on to third parties. This means that any potential record of user behavior remains permanently hidden.

Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine the user’s location. This means that the user cannot access content at home while traveling, and cannot access international content from home. With **VPN location spoofing** , the user can switch to a server to another country and effectively “change” the location.

Secure data transfer: If the user works remotely, he/she may need to access important files on company’s network. For security reasons, this kind of information requires a secure connection. To gain access to the network, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Reason of VPN connection:

The ISP usually sets up the connection when we connect to the internet. It tracks the user via an IP address. The network traffic is routed through the ISP's servers, which can log and display everything the user does online.

The ISP may share the browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, the personal and private data of the user can be compromised.

Responsibility of VPN:

VPN should perform one or more tasks. The VPN itself should also be protected against compromise. These are the features of VPN solution:

- **Encryption of IP address:** The primary job of a VPN is to hide IP address of the user from the ISP and other third parties. This allows the user to send and receive information online without the risk of anyone but the user and the VPN provider seeing it.
- **Encryption of protocols:** A VPN should also prevent the user from leaving traces, for example, in the form of internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.
- **Kill switch:** If the VPN connection is suddenly interrupted, the secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.
- **Two-factor authentication:** By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

The history of VPNs

Since humans have been using the internet, there has been a movement to protect and encrypt internet browser data. The US Department of Defense already got involved in projects working on the encryption of internet communication data back in the 1960s.

The predecessors of the VPN

Their efforts led to the creation of **ARPANET** (Advanced Research Projects Agency Network), a packet switching network, which in turn led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP).
The **TCP/IP** had four levels: **Link, internet, transport and application**. At the internet level, local networks and devices could be connected to the universal network – and this is where the risk of exposure became clear. In 1993, a team from Columbia University and AT&T Bell Labs finally succeeded in creating a kind of first version of the modern VPN, known as swIPe: Software IP encryption protocol.

VPNs and their current use

According to the ***GlobalWebIndex***, the number of VPN users worldwide increased more than fourfold between 2016 and 2018. In countries such as Thailand, Indonesia and China, where internet use is restricted and censored, **one in fiveinternet users** uses a VPN. In the USA, Great Britain and Germany, the proportion of VPN users is **lowerat around 5%**, but is growing.

One of the biggest drivers for VPN adoption in recent years has been the increasing demand for content with geographical access restrictions. For example, video streaming services such as Netflix or YouTube make certain videos available only in certain countries.

How to surf securely with a VPN

A VPN encrypts the surfing behavior, which can only be decoded with the help of a key. Only the user’s computer and the VPN know this key, so the ISP cannot recognize where the user is surfing. Different VPNs use different encryption processes, but generally function in three steps:

1. Once the user is online, start the VPN. The VPN acts as a secure tunnel between the user and the internet. The ISP and other third parties cannot detect this tunnel.
2. The user’s device is now on the local network of the VPN, and the IP address can be changed to an IP address provided by the VPN server.
3. The user can now surf the internet at will, as the VPN protects all the personal data.

Types of VPN:

There are many different types of VPNs, but you should definitely be familiar with the three main types:

SSL VPN

Often not all employees of a company have access to a company laptop they can use to work from home. During the corona crisis in Spring 2020, many companies faced the problem of not having enough equipment for their employees. In such cases, use of a private device (PC, laptop, tablet, mobile phone) is often resorted to. In this case, companies fall back on an **SSL-VPN** solution, which is usually implemented via a corresponding hardware box.

The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. HTML-5 capable browsers are available for virtually any operating system. Access is guarded with a username and password.

Site-to-site VPN

A **site-to-site VPN** is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

A site-to-site VPN is useful if there is multiple locations of a company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

Client-to-Server VPN

Connecting via a **VPN client** can be imagined as if you were connecting your home PC to the company with an extension cable. Employees can dial into the company network from their home office via the secure connection and act as if they were sitting in the office. However, a VPN client must first be installed and configured on the computer.

The advantage of this type of VPN access is greater efficiency and universal access to company resources.

Installation of VPN on computer?

Before installing a VPN, it is important to be familiar with the different implementation methods:

VPN client

Software must be installed for standalone VPN clients. This software is configured to meet the requirements of the endpoint. When setting up the VPN, the endpoint executes the VPN link and connects to the other endpoint, creating the encryption tunnel. In companies, this step usually requires the entry of a password issued by the company or the installation of an appropriate certificate. By using a password or certificate, the firewall can recognize that this is an authorized connection. The employee then identifies him/herself by means of credentials known to him/her.

Browser extensions

VPN extensions can be added to most web browsers such as Google Chrome and Firefox. Some browsers, including Opera, even have their own integrated VPN extensions. Extensions make it easier for users to quickly switch and configure their VPN while surfing the internet.

Users are also advised to choose a reputable extension, as ***data harvesters*** may attempt to use fake VPN extensions. Data harvesting is the collection of personal data, such as what marketing strategists do to create a personal profile of you. Advertising content is then personally tailored to you.

Router VPN

If multiple devices are connected to the same internet connection, it may be easier to implement the VPN directly on the router than to install a separate VPN on each device. A router VPN is especially useful if you want to protect devices with an internet connection that are not easy to configure, such as smart TVs. They can even help you access geographically restricted content through your home entertainment systems.

A router VPN is easy to install, always provides security and privacy, and prevents your network from being compromised when insecure devices log on. However, it may be more difficult to manage if your router does not have its own user interface. This can lead to incoming connections being blocked.

Company VPN

A company VPN is a custom solution that requires personalized setup and technical support. The VPN is usually created for you by the company's IT team. As a user, you have no administrative influence from the VPN itself and your activities and data transfers are logged by your company. This allows the company to minimize the potential risk of data leakage. The main advantage of a corporate VPN is a fully secure connection to the company's intranet and server, even for employees who work outside the company using their own internet connection.

VPN on smartphone or other devices

There are a number of VPN options for smartphones and other internet-connected devices. A VPN can be essential for mobile device if it is used to store payment information or other personal data or even just to surf the internet. Many VPN providers also offer mobile solutions - many of which can be downloaded directly from Google Play or the Apple App Store, such as Kaspersky VPN Secure Connection.

Is a VPN secure?

It is important to note that VPNs do not function like comprehensive anti-virus software. While they protect the IP and encrypt internet history, a VPN connection does not protect the computer from outside intrusion.

It is therefore important to use a VPN together with a comprehensive anti-virus program to ensure maximum security.

Selecting a secure VPN provider

It is also important that to choose a VPN provider that can be trusted. While the ISP cannot see the internet traffic, the VPN provider can. If the VPN provider is compromised, so the user connection is compromised. For this reason, it is crucial that to choose a trusted VPN provider to ensure both the concealment of internet activities and ensure the highest level of security.

Conclusion

A VPN connection establishes a secure connection between the user and the internet. Via the VPN, all the user data traffic is routed through an encrypted virtual tunnel. This disguises the user IP address when the user use the internet, making its location invisible to everyone.

From this experiment we also studied types of VPN and its working.