INFORMATION
SYSTEM SECURITY

UNDERSTAND THE FUNDAMENTAL OF INFOSEC

EDITION 2023

KAMARUDIN RIPIN
MOHD REDZUAN ROSLY
SITI NASRAH MUKHTAR

INFORMATION
SYSTEM SECURITY

Information & Communication Technology
Sultan Mizan Zainal Abidin Polytechnic
Dungun Terengganu
2023

Written By **Kamarudin Ripin, Mohd Redzuan Rosly**

Edited By **Siti Nasrah Mukhtar**

Publisher:

Sultan Mizan Zainal Abidin Polytechnic
Km 8, Jalan Paka
23000 Dungun Terengganu.
https://psmza.mypolycc.edu.my/

PREFACE

Information systems security management is the process of ensuring the confidentiality, integrity, and availability of information whenever and wherever it is transmitted, stored, and processed. While perfect security is desirable, it is unfortunately unattainable. There are numerous active and passive threats to the security of information, as well as responses to these threats that must be adopted by individuals, teams, and organizations. Various technical and behavioral controls are used to counter these threats, but this book will focus on the behavioral controls. Research findings support the importance of both internal and external threats, with internal threats demonstrating the greatest negative impact in most cases. Factors that contribute to individual compliance with security policies will be discussed, along with some discussion of the intentional violation of security protocols and policies by malicious individuals. Information systems are exposed to different types of security risks. The consequences of information systems security (ISS) breaches can vary. The sources of security risks are different, and can origin from inside or outside of information system facility, and can be intentional or unintentional. The precise calculation of loses caused by such incidents is often not possible because a number of small scale ISS incidents are never detected, or detected with a significant time delay, a part of incidents are interpreted as an accidental mistakes, and all that results with an underestimation of ISS risks.

CONTENTS

CHAPTER 1
Introduction To Information System Security

This chapter discusses the following topics:

- The need for Information System Security
- The increasing issues of on-line security

1.1 INFORMATION SYSTEM SECURITY

What Is Information Security?

The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.

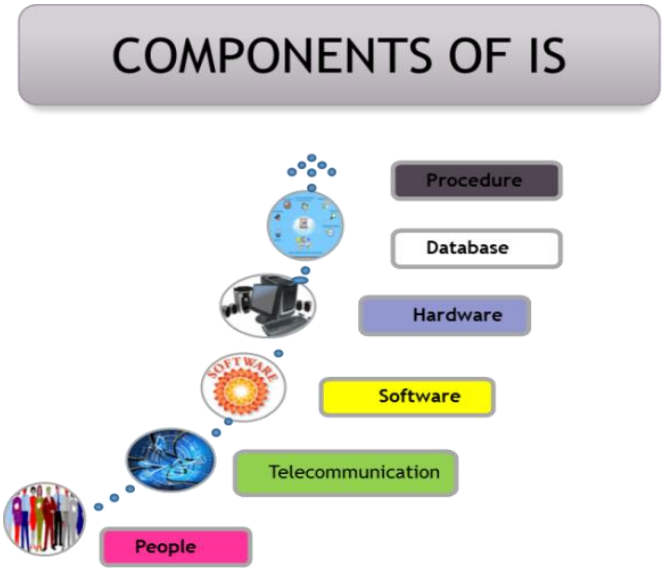


Figure 1.1: Components of Information System

1.1.1 THE NEED FOR INFORMATION SYSTEM SECURITY

Information System Security is the process by which digital information assets are protected. The goals of Information System Security are as follows:

- Prevent unauthorized access to the network that is of potential threat to the network and its resources.
- Ensure that the authentic users can effectively access the network and its services.
- Applications that can protect the network from unauthorized access are in place.

1.1.2 CHARACTERISTICS OF INFORMATION SYSTEM SECURITY

Figure 1.2: The Information System Security Goals

a) Confidentiality

Confidentiality is the protection of personal information. It means keeping a client's information between you and the client, and not telling others including co-workers, friends, family, etc.

b) Integrity

Integrity of information refers to protecting information from being modified by unauthorized parties.

- trustworthiness of information resources.
- assurance that data is genuine.
- Information needs to be changed constantly.
- Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

c) Availability

Availability means the information must be available when it is needed.

- unsprisingly to the avalability of information resources.
- System still functions efficiently after security provisions are in place.
- The information created and stored by an organization needs to be available to authorized entities 24x7.
- Information needs to be constantly changed, which means it must be accessible to authorized entities.

1.1.3 APPLY THE CHARACTERISTICS OF CIA IN REAL ENVIRONMENT

CONFIDENTIALITY

When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality.
For example, federal law requires that universities restrict access to private student information. The university must be sure that only those who are authorized have access to view the grade records.

INTEGRITY

Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. Just as a person with integrity means what he or she says and can be trusted to consistently represent the truth, information integrity means information truly represents its intended meaning. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something.
An example of this would be when a hacker is hired to go into the university's system and change a grade.
Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file or someone authorized to make a change accidentally deletes a file or enters incorrect information.

AVAILABILITY

Availability means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe.
For example, a stock trader needs information to be available immediately, while a sales person may be happy to get sales numbers for the day in a report the next morning. Companies such as Amazon.com will require their servers to be available twenty-four hours a day, seven days a week. Other companies may not suffer if their web servers are down for a few minutes once in a while.

1.1.4 POTENTIAL RISKS TO INFORMATION SYSTEM SECURITY

Categories of Risks

- **Physical damage** - Fire, water, vandalism, power loss, and natural disasters.
- **Human interaction** - Accidental or intentional action or inaction that can disrupt productivity.
- **Equipment malfunction** - Failure of systems and peripheral devices.
- **Inside and outside attacks** - Hacking, cracking, and attacking
- **Misuse of data** - Sharing trade secrets, fraud, espionage, and theft.
- **Loss of data** - Intentional or unintentional loss of information through destructive means.
- **Application error** - Computation errors, input errors, and buffer overflows.
- **Social Status** - Loss of Customer base and reputation.

1.1.5 THE GOALS OF SECURITY POLICIES

A security policy is a formal statement, supported by a company's highest levels of management, regarding the rules by which employees who have access to any corporate resource abide.

The security policy should focuses on:

- **Asset Identification**
  - To identify the resources used in network for various applications.
  - Network devices such as routers, switches and firewalls should be taken care.

- **Vulnerability Assessment**
  - The process of identifying the vulnerabilities in the system.
  - To ensure configurations are correctly set and the proper security patches are applied.

- **Threat Identification**
  - To identify a threat in the system.
  - Unauthorized access to information through networks.

1.1.6 OPEN SECURITY MODELS

- The **easiest** to implement.
- **Simple password and server security** becomes the foundation of this model.
- This model assumes that the protected assets are **minimal**, users are **trusted**, and threats are minimal.
- Suitable for LANs/public WANs that are **NOT connected** to the Internet.
- If security breaches occur, the result will be in great damage or loss.

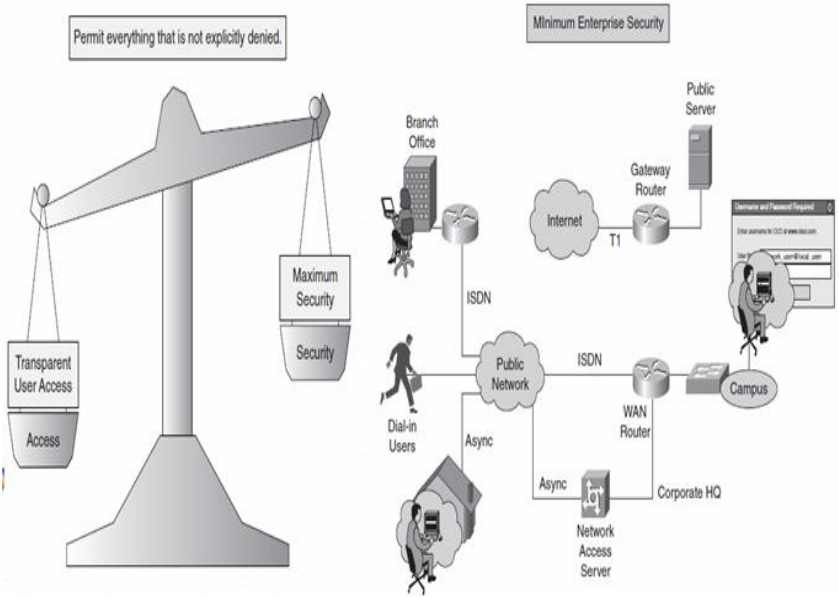


Figure 1.3: Open Security Models

1.1.7 RESTRICTIVE SECURITY MODELS

- **More** difficult to implement.
- **Firewalls** and identity **servers** become the foundation of this model.
- This model assumes that the protected assets are substantial, **some users** are not trustworthy, and that threats are likely.
- Suitable for LANs/public WANs that connect to the Internet.
- Ease of use for users diminishes as security tightens.

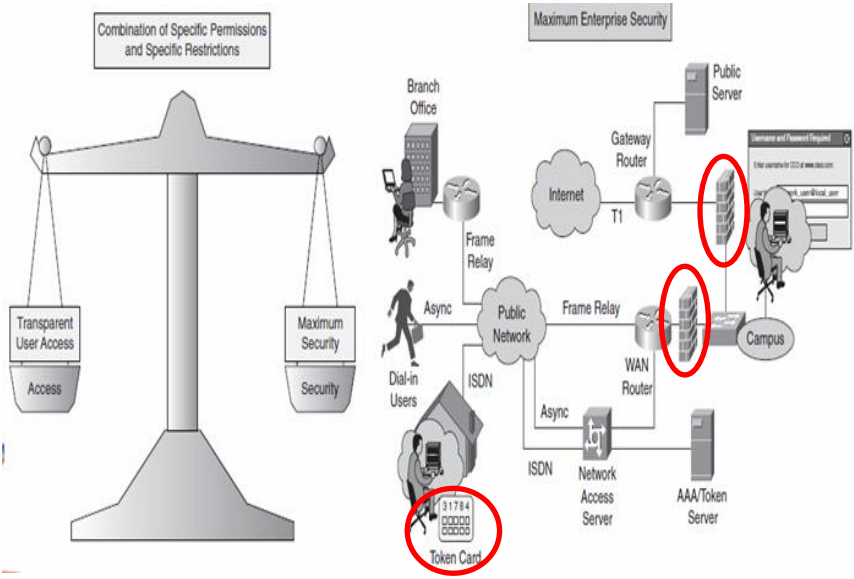


Figure 1.4: Restrictive Security Models

1.1.8 CLOSED SECURITY MODELS

- **Most** difficult to implement.
- **All** available security measures are implementing in this design.
- This model assumes that the protected assets are **premium**, **all users** are not trustworthy, and that threats are frequent.
- User access is **difficult and cumbersome**.
- Need many train network administrator to maintain the tight security applied.

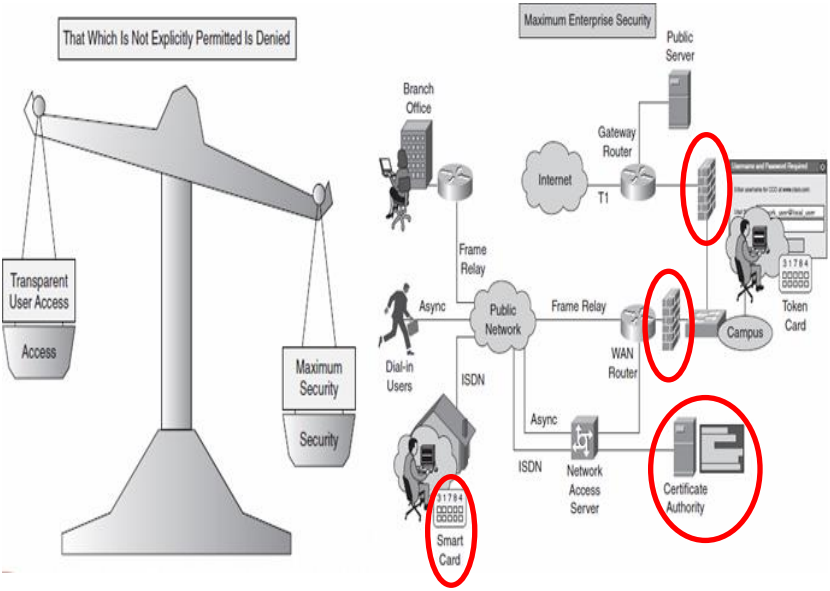


Figure 1.5: Close Security Models

1.1.9 THE ROLES OF THE INFORMATION SECURITY ORGANIZATIONS

a) CERT/CC

C*omputer* ***E****mergency* ***R****esponse* ***T****eam* ***C****oordination* ***C****enter*.

The CERT Coordination Center (CERT/CC) is a reporting center for **Internet security issues**. The CERT/CC plays a major role in coordinating responses to Internet security threats. The CERT/CC is located at the Software Engineering Institute (SEI) operated by Carnegie Mellon University.

Responsible for:

- Study internet security vulnerabilities
- Research networked system
- Develop info & training

b) US-CERT

The ***U****nited* ***S****tates* ***C****omputer* ***E****mergency* ***R****eadiness* ***T****eam* (US-CERT).

US-CERT was established in 2003 to protect the nation's Internet infrastructure by coordinating defense against and responses to Internet security threats.

US-CERT is responsible for the following:

- Analyzing and reducing cyber threats and vulnerabilities
- Disseminating cyber threat warning information
- Coordinating incident-response activities

c) SANS Institute

The **S**ysAdmin, **A**udit, **N**etwork, **S**ecurity (SANS) Institute was established in 1989.

Responsible for:

- Cooperative **research and education** organization.
- Develops and maintains research documents about various aspects of information security.
- Provide information security training and security certification.
- Operates the Internet's early warning system - the Internet Storm Centre.

d) (ISC)²

The **I**nternational **I**nformation **S**ystems **S**ecurity **C**ertification **C**onsortium, Inc. (ISC2) is a nonprofit organization that maintains a collection of industry best practices for information security. Educating and certifying information security professionals.

e) FIPS

The **F**ederal **I**nformation **P**rocessing **S**tandard (FIPS) are publicly announced standards developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors.

f) ICSA

ICSA Labs (International **C**omputer **S**ecurity **A**ssociation**)** began as NCSA (**N**ational **C**omputer **S**ecurity **A**ssociation). In its early days, NCSA focused almost solely on the **certification of anti-virus software**.

ICSA Labs is providing resources for research, intelligence, and certification and testing of products, including antivirus, firewall, IPsec VPN, Cryptography, SSL VPN, network IPS, anti-spyware and PC firewall products.

1.2 THE INCREASING ISSUES OF ON-LINE SECURITY

1.2.1 THREATS ISSUES OF ON-LINE SECURITY MEDIUM

a) Electronic Mail and News

Electronic mail has become an important communication tool using attaching and sending documents via network. But some characteristics of electronic mail, such as the anonymity of sender location, role of the sender, and even the identity of the sender, are problematic. Online news providers associated with an established news organization such as a television station or newspaper, were judged more credible than content providers without such identification.

b) File Transfer

The File Transfer tool permits files to be uploaded to the server to be shared with everyone in the session. Files and URLs can be transferred. Uploaded files and URLs are pushed out to everyone in the session and must be explicitly saved by the receiving participants and moderators. Use File Transfer to distribute handouts before, during or at the end of the session.

c) Remote Access to Hosts

Companies are finding that they must provide remote access to corporate resources for a number of different people for employees who work from home on a regular basis, employees who require access to resources such as email and enterprise applications after regular hours, on weekends or while travelling, business partners who need access to specific data, applications or other resources outsourced and off-shore workers.

d) Real Time Conferencing Services

Used to Sharing ideas, making decisions and building relationships. Global conferencing services can help accelerate decision making, allowing you to get your products to market quicker and more efficiently while affording your employees a better work-life balance. Can even work from home or anywhere else they have a phone and computer, in locations around in the world.

1.2.2 THREATS TERMINOLOGY

a) Information Theft

Get the private information (ID number/pin number/password) without any permission. It is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity. Examples of information theft are downloading sensitive files into personal removable media, copy-and-paste of confidential file content, and screen capture of protected document image and so on.

b) Unauthorized disclosure

An event involving the exposure of information to entities not authorized access to the information. That an organization suspects some of its employees leaking out the confidential information to its competitor. It is also usually believed that its competitor actually planted spies within the organization in order to target and steal new product plan.

c) Information Warfare

May involved collection of tactical information to demoralize the enemy and the public. It involved the use of information and communication technology in pursuit of a competitive advantage over an opponent.

d) Accidental data Loss

An error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing.

e) Data disclosure

Data or information is opened to unauthorized persons, processes, or devices. Make data available without permission or authority. Data is stolen but owner still has it.

f) Data modification

Data is altered without authorization. Data can be modified in store or in transmission.

g) Data availability

Means the property that data or information is accessible and useable upon demand by an authorized person. Timely, reliable access to data and information services for authorized users.

CHAPTER 2
Introduction To Vulnerabilities, Threats And Attack

This chapter discusses the following topics:

- Vulnerabilities, Threats and Attack.
- Various Tools In Network Security

2.1 VULNERABILITIES, THREATS AND ATTACK.

Vulnerabilities

Vulnerability is a weakness that is inherent in every network and device. This includes routers, switches, desktops, servers and even security devices themselves.

Threats

The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

Attacks

The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops.

2.1.1 VULNERABILITY IN RELATION TO SECURITY

Vulnerabilities in network security can be summed up as the "soft spots" that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network.

An experienced hacker knows that **every network or device has a certain degree of vulnerability** or **weakness**, and they take advantages of each security weakness or loophole to **exploit the network**.

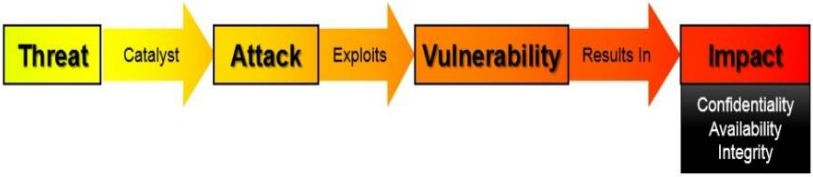


Figure 2.1: Vulnerability in relation to security

2.1.2 THE WEAKNESSES IN RELATION TO SECURITY VULNERABILITIES

a) Technology weaknesses

Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses and network equipment weaknesses.

- Lack of sophisticated hardware.
- There is still bugs and error in software development.
- Every computer network and device has security weakness/vulnerabilities.

Example:

- Hardware Issue (Routers, Firewalls, Switches etc.)
- Operating System Issue (Unix, Linux, Mac, Windows)
- Network Protocol Issue (HTTP, FTP, SMTP, SNMP)
- Application vulnerabilities

b) Configuration weaknesses

Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.

Configuration Weaknesses	Effect
Unsecured accounts	User account information might be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	Tis common problem is the result of poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites.
Unsecured default settings	Many products have default settings that enable security holes.
Misconfigurations of the equipment itself	Can cause significant security problems. For example, misconfigured access lists, routing protocols or SNMP community strings can open up large security holes.

c) Security Policy weaknesses

Security policy weaknesses can create unforeseen security threats. The network can pose security risks to the network if users do not follow the security policy. Every organisation must have a security policy that governs and maintains how the network or company information should be used.

- **Lack of a written security policy**
  An unwritten policy cannot be consistently applied or enforced.

- **Politics**
  Political battles and turf wars can make it difficult to implement a consistent security policy.

- **Concise access controls not applied**
  Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources.

- **Software and hardware installation and changes do not follow policy**
  Unauthorized changes to the network topology or installation of unapproved applications create security holes.

- **Nonexistent disaster recovery plan**
  The lack of a disaster recovery plan allows chaos, panic and is confusion to occur when someone attacks the enterprise.

2.1.3 SECURITY THREATS

A threat is defined as "*the potential for a threat-source to exercise a specific vulnerability*"

Threats

- Management must be informed of the various kinds of threats facing the organization.
- A threat is an object, person, or other entity that represents a constant danger to an asset.
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls.

