Unit-2

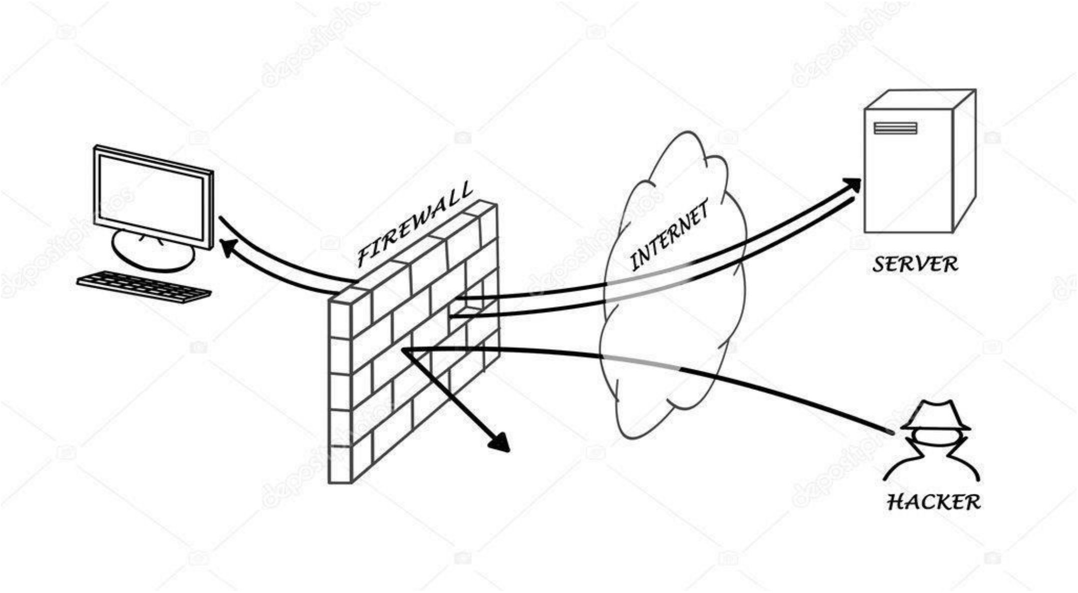
Security Technologies

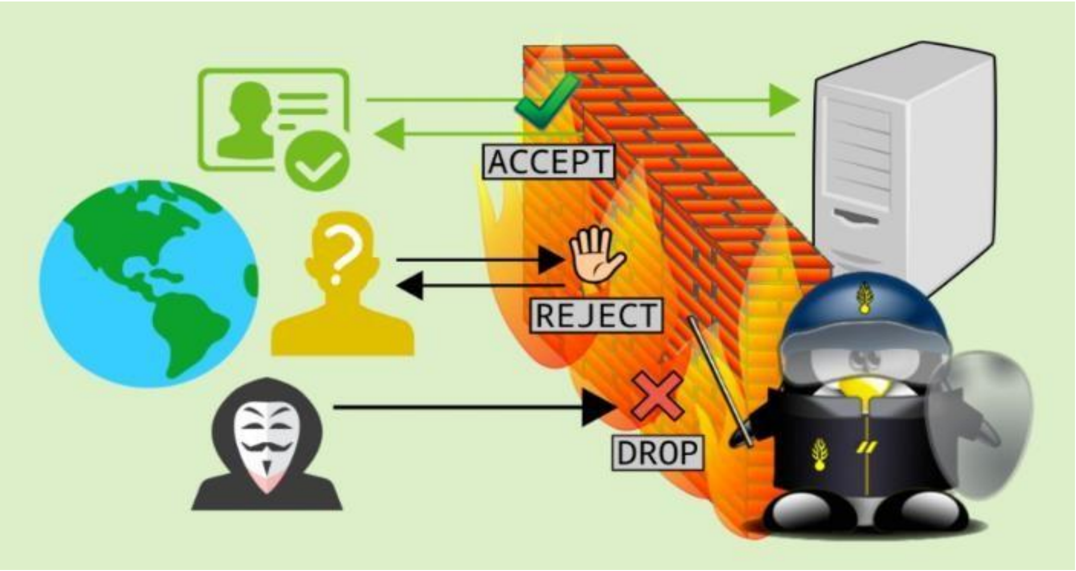
- Firewalls
- Virtual Private Networks
- Encryption
- Intrusion Detection
- Anti-Malicious Software
- Secure Software & Browser Security
- SSL and IPsec

Security technologies

- The Internet, like everything else, has its advantages and disadvantages.
- As Internet usage has grown rapidly, so have the number of attacks on organizations.
- This poses a challenge for businesses and organizations to protect themselves from cyber-attacks.
- To ensure smooth operations, security technologies are necessary.
- In this chapter, we will discuss a few of these securing technologies and techniques.

Firewall





- A firewall is a network security system that blocks unauthorized access to a private network.
- It can be a combination of hardware and software.
- Its main purpose is to prevent unauthorized users from accessing private networks, especially on the internet.
- A firewall monitors and controls network traffic based on predetermined security rules.
- It acts as a barrier between a trusted network and an untrusted network like the Internet.
- Firewalls are commonly used in personal and enterprise settings, and many devices, such as Mac, Windows, and Linux computers, have built-in firewall protection.
- They are widely recognized as a crucial part of network security.

What Firewalls Do?

Basically, firewalls need to be able to perform the following tasks:

- Defend resources
- Validate access
- Manage and control network traffic
- Record and report on events

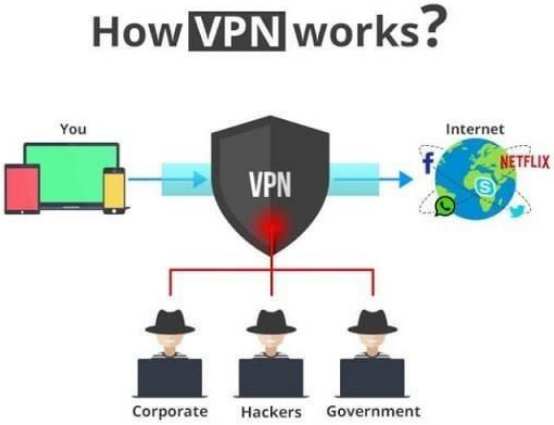
Advantages of firewall

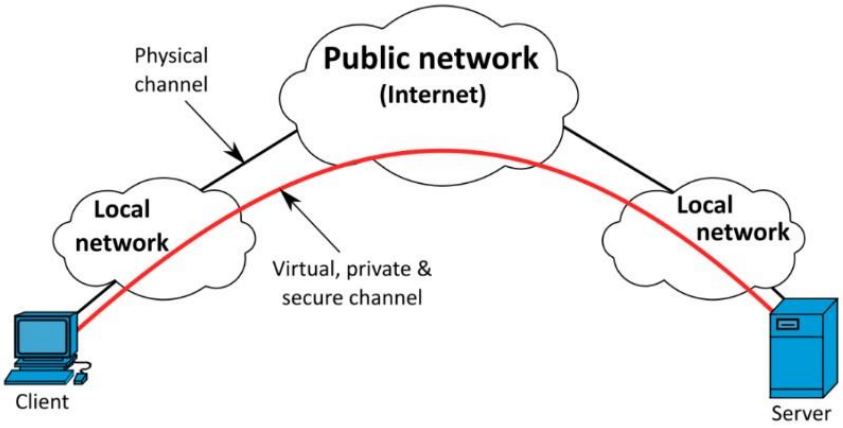
1. Network Isolation
2. Monitor Network Traffic
3. Protection against Trojans
4. Prevent Hackers
5. Access Control
6. Better Privacy

Disadvantages of firewall

1. Costly implementation
2. User Restriction
3. Reduced Performance
4. Defenseless against few other Malware Attacks

Virtual Private Network (VPN)





- A VPN is a service that protects our online privacy and sensitive data.
- It encrypts our internet traffic and routes it through a server.
- This makes it more difficult for anyone to track our online activity or steal our data.
- It extends a private network over a public network.
- With a VPN, our devices can send and receive data as if they were directly connected to the private network.
- VPNs are often used by businesses to allow employees to securely access corporate networks from home or while traveling.

- They can also be used by individuals to protect their privacy and security while browsing the internet.
- Users may need to authenticate themselves to access the VPN.

How VPN works?

1. We connect to a VPN server.
2. Our internet traffic is encrypted.
3. Our traffic is routed through the VPN server.
4. Our traffic is decrypted.
5. Our traffic is sent to the internet.

The VPN server acts as a middleman between our computer and the internet. This means that anyone who tries to track our online activity or steal your data will only see the encrypted traffic that is being sent to the VPN server. They will not be able to see the websites that we are visiting or the data that we are sending and receiving.

