Basic Of Information Security

- Information Security, Sometimes shortend to InfoSec.
- It is the practice of protecting information from unauthorized access.
- Information can be anything like your details or we can say your profile on social media, your data in mobile phone etc.
- August Kerckhoffs in the father of Information Security.
- There are 3 objectives of IS, Commonly known as CIA.

  Confidentiality

  Integrity

  Availability

Confidentiality

- It is the principle of keeping sensitive private information
- It ensures that secret information is protected from unauthorized access.
- It means information is not disclosed to unauthorized individuals.
- Encryption Technology protects sensitive information stored on systems.

Example: Personal bank details, credit card information, personal information, research data, password and other irelated information..

Integrity

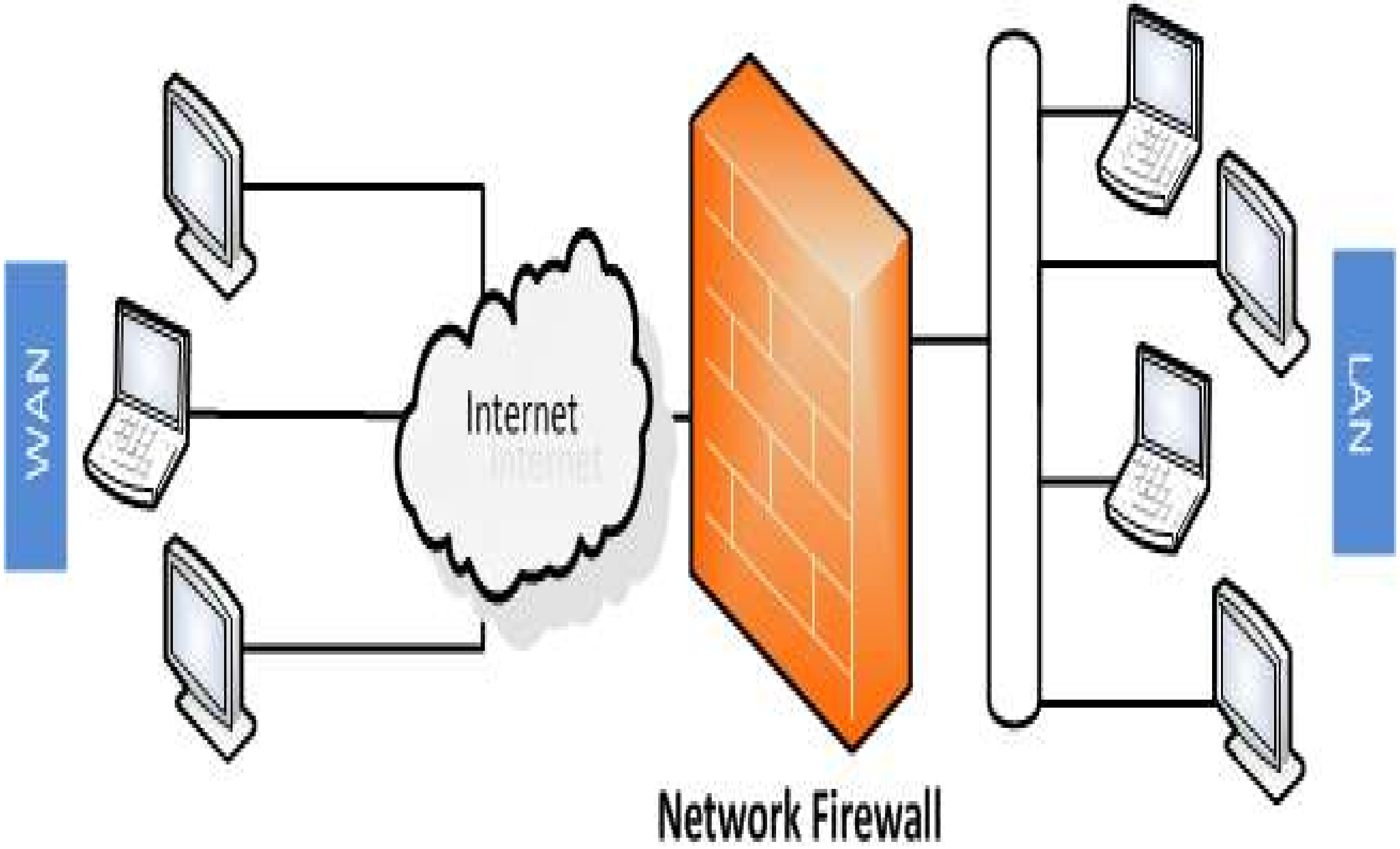
- It means maintaining accuracy and completeness of data.
- Data Integrity means that the data must arrive at the reciever. Exactly as it was sent.
- There must be no changes in the data content during transmission, either maliciously or accidently.
- This means data cannot be edited by unauthorized users.
- Integrity is the ability to ensure that a system and its data has not suffered unauthorized modification.

Availability

- It means information must be available when needed.
- It is one of the three basic functionc of security management that are present in all systems.
- It is the assertions that a computer system is available or accessible by an authorized user whenever it is needed.
- Availability gaurantees that systems, applications and data are available to users when they need them.

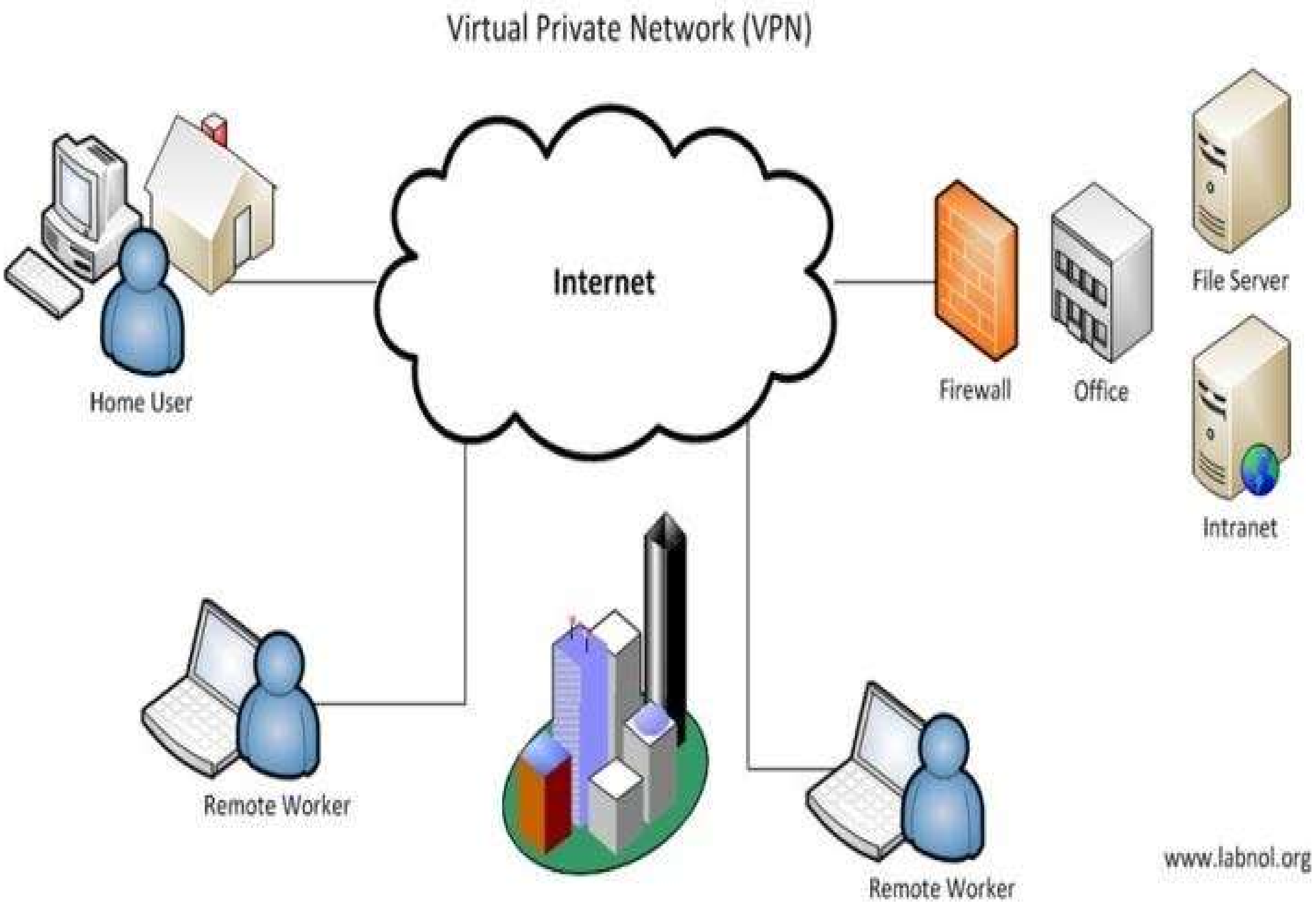
Firewalls

- A firewall is a network security system that manages the network traffic based on some protocols.
- It monitors and control incoming outgoing traffic based on predefined rules.
- It exist as software and hardware both.
- Most personal computers user software based firewalls to secure data from threats from the internet.
- Firwalls are commonly used in private networks or intranets to prevent unauthorized access from internet.