THREATS TO INFORMATION SECURITY

1. Human Error
2. Natural Disaster
3. System Failures

Category of Threat	Examples
1. Human error or failure	Accidents, employee mistakes, or failure to follow established policies or procedures
2. Compromises to intellectual property	Theft or unauthorized use of written documents, trade secrets, copyrights, trademarks, and patents, including software piracy
3. Espionage or trespass	Unauthorized access and/or data collection, hacking
4. Information extortion	Blackmail or information disclosure
5. Sabotage or vandalism	Destruction of systems or information
6. Theft	Illegal confiscation of equipment or information
7. Software attacks	Malicious code or malware attacks, including viruses, worms, macros, denial-of-service, and Trojan horses
8. Forces of nature	Fire, flood, earthquake, lightning, and electrostatic discharge
9. Deviations in quality of service	ISP, power, or WAN service issues from service providers
10. Hardware failures or errors	Equipment failure
11. Software failures or errors	Bugs, code problems, unknown loopholes
12. Obsolescence	Antiquated or outdated technologies

Figure 2.2: Category of Security threats

2.1.4 TYPES OF THREATS

There are four primary classes of threats to network security: -

- **a)** Unstructured threats
- **b)** Structured threats
- **c)** External threats
- **d)** Internal threats

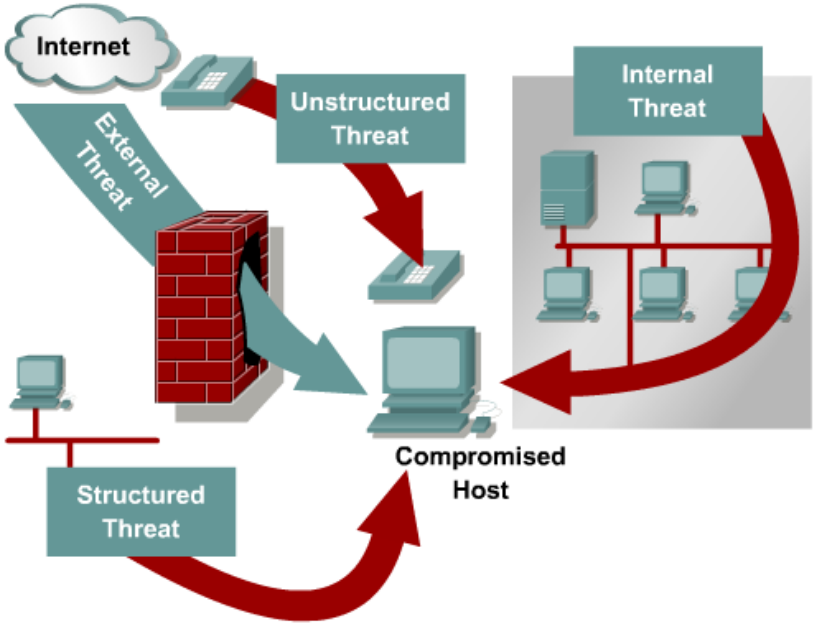


Figure 2.3: Security threats

a) Unstructured threats

- Unstructured threats consist of mostly **inexperienced individuals** using easily available **hacking tools** such as shell scripts and password crackers.
- Many tools available to anyone on the internet such as port scanning tools and address sweeping tools.
- This is especially focused on the internal users who are interested in what kinds of devices exist in their own network.
- It can be a serious damage to a company.

b) Structure threats

- Structured threats come from hackers who are more highly motivated and technically competent.
- Structured threats in implemented by a technically skilled person who is trying to gain access to the network.
- This hacker creates understand, develop, and use sophisticated tools to break into your network or to disrupt the service running in the network.
- These people know system vulnerabilities and can understand and develop exploit code and scripts.
- These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

c) External threats

- It can arise from individuals or organizations working outside of a company.
- They do not have authorized access to the computer systems or network.
- They work their way into a network mainly from the Internet or dialup access servers.

d) Internal threats

- It occurs when someone has authorized access to the network with either an account on a server or physical access to the network.

2.1.5 ATTACKERS IN INFORMATION SECURITY

a) Hackers

- Has deep understanding of a computers and networking.
- Not satisfied with simply executing a program.
- They need to know how everything works.

Classification of hackers

Types of Hackers	Description
White Hat	A person who works as an IT security and will try to defense and offense its own network for security measure.
Ethical hacker	A professional person that exploits the network with permission from the user to detect any vulnerability that may occur.
Black Hat	• Also called as cracker or dark side hacker • Negotiates the security of the system without authorized access
Grey Hat	• Combination of black hat and white hat hackers • Intrudes into a system and does no damage

b) Attackers

- Someone who wants to steal or disrupt a person asset.
- May be technically adept or an armature.

ATTACKER	HACKER
Someone who wants to actually attack your computer or cause harm.	Someone who just like to know exactly how things work. They don't cause harm. but rather explore. experiment and gain knowledge.
Involve aggressive plays and troubles to computer	Consist of 2 types: white-hats black-hats White-hats: help fix badly written software programs and write new programs . Black-hats: modify or create software for criminal purposes such as stealing your passwords and your identity.

Figure 2.4: Comparison between attacker and hacker

c) Script Kiddies

An unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface website.

d) Cybercriminals

Computer crime, or **Cybercrime**, refers to any crime that involves a computer and a network. Any crime that involve computer and network. It is criminal exploitation of the internet.

Cybercriminals use computers in three broad ways:

- **Select computer as their target:** These criminals attack other people's computers to perform malicious activities, such as spreading viruses, data theft, and identity theft.
- **Uses computer as their weapon:** They use the computer to carry out "conventional crime", such as spam, fraud, illegal gambling.
- **Uses computer as their accessory:** They use the computer to save stolen or illegal data.

2.1.6 VARIOUS TYPES OF ATTACKS

a) Reconnaissance attack (eg: Sniffing, spoofing)
b) Access attack (eg: hacking, brute force)
c) Denial of service attack (DoS)
d) Distributed Denial of Service attacks (DDoS)
e) Malicious code attack (worms, viruses, trojan horses)

a) Reconnaisance attack

- Reconnaissance attacks are used to gather information about a target network or system.
- It is also called **information gathering**.
- **No specific damage may be caused by the reconnaissance attack**, but it is like to burglars staking out a neighborhood, watching for times of inactivity, and occasionally testing windows and doors for access.

Example of Reconnaisance attack

- **Sniffing**
  - Activities that used to find or steal important information in the network.
  - These vulnerabilities will ensure that the port will become more easier to be attacked
  - Many tool available for network sniffing
  - 2 common :
    - Ethereal, Snort

- **Spoofing**
  - Spoofing is the practice of deceiving people into believing an email or Web site originates from a source that it does not.
  - The most common type of spoofing is email spoofing, but Web page spoofing and IP spoofing are also very common.
  - A spoofing attack is a situation where an individual or a successful program to disguise by falsifying data and utilize existing excess illegally.

b) Access Attack

- **Access attack** refers to unauthorized data retrieval, system access, or privilege escalation.
- System access is the **ability for an unauthorized intruder to gain access to a device** for which the intruder does not have an account or a password.
- Entering or accessing systems to which one does not have authority to access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Example of Access Attack

- **Hacking**
  - Method of breaking into information system without proper permission.

- **Cracking**
  - Process of recovering the original form of passwords or information that stored in encrypted form in a computer.

- **Brute Force**
  - Cryptanalytic attack that can be used against any encrypted data.
  - It consists of systematically checking all possible keys or password until the correct one is found.

c) Denial of Service Attack (DoS)

- Denial of service implies that an **attacker disables or corrupts networks, systems, or services** with the intent **to deny services to intended users.**
- DoS attacks involve either crashing the system or slowing it down to the point that it is unusable.
- But DoS can also be as simple as deleting or corrupting information.
- In most cases, performing the attack simply involves **running a hack or script.**
- **DoS attacks** are the **most feared.**

Examples of common DoS threats:

- **Ping of death**
  This attack modifies the IP portion of the header, indicating that there is more data in the packet than there actually is, causing the receiving system to crash.

- **SYN flood attack**
  This attack randomly opens up many TCP ports, tying up the network equipment or computer with so many bogus requests that sessions are thereby denied to others.

- **Packet fragmentation and reassembly**
  This attack exploits a buffer–overrun bug in hosts or internetworking equipment.

- **E-mail bombs**
  Programs can send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.

- **CPU hogging**
  These attacks constitute programs such as Trojan horses or viruses that tie up CPU cycles, memory, or other resources.

d) Distributed Denial of Service Attacks (DDoS)

DDoS attacks are designed to saturate network links with spurious data. This data can overwhelm an Internet link, causing legitimate traffic to be dropped.
DDoS uses attack methods similar to standard DoS attacks but operates on a **much larger scale**. Typically hundreds or thousands of attack points attempt to overwhelm a target.

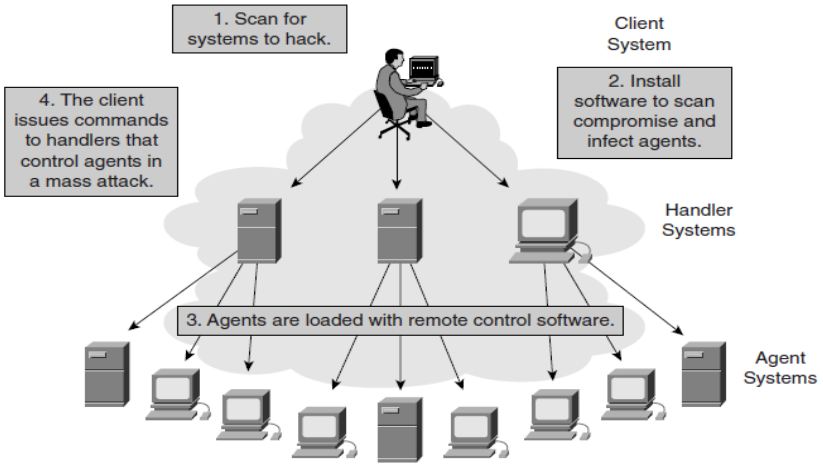


Figure 2.5: Distributed Denial of Service Attacks

Example DDoS Attack:-

- **Smurf**

  The Smurf attack starts with sending a large number of spoofed ICMP echo, or ping, requests to broadcast addresses, hoping that these packets will be magnified and sent to the spoofed addresses.

- **Tribe Flood Network**

  Tribe Flood Network (TFN) distributed tools used to launch coordinated DoS attacks from many sources against one or more targets.

e) Malicious Code Attack

Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services.

WORMS, VIRUSES AND TROJAN HORSES

i. **Worms**

An application that executes arbitrary code and installs **copies of itself** in the memory of the infected computer, which then infects other hosts.

ii. **Virus**

Malicious software that is attached to another program to execute a particular unwanted function on the user workstation. It replicates itself **with human intervention.**

iii. **Trojan Horses**

An application written to look like something else that in fact is an attack tool.

Virus	Worms	Trojan Horse
Require human action.	Spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.	Appear to be useful software but will actually do damage once installed or run on your computer.
Spreading of computer virus, mostly by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.	Replicate itself on your system, creating a huge devastating effect.	Designed to be annoying and malicious (like changing your desktop, adding silly active desktop icons) or can cause serious damage (create a backdoor, deleting files)
It also passing the infection from one infected system to another (attach to executable file)	Do not need to infect other file in order to reproduce.	Do not reproduces by infecting other files

Figure 2.6: Differences between virus, worm and Trojan horse.

2.1.7 HOW TO SECURE ASSETS

- An "asset" is any resource, product, process, system, or any other thing that has some value to an organization and, as such, must be protected. Assets can be physical/tangible items, such as equipment or computers, and they can also be non-tangibles, such as information or intellectual property.
- An asset will have some sort of "value" or worth to an organization based on various elements or factors important to the organization.
- some considerations when assigning value to information and assets should be:
  - Value of the asset to adversaries.
  - Cost to replace the asset if lost.
  - Operational and productivity costs incurred if the asset is unavailable.
  - Liability issues if the asset is compromised.

2.2 VARIOUS TOOLS IN NETWORK SECURITY

What is host analysis software?

- Port-scanning can determine which hosts are alive and what ports they have opened.
- It can be done just by entering a range of addresses or a name of a network.

2.2.1 NETWORK SCANNING TOOLS:

There are many example of host analysis software. Examples of them are:

a) Network Mapper (Nmap)
b) Netstat tool
c) NetScan tool

a) Network Mapper (Nmap)

- Nmap is a free and open source (license) utility for network discovery and security auditing.

- Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

- Nmap features include:
  - **Host discovery** – Identifying hosts on a network.
  - **Port scanning** – Enumerating the open ports on target hosts.
  - **Version detection** – to determine application name and version number.
  - **OS detection** – Determining the operating system and hardware characteristics of network devices.

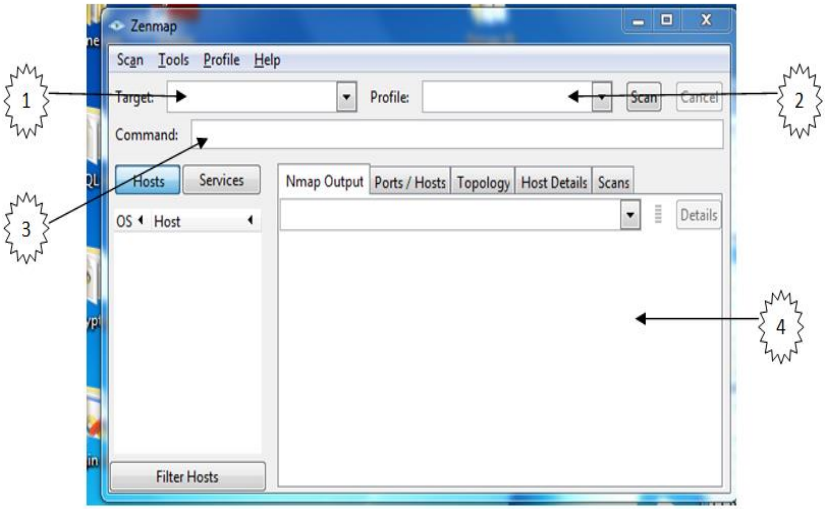


Figure 2.7: Using Nmap

1. This is a target or host text box. User must specify it first before scanning any network. It can be hostname, IP addresses or networks.
2. In this box, user can specified what type of scan they want to do. There is various type of scan such as ping scan, intense scan and etc.
3. After user has chosen their scan type, this box will show the command of the scan type. Various scan may have their own command.
4. This field will show the result of the scan

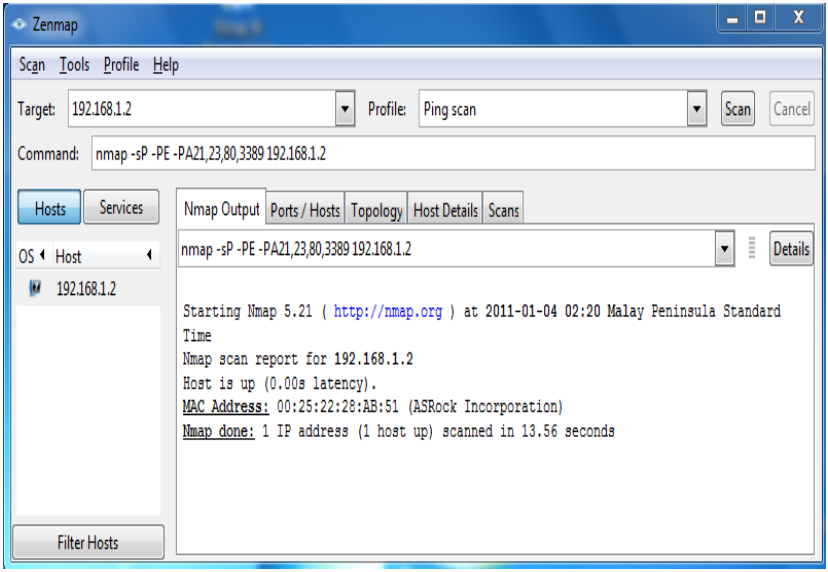


Figure 2.8: ping scanning a host using Nmap

b) Netstat tool

Netstat is a tool for managing and monitoring the status of your server's interfaces, routes, and connections, and it is a useful tool for checking network and Internet connections. Some useful applications for the average PC user are considered, including checking for malware connections.

- **Syntax and switches**

The command syntax isnetstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-v] [interval]

A brief description of the switches is given in Table I below. Some switches are only in certain Windows versions, as noted in the table..*Note that switches for Netstat use the dash symbol "-" rather than the slash "/"*.

c) Netscan tool

NetScanTools is an **Internet Information collection tool** for Windows that helps you track down information about an IP Address, Hostname, Domain Name, Email Address or URL (web address).

Example of Netscan Tool

- **Network Scanner** is an ***IP scanner*** that is used for scanning both large corporate networks that have hundred thousands of computers along with small home networks with several computers.
- Network Scanner will show you all the shared resources.
- To audit network computers or use it to search for available network resources, both network administrators and regular users can use Network Scanner.
- Network Scanner will not only find network computers and shared resources, but also check its access rights which the user can mount as a network drive or open them in Explorer or in their browser.
- You can easily export the results of scanning the network to an XML, HTML or text file or store them in the program itself.

2.2.2 VARIOUS SECURITY ANALYSIS TOOLS

a) Open Source Tools - KNOPPIX TOOLS

- **KNOPPIX** is a bootable live system on CD or DVD, consisting of a representative collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals.
- KNOPPIX can be used as a productive Linux system for the desktop, educational CD, rescue system, or adapted and used as a platform for commercial software product demos.
- Knoppix mostly consists of free and open source software.

Uses of Knoppix:

- It makes an excellent diagnostic tool.
- Spyware and software key loggers are useless against someone running Knoppix.
- Knoppix can and help us to get on the Internet and download the software and instructions to remove our uninvited guest.
- Under the right conditions, you can clean viruses off your Microsoft Windows machine directly from Knoppix.

b) Microsoft tools such as Microsoft Baseline Security Analyser (MBSA)

- Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool that helps **determine the security state of your computer** based on Microsoft security recommendations.
- After the tool completes the scan on your computer, you receive specific remediation suggestions.
- MBSA **improve your security management process** by detecting common security misconfigurations and missing security updates on your computer systems.
- MBSA **scan on all incoming computers** to reduce and eliminate possible threats caused by security misconfigurations and missing security updates.

Running MBSA

- Once you've downloaded and installed MBSA Setup-EN.msi, double-click on the MBSA "watering can" [padlock and checkmark] icon. This opens the MBSA welcome screen.
- Click "Scan a computer."

Figure 2.9: Microsoft Baseline Security Analyser (MBSA)

- On the next screen, don't change anything. Just make sure you are connected to the Internet and then click "Start scan."

- If scanning the local computer, it will be pre-selected for scanning. We can also choose to scan another computer if we are in a network by selecting its name or its IP address. Make sure the options "Check for Windows Administrative vulnerabilities", "Check for weak passwords" and "Check for security updates" are checked. Uncheck the options "Check for IIS vulnerabilities" and "Check for SQL vulnerabilities", if we don't have them installed.

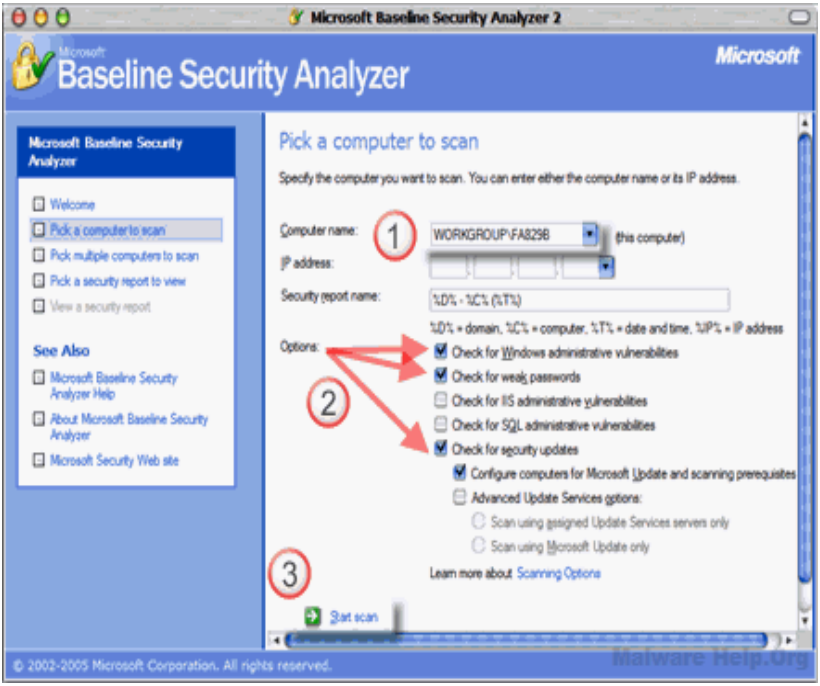


Figure 2.10: start scan

- MBSA calls home to Microsoft and downloads something called "MSSecure.cab." This file contains information about practically every patch Microsoft has released. MBSA scans your computer's operating system, system components, and Microsoft applications. MBSA then compares the version numbers of the Microsoft programs on your computer with the latest version numbers in the MSSecure.cab file.

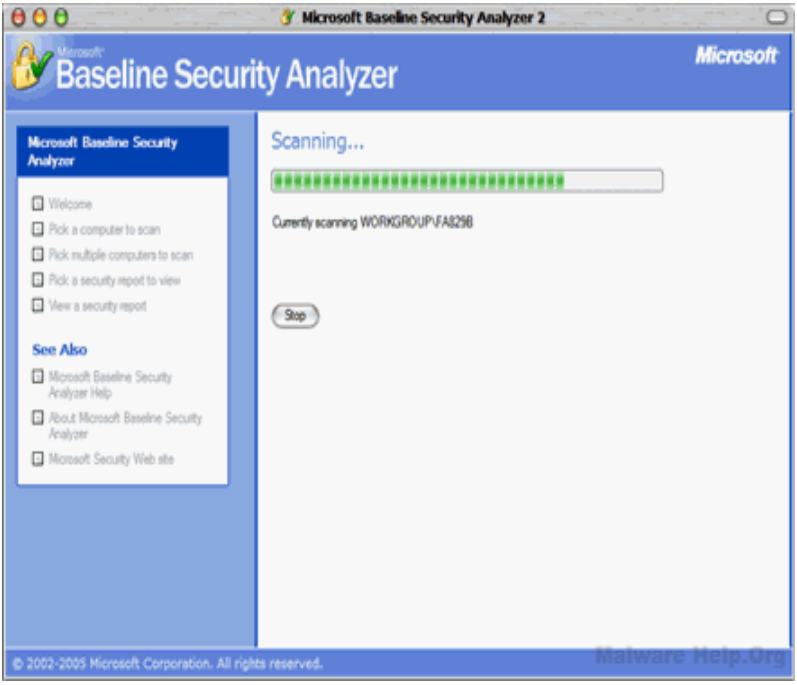


Figure 2.11: MBSA scanning progress

- Finally, MBSA shows you which update your computer are missing.

