Module: 13- Networking with Windows Server

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

ANS - Role of Windows Firewall in Windows Server:-

- Network Traffic Filtering: - Windows Firewall examines network traffic and blocks or allows it based on predefined rules. This helps prevent unauthorized access to your server and protects against malicious attacks.
- Protection Against Threats: - By filtering network traffic, Windows Firewall can help prevent malware from entering your server and limit the spread of threats within your network.
- Enhanced Security**: -** Windows Firewall provides an additional layer of security to your server, complementing other security measures like antivirus software and intrusion detection systems.

1. Configuring Windows Firewall :-

    1. Access the Windows Firewall with Advanced Security console
    2. Configure Inbound and Outbound Rules
    3. Define Rule Criteria
    4. Apply the Rule

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

ANS - Network Address Translation in Windows Server is a service that allows multiple devices on a private network to share a single public IP address to access the internet.

❖ Configuring Network Address Translation :-

1. Open Server Manager and add the Routing and Remote Access service.
2. Configure RRAS for NAT:-

- Open the Routing and Remote Access console.
- Right-click on the server and select "Configure and Enable Routing and Remote Access".
- Select "Custom Configuration" and click "Next".
- Select "NAT" and click "Next".
- Select the network interface that is connected to the internet and click "Next".
- Configure the NAT settings, such as the public IP address and the private IP address range.

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

ANS - Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of assigning IP addresses and other network configuration parameters to devices on a network. Instead of manually configuring each device, a DHCP server dynamically leases IP addresses and related information, simplifying network administration.

Configuring DHCP in Windows Server 2016:

1. Install the DHCP Server Role:
   - Open Server Manager and add the DHCP Server role.
2. Configure a DHCP Scope:
   - Open the DHCP Management console.
   - Right-click on your DHCP server and select "New Scope."
   - Provide a name and description for the scope.
   - Define the IP address range for the scope.
   - Specify the subnet mask.
   - Configure any exclusions within the IP address range.
   - Set the lease duration.
   - Configure DHCP options (e.g., default gateway, DNS server address). These are crucial. You *must* provide a valid default gateway and DNS server address for clients to function correctly.
   - Activate the scope.
3. Authorize the DHCP Server: In an Active Directory environment, you need to authorize the DHCP server to prevent rogue DHCP servers from operating on your network. This is done through the DHCP Management console.

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

ANS –

❖ Configuring DNS in Windows Server :-

1. Install the DNS Server Role:

- Open Server Manager.
- Click "Add roles and features."
- Select "Role-based or feature-based installation."
- Choose your server.
- Select the "DNS Server" role.
- Add any required features.
- Confirm the installation and click "Install."

2. Configure DNS Zones:

A zone is a portion of the DNS namespace for which a DNS server is authoritative. You'll typically create two main types of zones:

- Forward Lookup Zone: Resolves domain names to IP addresses.
- Reverse Lookup Zone: Resolves IP addresses to domain names.

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

ANS - Server Manager is a central management console in Windows Server that allows you to manage local and remote servers from a single interface .It provides a comprehensive overview of your servers and simplifies many administrative tasks.

How to Use Server Manager:

1. Open Server Manager:
   - You can usually find it in the Start Menu or on the taskbar.
2. Connect to Servers:
   - By default, Server Manager shows the local server.
   - To manage other servers, you need to add them to Server Manager. You can do this by clicking "Manage" and then "Add Servers." You can add servers by name, IP address, or by searching Active Directory.
3. Navigate the Interface:
   - The left pane provides access to different sections of Server Manager, including the Dashboard, Local Server, All Servers, and specific roles.

4. Perform Tasks:
    - Use the various sections and tools within Server Manager to perform administrative tasks. For example, you can use the "Add Roles and Features" wizard to install a new server role, or you can use the "Services" section to manage services on a server.

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

ANS - Remote Desktop Services (RDS), formerly known as Terminal Services, is a crucial component of Windows Server that enables users to access and interact with applications and desktops hosted on a remote server. It allows for centralized application management, improved security, and greater flexibility in how users access their work environments.

❖ Configuring RDS in Windows Server :-

1. Install the Remote Desktop Services Role:

- Open Server Manager.
- Add the "Remote Desktop Services" role.

2. Choose a Deployment Scenario:

- Standard Deployment: This is the typical scenario for deploying a full RDS environment with multiple servers handling different roles (like RD Session Host, RD Connection Broker, RD Web Access, etc.).
- Quick Start: A simplified deployment for testing or small environments, where all roles are installed on a single server. Not recommended for production.

3. Configure Server Roles (Standard Deployment): This is the more complex but robust setup:

- RD Session Host: This server hosts the applications and desktops that users access. You'll need at least one RD Session Host server.
- RD Web Access (Optional but Recommended): Allows users to access remote apps and desktops through a web browser.
- RD Licensing Server: Manages RDS client access licenses (CALs). You *must* have a licensing server and sufficient CALs for your users.

4. Create a Session Collection (or Virtual Desktop Collection for VDI):

- A session collection defines the applications and desktops that are available to users. You can publish individual applications or a full desktop.

5. Configure Client Settings:

- Users can connect to RDS resources using the Remote Desktop Connection client or through RD Web Access.