WAN
Internet
Network Firewall
LAN

Virtual Private Network

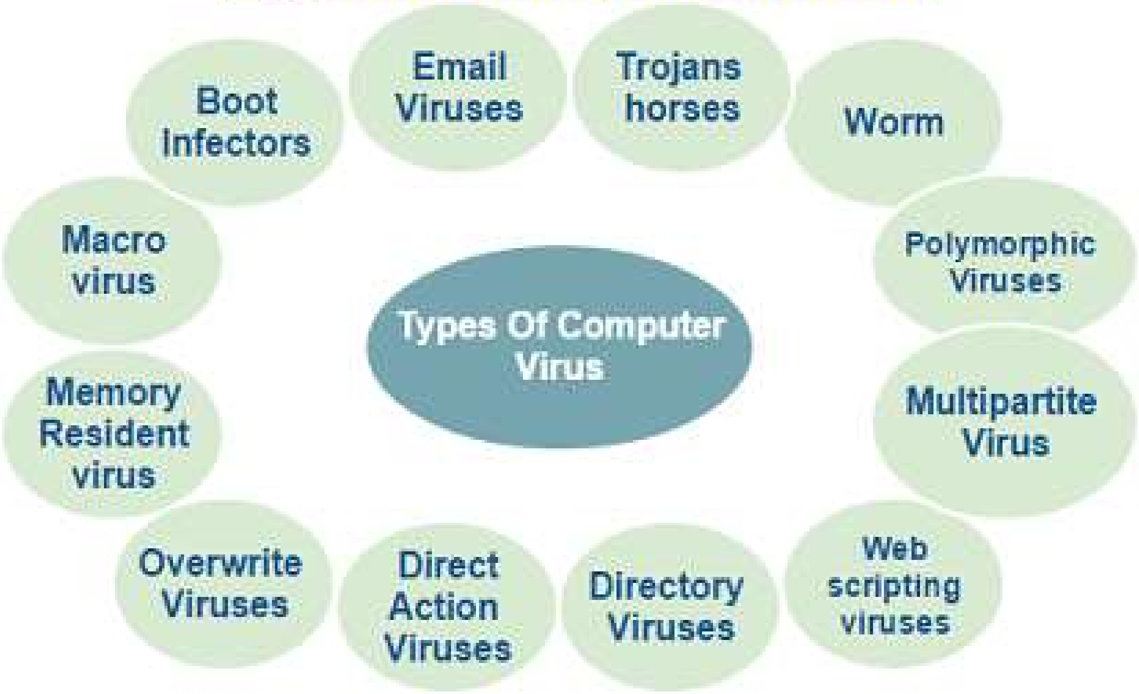
- A VPN is type of network security.
- It hides your IP address on the internet.
- It prevents unauthorized people and allows the unauthorized user.
- A VPN is an encrypted connection over the Internet.
- The encrypted connection helps ensure that sensitive data is safely transmitted.
- VPN Technology is widely used in corporate environments.

Virtual Private Network (VPN)
Internet
Home User
Firewall
Office
File Server
Intranet
Remote Worker
Remote Worker
www.labnol.org

VIRUS

- Virus stand for “Vital Information Resources Under Siege”
- A computer virus is a piece of software that can “infect” a computer.
- It install itself to the computers, without the users knowledge or permission.
- It usually attaches itself to other computer programs data files, or the boot sector of a Hard drive, pendrive etc.
- Malware is short for Malicious Softwares: Malware, Trojan horse, Worm, Spyware, Boot sector virus etc.

Types of Computer Viruses



Anti Virus

- It is also known as AV Software.
- It is kind of software used to prevent, scan, delet and deleted viruses from a computers.
- Antivirus software helps protect your computer against malware and cybercriminals.
- Antivirus software looks at data web pages, files, software, applications travelling over the network to your devices.
- It seeks to block or remove malwares as quickly as possible. Ex: AVG Antivirus Gaurd, McA free, Norton, Kespersky etc.

Protect Your Windows