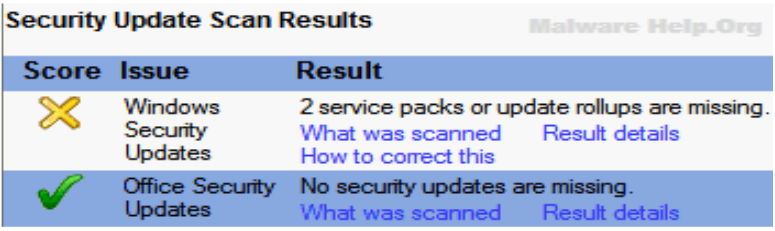
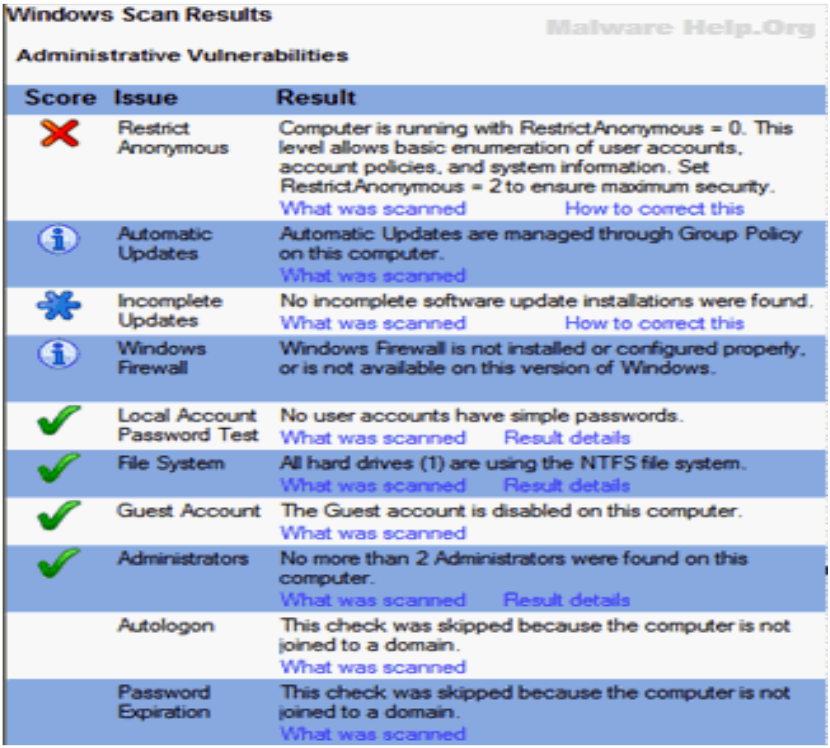


Figure 2.12: Security Update Scan Results



Windows Scan Results

Malware Help.Org

Administrative Vulnerabilities

Score	Issue	Result
✗	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level allows basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security. What was scanned How to correct this
ⓘ	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned
✱	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
ⓘ	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned

Figure 2.13: Windows Scan Results

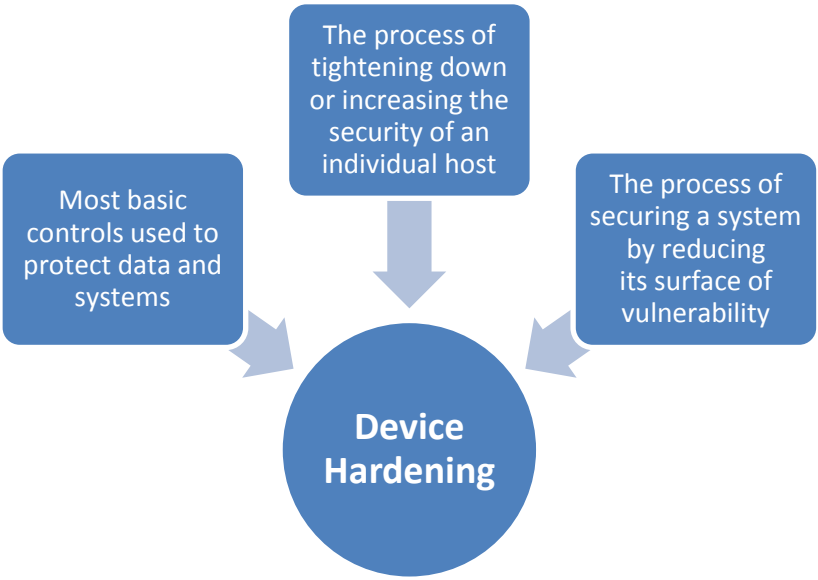
CHAPTER 3
Security Devices and Technologies

This chapter discusses the following topics:

- End point protection and management
- Firewalls
- Firewalls using Microsoft Windows Server / Open Source Software

3.1 END POINT PROTECTION AND MANAGEMENT

3.1.1 DEVICE HARDENING IN HOST AND SERVER BASED



Process of device hardening

- Protection in a computer system.
- Protect at the host level, the user level the physical level and all the sublevels in between. Each level requires a unique method of security.
- Example: Install antivirus, keeping security patches and hot fixed updated, creating strong passwords, not allowing file sharing among programs.

3.1.2 HOST AND SERVER BASED SECURITY COMPONENT AND TECHNOLOGIES

a) Anti-Virus Software

- It is a program that searches your drive for any known or potential viruses.
- Anti-virus program **should be kept updated** so it recognizes new version of malicious software.
- Antivirus or anti-virus software is used to prevent, detect, and remove computer viruses, worms, and trojan horses.
- It may also prevent and remove adware, spyware, and other forms of malware.
- Installed antivirus software running on an individual computer is only one method of guarding against viruses.
- Other methods are also used, including cloud-based antivirus, firewalls and on-line scanners.

There are several methods which antivirus software can use to identify Malware:

- **Signature based detection** is the most common method. To identify viruses and other malware, antivirus software compares the contents of a file to a dictionary of virus signatures.

- **Heuristic-based detection**, like malicious activity detection, can be used to identify unknown viruses.

- **File emulation** is another heuristic approach. File emulation involves executing a program in a virtual environment and **logging** what actions the program performs. Depending on the actions logged, the antivirus software can determine if the program is malicious or not and then carry out the appropriate disinfection actions.

b) Personal Firewall

- It is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.
- Typically it was designed for use by end-users. As a result, a personal firewall will usually protect only the computer on which it is installed.
- It may also provide some level of intrusion detection. Allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

Common personal firewall features:

- Block spyware: Blocks spyware before it installs in a computer and removes existing spyware.
- Stop Hackers: protects and conceals computer from hackers.
- Improves PC performance: Clean clutter off
- Backs up and restores files: Automated backup and one click restore.
- Secure Your Identity: Protects your online identity
- Root kit protection: find and removes hidden threats in the OS.
- Phishing protection: identifies and blocks fraudulent websites.
- Peer-to-peer network: filter incoming or outgoing traffic into the network.
- Alert the user about outgoing connection attempts.
- Allows the user to control which programs can and cannot access the local network and/or Internet.
- Hide the computer from port scans by not responding to unsolicited network traffic.
- Prevent unwanted network traffic from locally installed applications.
- Provide the user with information about an application that makes a connection attempt.
- Provide information about the destination server with which an application is attempting to communicate.

c) Operating System Patches

- Operating system patches are the latest security updates that are released by the operating system vendor such as Microsoft, Apple and Sun etc.
- To keep your computer protected from the viruses, spyware, adware, Trojan horses, malware and hackers attacks and other online threats it is highly recommended that you update your operating system regularly.
- Operating system contains the vulnerabilities and security lapses and that can be fixed by installing the latest services packs, hot fixes and the security patches.

d) Intrusion detection and prevention

- An intrusion detection system (IDS) is software that automates the intrusion detection process.
- An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Uses of IDPS Technologies

- **Identifying security policy problems.**
  - An IDPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rule sets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.

- **Deterring individuals from violating security policies.**
  - If individuals are aware that their actions are being monitored by IDPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection.

e) Host-based Intrusion Detection System

Host based IDS typically monitor system, event, and security logs on Windows NT and syslog in UNIX environments. When any of these files has been changed, the IDS compare the new log entry with attack signatures to see if there is a match. If so, the system responds with administrator alerts and other calls to action.

Advantages of Host-Based Intrusion Detection Systems

- **Detects attacks that network-based systems miss**
  - Host-based systems can detect attacks that cannot be seen by network-based products. For example, attacks from the keyboard of a critical server do not cross the network, and so cannot be seen by a network-based intrusion detection system.

- **Requires no additional hardware**
  - Host-based intrusion detection resides on existing network infrastructure, including file servers, Web servers, and other shared resources. This efficiency can make host-based systems very cost effective because they do not require another box on the network that requires addressing, maintenance, and management.

- **Lower cost of entry**
  - While network-based intrusion detection systems can offer wide coverage for little effort, they are often expensive. Deploying a single intrusion detection system can cost more than $10,000 for NIDS.

HIDS vs NIDS

Host-Based Intrusion Detection System (HIDS)	**Network-Based Intrusion Detection System (NIDS)**
Uses information obtained from a single host.	Uses information obtained from a total section of network.
More adaptable with version of system.	Less adaptable as related with whole network.
Requires less training.	Requires more training.
Scan local machine registry.	Uses LAN bandwidth.
Better for detecting inbound attacks NIDS.	Better for detecting outbound attacks.

3.2 FIREWALLS

A firewall is a part of a computer system or network that is designed to **block unauthorized access while permitting authorized communications**. Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

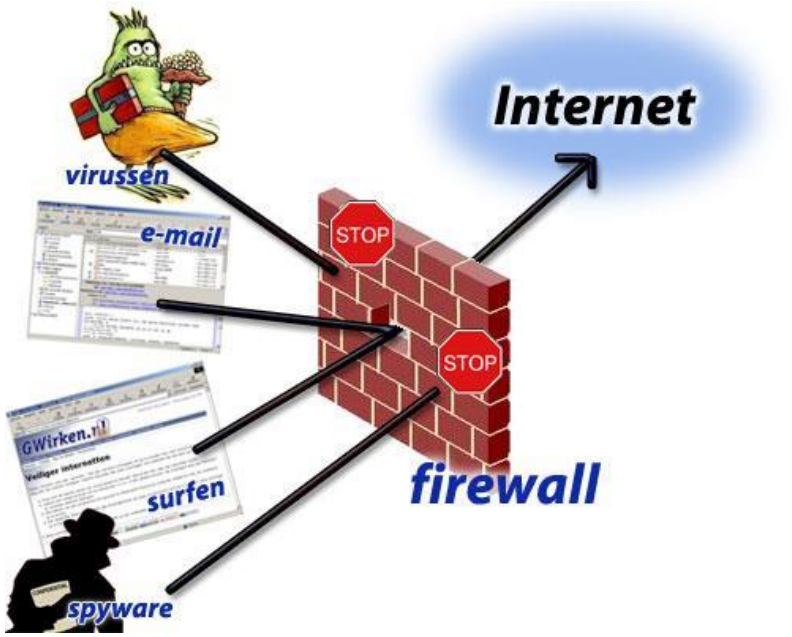


Figure 3.1: Firewalls

Firewall Limitations

- Cannot protect from attacks bypassing it.
- Cannot protect against internal threats.
  - e.g. disgruntled employee
- Cannot protect against transfer of all virus infected programs or files.

3.2.1 FIREWALLS ARCHITECTURE

Dual-Homed Gateway	▯ "Fail-safe" mode ▯ Internal structure hidden from outside	▯ Inconvenient to users ▯ Requires modification of user behavior ▯ Multiple proxies necessary ▯ Proxies not always available

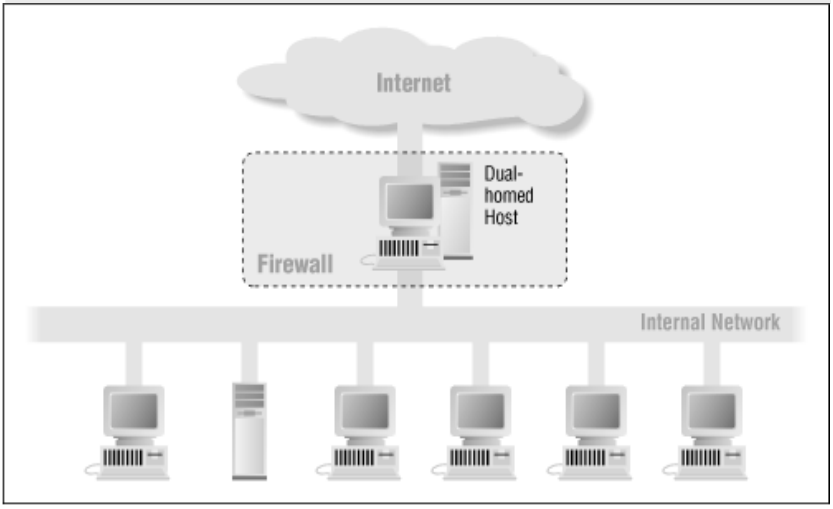


Figure 3.2: Dual-Homed Host Architecture

Architecture	Advantages	Disadvantages
Screening Router	Completely transparent Relatively easy and cheap	Difficulty handling certain traffic Difficult to configure Limited or no logging Lack of user authentication Difficult to hide internal network structure

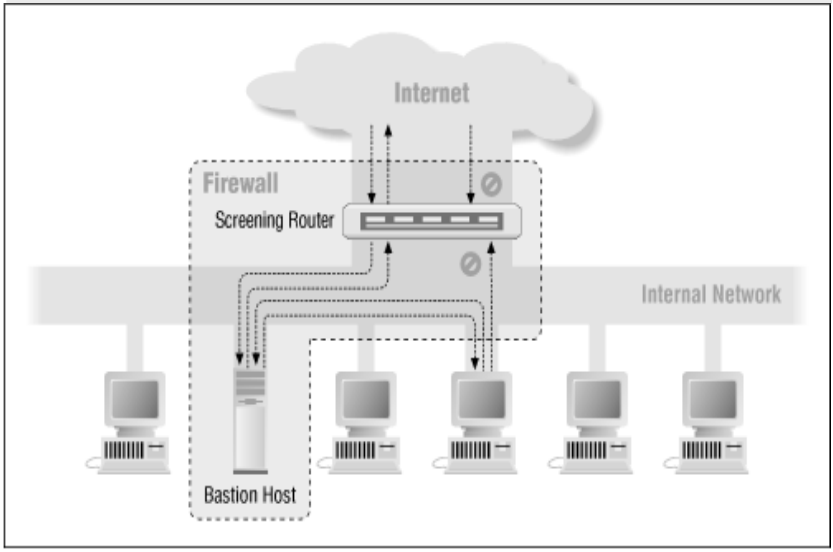


Figure 3.3*:* Screened-Host Architecture

Architecture	Advantages	Disadvantages
Screened Subnet	Transparent to end users Flexible Internal network structure hidden Provides services to outside without compromising inside	All security functions provided by gateway, a single point of security failure

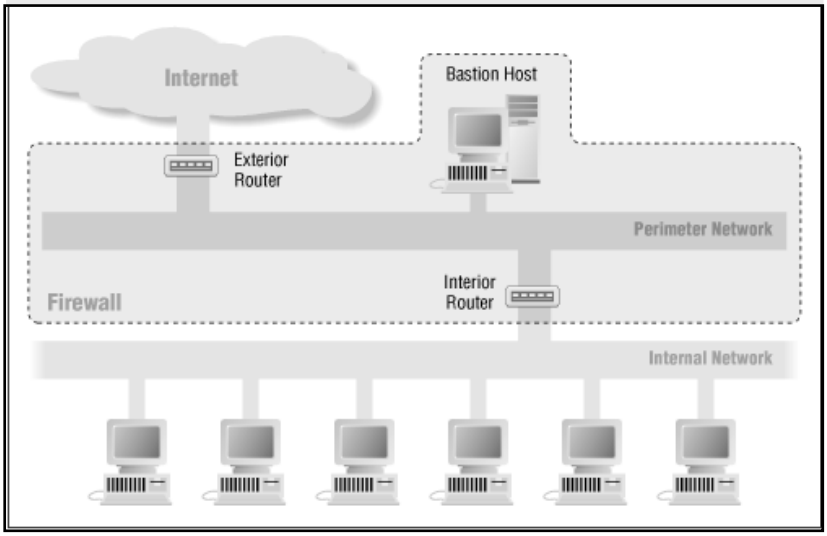


Figure 3.4: Screened-subnet Architecture

3.2.2 TYPES OF FIREWALL

a) Packet filtering firewall

Packet filtering inspects each packet passing through the network and accepts or rejects based on user-defined rules. Packet filtering firewalls don't do anything else. They analyze each packet in isolation and don't have any context (or "state") information to compare the current packet with previous packets.

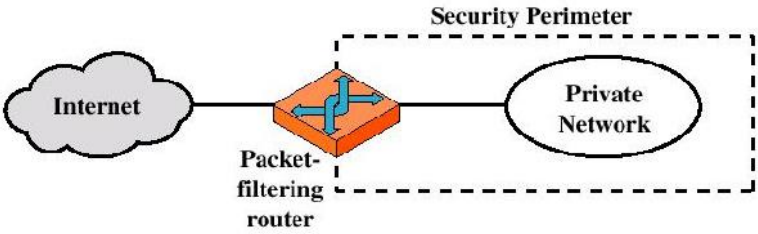


Figure 3.5: Packet filtering firewall

Advantages:

- Simplicity
- Transparency to users
- High speed

Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication

b) Circuit-level gateway

- Circuit-level gateways are often referred to as stateful inspection firewalls.
- Once the connection has been made, packets can flow between the hosts without further checking.
- These applications, which represent the second-generation of technology, monitor TCP handshaking between packets to make sure a session is legitimate.
- Traffic is filtered based on specified session rules and may be restricted to recognized computers only.
- Circuit-level firewalls hide the network itself from the outside, which is useful for denying access to intruders. But they don't filter individual packets.

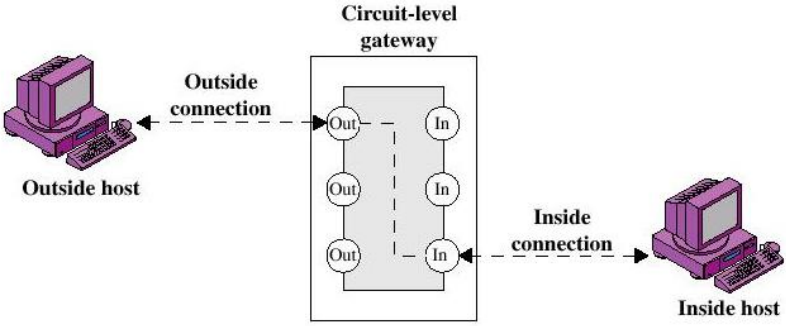


Figure 3.6: Circuit-level gateway

Circuit-level Gateway

- The security function consists of determining which connections will be allowed.
- Typically use is a situation in which the system administrator trusts the internal users.

c) Application level firewall

- Application-level firewalls (sometimes called proxies) have been looking more deeply into the application data going through their filters.
- By considering the context of client requests and application responses, these firewalls attempt to enforce correct application behavior; block malicious activity and help organizations ensure the safety of sensitive information and systems.
- They can log user activity too.
- Application-level filtering may include protection against spam and viruses as well, and be able to block undesirable Web sites based on content rather than just their IP address.

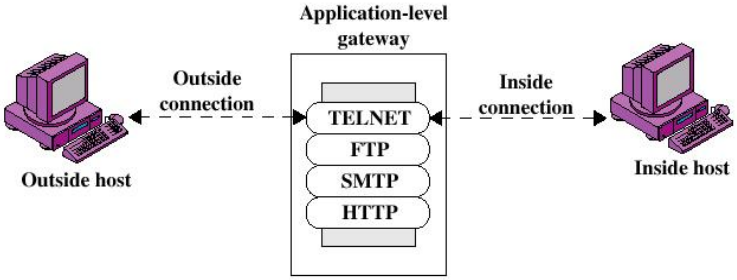


Figure 3.7: Application-level gateway

Application-level Gateway

- Also called proxy server
- Acts as a relay of application-level traffic
- There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

- **Advantages:**
  - Higher security than packet filters.
  - Only need to review a few allowable applications.
  - Easy to log and audit all incoming traffic.
- **Disadvantages:**
  - Additional processing overhead on each connection (gateway as splice point).

3.2.3 COMMON TECHNOLOGIES EMPLOYED IN BUILDING FIREWALLS

Static Packet filtering

- Simples and least expensive forms of firewall protection.
- Each packet entering or leaving the network is checked and either passed or rejected depending on a set of user-defined rules.

Dynamic Packet filtering

- Examine the contents of packet rather than just filtering them.
- A dynamic state list, keep track of all communication session between stations.

Proxy

- Policy rules are enforced through the use of proxies.
- Each protocol to be allowed must have its own proxy.
- **It also hide and user IP to prevent outsider know about it.**

3.2.4 HOW STATIC PACKET FILTERING WORKS

- Static packet filtering is a firewall and routing capability that provides network packet filtering based only on packet information in the current packet and administrator rules.
- Simples and least expensive forms of firewall protection.
- Each packet entering or leaving the network is checked and either passed or rejected depending on a set of user-defined rules.
- Dealing with each individual packet, the firewall applies its rule set to determine which packet to allow or disallow.

"Static" = "doors" are open at all times

Advantages

- Inexpensive *(economical)* or free
- Good for traffic management

Disadvantages

- Allows dangerous direct connections
- Leaves holes open
- Unsuitable for complex *(complicated)* environmen

3.2.5 HOW DYNAMIC PACKET FILTERING WORKS

- Dynamic packet filtering is a firewall and routing capability that provides network packet filtering based not only on packet information in the current packet, but also on previous packets that have been sent.
- For example without dynamic packet filtering, a connection response may be allowed to go from the internet to the secure part of the network.
- Dynamic packet filtering would consider whether a connection was started from inside the secure part of the network and only allow a connection response from the internet if the packet appeared to be a response to the request.

"Dynamic" = opens and closes "doors" according packet header data can keep track of context information about a session. (stateful filtering)

Advantages

- Only temporarily opens holes in Network Perimeter
- Supports almost any service

Disadvantages

- Allows direct IP connections
- No user authentication (requires application gateway)

3.2.6 HOW A PROXY PASSES THE NETWORK TRAFFIC

- 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.

3.2.7 COMPARISON BETWEEN STATIC PACKET FILTERS, DYNAMIC PACKET FILTER AND PROXY-BASED

STATIC PACKET FILTERS	DYNAMIC PACKET FILTERS	PROXY-BASED FIREWALLS
1. **Static packet** filters packets based on administrator defined rules governing allowed ports and IP addresses at the network and transport layers of the OSI network model as mentioned in item 1 above	1. Dynamic packet filtering also called stateful inspection provides additional capabilities including inspection of packet contents up to the application layer and consideration of the state of any connections.	1. 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.

3. Permanently allow in replies from all external addresses, assuming that users were free to visit any site on the Internet. This kind of filter would allow an attacker to sneak information past the filter by making the packet look like a reply	3. Dynamic packet filter can screen for replies that don't match a request. When a request is recorded, the dynamic packet filter opens up a small inbound hole so only the expected data reply is let back through.	3. The proxy does not simply pass the request along; it generates a new request for the remote information.
2. 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.	2. Dynamic packet filters are intelligent devices that make traffic-control decisions based on packet attributes and state tables. Dynamic packet filtering provides a better level of security than static packet filtering since it takes a closer look at the contents of the packet and also considers previous connection.	2. The proxy constantly butts into the conversation to make sure that all goes securely.

Figure 3.8: Comparison between Static Packet Filters, Dynamic Packet Filter and Proxy Based Firewalls.

Static vs Dynamic

Static / Stateless Packet Filtering	Dynamic/Statefull Packet Filtering
Is non-intelligent filtering devices. They offer little protection against advanced types of attack.	Intelligent devices that make traffic-control decisions based on packet attributes and state tables.
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.	State tables enable the firewalling device to "remember" previous communication packet exchanges and make judgments based on this additional information.
Many routers have the ability to perform static packet filtering.	The biggest limitation: 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.

Figure 3.9: Comparison between Static Packet Filtering and Dynamic Packet Filtering

Packet Filter vs Proxy Server

Packet Filter	Proxy Server
Simply looks at two types of information, port number and IP.	Opens every packet and examines the data for content that is not allowed.
A filter reads the Source IP, Destination IP, Source Port, & Destination Port.	More secure but the process of opening the packets can cause certain types of traffic problems.
Based off of these 4 factors makes a decision on whether to allow the connection or deny the packet.	Can be applied to many types of traffic web (HTTP), email (SMTP, POP3, and FTP.
Does not examine the data section of a packet.	Operate at the application level.
Cheap, fast and easy to maintain.	Expensive, slower and much more difficult to maintain.

Figure 3.10: Comparison between Static Packet Filter and Proxy Server

3.3 CONFIGURE FIREWALLS USING MICROSOFT WINDOWS SERVER / OPEN SOURCE SOFTWARE

3.3.1 CREATE A FIREWALL THAT RUNS ON OPEN SOURCE SOFTWARE

- **Open Source Firewall**
  - A firewall is one of the tools used to secure a computer network.
  - A firewall can prevent unwanted access to departmental systems while preventing local systems from attacking systems on other networks.
  - Firewalls require on-going monitoring in order to ensure that they do not unnecessarily restrict access to important computer resources while preventing unwanted access and to ensure that the firewall is operating as expected

- **Creating an open source firewall**
  - The most obvious use for a firewall is to block unwanted traffic from entering or leaving a network.
  - Firewalls can also make specific connections from outside hosts to internal systems, such as a mail or Web server, either behind the firewall or on a trusted or "de-militarized zone" (DMZ) segment.

3.3.2 CREATE A PROXY THAT RUNS ON OPEN SOURCE SOFTWARE

- **Open-source HTTP proxies**

  - A HTTP proxy is a piece of software that acts as an intermediary between HTTP client software and HTTP server software.
  - The proxy receives all requests from the browser, and relays onto the server.
  - it receives all responses from the server, and relays them (possibly modified) to the client.
  - HTTP Proxies can be used for a wide variety of tasks, including filtering, logging, caching.
  - The difficulty sometimes arises that it's not easy to find a proxy which implements exactly the function which is required.

- **Build a Proxy Using Squid**

  - Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more.
  - It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages.
  - Squid has extensive access controls and makes a great server accelerator.
  - It runs on most available operating systems, including Windows and is licensed under the GNU GPL.

3.3.3 CREATE A FIREWALL THAT RUN ON WINDOWS SERVER (ISA SERVER)

- To develop a Firewall for Linux, the lot of information and source code will be finding, all free.
- However, the Firewall for Windows Platforms have a little more difficult not only for find information, find free source code is a task impossible.
- NetDefender is a Free Firewall with source code, which can be downloaded along with firewall executables.

3.3.4 CREATE PROXY THAT RUNS ON WINDOWS SERVER

- CCProxy is one of example of Proxy Server. It is easy-to-use and powerful Internet connection sharing software.
- Supporting broadband, DSL, dial-up, optical fiber, satellite, ISDN and DDN connections, it helps user to build their own proxy server and share Internet access within the LAN efficiently and easily.
- It features powerful account management functions, including Internet access control, bandwidth control, Internet web filtering, content filtering and time control.
- It also provides web caching, online access monitoring, access logging and bandwidth usage statistics functions.

The benefits of Linux based Proxy Server implementation.

- A modern.
- Very stable.
- Multi-user.
- Multitasking environment on your inexpensive PC hardware, at no (or almost no) monetary cost for the software.
- Linux is a rich and powerful platform--don't think of it as a "poor people" operating system.
- Advanced graphical user interface.
- Linux uses a standard, network-transparent X-windowing system with a "window manager" (typically KDE or GNOME).

The benefits of Linux based Proxy Server over Windows.

- It is availability as free version
- It is more secure than windows
- Updates are available faster than windows.

CHAPTER 4
Operating Systems and Security

This chapter discusses the following topics:

- Microsoft Windows Security Approaches
- Open Source Software Security Approaches
- Linux Based Proxy Servers

4.1 MICROSOFT WINDOWS SECURITY APPROACHES

The first step in securing your Windows computer is to determine where you are at risk. By learning as much as you can about computer and network security and assessing how your system is at risk you will greatly improve your odds of staying secure. Obviously, a computer that never accesses the Internet has only one user and is only used for writing letters to friends and family is more secure than a computer that is shared by multiple members of the household, possibly hosting a personal web site, used for downloading files or participating in online chat sessions.

Regardless of the intended use, **the three basic keys** are:

i. Install anti-virus software (and keep it up to date),
ii. Never open files from sources you don't know
iii. Keep your system properly patched against known vulnerabilities.

4.1.1 MINIMUM SYSTEM SERVICES

Minimum System Security Services

- Use passwords on all user accounts
- Setting password to change every 3 months
- Limit the number of unnecessary accounts
- Rename the Administrator Account
- Make sure that Remote Desktop is disabled
- Disable unnecessary services
- Enable EFS (Encrypting File System)
- Use software restriction policies

Configure System Services

You can implement security on *system services in Windows*. This allows you to control who can manage services on a workstation, member server, or domain controller.

- **Windows service** is a long-running executable that performs specific functions.
- Windows services can be configured to start when the OS is booted and run in the background as long as Windows is running, or they can be started manually when required.
- Many appear in the processes list in the Windows Task Manager, most often with a username of SYSTEM, LOCAL SERVICE or NETWORK SERVICE, though not all processes with the SYSTEM username are services.

To Start, Stop, and Disable Services in "Services" Window

Step 1: Open the Control Panel, click on the Administrative Tools icon, click on Services, and go to step 3 below.

OR

Step 2: Open the Start Menu, type services.msc in the search box, press Enter, and go to step 3 below.

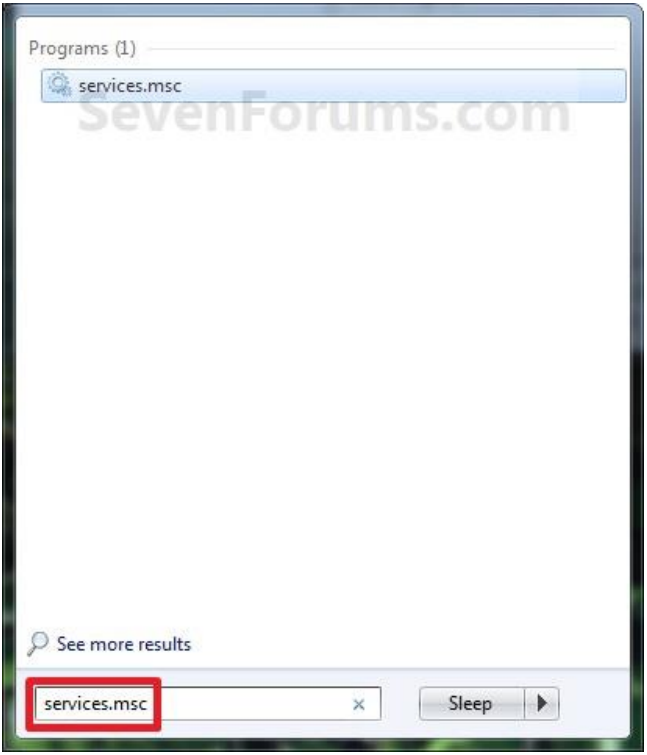


Figure 4.1: search box menu

Step 3: If prompted by UAC, then click on **Yes**.
Step 4: Right click on the service you want to disable or start and click on **Properties**. (See screenshot below)

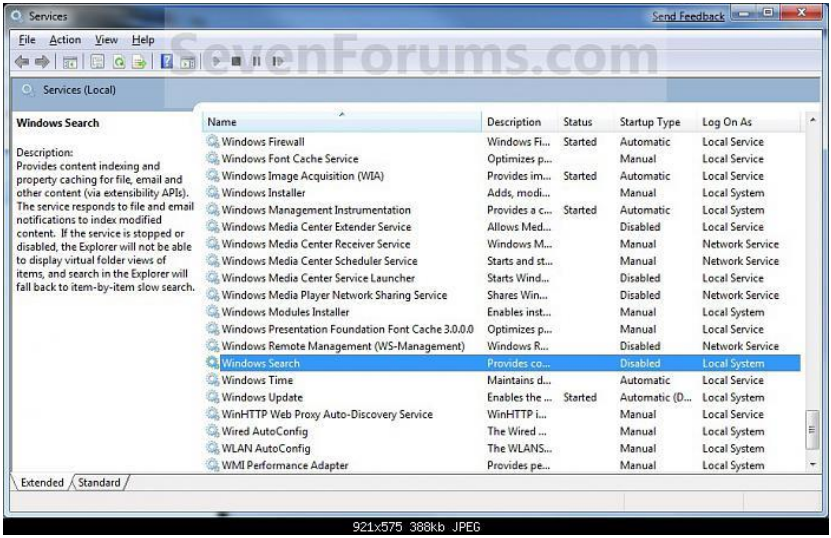


Figure 4.2: Services properties menu

Step 5: To Disable a Service

a) Click on the Stop button and wait a sec for the service to stop.
b) Next to Startup type, click on the drop down menu and select Disable.
c) Click on the Apply button.
d) NOTE: If the service will not stop and gives a error, then you will need to restart the computer to stop it after you set it to Disabled and clicked on OK.
e) Go to step 7

Step 6: To Start a Service

a) Next to Startup type, click on the drop down menu and select *Automatic* or *Manual* and click Apply.
b) Click on the Start button.

NOTE: If the Start option is grayed out and will not start, then you will need to restart the computer to start it after you set it to Automatic and clicked OK.

Step 7: Click on OK.

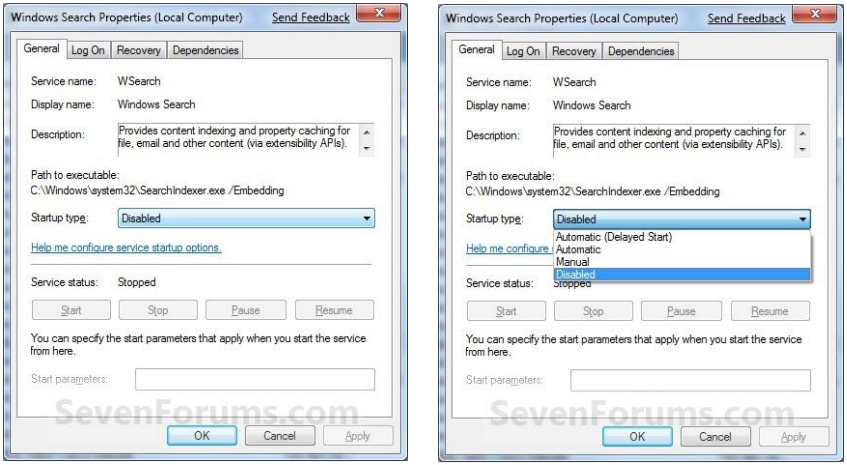


Figure 4.3: Windows Search properties menu

Step 8: Close the Services window.
NOTE: You may need to restart the computer for the changes to the services to take effect.

4.1.2 SYSTEM POLICY

- **Password**
- **Account**
- **Audit**
- **User Right**

a. PASSWORD POLICY

Used as a way of authentication before retrieving any confidential sources.

- Access to the computer will be controlled by the use of system passwords. Individual user accounts will be created and a password assigned to that account
- A Strong password should have the following characteristics:
  i. **English uppercase characters (A through Z).**
  ii. **English lowercase characters (a through z).**
  iii. **Base 10 digits (0 through 9).**
  iv. **Symbols (for example, !, $, #, %).**

- Minimum length of password be to deter dictionary password cracks is 8 characters.
- You should also change your password frequently- at least every 30 days or within 3 months**.**

b. ACCOUNT POLICY

Account policies are defined on computers and contain three subsets:

i. Account Policy

- *It defines how user accounts can interact with the computer or domain.*
- Do not disclose a computer's identity until login is completed successfully.
- Set up the operating system so that the system login screen does not identify the computer system by name or function until after login is Complete.
- Unauthorized personnel do not need to know the identity of machines unless they need to use them.
- Valuable since it may identify valuable targets to break into.

ii. Account Lockout Policy

- Account lockout policy disables a user accounts if an incorrect password is entered a specified number of times over a specified period.
- These policy settings help you to prevent attackers from guessing users passwords.

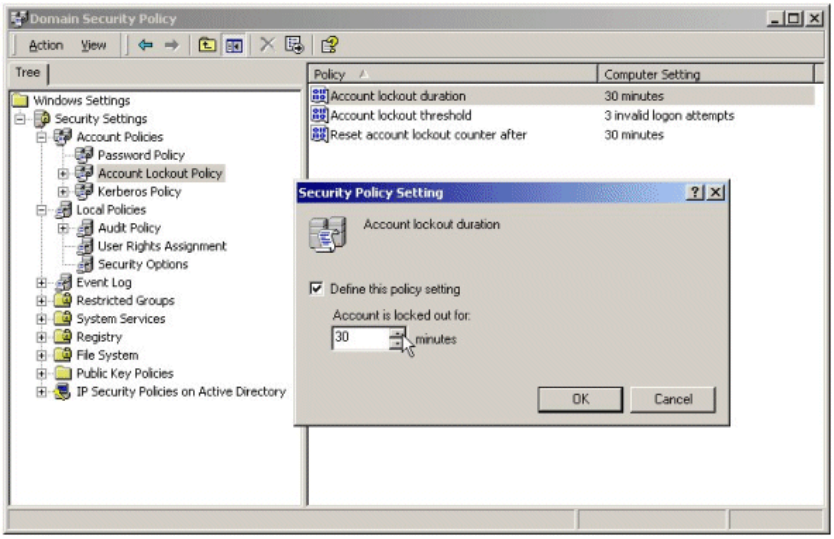


Figure 4.4: Example of Account Lockout Policy Setting

iii. Kerberos Policy

- Kerberos is a secure method for authenticating a request for a service in a computer network.
- Kerberos policy is defined at the domain level and implemented by the domain's Key Distribution Center (KDC).
- Kerberos policies are used for domain user accounts.
- Kerberos policies do not exist in Local Computer Policy.

c. AUDIT POLICY

iv. *An audit log records an entry whenever users perform certain specified actions.*

v. For example, the modification of a file or a policy can trigger an audit entry that shows the action that was performed, the associated user account, and the date and time of the action.

vi. You can audit both successful and failed attempts at actions.

vii. You can configure the Audit policy settings in the following location within the Group Policy Object Editor: ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\Audit Policy.

d. USER RIGHTS POLICY

Allow users to perform tasks on a computer or a domain.

User rights include *logon rights* and *privileges*.

- **Logon rights**
  - Control who is authorized to log on to a computer and how they can log on.
  - Example: The ability to log on to a computer locally.

- **Privileges**
  - Control access to computer and domain resources, and can override permissions that have been set on specific objects.
  - Example: The ability to shut down the computer.

- Both types of user rights are assigned by administrators to individual users or groups as part of the security settings for the computer.
- You can configure the user rights assignment settings in the following location within the Group Policy Object Editor: ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\User Rights Assignment.

Configuring User Rights

User Rights Types:

- Privileges
- Logon Rights

Examples:

- Add workstations to a domain
- Allow log on locally
- Back up files and directories
- Change the system time
- Force shutdown from a remote computer
- Shut down the system

4.1.3 CONFIGURATION OF TCP/IP AND IPSEC FILTERING

All IP Security implementations include a common set of protocols and tools to enable interoperability between different platforms, and provide the following 3 benefits:

- ***Authentication*:** proof that the identity of the host on the other end of the connection is valid and correct.
- ***Integrity Checking*:** assurance that no data sent over the network connection was modified in transit.
- ***Encryption*:** the rendering of network communications is encrypted to anyone who might intercept the transmitted data.

IPSec implementations also include a method of restricting connections to various services, based on their origin and destination. This feature, often present in firewall devices, is known as ***packet filtering***.

Configuring TCP/IPsec Filtering

Step 1: Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
Step 2: Right-click the network connection you want to configure, and then click **Properties**.
Step 3: On the **General** tab (for a local area connection) or the **Networking** tab (for all other connections), click **Internet Protocol (TCP/IP)**, and then click **Properties**.
Step 4: Click **Advanced**.
Step 5: Click **Options**, click **TCP/IP Filtering**, and then click **Properties**.

Do one of the following:

- To enable TCP/IP filtering for all adapters, select the **Enable Filtering Adapters)** check box
- To disable TCP/IP filtering for all adapters, clear the **Enable TCP/IP Filtering (all adapters)** check box.

Step 6: There are three columns with the following labels:

- **TCP Ports**
- **UDP Ports**
- **IP Protocols**

Step 7: If you want to block all UDP or TCP traffic, click **Permit only**, but do not add any port numbers in the **UDP Ports** or **TCP Port** column.

Step 8: You cannot block UDP or TCP traffic by selecting **Permit Only** for **IP Protocols** and excluding IP protocols 6 and 17.

Step 9: Permit All. If you want to permit all packets for TCP or UDP traffic, leave **Permit All** activated.

Step 10: Permit Only. If you want to allow only selected TCP or UDP traffic, click **Permit Only**,

Step 11: Click **Add**, and then type the appropriate port in the **Add Filter** dialog box.

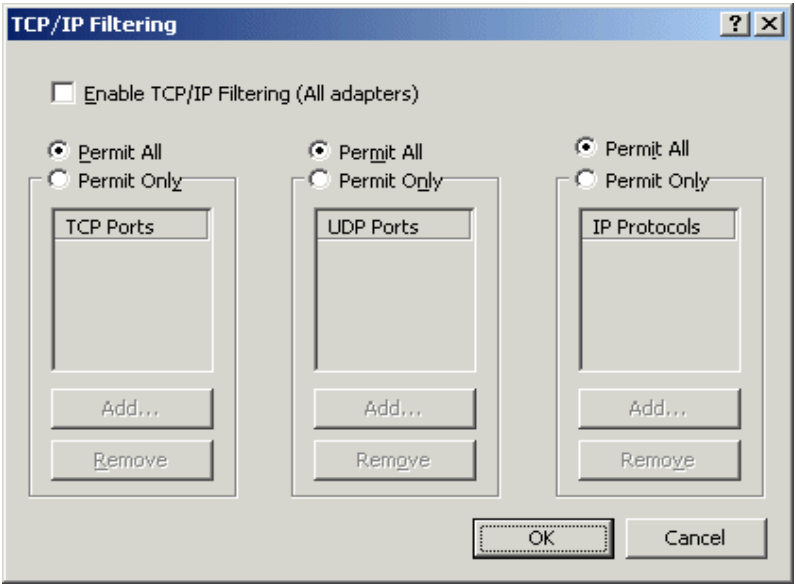
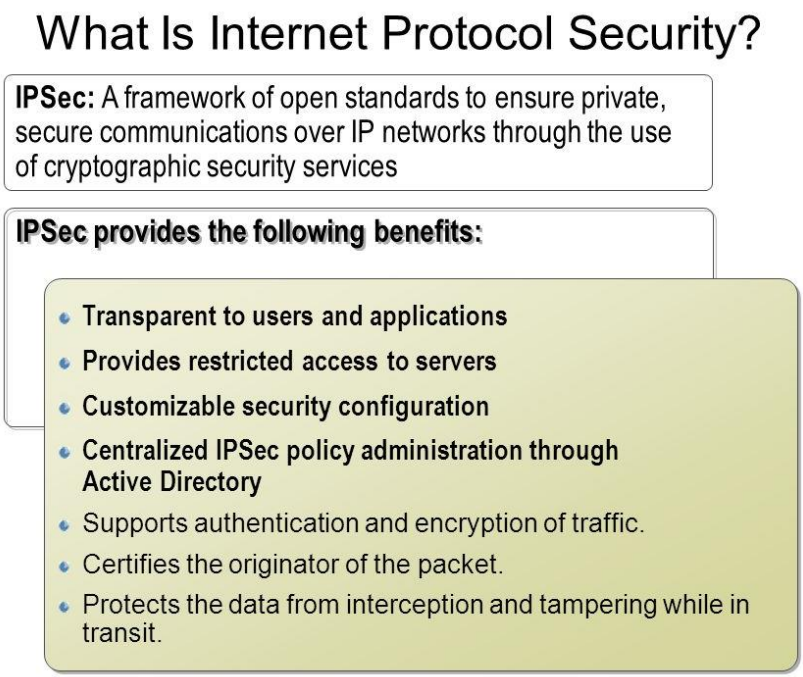


Figure 4.5: TCP/IP Filtering

TCP/IP Configuration Task List

To configure TCP/IP, you must assign an IP address to the network interface. The following list summarizes the tasks for configuring TCP/IP. At a minimum, you must assign IP addresses to network interfaces.