What does VPN do? Application/Advantages of VPN

- **Hides IP address:** Masking our IP address is essential to becoming private online. A VPN makes sure that our city, country, and torrent download history aren't linked to our identity.
- **Protects us on public Wi-Fi**: A VPN encrypts our online data and helps to secure our personal information when we use free Wi-Fi in airports or anywhere else.
- **Unlocks blocked websites**: We can unblock sites by connecting to a VPN server in a different country. Access to various websites is restricted in many countries due to growing internet censorship or geo-blocking.
- **Protects online identity:** With VPN we can protect ourself from data theft, tracking, surveillance, and commercial targeting.
- **Secures crypto assets:** Encrypt our data and avoid malware. Make sure our wallet cannot be traced and identified via our IP address.
- **Access a Business Network While Traveling:** VPNs are frequently used by business travelers to access their business' network, including all its local network resources, while on the road. The local resources don't have to be exposed directly to the Internet, which increases security.
- **Access Home Network While Travelling:** we can also set up our own VPN to access our own network while travelling. This will allow us to access a Windows Remote Desktop

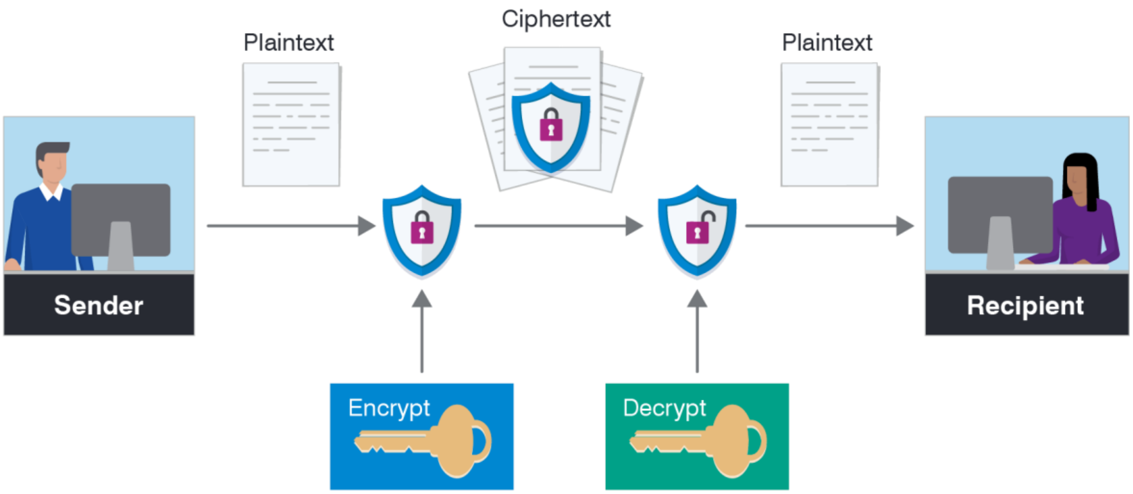
over the Internet, use local file shares, and play games over the Internet as if we were on the same LAN (local area network).

- **Hides our Browsing Activity From our Local Network and ISP:** If we want to hide our browsing activity for a bit more privacy, we can connect to a VPN. The local network will only see a single, secure VPN connection.
- **VPN makes online gaming better.**
- **It protects against cyber-attack.**
- **VPN offers secure torrenting.**
- **VPN can bypass firewall.**
- **VPNs Might Help us Avoid Online Price Discrimination**

Disadvantages of VPN

- VPNs can sometimes slow down our online speeds.
- Using wrong VPN can put our privacy in danger.
- Quality VPN will cost more money.
- Not all devices natively support VPNs.
- VPNs may have legality issues in some regions.

Encryption:



Different keys are used to encrypt and decrypt messages

- Encryption helps us to secure data that we send, receive, and store.
- It can consist text messages saved on our cell-phone, logs stored on our fitness watch, and details of banking sent by our online account.

- **Encryption** is the transformation of information from one form (plain-text) to another (cipher-text).
- **Decryption**, the opposite of encryption, is the transformation of encrypted information (cipher-text) back into an intelligible form (plain-text).

Types of Encryptions:

There are two types of encryptions schemes as listed below:

- Symmetric encryption
- Asymmetric encryption

Symmetric Key encryption

- Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.

Public Key encryption

- Public key encryption algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.

