

## **Module: 13- Networking with Windows Server**

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

**ANS:** -Windows Firewall is a security feature in Windows Server that helps control incoming and outgoing network traffic based on predefined security rules. It protects the server from unauthorized access, malware, and network-based threats.

### **Key Functions:**

- **Packet Filtering:** Filters network traffic based on rules.
- **Blocking Unauthorized Access:** Restricts access to specific applications and services.
- **Traffic Logging:** Keeps logs of blocked and allowed traffic for security analysis.
- **Integration with Group Policy:** Enables centralized firewall rule management in domain environments.

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

- 1. Open Windows Firewall:**
  - Open Server Manager - Tools - Windows Defender Firewall with Advanced Security.
- 2. Create Inbound/Outbound Rules:**
  - Navigate to Inbound Rules or Outbound Rules - Click New Rule.
  - Choose Port, Program, Predefined, or Custom Rule.
  - Define specific settings like ports or applications.
  - Set action: Allow or Block.
  - Assign the rule to specific profiles (Domain, Private, or Public).
- 3. Enable/Disable Firewall:**
  - In Windows Defender Firewall, click Turn Windows Defender Firewall on or off.
- 4. Allow Specific Apps or Ports:**

- Navigate to Allow an app or feature through Windows Defender Firewall.
- Select the required application and check the appropriate network profile.

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

**ANS:** -NAT is a feature that allows multiple devices on a private network to access the internet using a single public IP address. It is useful in scenarios where public IPv4 addresses are limited.

### **Types of NAT:**

- **Static NAT:** Maps a private IP to a public IP one-to-one.
- **Dynamic NAT:** Uses a pool of public IPs and assigns them dynamically.
- **PAT (Port Address Translation):** Translates multiple private IPs to a single public IP using different ports.

### **How to Configure NAT in Windows Server:**

#### **1. Install the NAT Role:**

- Open Server Manager - Click Manage - Add Roles and Features.
- Select Remote Access - Enable Routing - Click Next - Install.

#### **2. Configure NAT via Routing and Remote Access:**

- Open Routing and Remote Access via Server Manager.
- Right-click on the server - Configure and Enable Routing and Remote Access.
- Select Network Address Translation (NAT) - Choose the internet-connected interface.
- Configure the private network interface and enable NAT.

### **3. Test Connectivity:**

- Ensure client devices have proper IP and gateway configurations.
- Verify internet access via NAT.

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

**ANS;** - DHCP is a network protocol that automatically assigns IP addresses and network settings (subnet mask, default gateway, DNS) to devices on a network.

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

##### **1. Install the DHCP Role:**

- Open Server Manager - Click Add Roles and Features.
- Select DHCP Server - Click Next - Install.

##### **2. Authorize the DHCP Server:**

- Open DHCP Console - Right-click the server - Authorize.

##### **3. Create a DHCP Scope:**

- Expand the server node - Right-click IPv4 - New Scope.
- Define scope name and address range (e.g., 192.168.1.100 – 192.168.1.200).
- Set subnet mask and default gateway.
- Add DNS and WINS settings (if applicable).
- Activate the scope.

##### **4. Configure Reservations and Options (Optional):**

- Right-click Reservations - New Reservation to assign static IPs to specific devices.
- Configure scope options like default gateway, DNS, and lease duration.

#### **4. Describe the process of configuring DNS (Domain Name System) in Windows Server.**

**ANS:** -DNS translates domain names (e.g., example.com) into IP addresses.

#### **How to Configure DNS in Windows Server:**

##### **1. Install the DNS Role:**

- Open Server Manager - Add Roles and Features.
- Select DNS Server - Click Install.

##### **2. Configure Forward Lookup Zone:**

- Open DNS Manager - Right-click Forward Lookup Zones - New Zone.
- Choose Primary Zone - Enter domain name (e.g., example.com).
- Configure Dynamic Updates settings.

##### **3. Configure Reverse Lookup Zone (Optional, for PTR Records):**

- Right-click Reverse Lookup Zones – New Zone.
- Define network ID (e.g., 192.168.1).
- Create PTR records for IP-to-hostname mapping.

##### **4. Create Host (A) Records:**

- Right-click the zone – New Host (A or AAAA).
- Enter hostname and IP address.
- Optionally, create a PTR record.

##### **5. Configure Forwarders (Optional, for External Name Resolution):**

- Right-click the server - Properties - Forwarders.
- Add external DNS servers (e.g., 8.8.8.8 for Google DNS).

##### **6. Test DNS Configuration:**

- Use nslookup from the command prompt to verify resolution.

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

**ANS:** -Server Manager is a management console in Windows Server that allows administrators to monitor and configure servers.

### **Key Features:**

- **Dashboard View:** Provides an overview of server roles and status.
- **Role & Feature Management:** Enables the installation, configuration, and removal of server roles.
- **Event Logs & Performance Monitoring:** Displays system health, logs, and resource utilization.
- **Remote Management:** Manages multiple servers from a single console.

### **How to Use Server Manager:**

- 1. Open Server Manager:**
  - Press Windows + R – Type servermanager – Press Enter.
- 2. Add Remote Servers for Management:**
  - Click Manage - Add Servers → Enter the server name or IP.
- 3. Install and Configure Roles:**
  - Click Manage - Add Roles and Features - Select a server and role.
- 4. Monitor Server Health:**
  - Check alerts, performance metrics, and event logs.
- 5. Perform Remote Administration:**
  - Use PowerShell or MMC snap-ins for advanced tasks.

## **6. 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 applications and desktops remotely over a network.

### **Components of RDS:**

- **Remote Desktop Session Host (RDSH):** Hosts remote desktop sessions.
- **Remote Desktop Connection Broker (RDCB):** Manages session connections.
- **Remote Desktop Gateway (RDG):** Enables remote access over the internet.

### **How to Configure RDS in Windows Server:**

#### **1. Install RDS Role:**

- Open Server Manager - Click Add Roles and Features.
- Select Remote Desktop Services Installation - Choose Standard Deployment.

#### **2. Deploy RDS Components:**

- Select Session-Based Desktop Deployment.
- Add RD Connection Broker, RD Web Access, and RD Session Host roles.

#### **3. Configure Licensing (Required after 120 days trial):**

- Open Remote Desktop Licensing Manager.
- Activate the server and install licenses.

#### **4. Configure Remote Desktop Access:**

- Open System Properties - Enable Remote Desktop.
- Add allowed users under Select Users.

#### **5. Test Remote Desktop Connection:**

- Use `mstsc` (Remote Desktop Connection) from a client PC.
- Enter the server's IP and login credentials.