**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**

Windows Firewall is a security feature that controls incoming and outgoing network traffic based on predefined security rules. It helps to:

* Block unauthorized access while allowing legitimate traffic.
* Protect the server from network attacks like malware and hacking attempts.
* Manage traffic based on rules.
* Improve network security by defining firewall policies for different profiles.

**How to Configure Windows Firewall in Windows Server**

**Open Windows Firewall**

1.Open Server Manager > Click Tools > Select Windows Defender Firewall with Advanced Security.

2. Click Inbound Rules or Outbound Rules

3. Click New Rule, select Rule Type.

4. Choose Port > Select TCP and enter 80.

5. Enable or Disable Firewall

6. Manage Firewall via PowerShell

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

**ANS:** Network Address Translation (NAT) is a method that allows multiple devices on a private network to access the internet using a single public IP address. It acts as a gateway between the internal network and external networks.

**How to Configure NAT in Windows Server**

**Step 1: Install the Remote Access Role**

1. Open Server Manager > Click Manage > Select Add Roles and Features.
2. Choose Role-based or feature-based installation > Select Remote Access.
3. Under Role Services, check Routing and click Next.
4. Click Install and wait for completion.

Step 2: Configure NAT

1. Open Routing and Remote Access (RRAS) (rrasmgmt.msc in Run).
2. Right-click the Server Name > Select Configure and Enable Routing and Remote Access.
3. Choose Network Address Translation (NAT) and click Next.
4. Select the interface connected to the internet as the Public Interface.
5. Select the interface connected to the internal network as the Private Interface.
6. Click Finish and start the RRAS service.

* Use ipconfig on client machines to check assigned private IPs.

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 service that automatically assigns IP addresses to devices in a network, eliminating the need for manual configuration.

**Benefits of DHCP**

* Automates IP address assignment, reducing configuration errors.
* Prevents IP conflicts by managing address allocation.
* Supports centralized IP management for large networks.
* Simplifies network configuration for new devices.

**How to Configure DHCP in Windows Server 2016**

**Step 1: Install the DHCP Role**

1. Open Server Manager > Click Manage > Select Add Roles and Features.
2. Select Role-based or feature-based installation.
3. Choose the server and select DHCP Server.
4. Click Next and Install.

**Step 2: Configure DHCP Scope**

1. Open DHCP Manager.
2. Expand the Server Name > Right-click IPv4 > Click New Scope.
3. Enter a Scope Name (e.g., "Office DHCP").
4. Define the IP Address Range (e.g., 192.168.1.100 - 192.168.1.200).
5. Set the Subnet Mask (default: 255.255.255.0).
6. Specify any Excluded Addresses (optional).
7. Set the Lease Duration (default: 8 days).
8. Configure Gateway (Router), DNS, and WINS settings if required.
9. Activate the scope to start assigning IPs.

**Step 3: Authorize the DHCP Server**

1. Open DHCP Manager.
2. Right-click the Server Name > Click Authorize.
3. Wait a few seconds, then refresh to see it as Active.

**Step 4: Verify DHCP Configuration**

* On a client machine, run ipconfig /renew to request a new IP.
* Use ipconfig /all to check if the client received the assigned DHCP IP.

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

**ANS:** DNS is a crucial service that resolves domain names into IP addresses. Follow these steps to configure DNS in Windows Server:

**Step 1: Install the DNS Role**

1. Open **Server Manager** and click on **Manage** > **Add Roles and Features**.
2. Select **Role-based or feature-based installation** and click **Next**.
3. Select your server and click **Next**.
4. Choose **DNS Server**, click **Add Features**, then click **Next**.
5. Click **Install** and wait for the installation to complete.

**Step 2: Configure DNS Zones**

1. Open **DNS Manager**.
2. Expand your server name, right-click **Forward Lookup Zones**, and select **New Zone**.
3. Choose **Primary Zone**, click Next, then enter a domain name (e.g., example.com).
4. Select **Allow dynamic updates** and complete the wizard.
5. Repeat the process for **Reverse Lookup Zone**.

**Step 3: Create DNS Records**

1. In **DNS Manager**, right-click your **Forward Lookup Zone** and choose **New Host (A or AAAA)**.
2. Enter the hostname and IP address.
3. Click **Add Host**.

Your DNS Server is now configured and ready to resolve domain names.

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

ANS:

Server Manager is a centralized management tool in Windows Server that allows administrators to configure, monitor, and manage server roles and features.

**Key Features of Server Manager:**

* **Role and Feature Management**: Add or remove roles like DNS, DHCP, and IIS.
* **Server Monitoring**: Provides an overview of server health and alerts.
* **Remote Management**: Allows control of multiple servers from a single console.
* **Event Viewer Integration**: Shows system logs and errors.

**How to Use Server Manager:**

1. Open **Server Manager** from the Start menu or type servermanager in Run.
2. Click **Local Server** to view system details.
3. Click **Manage** > **Add Roles and Features** to install new roles.
4. Use **Tools** to open utilities like DNS Manager, DHCP, and Active Directory.
5. Click **All Servers** to manage multiple servers from a single console.

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)** allows users to access a server remotely, providing virtual desktops and applications.

**Steps to Configure RDS:**

**Step 1: Install RDS Role**

1. Open **Server Manager**, click **Manage** > **Add Roles and Features**.
2. Select **Remote Desktop Services Installation**, then **Standard Deployment**.
3. Choose **Session-Based Desktop Deployment** and click **Next**.
4. Select a server for the roles:
   * **RD Connection Broker**
   * **RD Web Access**
   * **RD Session Host**
5. Click **Install** and wait for the installation to complete.

**Step 2: Configure Remote Desktop Licensing**

1. Open **Remote Desktop Licensing Manager** (licmgr.exe).
2. Right-click the server and choose **Activate Server**.
3. Follow the wizard and enter the licensing details.

**Step 3: Allow Users to Connect**

1. Open **System Properties** (sysdm.cpl in Run).
2. Go to the **Remote** tab and enable **Allow remote connections to this computer**.
3. Click **Select Users** and add users who can connect.

Now, users can connect using **Remote Desktop Connection (RDP)** with the server's IP or hostname.