25. Discuss the role of Windows Firewall in Windows Server and how to configure it.

Windows Firewall plays a vital role in enhancing server security by controlling the flow of network traffic. It helps protect the system from malicious attacks by allowing or blocking traffic based on specific rules.

To configure Windows Firewall:
1. Open Server Manager > Tools > Windows Defender Firewall with Advanced Security*.
2. Choose *Inbound Rules* or *Outbound Rules* to view or create new rules.
3. Click *New Rule*, select type (Port, Program, etc.), and follow the wizard.
4. Set rule conditions, actions (Allow/Block), and apply the rule to required profiles.

26. What is Network Address Translation (NAT) in Windows Server, and how do you configure it?

NAT (Network Address Translation) allows devices on a private network to access external networks (like the internet) using a single public IP. It enhances security by hiding internal IP addresses and reduces the need for multiple public IPs.

To configure NAT in Windows Server:
1. Install *Remote Access* role with the *Routing* service.
2. Open *Routing and Remote Access (RRAS)*, right-click the server, and select *Configure and Enable Routing and Remote Access*.
3. Select *Network Address Translation (NAT)*, choose the internet-connected interface.
4. Configure the private interface to allow internal clients.

27. Explain the concept of Dynamic Host Configuration Protocol (DHCP) and how to configure it in Windows Server 2016.

DHCP automatically assigns IP addresses and other network settings to client devices, reducing manual configuration and preventing IP conflicts.

To configure DHCP in Windows Server 2016:
1. Add the *DHCP Server* role via *Server Manager*.
2. Authorize the server in Active Directory.
3. Open *DHCP Manager*, create a new scope (define IP range, subnet mask, lease duration).
4. Set additional options such as default gateway and DNS server.

28. Describe the process of configuring DNS (Domain Name System) in Windows Server.

DNS translates human-readable domain names into IP addresses. It enables users and systems to access websites or devices easily using names instead of IPs.

To configure DNS:

1. Install the *DNS Server* role via *Server Manager*.
2. Open *DNS Manager*, create a *Forward Lookup Zone* (for name-to-IP resolution).
3. Add records (A, CNAME, MX, etc.) in the zone.
4. Optionally, configure a *Reverse Lookup Zone* to resolve IPs to hostnames.

29. What is Server Manager, and how do you use it to manage servers in Windows Server?

Server Manager is a centralized console used to manage local and remote Windows Servers. It simplifies administrative tasks across multiple servers.

Key features and uses:
1. Add or remove server roles and features.
2. Monitor performance, events, and services.
3. Manage multiple servers from a single console.
4. Use PowerShell integration for automation and bulk operations.

30. Discuss the role of Remote Desktop Services (RDS) in Windows Server 2016 or 2019 and how to configure it.

RDS allows users to remotely access applications or full desktops hosted on a Windows Server. It supports centralized application deployment and remote workforce.

To configure RDS:
1. Use *Server Manager* > *Add Roles and Features* > select *Remote Desktop Services Installation*.
2. Choose *Quick Start* or *Standard Deployment* based on need.
3. Install roles: RD Session Host, RD Licensing, RD Connection Broker.
4. Publish RemoteApps or full desktops, configure user access, and set up licensing.