Types of network Security features :-

1. Firewalls : They use a set of defined rules to allow or block traffic. A firewall can be ~~both~~ hardware, software or both.

2. Email Security : An email security application blocks incoming attacks and controls outbound message to prevent the loss of sensitive data.

3. Antivirus and antimalware Software :- "Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware and Spyware. The best antimalware programs not only scan your malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

4. Network Segmentation : Software-defined segmentation puts network traffic into different classifications and make enforcing security policies easier.

5. Access control : Not every user should have access to your network. To keep

Date.....

out potential attackers, you need to recognize each user and each device. Then you can enforce your Security policies. you can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

6. Application Security :- Application Security encompasses the hardware, Software, and processes you use to close those.
7. Web Security :- Web Security also refers to the steps you take to protect your own website.
8. Wireless Security :- Wireless Security networks are not as Secure as wired ones. you need products specifically designed to protect a wireless network.

Cryptography :-

It is the Science of information Security. Cryptography include techniques such as merging words with images and other way to hide information in storage.

Cryptography is most associated with scrumbling plaintext (ordinary text) into cipher text (incryption) then plaintext (ordinary text).

Cryptography concerned with following four objectives :-

1) Confidentiality :- It means that the content of a message when transmitted across a network must remain confidential i.e only the intended receiver and no one else should be able to read the message.

2) Data Integrity :-
Data integrity refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

3) Non-repudiation :-
The sender of information can deny at the later stage.

4) Authentication :-
The sender and reciever can conform each other identity and the original destination of the information.