Network security refers to any activities designed to protect the network.

Network security targets a variety of threats and stops them from entering or spreading on your network.

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Key principles of security:

Confidentiality:

Only sender, intendent receiver should understand message content,

- Sender encrypts message.
- Receiver decrypts message.

Authentication:

Sender, receiver want to confirm identity of each other.

Message integrity:

Sender receiver wants to ensure message not altered without detection. Data must be arrived at the receiver exactly as it was sent.

Accessibility & availability:

Service must be accessible and available to users.

Non-Reduplication:

Non reduplication means that a receiver must be able to prove that a receiver message came from a specific sender.

Privacy is achieved through encryption of plain text and decryption of the Cipher text.

Authentication, integrity and non-reduplication are achieved through a method called digital signature.

Access authorization is a security procedure in which the identity of a sender is verified prior to the sending of a message.

A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

Network security components often include :

- Anti-virus and anti-spyware.
- Firewall, to block unauthorized access to your network.
- Intrusion prevention systems (IPS), to identify fast-spreading threats.
- Virtual Private Networks (VPNs), to provide secure remote access.

Related posts:

1. Types of Attack
2. Security threats
3. Computer and cyber security
4. Intrusion detection tool
5. Categories of security assessments
6. Security terminologies and principals
7. Intoduction to intrusion
8. Intrusion detection tool
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer