**MODULE 13 Networking with Windows Server**

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

Role of Windows Firewall in Windows Server

Windows Firewall in Windows Server acts as a security feature to protect the server by filtering incoming and outgoing network traffic. It blocks unauthorized access while allowing legitimate communication based on predefined rules.

How to Configure Windows Firewall

1. Access Firewall Settings: Open Control Panel > Windows Defender Firewall > Advanced Settings.
2. Inbound/Outbound Rules:
   * Create or modify rules under Inbound Rules or Outbound Rules to allow or block specific traffic.
3. Enable/Disable Firewall: Use the Domain, Private, or Public Profile tabs to enable/disable the firewall for each network type.
4. Exceptions: Add programs, ports, or services as exceptions in the allowed list.
5. Command-Line Configuration: Use netsh adv-firewall or PowerShell cmdlets like New-Net Firewall Rule for advanced setups.

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

Network Address Translation (NAT) in Windows Server

NAT allows multiple devices on a private network to access external networks (e.g., the internet) using a single public IP address. It translates private IP addresses to a public IP for outbound traffic and vice versa for inbound traffic.

How to Configure NAT

1. Install NAT Role:
   * Open Server Manager, add the Remote Access role, and select the Routing feature.
2. Configure NAT:
   * Open Routing and Remote Access tool.
   * Right-click the server name and select Configure and Enable Routing and Remote Access.
   * Choose NAT as the configuration type.
3. Assign Network Interfaces:
   * Designate one interface as the public-facing network and another as the private network.
4. Configure Address Pool (Optional):
   * Set up a public IP address pool for NAT translations if needed.

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

Dynamic Host Configuration Protocol (DHCP)

DHCP automatically assigns IP addresses and other network configuration settings (e.g., subnet mask, default gateway) to devices on a network, reducing manual configuration.

How to Configure DHCP in Windows Server 2016

1. Install DHCP Role:
   * Open Server Manager, add the DHCP Server role, and complete the wizard.
2. Authorize DHCP:
   * Open DHCP Manager, right-click the server, and select Authorize.
3. Create a Scope:
   * Right-click on IPv4 and select New Scope.
   * Define the IP address range, exclusions, lease duration, and other options.
4. Configure Options:
   * Set up options like default gateway (router), DNS servers, and WINS servers.
5. Activate Scope:
   * Right-click the new scope and select Activate.

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

Configuring DNS in Windows Server

1. Install DNS Role:
   * Open Server Manager, add the DNS Server role, and complete the wizard.
2. Create a Forward Lookup Zone:
   * Open DNS Manager and select New Zone.
   * Choose Primary Zone and configure a zone name (e.g., example.com).
3. Add Resource Records:
   * Add records like A (Host), CNAME (Alias), MX (Mail), or PTR (Reverse Lookup) based on requirements.
4. Configure Reverse Lookup Zone (Optional):
   * Create a reverse zone to resolve IP addresses to domain names.
5. Test DNS:
   * Use commands like nslookup to verify name resolution.

29. **Role of Remote Desktop Services (RDS)**

RDS enables remote access to desktops, applications, and virtualized environments hosted on a Windows Server. It supports centralized resource management, secure access, and multi-user environments.

**How to Configure RDS**

1. **Install RDS Role**:
   * Open **Server Manager**, add the **Remote Desktop Services** role, and select the desired RDS components (e.g., RD Session Host, RD Licensing).
2. **Configure RDS Deployment**:
   * Use the **Remote Desktop Services Deployment Wizard** to configure session-based or virtual desktop deployments.
3. **Set Up RD Licensing**:
   * Install and activate RD Licensing and add licenses.
4. **Publish Applications**:
   * Use **RemoteApp Manager** to publish applications for remote access.
5. **Enable Remote Desktop**:
   * Configure firewall rules and enable remote desktop access via **System Properties > Remote**.