- Assign an IP address to a network interface
- Configure IP addressing options
- Assign an IP address to a TCP service
- Configure routing assistance when IP routing is disabled
- Configure broadcast packet handling
- Configure IP services
- Control access to IP networks
- Configure IP security options
- Optimize lines for Telnet
- Monitor and maintain the TCP/IP network.



Internet Protocol Security (IPSec) Filtering

- It is a rule can be used to help protect Windows 2000-based, Windows XP-based, and Windows Server 2003-based computers from network-based attacks from threats such as viruses and worms.
- Filter a particular protocol and port combination for both inbound and outbound network traffic.
- Can cause network programs to lose data and to stop responding to network requests, including failure to authenticate users.
- To set IPSec filtering must install ***IPSeccmd.exe.*** IPSeccmd.exe is part of Windows XP SP2 Support Tools.

IPSec policies

- IPSec policies determines
  - which IP traffic should be secured and
  - which IP packets should not be secured,
  - what type of security should be applied to the IP packets.
- IPSec polices contain IPSec rules and IPSec rules contain filter lists and filter actions.

4.1.4 SYSTEM UPDATES AND HOTFIXES

i. Updates

- Microsoft regularly issues patches or updates to solve security problems in their software.
- The critical updates are the ones you should be concerned about.
- If these are not applied, it leaves your computer vulnerable to hackers.
- **Service Packs** are ***larger updates*** which upgrade and fix security problems.

ii. Hotfixes

- Hotfixes are **bits of code** in the form of **small files** that patch bugs or problems in software, most notably in Microsoft™ operating systems (OSs).
- As vulnerabilities are discovered, Microsoft releases hotfixes or patches to keep the software as secure as possible.
- A hotfix is code that fixes a bug in a product.
- A *Service Pack (SP)* is a collection of hotfixes bundled together.

How can a system update, patches and hotfixes assist in preventing system attacks?

- Window update features or automatic updates keep the system up to date with recent virus and attack signature. Those reducing the risk of intrusion, prevention from malicious code, prevention from virus and worm attack.

4.1.5 INTERNET INFORMATION SERVICES (IIS) VULNERABILITY

Internet Information Server (IIS)

- IIS is a set of *Internet-based services* for servers created by Microsoft for use with Microsoft Windows.
- With IIS, Microsoft includes a set of programs for building and administering Web sites, a search engine, and support for writing Web-based applications that access databases.

Identify IIS vulnerability

- Microsoft Internet Information Services (IIS) is exposing to multiple vulnerabilities.

Example of vulnerabilities:

- A hacker has posted code on his Milw0rm website that could be used to attack a system running Microsoft Internet Information Services (IIS) server and install unauthorized software on it.

The vulnerabilities of Internet Information Services (IIS).

1. **Default installs of operating system and applications**
   Many users fail to appreciate what an installation program actually installs on their machine.

2. **Accounts with weak or nonexistent passwords**
   IIS uses several built-in or default accounts. Attackers commonly look for these accounts. They should be identified and changed.

3. **Large number of open ports**
   Every visitor, good or bad, connects to a site and system via an open port. By default, Windows and IIS ship with more ports open than are required to function correctly.

4. **Windows License Logging Service overflows**
   By sending a specially formatted message to a Web server running the License Logging Service, an attacker can exploit an unchecked buffer.

5. **Microsoft Server Message Block (SMB) vulnerability**
   The Server Message Block Protocol is used by Windows to share files and printers and to communicate between computers.

6. **ISAPI Extension Buffer Overflows**
   Several Internet Server Application Program Interface (ISAPI) extensions are automatically installed with IIS. ISAPI extensions, which are actually dynamic link libraries, extend the capabilities of an IIS server.

4.1.6 CONFIGURE SECURITY ENHANCEMENT FOR IIS

- Block external access at the network boundary, unless service is required by external parties.

- Disallow anonymous access to services. Permit access for trusted individuals only.
  - Do not allow unknown or untrusted individuals to upload files onto critical or sensitive systems

- Do not follow links provided by unknown or untrusted sources.

- Modify default configuration files, to disable any unwanted behavior.
  - Delete any sample files and directories that may be installed by default.

4.1.7 MICROSOFT SECURITY SERVER (ISA Server)

Firewalling & Security product based on Microsoft Windows primarily designed to securely publish web servers and other server systems.

ISA Server provides the two **basic services**

i. enterprise firewall
ii. Web proxy/cache server.

The Web cache stores and serves all regularly accessed Web content in order to reduce network traffic and provide faster access to frequently-accessed Web pages.

ISA Server also schedules download of Web page updates for non-peak times.

ISA Server comes in two editions.

i. **Standard Edition** is a stand-alone server that supports up to four processors.

ii. **Enterprise Edition** is for large-scale deployments, server array support, multi-level policy, and computers with more than four processors. Licenses are based on the number of processors.

Features of Microsoft Security Server (ISA)

- **Network connectivity**
  Network Address Translation (NAT) and Port Address Translation (PAT), NAT is a firewall functionality with a small cost.
- **Proxy connectivity**
  It has HTTP proxy, FTP proxy, Direct Mapping and POP 3 proxy.
- **Proxy security**
  Proxies are very secure because they offer a variety of security options.

4.1.8 CONFIGURING A MICROSOFT SECURITY SERVER (ISA)

A Windows 2000 Server with a full implementation of Active Directory is the minimum on which it is possible to install Microsoft ISA Server. Before installing ISA Server, one must configure Active Directory (adding required classes and selecting object properties).

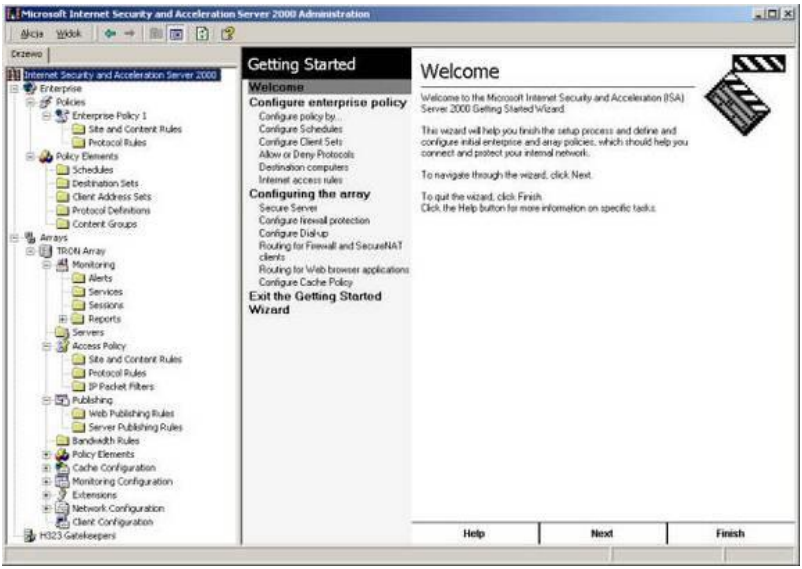


Figure 4.6: Microsoft ISA Server Administrator utility and Getting Started Wizard

To manage this utility, use the Microsoft Management Console (MMC) feature. The left dialog box contains all options that are necessary for setup whilst the right box provides the settings available for such options.

4.2 MANAGE OPEN SOURCE SOFTWARE SECURITY APPROACHES

Definition of Linux

Linux (often pronounced LIH-nuhks with a short "i") is a Unix-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to Microsoft Windows.

4.2.1 PERFORM OPEN SOURCE OPERATING SYSTEM UPDATES

- There are several methods remote attackers can use to break into your machine. Usually they are exploiting problems with existing programs. The open source community always quickly spots this exploitation and release a fix.
- Linux system may contain many security vulnerabilities and software bugs when it is first released.
- Vendors, such as Red Hat, provide updates to the operating system to fix these vulnerabilities and bugs.
- Linux which is known as a free open source operating system.
- Linux is constantly being modified by people around the world.
- It is usually very easy to update.

4.2.2 IDENTIFY AND DISABLE UNNECESSARY SERVICES AND PORTS

Manually Disabling Unnecessary Services and Ports

- To harden a server, you must first disable any unnecessary services and ports.
- This process involves removing any unnecessary services and locking down unnecessary Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports.
- Linux, by nature, is more secure than most operating systems.
- However, an administrator can reduce the amount of risk by removing unnecessary services.

4.2.3 SYSTEM HARDENING WITH BASTILLE (LINUX BASTION HOSTS)

- Hardening is a process of modifying a system to make it highly secure.
- Making Linux system more resistant to attacks, including securing the boot process and local file systems.
- For hardening activities to be most successful should :
    - Do hardening activities before the system is connected to the network to avoid attacks.
    - Base configuration on the *least-privilege model*: users should be allowed only the minimum set of access rights they need.

Using the Bastille Hardening Script

- Bastille's focuses on letting the system's user/administrator choose exactly how to harden the operating system on Linux System.
- In its default hardening mode, it interactively asks the user questions, explains the topics of those questions, and builds a policy based on the user's answers.
- It then applies the policy to the system.
- Bastille is written in Pearl Script and work with Red Hat.

Bastion host

- A general-purpose computer used to control access between the internal (private) network (intranet) and the Internet (or any other untrusted network).
- Bastille is an open source program that facilitates the hardening of a Linux system.
- **Bastille** is a software tool that **eases the process of hardening a Linux system**.

- The best descriptions for Bastille are:
  - Written in Perl script
  - Non-interactive program
  - Work with Windows 7
  - Work with Red Hat

4.2.4 MAINTAIN CONTROLLING AND AUDITING OF ROOT ACCESS WITH SUDO

- Superuser Do (sudo) is an open source security tool that allows an administrator to give specific users or groups the ability to run certain commands as root or as another user.
- The program can also log commands and arguments entered by specified system users.
- Because sudo logs all commands run as root (or specified otherwise), many administrators use it instead of using the root shell.
- This allows them to log their own commands for troubleshooting and additional security.

4.2.5 MANAGE SYSTEM LOG FILES USING LOGGING ENHANCERS

- Another aspect of system security is managing your log files. By default, Linux offer modest logging so that administrators can see who and what has accessed their system.
- Linux offers commands that allow administrators to access useful log files. Two commands of interest are *last* and *lastlog*.

The last command

- Displays data such as who is logged on to the system, who recently logged on, and when the system has rebooted.

The lastlog command

- Displays the users and services that have accounts on your machine.
- It lists the last time each account logged in to the system, or if the account has ever logged in.

Using Logging Enhancers

- Logging enhancers are tools that simplify logging by allowing logging information to be filtered and often displaying logs in simplified formats.
- Viewing text-based files with hundreds or thousands of entries can be burdensome, especially if you are only looking for one specific error entry.
- Logging enhancers can make logging a much more user-friendly experience, and greatly expand and customize the information you need to log.

The purpose of managing System Log Files using Log Enhancer

- System log file analysis is one of the most important tasks when analysing the system. In fact, looking at the system log files should be the first thing to do when maintaning or troubleshooting a system

By Using LINUX like operating system. There have 2 way (command) how to get the system log files.

```
# tail –f/var/log/messages
# less /var/log/messages
# more –f/var/log/messages
# vi/var/log/messages
```

4.3 LINUX BASED PROXY SERVERS

- Proxy servers are **software applications** that run on your firewall machine in order to provide indirect Internet access to your network
- The proxy server is used **to allow Internet access from inside** the protected network through either the single or dual-homed host firewall.
- A **single-homed host** is a machine with one network card. This configuration relies on the Internet router to block all packets to any machine except the firewall.
- A **dual-homed host** is a machine with two network cards that has routing capabilities disabled.

4.3.1 BENEFITS OF LINUX BASED PROXY SERVER IMPLEMENTATION

1. Share Internet connection within the Intranet.
2. Implement Internet access control such as to prevent certain access to forbidden sites.
3. To speed up Internet surfing.
4. To filter inbound connections or messages.
5. To limit bandwidth and schedule online time for internal end users.
6. allowing real network addresses to be hidden.
7. to improve the performance and security of communications.

Linux also can give you:

- A modern, very stable, multi-user, multitasking environment
- Available as free version
- More secure than Windows
- Updates are available faster than Windows

4.3.2 DIFFERENTIATE BETWEEN A PACKET FILTER AND A PROXY SERVER

(a) PACKET FILTERS

- **Packet filters:** security method that filter by IP address; not adequate security for a network.
- Blocks or allows transmission of packets on the basic of port, IP address and protocol.
- Cheap, fast and easy to maintain
- Does not examine data section of a packet

(b) PROXY SERVER

- In computer networks, a proxy server is a server which services the requests of its clients by forwarding requests to other servers.
- It effectively hides the true network addresses
- Expensive, slower and difficult to maintain
- http proxy server will make decision to accept/deny from client

4.3.3 IMPLEMENT A LINUX BASED PROXY SERVER (E.G: SQUID WEB PROXY CACHE SERVER)

SQUID

- Squid is a caching proxy server that can help
  - reduce internet bandwidth usage
  - improving response time of loading a website by caching and re-using frequently opened web page.
- Squid reduce the bandwidth usage and accelerate the website loading by caching static website objects such as images, flash objects and text files, with some modification Squid can cache larger files such as PDF, MP3, executable, flash videos, etc.
- A Squid proxy server is generally installed on a separate server than the Web server with the original files.
- Squid works by tracking object use over the network.
- Squid will initially act as an intermediary, simply passing the client's request on to the server and saving a copy of the requested object.
- If the same client or multiple clients request the same object before it expires from Squid's cache, Squid can immediately serve it.

- That can accelerating the download and saving bandwidth
- Internet Service Providers (ISPs) have used Squid proxy servers since the early 1990s to provide faster download speeds and reduce latency, especially for delivering rich media and streaming video.
- Squid is provided as free, open source software
- **Features:**
    - Cache
    - ACL(Access Control List)

a. Install the Proxy Cache Server

The step to install squid on windows 7:

Step 1:

Extract squid 7 and put it on example "c:\squid".

Step 2:

Get squid.conf sample and save it as "squid.conf" put this files on example "c:\squid\etc"

Partition before you install squid:

Step 3:

Now the important step! we have to disable UAC (User Account Control) if we didn't disable this we will got problem on installing squid as windows service. Mostly a lot of people try to install squid on windows 7 has problem on this step.

Control Panel -> System and Security -> Change User Account Control Settings

Slide the bar into "Never Notify" You need to restart your computer after doing this step.

Step 4:

Open command prompt. Then install squid service by typing "squid -i" in your command prompt.

Step 5:

Build your squid cache by typing "squid -z" You will see this message "Creating Swap Directories" in your command prompt, just waiting until it finished.

Step 6:

After squid service installed and squid cache finish building now you have to start this service.

Control Panel -> Administrative Tools -> Services

Look for service with name "squid" the start this service (you can also configure it too to auto start each time your computer on)

Step 7:

Make sure squid process is running on your computer background. You can see this on task manager in services tab.

Step 8:

It's might important and secure to re-enable back again User Account Control Settings.

Step 9:

You just finished installing squid, congratulation

Now you have to configure your web browser to use this squid. Open your web browser and looking for (mostly network) then writes your squid IP and squid Port. Example my squid IP server is 127.0.0.1 and port 3128.

b. Configure the Proxy Cache Server

With some minor modification to the **squid.conf** file we have defined above to run in **httpd- accelerator** mode, we can run Squid as a proxy-caching server. With a proxy cache server, all users in your corporate network use Squid to access the Internet. With this configuration, you can have complete control, and apply special policies on what can be viewed, accessed, and downloaded. You can also control bandwidth usage, connection time, and so on. A proxy cache server can be configured to run as stand-alone server for your corporation, or to use and share caches hierarchically with other proxy servers around the Internet.

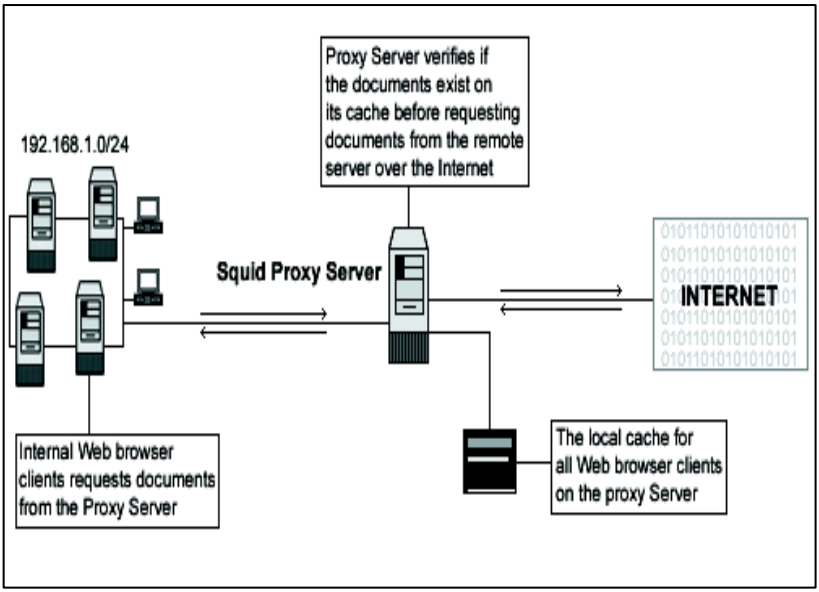


Figure 4.7: Proxy Cache Server

With the first example below we show you how to configure Squid as a stand-alone server, and then speak a little bit about a cache hierarchy configuration, where two or more proxy-cache servers cooperate by serving documents to each other. Edit the squid.conf file, **vi** /etc/squid/squid.conf and add/change the following options for proxy cache that run as a stand-alone server:

```
http_port 8080
icp_port 0
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 16 MB
cache_dir ufs /cache 200 16 256
redirect_rewrites_host_header off
replacement_policy GDSF
acl localnet src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
acl Safe_ports port 80 443 210 119 70 21 1025-65535
acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0
http_access allow localnet
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
http_access deny all
cache_mgr admin@openna.com
cache_effective_user squid
cache_effective_group squid
log_icp_queries off
cachemgr_passwd my-secret-pass all
buffered_logs on
```

The big difference with the httpd-accellerator mode configuration is the use of access control lists (ACL). This feature allows you to restrict access based on source IP address (src), destination IP address (dst), source domain, destination domain, time, and so on. Many types exist with this feature, and you should consult the Squid.conf file for a complete list. The four most used types are as follows:

```
acl name type data
        acl some-name src a.b.c.d/e.f.g.h
    # ACL restrict access based on source IP address
        acl some-name dst a.b.c.d/e.f.g.h
    # ACL restrict access based on destination IP address
        acl some-name srcdomain foo.com
    # ACL restrict access based on source domain
        acl some-name dstdomain foo.com
    # ACL restrict access based on destination domain
```

As an example, to restrict access to your Squid proxy server to only your internal clients, and to a specific range of designated ports, something like the following will make the job:

```
acl localnet src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
acl Safe_ports port 80 443 210 119 70 21 1025-65535
acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0
http_access allow localnet
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
http_access deny all
```

This acl configuration will allow all internal clients from the private class C 192.168.1.0 to access the proxy server; it's also recommended that you allow the localhost IP (a special IP address used by your own server) to access the proxy.
After we choose a range of ports (80=http, 443=https, 210=wais, 119=nntp, 70=gopher, and 21=ftp) which our internal clients can use to access the Internet, we deny the **CONNECT** method to prevent outside people from trying to connect to the proxy server, and finally, we deny all source IP address and ports on the proxy server.

4.3.4 TEST AND VERIFY THE SERVER

The proxy and cache services manage the interconnection between a companies's internal network and the Internet. They accelerate and control access to hypertext transfer protocol (HTTP), secure socket layer (SSL), and file transfer protocol (FTP)-based resources (internal or external). This section describes the processes involved in testing the proxy and cache services and provides details of the test cases performed in the WSSRA configuration. The test results are also presented in the "Appendixes" section in this guide.

Test Lab Test Methodology

To test proxy and cache service, the proxy servers were built according to the build guidance. They were then verified through a set of build and verification test cases (BVTs). Once service build was verified, the availability of the proxy servers was tested by verifying redundancy of the servers and network connectivity. To ensure that the proxy servers are highly secure, they were tested for possible security loopholes.

Test Lab Functional Tests

The objective of the functional tests for the proxy and cache service was to verify the functionality of the proxy/cache service components and their integration with other services in the WSSRA test environment.

Auditing and Build Verification Testing

Audits and BVTs were performed on both the internal and external proxy servers to validate the build of the service and verify the basic functionality of the service. The following proxy cache audits and BVTs were executed to validate the configuration.

- Hardware configuration (processor, machine type, memory, and number of disk drives).
- Logical disk partition of the disk drives.
- Network adapters on all the proxy servers were verified to be configured in fault tolerant mode with their speed set to 100Mbps/Full Duplex.
- TCP/IP configurations were verified on the teamed network adapters against the *ConfigurationMatrix.xls* file

Verify

This section provides information you can use to confirm your configuration functions properly.