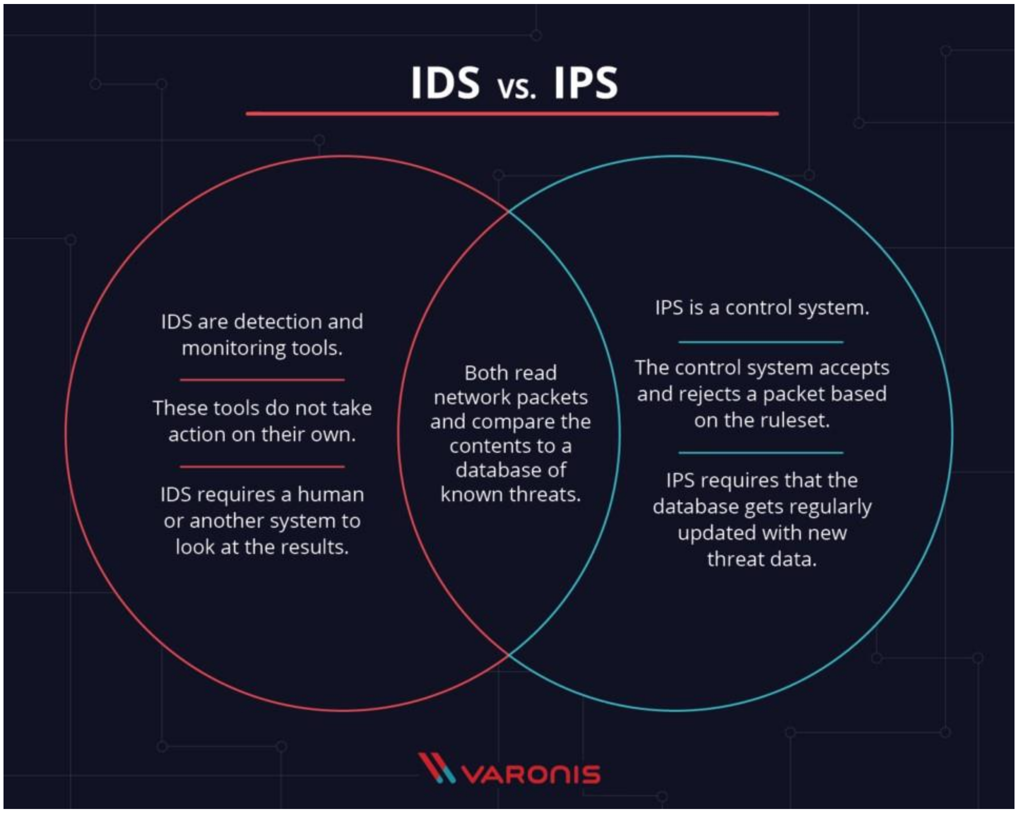
Advantages of encryption:

1. Encryption provides privacy.
2. Encryption helps move to the cloud.
3. When you own the keys, you can easily decommission/deprovision.
4. Encryption key services prevent service providers from accessing your data.
5. Encryption provides confidence that your backups are safe.

Intrusion Detection

- Intrusion detection involves monitoring network traffic for suspicious activity and sending alerts when such activity is found.
- Intrusion detection is commonly done using a system called an Intrusion Detection System (IDS).
- An IDS is a software or hardware tool that scans networks or systems to detect harmful activity or policy violations.
- Any malicious activity is typically reported to an administrator or collected centrally using a security information and event management (SIEM) system.
- A SIEM system combines information from multiple sources and uses filtering techniques to distinguish between malicious activity and false alarms.
- Intrusion prevention systems (IPS) are a type of security tool that falls under this classification.

Intrusion detection system vs Intrusion prevention system



IDS vs. IPS

IDS are detection and monitoring tools.

These tools do not take action on their own.

IDS requires a human or another system to look at the results.

Both read network packets and compare the contents to a database of known threats.

IPS is a control system.

The control system accepts and rejects a packet based on the ruleset.

IPS requires that the database gets regularly updated with new threat data.

Anti-Malicious Software

- An anti-malicious is a software that protects the computer from malware such as spyware, adware, and worms.
- It scans the system for all types of malicious software that manage to reach the computer.
- An anti-malicious program is one of the best tools to keep the computer and personal information protected.
- An anti-malicious is designed to eliminate malware from the computer.
- Although it has similarities with antivirus, an anti-malware program is different from antivirus.
- An anti-malware program has more advanced features and broader coverage. It addresses spyware, spam, and other threat issues that antivirus doesn’t.
- Anti-malicious software is designed to find known viruses and oftentimes other malware such as Ransomware, Trojan Horses, worms, spyware, adware, etc., that can have a detrimental impact to the user or device.

