Dissect the basic concept of cryptography and firewall.

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank card, computer passwords, & ecommerce. Modern cryptography techniques include algorithms and ciphers that enable the encryption and decryption of information, such as 128-bit and 256-bit encryption keys.

Firewall is a network security device that prevent unauthorized access to a network. It inspects access to a network. It inspects incoming and outgoing traffic using a set a security rules to identify and block threats. A firewall can be physical hardware, digital software. software as a service (SaaS) or a virtual private cloud.

Interpret the Dos influencing techniques: Leaky Bucket & Token Bucket algorithm.

Leaky bucket:- In computer networking, the leaky bucket algorithm regulates the speed at which data is transferred. It is a method that ensures that data transmission rates are kept to the maximum allowed level to check the flow of information through a network. The algorithm visualises a "bucket" with a specific data capacity.

Token bucket :- A token bucket is a traffic shaping method that operates by using smaller tokens at the byte level to control the transmission of packet, ensuring that traffic adheres to predefined service level agreements and helps in minizing downstream congestion in egress switch ports. A token bucket is a traffic shaping method that operates by using smaller tokens at the byte level to control the transmission of packets.

Q5) a) Classify the DNS & DDNS ; IPV4 & IPV6.

Ans a) DDNS (Dynamic Domain Name System) :- It is a method of automatically updating a name server in the Domain Name Server (DNS), often in real-time, with the active DDNS configuration of its configured hostnames, addresses, or other information. In DDNS, when a binding between a name and an address is determined, the information is sent usually by DHCP (Dynamic Host Configuration Protocol).

DNS (Domain Name System) :- The DNS is like the internet's phonebook. It helps you find websites by translating easy-to-remember names (like www.example.com) into the numerical IP addresses (like 192.0.2.1) that computers use to locate each other on the internet. Without DNS, you would have to remember long strings of numbers to visit your favorite websites.

IPV4:- IPV4 addresses consist of two things: the network address and the host address. It stands for Internet protocol version four. It was introduced in 1981 by DARPA and was the first deployed version in 1982 for production on SATNET and on the ARPANET in January 1983. IPV4 addresses are 32-bit integers that have to be expressed in Decimal Notation.

IPV6:- IPV6 is based on IPV4 and stands for Internet Protocol Version 6. It was first introduced in December 1995 by Internet Engineering Task Force. IP version 6 is the new version of Internet Protocols, which is way better than IP version 4 in terms of complexity and efficiency. IPV6 is written as a group of 8 hexadecimal numbers separated by colon(:). It can be written as 128 bits of 0s and 1s.

8. Identify the main concept of UDP & TCP along with quality of services.

Ans TCP and UDP:- differences blw the protocols. The main differences between TCP (transmission control protocol) and UCP (user datagram protocol) is that TCP is a connection-based protocol and UDP is connectionless. While TCP is more reliable, it transfers data more slowly. UDP is less reliable but works more quickly. In digital communication, networking protocols, such as TCP and UDP protocols, play a crucial role in ensuring seamless data exchange. Choosing the right protocol is essential to influence performance, data integrity, and user experience (UX).

Q56 Evaluate the unicast Routing Protocol working along with forwarding protocol.

Ans

Unicast Routing Protocol refers to a protocol specifically designed for mobile ad hoc Network (MANETs) to efficiently transmit data packets from a single source to a single destination. These protocols are not directly applicable to Vehicular Ad hoc Networks (VANETs) due to their unique characteristics. Even though several unicast routing protocols have been developing for MANETs [4,5,32,6,9 – 12,16, 18,20, 28 – 31, 33, 40, 41, 46, 52 – 54, 57, 60, 61, 66, 70] because of the unique characteristics of VANETs, these protocols cannot be directly used in VANETs efficiently. Hence, because of the expected potential impact of VANETs, several researches have developed unicast routing protocols that are suitable for VANETs.