Since a real cache server is not used for the proxy cache test, append **:8080** to the URL. For example,

http://10.1.1.100/1.html:8080

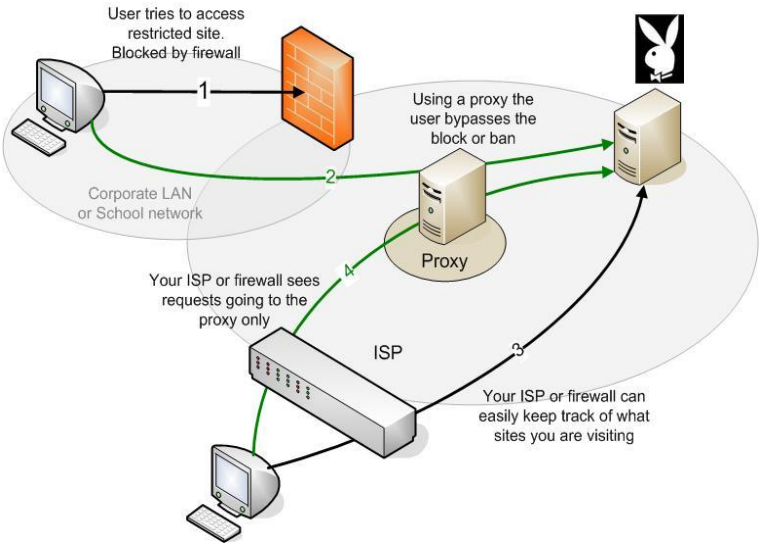


Figure 4.8: How proxy works

CHAPTER 5
Authentication and Encryption Technology

This chapter discusses the following topics:

- Authentication and Encryption Technology
- Virtual Private Network (VPN) Fundamentals

5.1 AUTHENTICATION AND ENCRYPTION TECHNOLOGY

- Authentication and encryption are two interrelated technologies that help to insure that your data remains secure.
- ***Authentication*** is the process of proving one's identity to someone else.
- ***Encryption*** helps to insure that the information within a session is not compromised.

5.1.1 THE PURPOSE OF AUTHENTICATION

- Authentication services are used to determine infusers are who they claim to be and are allowed to access what they are trying to access.
- Purpose is
    - to restrict access to network device.
    - to prove someone authorization based on unique username and password.

5.1.2 VARIOUS AUTHENTICATION APPLICATION TECHNOLOGIES

The Important Of Authentication

Secure Access

- Authentication's importance can be seen when looking at how the Internet has effected access security.
- When giving access to internal assets and systems, organizations now need to look at how users are authenticated with a new perspective such as using **Smart Card.**

Transactional vs. Continuous Authentication

- **Transactional authentication** used by **online banking** services as a form of *single use* **one-time passwords** to authorize financial transactions.

- **Continuous Authentication -** Right from login, through logout, you are protected. The **software intelligently** analyzes your keystroke and mouse movement patterns to ensure that you are who you say you are.
- Eg: BioTracker

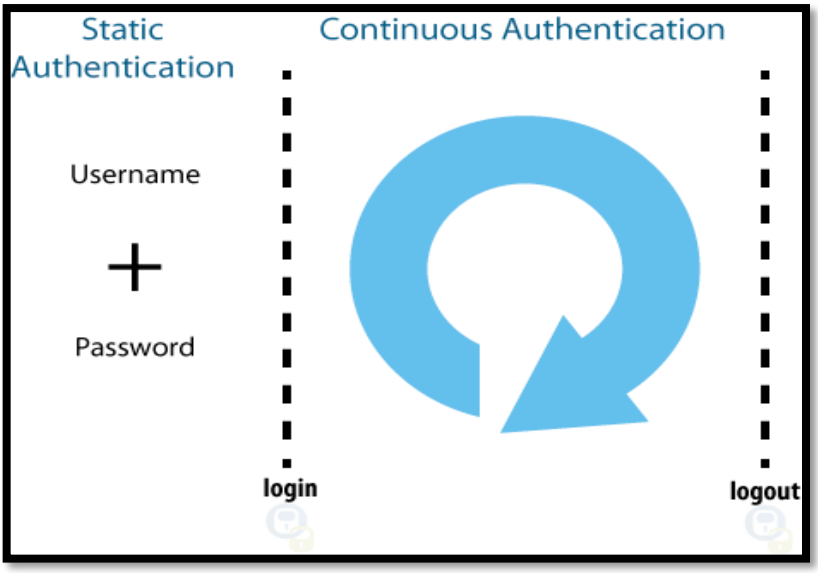


Figure 5.1: Continuous Authentication

Single-Factor Authentication

- The traditional form of single-factor authentication is the use of a standard **user ID and password** pair.
- While there is nothing inherently wrong with IDs and passwords, they do not provide very strong security when used as the only form of authentication.
- Passwords are often re-used and easy to decipher, in which case they can be easily stolen and reused by attackers.

Multi-Factor Authentication

- Multifactor authentication (MFA) is a security system that requires **more than one form of authentication** to verify the legitimacy of a transaction.

MFA combines two or more independent credentials:

i. what the user has (security token)

ii. what the user knows (password),

iii. what the user is (biometric verification).

5.1.3 VARIOUS ATTACKS THAT CAN BE LAUNCHED IF AUTHENTICATION IS NOT IMPLEMENTED.

- **Individual attacks** - caused in damages to individual organizations.
- Organizations suffered - the greatest **financial loss and damage**, when attackers used stolen IDs and passwords.
- **Most crimes -** could have been prevented if the identity of the computers connecting were checked in addition to user IDs and passwords.

- Losses from stolen IDs and passwords - **far exceeded damages** from worms, viruses, and other attack methods not utilizing logon accounts
- **Trojans** - software or program that has a hidden agenda, most Trojan creates loopholes or backdoor program on user systems.
- **Bankers** - that trying to steal username and password from victims.
- **Phishing** - process of attempting to acquire sensitive information such as user names, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
    - Typically, the phisher sends an e-mail that appears to come from a legitimate business such as a bank, or credit card company that requesting "verification" of information.
- **Man in the middle** - middleman changing info that travels from original sender to original receiver. So that both original sender and original receiver think that they have secure communication.
- **Social engineering** - the art of manipulating people into performing actions or reveal confidential information.
- **DOS/DDOS** - attempt to make a computer or **network resource unavailable** to its intended users.
- **Wiretapping** - attack that intercepts and accesses information contained in a data flow in a communication system.

5.1.4 CRYPTOGRAPHIC TERMINOLOGIES:

a) Encryption

- A process of converting a data into a form that cannot be easily understood by unauthorized people
- The technique of converting data to a format that is meaningless to anyone who does not have the proper key.
- A good method of protecting data transmitted over the Internet.

Used Of Encryption

- Encryption can be used to protect data such as files on storage devices.
- Used to protect data in transit, for example data being transferred via networks.
    - Even if the message transferred via network is being intercepted by the intruders, it would be unusable.

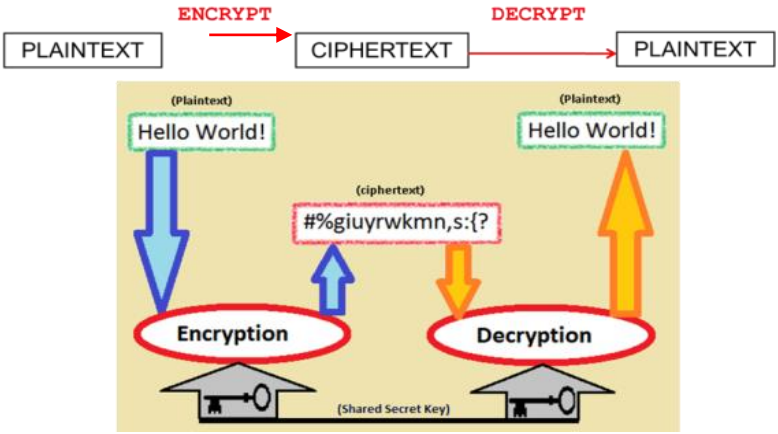


Figure 5.2: Encryption Algorithm

b) Ciphertext

- The encrypted file or message that could not been read directly.

c) Decryption

- Process to convert the ciphertext into the plaintext. Decryption requires a secret key or password.

d) Cryptanalysis

- The art of deciphering encrypted communications without knowing the proper keys.
- Cryptanalysis refers to the study of ciphers, ciphertext, or cryptosystems with a view to finding weaknesses in them that will permit retrieval of the plaintext from the ciphertext, without necessarily knowing the key or the algorithm.
- This is known **breaking the secret codes**.

5.1.5 HOW ENCRYPTION CAN PROTECT DATA FROM SNOOPING AND BEING ALTERED

Data interception occurs when an unauthorized person is able to seize a piece of information that is being sent from person A to person B before B receives that information.

Example

I wanted to send Ali a message that reads, "HELLO." The problem is that a hacker might intercept my message before Ali receives the message and be able to read what I am trying to communicate. Now, in a message as simple as "HELLO," this interception may seem rather harmless. But suppose that instead of just sending Ali a "HELLO" message, I was sending Ali my credit card number for an online purchase of books. When we think about the possibility of credit card numbers getting into the wrong hands, we see the potential seriousness of data interception.

How can I protect my messages from being intercepted by unauthorized people?

The process of translating data into a code that makes it more difficult for unauthorized users to read is called **ENCRYPTION**, or **CRYPTOGRAPHY**.

5.1.6 DIFFERENTIATE BETWEEN THE TWO CLASSES OF KEY-BASED ENCRYPTION ALGORITHMS

Encryption Overview

Encryption refers to the translation of data into an encoded format for the purpose of achieving data security. Reading an encrypted file requires access to a secret key, which enables the decryption of this file. The two primary encryption methods in existence today are:

a) Symmetric (secret-key)
b) Asymmetric (public-key)

a) Symmetric encryption,

It also known as secret key cryptography, which requires the sender and receiver of a message to share the use of a single, common key for encryption and decryption.

- Based on **single key.**
- **Private Key** or **secret key.**
- Algorithm is being shared between the parties who are exchanging encrypted information.
- The **same key** both encrypts and decrypts messages.
    - In this case everyone wanting to read encrypted data must share the same key

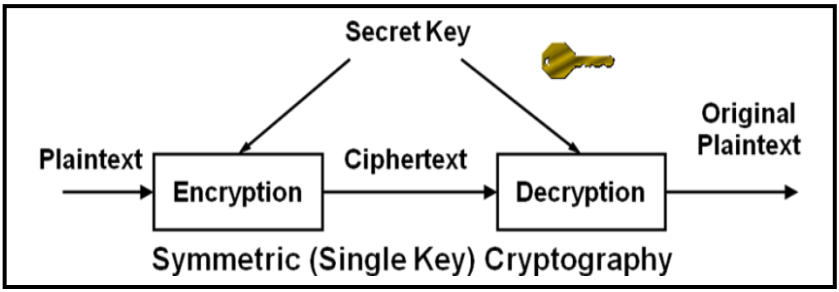


Figure 5.3: Symmetric Encryption

EXAMPLE SYMMETRIC KEY

- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- CAST
- Rivest Cipher #4 (RC4)
- Serpent

b) Asymmetric encryption

- Public cryptography.
- **Uses two keys** – Public and Private.

A **public key to encrypt** messages and a **private key to decrypt them.**

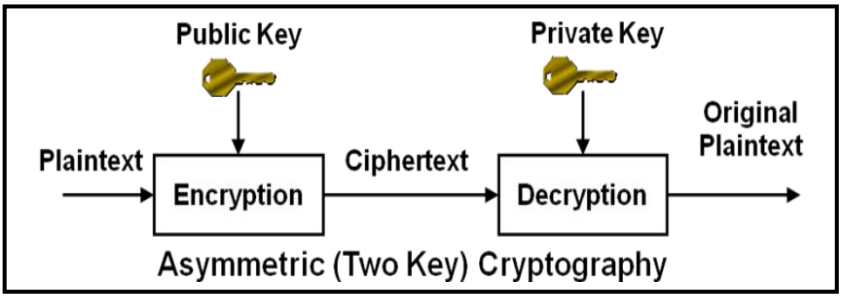


Figure 5.4: Asymmetric Encryption

EXAMPLE OF ASYMMETRIC KEY

- DIFFIE-HELMAN
- RIVEST, SHAMIR, ADELMAN (RSA)
- MD4, MD5
- ELGAMAL

Summarise

Symmetric key

- Both parties share the same key for encryption and decryption.
- Key needs to be kept secret.
- Ex; DES, Triple-DES (3DES), IDEA, CAST5, BLOWFISH, TWOFISH.
- Not consuming too much computing power.

Asymmetric key

- Use pairs of keys.
- One is used for encryption and the other one for decryption.
- Decryption key is typically kept secret, therefore called ``private key'' or ``secret key'', while the encryption key is spread to all who might want to send encrypted messages, therefore called ``public key''.
- Ex; RSA, DSA, ELGAMAL
- Are much slower than symmetric key encryption

5.1.7 METHOD OF ENCRYPTION

a) Caesar Chiper
b) Substitution Chiper
c) Vigenere Tableu
d) Grid Encryption

a), b) → Monoalphabetic Ciphers
c), d) → Polyalphabetic Ciphers

a) Caesar Cipher

- One of the simplest and most widely known encryption techniques.
- It replaced by a letter some fixed number of positions down the alphabet.
- The method is named after Julius Caesar, who used it to communicate with his generals.

Example

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions.

For instance, here is a Caesar cipher using a left rotation of three places (the shift parameter, here 3, is used as the key):

Plain: ABCDEFGHI J KLMNOPQRSTUVWXYZ
Cipher: DEFGH I JKLMNOPQRSTUVWXYZABC

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.

Deciphering is done in reverse.

Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
Plaintext: the quick brown fox jumps over the lazy dog

EXAMPLE

- For a key K=3,
  plaintext letter: ABCDEF...UVWXYZ
  ciphtertext letter: DEF...UVWXYZABC

- Hence
  TREATY IMPOSSIBLE
  is translated into
  WUHDWB LPSRVVLEOH

b) Substitution Cipher

Changes characters in the plaintext to produce the ciphertext.

Examples

- monoalphabetic ciphers
- polyalphabetic ciphers

Example

Keys for the simple substitution cipher usually consist of 26 letters (compared to the caeser cipher's single number). An example key is: **"zebras"**

plain alphabet : abcdefghijklmnopqrstuvwxyz
cipher alphabet: ZEBRAScdfgijklmnopqtuvwxy

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	E	B	R	A	S	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	T	U	V	W	X	Y

An example encryption using the above key:

plaintext : polytechnic
ciphertext: MLIXQABDKFB

Another Classical Substitution Ciphers

- **Keyword mixed**

Example:
keyword= AHMAD *becomes* AHMD

K= 3

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	Y	Z	A	H	M	D	B	C	E	F	G	I	J	K	L	N	O	P	Q	R	S	T	U	V	W

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
X Y Z A H M D B C E F G I J K L N O P Q R S T U V W

Plaintext = BE OR NOT TO BE
Ciphertext = YH KO JKQ QK YH

c) Vigenere Tableu

- The Vigenère cipher chooses a sequence of keys, represented by a string.
- Key letters are applied to successive plaintext.
- When the end of the key sequence is reached, the key starts over again.
- The length of the key is called the period of the cipher.

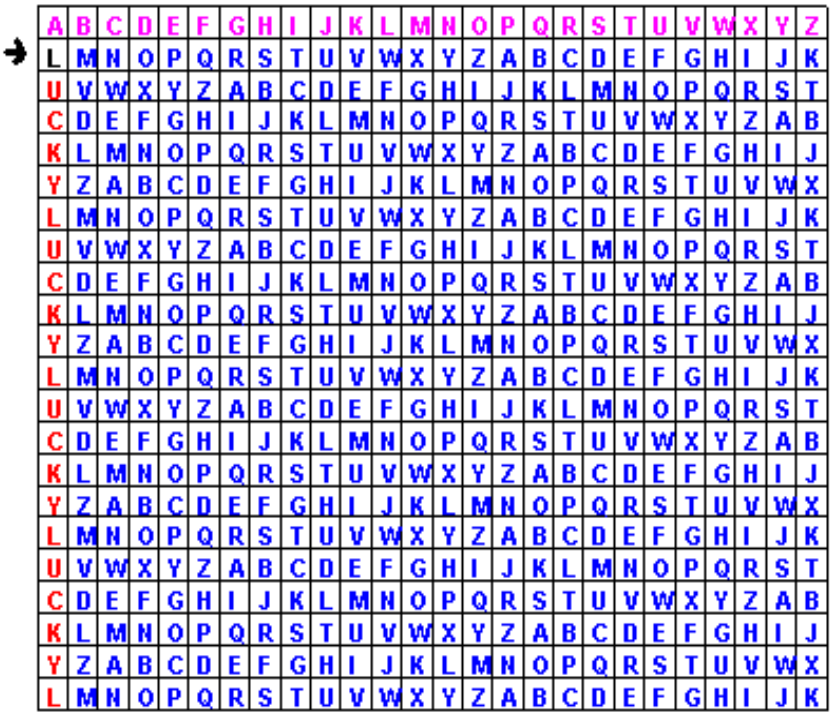
Example 1:

Plaintext: C R Y P T O G R A P H Y

Key: L U C K Y L U C K Y L U

Ciphertext: N L A Z R Z A T K N S S

CODE TABLE



Example 2:

For the message **COMPUTING GIVES INSIGHT** and keyword LUCKY we proceed by repeating the keyword as many times as needed above the message, as follows.

L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
=>	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
=>	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L	U	C	K	Y	L			
C	O	M	P	U	T	I	N	G	G	I	V	E	S	I	N	S	I	G	H	T			<==MESSAGE
N	I	O	Z	S	E	C	P	Q	E	T	P	G	C	G	Y	M	K	Q	F	E			<==Encoded Message

d) Grid Encryption

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

By using the Grid encryption method, the following plaintext can be encrypt as a

Information Technology Department

42 33 12 43 24 23 11 44 42 43 33
44 51 31 32 33 43 13 43 22 45
41 51 53 11 24 44 23 51 33 44

5.2 VIRTUAL PRIVATE NETWORK (VPN)

A virtual private network (VPN) is a private network that uses a public network (the Internet) to connect users.

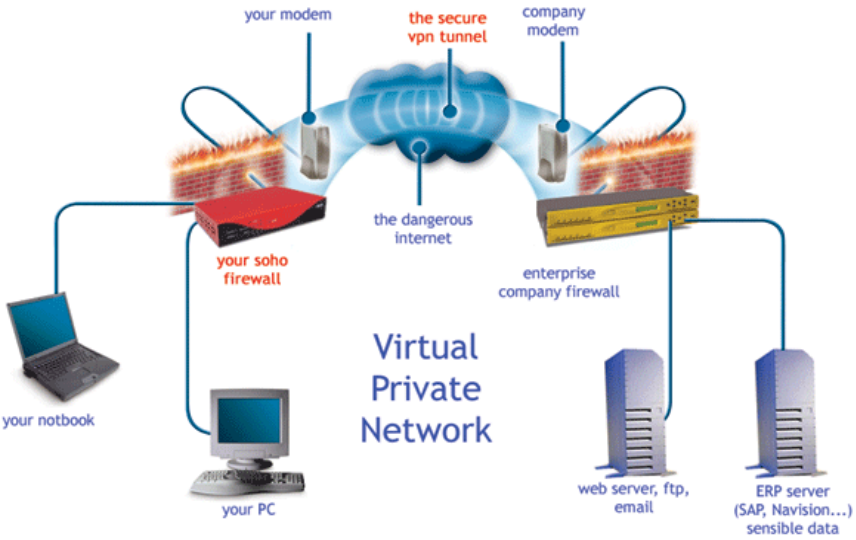


Figure 5.5: Virtual Private Network (VPN)

Typical uses of a VPN

a) The mobile employee who uses hotel Internet facilities to establish a VPN tunnel and connects to servers at the office.

b) To establish a secure link from a regional office to a corporate HQ.

The key components of VPN

- VPN client
- VPN protocol
- Authentication system
- Encryption algorithms

5.2.1 VPN SESSION

VPN session is an *authenticated and encrypted communication* channel across some form of public network, such as Internet.

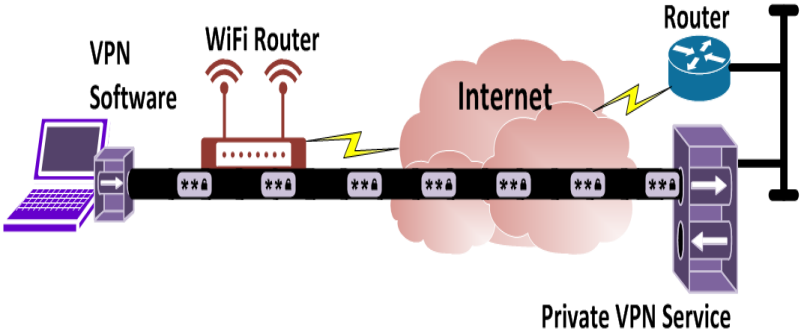


Figure 5.6: VPN Session

The **virtual private network** (**VPN**) technology included in Windows Server 2003 helps enable cost-effective, secure remote access to private networks.

VPN allows administrators to take advantage of the Internet to help provide the functionality and security of private WAN connections at a lower cost.

Advantages of a VPN are

- encrypted security – strong authentication
- broadband network support,
- ease of maintenance,
- simplified network topology and
- the ability to provide support to individual users or branch offices.

5.2.2 TYPES OF VPN

VPN can be classifying by the arrangement of entities that have a data encryption/decryption function and an authentication function. There have three categories of VPN:

a) Intranet VPNs
b) Remote Access VPNs
c) Extranet VPNs

a) Intranet VPNs

- Provide a link over a shared infrastructure.
- They connect:
  - Corporate headquarters
  - Remote Offices
  - Branch Offices
- Also used for e-mail, sharing files and sharing applications.

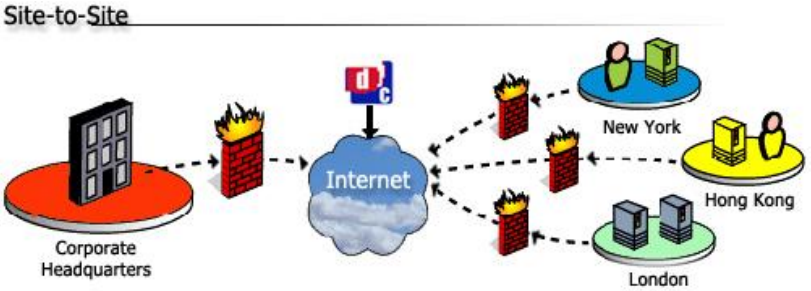


Figure 5.7: Intranet VPNs Infrastructures

- **The benefits of an intranet VPN are as follows:**
  - Reduced WAN bandwidth costs
  - Connect new sites easily
  - Increased network uptime by enabling WAN link redundancy across service providers.

b) Remote access VPNs

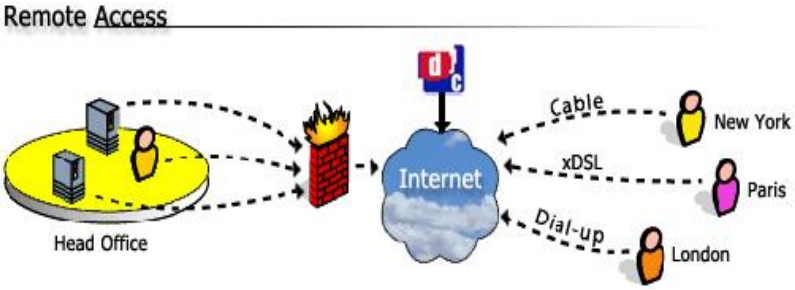


Figure 5.8: Remote Access VPNs Infrastructures

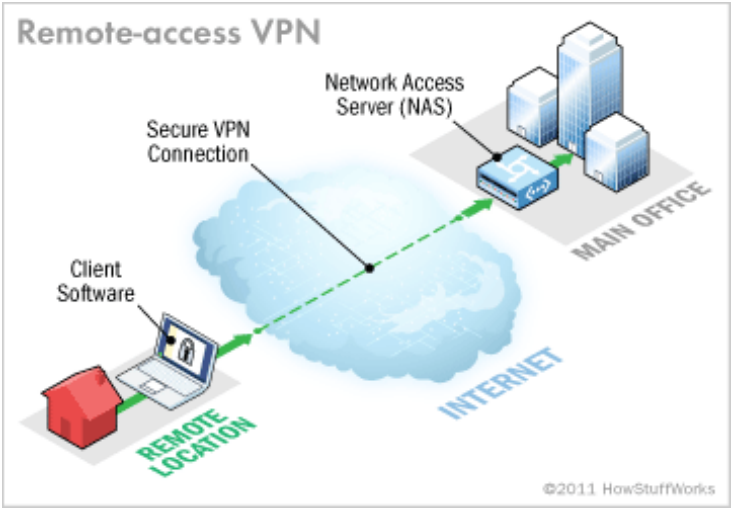


Figure 5.9: Remote-Access VPN

- A **remote-access VPN** allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers.

c) Extranet VPNs

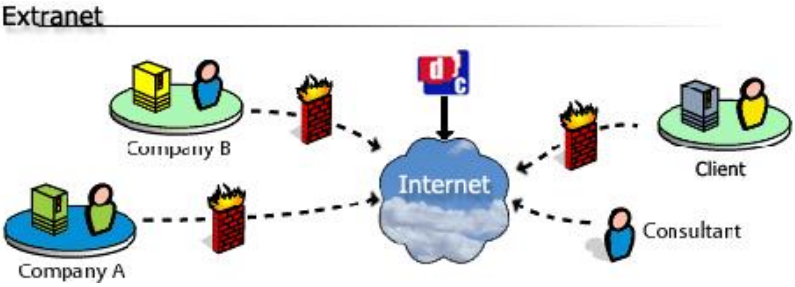


Figure 5.10: Extranet VPNs Infrastructures

- Extranet VPNs provide a link to a corporate Intranet over a shared infrastructure.
- They connect:
    - Customers
    - Suppliers
    - Partners
    - Other communities of interest
- Extending connectivity to **corporate partners and suppliers** in a private network environment.
- benefits of a VPN WAN architecture is
    - The ease of extranet deployment and management.
    - The primary difference is the access permission extranet users are granted once connected to their partner's network.
    - Extends selected resources and applications from a company network to users from other companies partners.

VPN Security

- VPNs use many security mechanisms
    - **Authentication:** Identify VPN users and devices
    - **Access control:** Ensure authorized use of VPN resources
    - **Data security:** Use cryptography to obscure content transmitted over VPN

5.2.3 VPN TUNNELING PROTOCOLS

A technology that enables one network to send the data via another network's connections. VPN Tunneling works by

i. Support authentication and encryption to keep the tunnels secure.
ii. Establish and maintain a logical network connection (that may contain intermediate hops).

iii. Carry out the process of capsulating and encapsulating of packets between client and server.

a) Point to Point Tunneling protocol (PPTP)

- **Encapsulate and encrypt** the data to be sent over a corporate or public IP network
- Because the Internet is essentially an open network, the Point-to-Point Tunneling Protocol (PPTP) is **used to ensure that messages transmitted from one VPN node to another are secure.**
- With PPTP, users can dial in to their corporate network via the Internet safely.

b) Layer 2 Tunneling Protocol (L2TP)

- Developed to facilitate PPP access by remote computers to a private network **over an IP-based** network
- PPTP and L2TP have mostly the same functionality.
- Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.
- L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines.

L2TP Benefits

- Supporting Multi-hop
- Operate like a client initiated Virtual Private Network (VPN) solution
- Cisco's L2F offered value-added traits, as load sharing plus backup support

Types of VPN L2TP Tunneling

- **Voluntary L2TP tunneling**
  - The *VPN client manages connection setup.*
  - The client first makes a connection to the ISP.
  - Then, the VPN client application creates the tunnel to a VPN server over this live connection.

- **Compulsory L2TP tunneling**
  - The *ISP manages VPN connection setup.*
  - When the client first makes an ordinary connection to the ISP, the ISP in turn immediately a VPN connection between that client and a VPN server.
  - From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

- **How VPN works between remote client and server.**
  - User connect to the ISP
  - The VPN client software must be installed in the user computer. Then the software will initiates through the VPN server to provide user login ID and password.
  - The VPN server encrypts the data on the connection so it cannot be read by others while it is in transit.
  - The VPN server decrypts the data and passes it on to other server and its resources.

c) Internet Protocol Security(IPSec)

- IPSec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.

- IPSec protect data flows between:
  i. Pair of hosts
  ii. Pair of security gateways
  iii. Security gateway and a host

Advantages

- Provides seamless security to application and transport layers.
- Allows per flow or per connection security and thus allows for very fine-grained security control.

Disadvantages

- More difficult to to exercise on a per user basis on a multi-user machine.

TWO(2) types of IPSec mode:

i. **Transport mode:** only the payload (the data you transfer) of the IP packet is usually encrypted and/or authenticated. IPSec Transport mode is used for end-to-end communications,

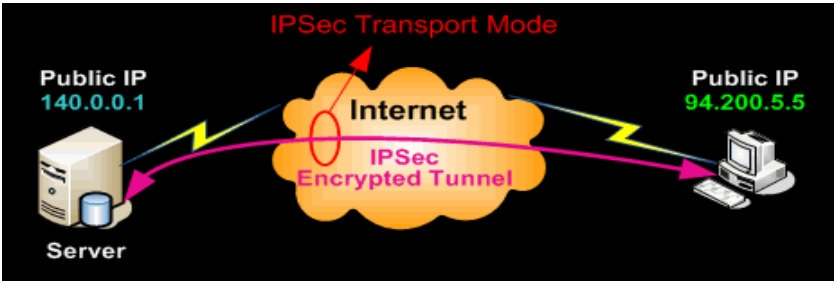


Figure 5.11: IPSec Transport Mode

ii. **Tunnel mode:** the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel

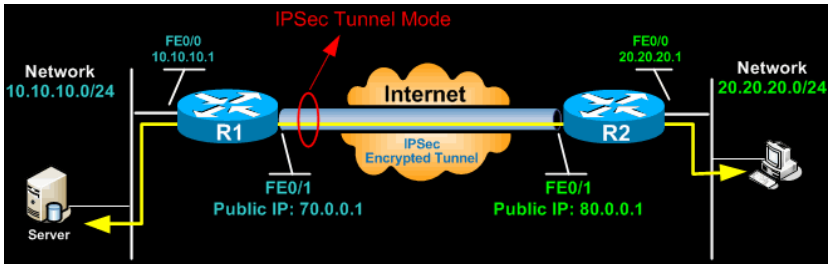


Figure 5.12: IPSec Tunnel Mode

5.2.4 PROCEDURE TO SET UP A VPN

There are two principal ways to configure VPN.

i. *Outgoing* - is setting up a remote computer to call into the office network.

ii. *Incoming* - occurs on the network side, where a computer allows secure connections from other computers.

Before establishing a VPN, several steps must be taken:

i. Setup a VPN-capable device (router, firewall and etc.) on the network perimeter.

ii. Know the IP subnet addresses used by the other side.

iii. Agree on a method of authentication and exchange digital certificates if required.

iv. Agree on a method of encryption and exchange encryption keys as required.

Step by Step: Connecting to a VPN (Outgoing)

Step 1:

Click the *Start* button. In the search bar, type **VPN** and then select *Set up a virtual private network (VPN) connection*.

Step 2:

Enter the IP address or domain name of the server to which you want to connect. If you're connecting to a work network, your IT administrator can provide the best address.

Step 3:

If you want to set up the connection, but not connect, select *Don't connect now*; otherwise, leave it blank and click *Next*.

Step 4:

On this next screen, you can either put in your username and password, or leave it blank. You'll be prompted for it again on the actual connection. Click *Connect*.

Step 5:

To connect, click on the Windows network logo on the lower-right part of your screen; and then select *Connect* under VPN Connection.

Step 6:

In the Connect VPN Connection box, enter the appropriate domain and your log-in credentials; and then click *Connect*.

Figure 5.13: Connect VPN Connection box

Step 7:

If you can't connect, the problem could be due to the server configuration. (There are different types of VPN.) Check with your network administrator to see what kind is in use--such as PPTP--then, on the Connect VPN Connection screen, select *Properties*.

Step 8:

Navigate to the Security tab and select the specific Type of VPN from the drop-down list. You may also have to unselect *Include Windows logon domain* under the Options tab. Then click *OK* and *Connect*.

Step by Step: Building a VPN (Incoming)

Step 1:
Click the *Start* button, and, in the search bar, type **Network and Sharing**.

Step 2:
Click *Change Adapter Settings* in the left-hand menu.

Step 3:
Click *File*, and then *New Incoming Connection*.

Step 4:
Select the users you'd like to give access to and click *Next*.

Step 5:
Click *Through the Internet* and select *Next*.

Step 6:
Select the Internet Protocol you'd like to use. (The default TCP/IPv4--the line highlighted in the screenshot below--will work fine.)

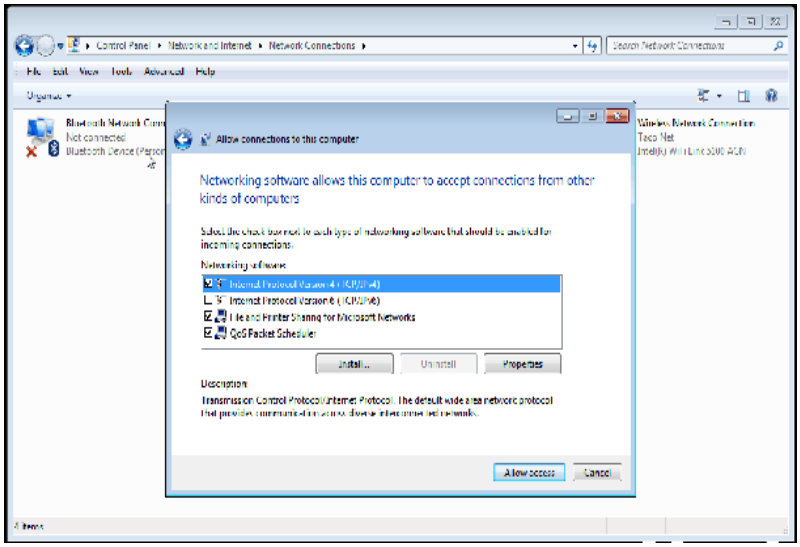


Figure 5.14: Allow Access Connection

Step 7:
Finally, click *Allow access*; you've now set up an incoming VPN connection.

5.2.5 VPN CONFIGURATION (VPN BETWEEN TWO INTERNET SITES)

Before establishing a VPN, the two networks must do the following:

- Set up a VPN-capable device on the network perimeter. This can be a router, a firewall, or a device dedicated to VPN activity.
- Know the IP subnet addresses used by the other site.
- Agree on a method of authentication and exchange digital certificates if required.
- Agree on a method of encryption and exchange encryption keys as required.

A typical VPN includes the following components:

a) Software installed (VPN client) on end user's computer or a hardware VPN device – this encrypts data.
b) A connection from the computer to the public Internet.
c) A connection from the Internet to corporate HQ.
d) VPN Hardware or Server at HQ to authenticate users and decrypt their data.

Figure 5.15: VPN configuration (VPN between two Internet sites)

5.2.6 VARIOUS DEVICES FOR A VPN CONNECTION:

a) Firewall based VPNs.

A firewall-based VPN is one that is equipped with both firewall and VPN capabilities. This type of VPN makes use of the security mechanisms in firewalls to restrict access to an internal network. The features it provides include address translation, user authentication, real time alarms and extensive logging.

Firewall VPNs provide greater security for connections and should be included in the branch office VPN overall design. Firewall-based VPNs are considered among the most secure, as they take advantage of the firewall's existing security mechanisms.

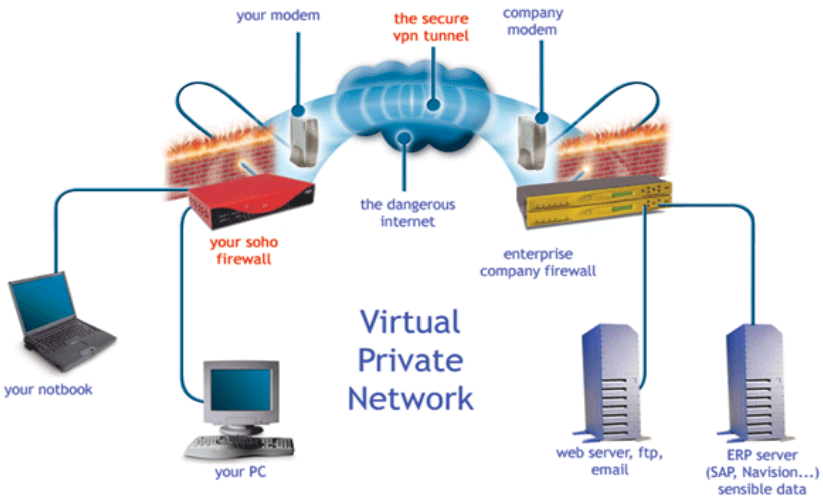


Figure 5.16: Firewall-Based VPN

b) Router-based VPNs

Router-based VPNs are for an organization that has a large capital investment in routers and an experienced IT staff. Many router vendors support router-based VPN configurations.

There are two ways to go about implementing router-based VPNs:

i. Software is added to the router to allow an encryption process to occur.
ii. An external card from a third-party vendor is inserted into the router chassis. This method is designed to off-load the encryption process from the router CPU to the additional card.

Performance can be an issue with router-based VPNs because of the addition of an encryption process to the routing process; a heavier burden may be added to the router CPU, more than ever if the router is handling a large number of routes or implementing an intensive routing algorithm.

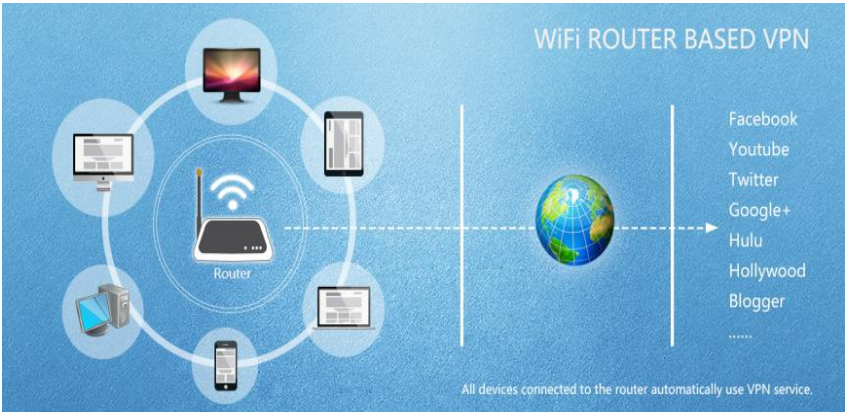


Figure 5.17: Router-Based VPN

The drawback to a router-based VPN is security. Routers are considered to be poor at providing network security compared to a firewall. It is possible that an attacker will spoof traffic past the router, in turn fooling the firewall because the firewall will interpret these packets as originating from the other side of the VPN tunnel. This spoofing allows the attacker to gain access to services that are not visible from other locations on the Internet.

c) Dedicated software or hardware

Software VPNs

Software VPN technology is available in multiple forms. One form is an application added to an existing server on a network. Another is a software upgrade to an existing piece of network equipment. A hardware vendor may provide added functionality for a network appliance, such as a router, as a software upgrade.
Software VPN has an advantage of being inexpensive relative to hardware VPN appliances. Since the software can be installed on existing equipment, there also may be less training necessary for an organization's IT staff because the same vendor may maintain

a similar application interface. Software VPN is also a way of maintaining a simpler hardware topology for a network.

- **Hardware VPNs**

Hardware VPN appliances are network equipment dedicated only to the purpose of VPN. Although generally more expensive than software VPN, hardware VPN can offer the best performance for organizations and companies relying heavily on VPN. There are considerations about network topology to be weighed, as a hardware VPN is an additional appliance and may require extensive training for an IT department. Hardware VPN appliances are built specifically for the purpose of VPN and can provide the most efficient VPN capability for an organization or company.

A hardware VPN is a virtual private network (VPN) based on a single, stand-alone device. The device, which contains a dedicated processor, manages authentication, encryption and other VPN functions, and provides a hardware firewall. Hardware VPNs provide enhanced security for the enterprise in much the same way that hardware routers offer additional security (when compared to firewall programs) for home and small-business computer users.

A traditional VPN is, essentially, a set of programs on the same platform as the network operating system. Such a VPN provides remote offices or individual users with secure access to their organization's network by using the shared public telecommunications infrastructure and standard security measures. Hardware VPNs offer a number of advantages over the software-based VPN. In addition to enhanced security, hardware VPNs provides load balancing and the ability to handle large client loads.

Software vs. Hardware

1. Cost

- Dedicated hardware VPN appliances are generally more expensive

2. Security

- Hardware VPNs are considered more secure.
- Software-based VPNs often are forced to share a server with other applications and operating systems, which makes them more prone to attacks and less secure.

3. Scalability

- Software VPN solutions have the advantage because upgrading usually translates to replacing an onboard processor or adding memory to the system.
- Hardware VPNs are limited depending on the selected model. You would need to spend more money and upgrade to a larger model.

4. Performance

- dedicated VPN appliances also offer load balancing features not easily found on software VPN solutions.

5. Maintenance

- Hardware VPNs sometimes offer more options when configuring the VPN service but require more advanced skills like knowing how to use the command line interface (CLI).

5.2.7 FEATURES OF GOOD VPN PRODUCTS:

a. Strong authentication

- Require more than a username and a reusable password to authenticate a user or device.
- It is necessary for identity theft protection and data protection on computers, the Internet, and corporate networks.

b. Adequate Encryption

- Virtual private networks employ a combination of technologies that allows users to transmit traffic over the Internet with the information privacy and security assurances equal to what can be expected from facilities-based private networks.
- Reliable method to identify and authenticate users seeking to gain intranet access.
- Protects sensitive information content being revealed or compromised by intentional or unintentional eavesdroppers.
- Available to prevent malicious data tampering, and in particular undetected data manipulation.

c. Adherence to standards

- Include programs, practices, policies, protocols, and awareness materials that have been developed and implemented in specific settings.
- Adherence to the service-level agreements is being measured and monitored, and problems, if appropriate, are elevated for management action.

CHAPTER 6

Disaster Prevention and Recovery

This chapter discusses the following topics:

- Disaster Solutions
- Manage Hardware for Disasters Handling

6.1 DISASTER SOLUTIONS

6.1.1 DISASTER

A **disaster** is a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society.

6.1.2 TYPE OF DISASTER

a) Natural

A Natural Hazard is a natural process or phenomenon that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage.

Various phenomena like earthquakes, landslides, volcanic floods, hurricanes, tornadoes, blizzards, tsunamis, and cyclones are all natural hazards that kill thousands of people and destroy billions of dollars of habitat and property each year.

b) Man-Made

Human-Instigated disasters are the consequence of technological hazards. Examples include stampedes, fires, transport accidents, industrial accidents, oil spills and nuclear explosions/radiation. War and deliberate attacks may also be put in this category. As with natural hazards, man-made hazards are events that have not happened, for instance terrorism. Man-made disasters are examples of specific cases where man-made hazards have become reality in an event.

6.1.3 TWO CATEGORIES OF DISASTER SOLUTIONS

a) Maintaining or restoring a service

- A backup and recovery are integral parts of a company's ability to restore operations after failure.
- The more current the backups, the easier it is for organization to restore operations.
- Information on server systems should be backups daily.

b) Protecting or restoring lost, corrupted or deleted information

- Data protection measures are an effective strategy to secure and maintain sensitive information on a personal or business computer.
- Data protection can involve downloading and installing a variety of software programs that can help with backup of files, system restoration, and periodic updates for storing and filing critical applications.

6.1.4 THE DISASTER RECOVERY PRINCIPLES

- Support and involvement of upper level managers lead to a robust disaster recovery plan.
- Assess the organization on a regular basis.
- Policies and procedures adopted must be documented, made available to the intended staff to meet the business operational needs.
- Determine the managers responsible for declaring, responding and recovering from a disaster.
- Restrict communications among internal and external supporters of the organizations.
- Train employees against unforeseen crisis.
- Procedures must be tested and rehearsed to detect the vulnerabilities in the plan.
- Planners must identify new threats and update plans accordingly.
- Evaluate the effectiveness of the procedure and monitor safety and hygienic issues of the employees.

