CYBER SECURITY IN NETWORK SECURITY

PRESENTED BY: **P.RAGUL**

THE KAVERY ENGINEERING COLLEGE

Network Security

Network Security

Network security is defined as the activity created to protect the integrity of your network and data. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.

Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. This is a broad, all-encompassing phrase that covers software and hardware solutions, as well as procedures, guidelines, and setups for network usage, accessibility, and general threat protection.

The most basic example of Network Security is password protection which the user of the network chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as:

1. Users
2. Locations
3. Data
4. Devices
5. Applications

Types of Network Security

The few types of network securities are discussed below:

- Access Control
- Antivirus and Anti-Malware Software
- Cloud Security
- Email Security
- Firewalls
- Application Security
- Intrusion Prevention System(IPS)

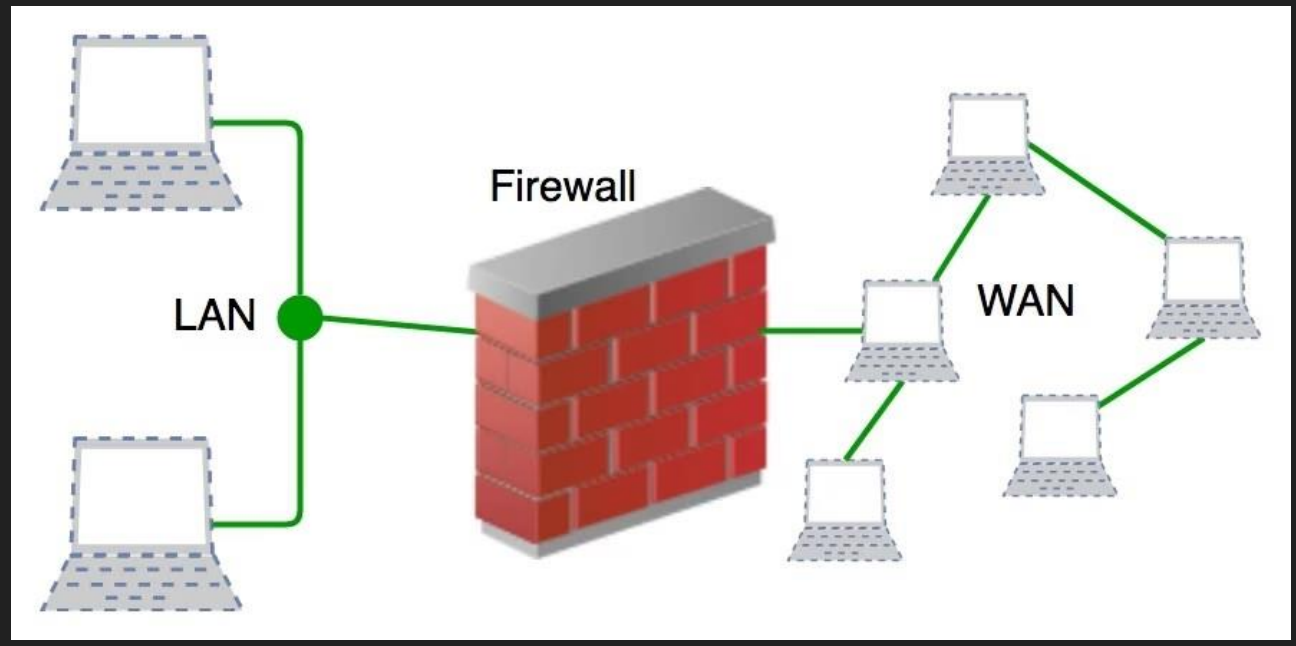
1. Access Control: Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.

2. Antivirus and Anti-malware Software: This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.

3. Cloud Security: This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

4. Email Security: Email Security is defined as the process designed to protect the Email Account and its contents safe from unauthorized access. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.

5. Firewalls: A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.



6. Application Security: Application security denotes the security precautionary measures utilized at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever.

7. Intrusion Prevention System(IPS): An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

Working on Network Security

The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data.
These levels are:

- Physical Network Security
- Technical Network Security
- Administrative Network Security

1. Physical Network Security: This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. The same can be achieved by using devices like biometric systems.

2. Technical Network Security: It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.

3. Administrative Network Security: This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Benefits of Network Security

Network Security has several benefits, some of which are mentioned below:

- Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.

•Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.

•It overall protects the reputation of the organization as it protects the data and confidential items.

The following are the main benefits of network security:

•**Functionality.** Network security ensures the ongoing high performance of the networks that businesses and individual users rely on.

Privacy and security. Many organizations handle user data and must ensure the confidentiality, integrity and availability of data on a network, known as the *CIA triad*. Network security prevents the security breaches that can expose PII and other sensitive information, damage a business's reputation and result in financial losses.

- **Intellectual property protection.** Intellectual property is key to many companies' ability to compete. Securing access to intellectual property related to products, services and business strategies helps organizations maintain their competitive edge.

- **Compliance.** Complying with data security and privacy regulations, such as HIPAA and GDPR, is legally required in many countries. Secure networks are a key part of adhering to these mandates.

Challenges of network security

- **Evolving network attack methods.** The biggest network security challenge is the rate at which cyber attacks evolve. Threat actors and their methods constantly change as technology changes. For example, new technology, such as blockchain, has led to new types of malware attacks, such as cryptojacking. As a result, network security defense strategies must adapt to these new threats.

- **User adherence.** As mentioned, security is every network user's responsibility. It can be difficult for organizations to ensure that everyone is adhering to network security best practices, while simultaneously evolving those strategies to address the newest threats.

- **Remote and mobile access.** More companies are adopting bring your own device policies, which means a more distributed and complex network of devices for organizations to protect. Remote work is also more prevalent. This makes wireless security more important, as users are more likely to be using a personal or public network when accessing company networks.

- **Third-party partners.** Cloud providers, managed security services and security product vendors often get access to an organization's network, opening new potential vulnerabilities.

Conclusion

The conclusion of network security emphasizes the critical importance of protecting data and systems from unauthorized access, misuse, or modification. It underscores the need for robust security measures, including firewalls, encryption, intrusion detection systems, and regular updates to mitigate emerging threats. Continuous vigilance, proactive monitoring, and user education are essential to maintaining a secure network environment. Additionally, fostering a culture of security awareness and compliance throughout an organization is vital for ensuring the integrity, confidentiality, and availability of sensitive information and services.