Features of Anti-malicious Software

- Real Time Scanning
- Automatic Updates
- Protection for Multiple Apps
- Auto Clean
- Fight against all types of malwares
- Web and e-mail Protection

Benefits of Anti Malware Software

An anti-malware program has many benefits, particularly keeping your computer secure. But that's not all anti malware has to offer, you can benefit from anti malware in many ways.

- **You're protected from hackers**- hackers gain access to your computer through malware. With the anti-malware installed, you can browse the web safely.
- **Your privacy is protected**- cyber criminals use your personal information to their advantage. An anti-malware prevents any software that steal personal from installing.
- **Your valuable files are secured**- if malware and viruses are out of the computer, you can be assured that your data are protected.
- **Your software is up-to-date**- nobody wants outdated software. An anti-malware keeps your software updated. It will remind you if a new version or an update is available online.
- **Your computer is free of junk**- an antimalware notifies you if junks are consuming your computer memory, so you can free up some space. This eliminates useless files stored in your computer.

Secure software and Browser Security:

Secure Software

- The protection of data and programs used in computer system is known as software security.
- Software security provides barriers and other cyber-tools that protect programs, files, operation systems and the information flow to and from a computer.
- Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly under such potential risks.
- Security is necessary to provide integrity, authentication and availability.

How to keep software safe

1. Protect Your Database from SQL Injection.
2. Validate Input Data Before You Use It or Store It.
3. Patch your software and systems.
4. Educate and train users.
5. Enforce least privilege (Permissions).
6. Monitor user activity.
7. Encrypt the data.
8. Use antivirus.

Browser Security:

Browser security is the application of Internet security to web browsers in order to protect networked data and computer systems from breaches of privacy or malware. Security exploits of browsers often use JavaScript, sometimes with cross-site scripting (XSS) .

How to keep browser secure

- Keep your browser software up-to-date.
- Review your browser's security settings and preferences.
- If you do not need pop-ups, disable them or install software that will prevent pop-up windows. Pop-ups can be used to run malicious software on your computer.
- Install an adblocker.
- Install browser add-ons, plug-ins, toolbars, and extensions sparingly and with care.
- Private Web Browsing.
- Use VPN.

SSL and IPSec

SSL

□ SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol.

□ It is a networking protocol designed for securing connections between web clients and web servers over an insecure network and transmitting private documents via the Internet.

□ It was first developed by Netscape in 1995 for the purpose of ensuring

  - Privacy
  - Authentication
  - Encryption
  - Integrity
  - Non-repudiability
- SSL is the predecessor to the modern TLS encryption used today.
- SSL has not been updated since SSL 3.0 and has been replaced by the Transport Layer Security (TLS) protocol.

SSL can be used to secure:

- Online credit card transactions or other online payments.
- Intranet-based traffic, such as internal networks, file sharing, extranets and database connections.
- Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
- The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.

IPsec

- IPsec is suite of protocols to provides security services during communications between networks.
- It supports network level peer authentication, data origin authentication, data integrity, data encryption and data decryption.

Key Features of IPsec are:

1. **Confidentiality**: by encrypting our data, nobody except the sender and receiver will be able to read our data.
2. **Integrity**: we want to make sure that nobody changes the data in our packets. By calculating a hash value, the sender and receiver will be able to check if changes have been made to the packet.
3. **Authentication**: the sender and receiver will authenticate each other to make sure that we are really talking with the device we intend to.
4. **Anti-replay:** even if a packet is encrypted and authenticated, an attacker could try to capture these packets and send them again. By using sequence numbers, IPsec will not transmit any duplicate packets.

Differences between IPSec and SSL

Sr. No.	Key	IPSec	SSL
1	Concept	IPSec, Internet Protocol Security, is a suite of protocols to provide security for internet protocol.	SSL, is a secure protocol to send information securely over internet.
2	Layer	IPSec works in internet layer of OSI model.	SSL works in transport and application layer of OSI model.
3	Configuration	IPSec is complex to configure.	SSL is simple to configure.
4	Usage	IPSec is used to secure VPN, Virtual Private Network.	SSL is used to secure web-based communications/ transactions.
5	Installation	Installation is vendor neutral.	Installation is vendor specific.
6	Changes in OS	Changes required to OS during implementation.	No changes required to OS during implementation.
7	Changes to Application	No changes required to Application during implementation.	Changes are required to Application during implementation.
8	Location	IPSec is present in OS space.	SSL is present in User space.