6.1.5 TWO TYPES OF DISASTER RECOVERY SYSTEM

a) Synchronous System

Synchronous systems (also called “two-stage commit systems") are designed to make sure that no I/O transaction can be committed to the disk of the primary system unless and until it has also been committed to the disk systems of the backup system. Most of these systems are hardware based and involve the use of attached storage, like NAS or SAN systems. However, software-based synchronous systems are also available today.

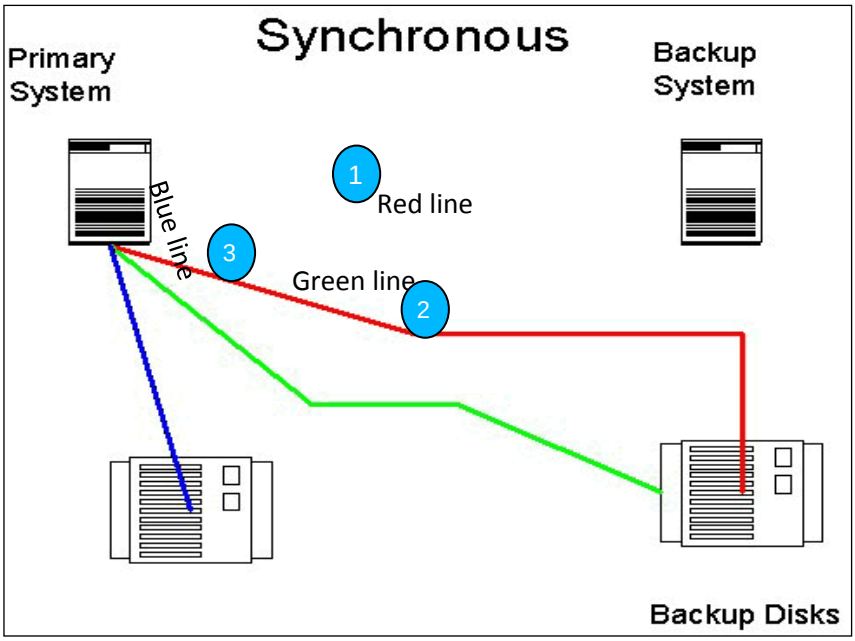


Figure 6.1 Typical software-based synchronous DR system.

- When an I/O request is initiated by any application on the primary system,
- That request is sent to the backup disk systems first (red line) and committed there.
- The system then waits for the confirmation of that commit to return from the backup disk systems (green line).
- Only then is the I/O committed to the primary disk systems (blue line).
- This ensures that nothing can be committed to the primary system unless it already exists on the backup.

b) Asynchronous System

For most applications and businesses, asynchronous DR technologies offer a much more cost-effective and still quite sufficient solution.
These systems are generally software-based and reside on the host server rather than on the attached storage array. They can protect both local and attached disk systems.

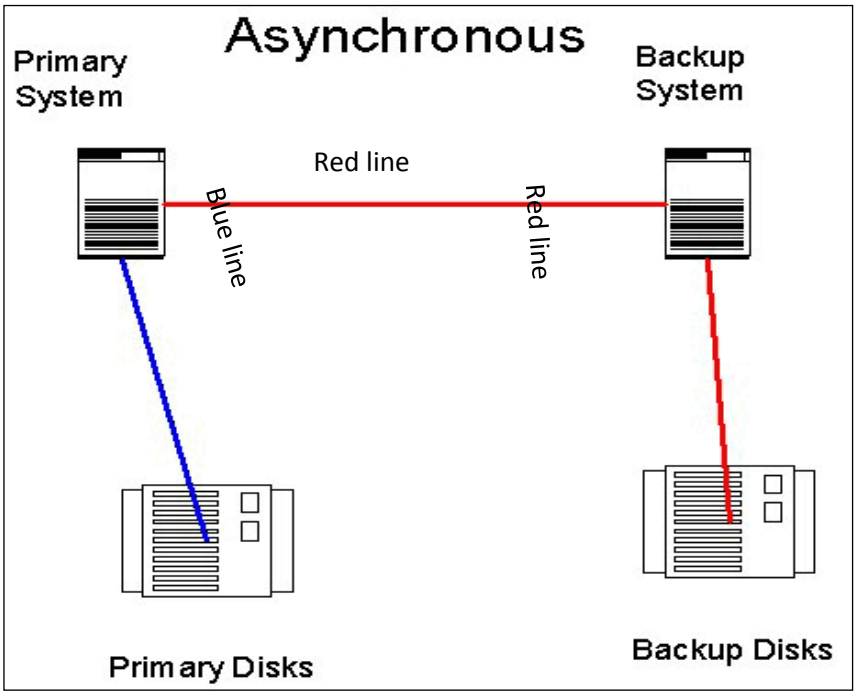


Figure 6.2 Typical asynchronous system.

- Firstly, I/O requests are committed to the primary disk systems immediately (blue line)
- While a copy of that I/O is sent via some medium (usually TCP/IP) to the backup disk systems (red line).

- Since there is no waiting for the commit signal from the remote systems, these systems can send a continuous stream of I/O data to the backup systems without slowing down I/O response time on the primary disks system.
- Most asynchronous systems have some methodology to make sure that if something is lost in transmission, it can be resent.

Differences between Synchrounous and Asynchronous Disaster Recovery System.

Synchronous	Asynchronous
Write data to the primary secondary sites at the same time so that the data remains current between sites.	A process where there is a delay before data is copied to a secondary site.
Only works over distances up to 300km.	Can tolerate some degradation in connectivity and does not require much bandwidth. Suitable for work over long distances.

6.1.6 THE PURPOSE OF DISASTER RECOVERY PLAN

All organizations are susceptible to disasters of all types, which can interrupt their business, or in the worst cases, shut them down permanently.
Contingency planning is the identification, prior to a disaster, of all critical procedures and resources necessary for the organizations survival. The purpose of such a program is to anticipate, and plan for these emergency situations before they arise, thus lessening their effects. A properly organized plan will ultimately take into consideration the safety of clients, students and employees first, and will also minimize the business interruption, which usually succeeds a disaster.

PLAN FOR DISASTER RECOVERY

1) Develop a disaster recovery plan.
2) Implement a disaster recovery plan.
3) Document and regularly test the disaster recovery plan.
4) Explain standard backup procedures and backup media storage practices.
5) Identify types of backups and restoration schemes *(method).*
6) Confirm and use off-site storage of backups.

6.1.7 THE DISASTER RECOVERY PLANNING

1) Security Planning

a) Short-term, High-impact Strategy

- Create a policy statement covering disaster recovery planning
- Compile an emergency telephone or contact list consisting of Departmental personnel, CCIT personnel, user personnel, vendors, and emergency services.
- Assemble all readily available operations and systems documentation
- Create lists of all operating systems software by hardware configuration
- Obtain a copy of all Emergency Procedures documentation
- Verify that all systems are backed up as required and stored in a secure site
- Determine the minimum hardware configuration on which mandatory components of application systems can run and arrange for tests
- Create a priority ordered list by application operating system segmented by major organizational function
- Consult with senior management in the financial, student, administrative, and operational areas to get their opinions as to the mandatory and necessary applications in an agreed order of priority.

b) Long-term, Extended Strategy

The Long-term Strategy differs from the short-term by emphasizing greater and continued participation by the department's administrative officers and users of departmental services. The long-term strategy is directed towards creating a full, effective, disaster recovery capability by:

- Assigning a full-time person or persons to maintain and oversee the plan
- Assigning task groups that report regularly to the Disaster Management Team on developing areas of the plan
- Obtaining budget funding necessary for continued maintenance of the plan
- Involving all organizational groups, such as Security, Risk Management, Facilities, and Procurement and Contracting
- Developing a full disaster recovery capability covering all areas IT use
- Having regular training of all staff in the plan actions and requirements
- Testing the plan realistically and regularly, and report on the results of the testing including recommendations.

c) Types of disaster to consider

- Natural disasters: Floods, Storms, Fires, Earthquakes, Lightning, Loss of a Disk Drive or Computer System, etc.
- Man-made disasters: Fire, Transportation Accidents, Chemical Accidents, Sabotage or Willful Destruction, Bomb Threats, Burst Pipes, Electrical Outage, Loss of Environmental Controls, etc.
- Political disasters: Riots, Public Demonstrations, Civil Disturbances, etc.

- Electronic Warfare: Hackers, Cyber terrorism, Computer Viruses, Intrusion Detection, Denial of Service, etc.

The types of disasters that should be considered depend on the team's area of responsibility and operating parameters and may be specific to a particular application. Some disasters, such as major building fires, would probably affect all teams and must be planned for accordingly. The most likely threats to occur should receive the most attention. These more common disasters may be localized in the computer, communications, or data input areas.

2) Program Budget

There are three ways to fund disaster recovery planning for an organization:

a) corporate funding,
b) business unit funding, or
c) information technology funding.

When funding your disaster recovery program, the key questions to be answered are:

- Who should fund your disaster recovery program?
- What should be funded?
- How much should be invested now, next year and five years ahead?
- How should we continue justifying the ongoing investment in disaster recovery?

3) Organizing

Separate Coordination teams responsible for all activities within your department that will manage the recovery process. This breakout of teams enables the activation of any or all of your department's personnel and/or plans so that the recovery process can scale appropriately based on the requirement. The team leader from each of these coordination teams will be a member of the Disaster Management Team which provides overarching responsibility and direction for plan development, plan maintenance and plan execution. Each coordination team should be further divided into appropriate sub groups as necessary to develop and manage specific requirements. The disaster teams identified in this section are loosely coupled to the organizational structure of your department. To assist in the implementation of the Disaster Recovery Plan, the following teams should be established.

4) Training

The recovery plan must provide for initial and ongoing employee training. Skills are needed in the reconstruction and salvage phases of the recovery process. Your initial training can be accomplished through professional seminars, special in-house educational programs, the wise use of consultants and vendors, and individual study tailored to the needs of your department.
A minimal amount of training is necessary to assist professional restorers/recovery contractors and others having little knowledge of your information, level of importance, or general operations.

5) Implementation

- Building an implementation plan
- Allocating tasks for implementation
- Creating an implementation schedule
- Allocating the disaster recovery documentation
- Evaluating the worth and efficiency of mitigation steps
- Administering internal and external knowledge campaigns
- Implementing training program for disaster recovery

Activity of Disaster recovery testing

1. **Procedure audits:**
   Employees view the procedure to determine its authenticity and efficiency in executing procedures.
2. **Live walk-throughs of procedures:**
   Determines procedures effectiveness.
3. **Live walk-throughs of related process:**
   Related procedures are implemented to check their effectiveness.
4. **Scenario testing:**
   Creates a mock disaster that inspects the events working process.
5. **Work group level tests:**
   Creates a mock disaster for a specific group of people.
6. **Department-level test:**
   Creates a mock disaster for which the entire department must respond.
7. **Facility-level tests:**
   Creates a mock disaster for which an entire facility is liable.

8. **Enterprise-level tests:**
   Creates a mock disaster for which the entire organization must respond.

6.2 MANAGE HARDWARE FOR DISASTERS HANDLING

6.2.1 THE HARDWARE AND FUNCTION IN HANDLING SERVER DISASTERS.

a. UPS

Uninterruptible Power Supply (UPS) is also known as Battery Backup. While all computers need a source of clean and steady power, this is even more important when the computer will act as a server, because multiple users will rely on the system. A good power source is not just one that is free from blackout or brownout condition, but it should be free of surges and spikes as well. While brownout or blackouts are easy to identify because they will cause the system to reboot, spikes, surges, and noise can cause far more subtle problem, such as the application error just described. Electrical power is like network wiring, we do not think to check it until we have spent time chasing our tails replacing drivers and loading patches.

b. RAID

A RAID array **joins two or more** hard disks so that they make a logical disk. A technology that allowed computer users to achieve high levels of storage reliability from low-cost and less reliable PC-class disk-drive components, via the technique of arranging the devices into arrays for redundancy.

Computer data storage schemes that can divide and replicate data among multiple hard disk drives.

- Two key design goals:
  - increased data reliability.
  - increased input/output performance.

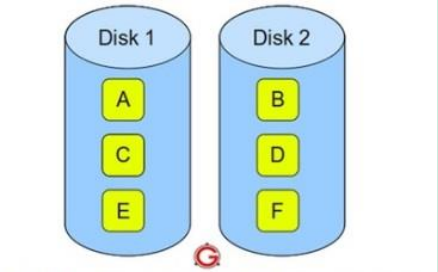
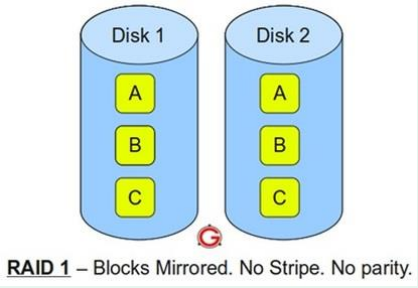
When multiple physical disks are set up to use RAID technology, they are said to be *in* a *RAID* array. This array distributes data across multiple disks, but the array is seen by the computer user and operating system as one single disk.

RAID Technology:

- RAID not only provides fault tolerance against hard disk crashes; it can also improve system performance.
- RAID breaks up or copies the data user want to save across multiple hard disks.
- This approach prevents a system failure due to the crash of a single drive.
- It also improves performance, because multiple disks can work together to save large files simultaneously.

RAID levels

- **Three (3) most commonly found:**

RAID level	Description
RAID 0 (striped disks) ~**Minimum 2 disks**. ~Excellent performance (As blocks are striped). ~ No redundancy (No mirror, no parity). ~Don't use this for any critical system. ~ provides maximum usable disk space.	Distributes data across several disks in a way that gives improved speed and no lost capacity, but all data on all disks will be lost if any one disk fails.  RAID 0 – Blocks Striped. No Mirror. No Parity.
RAID 1 (mirrored settings/disks) ~ **Minimum 2 disks**. ~ Good performance read (no striping. no parity). ~ Excellent redundancy (as blocks are mirrored).	Duplicates data across every disk in the array, providing full redundancy. Two (or more) disks each store exactly the same data Data is not lost as long as one disk survives. Total capacity of the array equals the capacity of the smallest disk in the array.  RAID 1 – Blocks Mirrored. No Stripe. No parity.

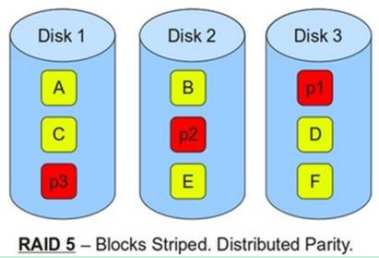
RAID 5 (striped disks with parity) ~**Minimum 3 disks**. ~ Good performance (As blocks are striped). ~Good redundancy (**distributed parity**). ~Best cost effective opti on providing both perfor mance and redundancy.	Combines three or more disks in a way that protects data against loss of any one disk The storage capacity of the array is reduced by one disk. 

Figure 6.3: RAID Comparison

Key concepts in RAID

- **Mirroring** :
  - The copying of data to more than one disk.
  - can speed up reading data as a system can read different data from both the disks, but it may be slow for writing.

- **Striping** :
  - Splitting of data across more than one disk.
  - is often used for performance, where it allows sequences of data to be read from multiple disks at the same time.

- **Error correction** :
  - Redundant data is stored to allow problems to be detected and possibly fixed (known as fault tolerance).
  - typically will slow the system down as data needs to be read from several places and compared.

c. Redundant servers

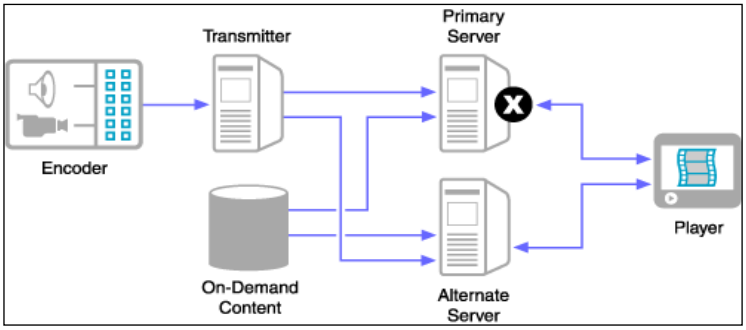


Figure 6.4: Diagram of Redundant Servers

- A redundant server is a backup server, provide one or more entire systems to be available in case the primary system crashes.
- It does not matter if the crash is due to a drive failure, a memory error, or even a motherboard failure.
- Once the primary server stops responding to requests, the redundant system steps in to take over until the primary is back on line.
- Often, if the primary and secondary are both functional, both will share duties, increasing overall throughput.

d. Clustering

- A group of linked computers, working together closely so that in many respects they form a single computer.
- Commonly connected to each other through fast local area networks.
- Deployed to improve performance and/or availability over that provided by a single computer.

Figure 6.5: Example of Computer Cluster

The purpose of clustering is to improving the availability of services which the cluster provides. They operate by having redundant nodes, which are then **used to provide service when system components fail**. The most common size for a cluster is two nodes, which is the minimum requirement to provide redundancy. HA cluster implementations attempt to use redundancy of cluster components to eliminate single points of failure. For instance, a single compute job may require frequent communication among nodes - this implies that the cluster shares a dedicated network, is densely located, and probably has homogenous nodes.

Two common types of cluster:

Active/Passive:

- Active server handle all client request; passive server stand-by to take over if active server fail.
- Passive server only participates only during failover of active server.

Active/Active:

- All system takes part in processing service request.
- The clusters act as intelligent unit to balance traffic load between nodes.
- Client perspectives; a cluster looks like a single, yet very fast server.
- If one server fail, the other work will be take over respectively by others but with an obvious degradation in performance.

e. Tape Backup

- Tape backup is the ability to periodically copy the contents of all or a designated amount of data from its usual storage device to a tape cartridge device so that, in the event of a hard disk crash or comparable failure, the data will not be lost.
- The method of choice for protecting or restoring lost, corrupted, or deleted information.

Type Of Backup

i. Full backup

- The backup of all files on the drive.
- Takes the longest time to record because every file is copied.
- Takes the shortest time to restore because everything is on a single tape.
- Requires the greatest storage capacity for the same reason.

The Full Backup is a straightforward method of insuring good backups and quick, easy restorations. The starting point for the Incremental and the Differential Backups.

ii. Incremental backup

- Records only those files that have changed since the last Incremental Backup.
- Takes the shortest time to record.
- Generally takes the longest time to restore.
- Generally requires several tapes to restore.

iii. Differential backup

- Records only those files that have changed since the last Full backup.
- Takes less time to record than a Full backup.
- Takes less time to restore than an Incremental backup.
- The restore process requires only two tapes.

Backup Type	Advantages	Disadvantages
Normal (full)	Files are easier to find because they are on the current backup medium. Requires only one medium or set of media for file recovery.	Is time consuming. If files change infrequently, backups are nearly identical.
Incremental	Requires the least amount of data storage. Provides the fastest backups.	Complete system restoration may take longer than using normal or differential backup.
Differential	Recovery requires media from last normal and last differential backups only. Provides faster backup than normal.	Complete system restoration may take longer than using normal backup. If large amounts of data changes occur, backups may take longer than incremental type.

Figure 6.6: Comparison of Tape Backup

	Incremental Backup	Differential Backup	Full Backup
What is it	A backup of all changed and new files since the last backup	A backup of all changed and new files since the last full backup	A backup of all files in a specified backup set or job
Backup Speed	Fastest	Faster	Slowest
Restore Speed	Slowest	Faster	Fastest
Storage Needed	Least	More	Most
Advantages	•Faster backups •Less storage space used. •No duplicate files	•Faster & simpler restores then incremental backup •Only needs the first full backup and last differential backup to restore	•Fastest restore •Only needs the last full backup set to restore
Disadvantages	•Slowest restores •Needs all backup sets full + all increments to restores	•Slower backups •Still stores a lot of duplicate files	•Needs the most storage space •Inefficient storage with a lots of duplicates stored

Figure 6.7: Summary of Tape Backup

References

Main :

David R. Miller, Michael Gregg(2009), Security Administrator Street Smarts. Wiley Publishing, Inc.
(ISDN: 978-0-470-40485-0)

Mark Ciampa, Security + Guide to Network Security Fundamentals, Third Edition(2009). Course Technology, Cengage Learning. (ISDN: 978-1-428-34066-4)

Mike Pastore, Emmet Dulaney(2006), CompTIA Security+. Wiley Publishing, Inc. (ISDN: 978-0-4700-3821-5)

Additional :

Siti Rahayu Selamat et al. (2006), Information Technology Security. Pearson Prentice Hall. (ISDN: 978-983-3655-47-2)

Department of Skills Development MOHR(2010), Occupational Structure – Information and Communication Technology (ICT) Industry. Perpustakaan Negara Malaysia. (ISDN:978-967-5236-31-0)

EC-Council Academy (2010), EC-Council Network Security Administrator Official Courseware(Version 4.0. EC-Council Organisation. (http://www.eccouncil.org)

JPK (2010), Executive Summary-ICT System Security Technologist Level 4 & 5. Department of Skills Development MOHR

AUTHOR BIOGRAPHY

Kamarudin Ripin
Graduated from University Technology Malaysia, with Bachelor in Computer Science, Majoring in Information System.

Mohd Redzuan Rosly
Graduated from University Putra Malaysia, with Bachelor in Computer Science, Majoring in Software Engineering.

Siti Nasrah Mukhtar
Graduated from University Malaysia Pahang, with Bachelor in Computer Science, Majoring in Computer System & Networking.

INFORMATION SYSTEM SECURITY

e ISBN 978-967-0047-36-2

9 789670 047362

EDITION 2023