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

**1. Role of Windows Firewall in Windows Server and How to Configure It**

**ANS: Role of Windows Firewall in Windows Server**

Windows Firewall (now called **Windows Defender Firewall**) is an essential security feature in Windows Server that helps protect the system from unauthorized access, malware, and network-based threats. Its primary roles include:

* **Traffic Filtering**: Blocks or allows traffic based on predefined or custom rules.
* **Prevention of Unauthorized Access**: Restricts inbound and outbound network connections.
* **Integration with Group Policy**: Allows centralized firewall policy enforcement across multiple servers.
* **Network Isolation**: Prevents lateral movement of attackers within a network.
* **Advanced Security Features**: Supports IPsec for encryption and authentication.

**Configuring Windows Firewall in Windows Server**

1. **Open Windows Firewall**
   * Open **Server Manager** → Click **Tools** → Select **Windows Defender Firewall with Advanced Security**.
2. **Create an Inbound Rule**
   * Navigate to **Inbound Rules** → Click **New Rule**.
   * Choose the rule type (**Port**, **Program**, **Predefined**, or **Custom**).
   * If selecting **Port**, specify **TCP/UDP** and port number (e.g., 80 for HTTP).
   * Select **Allow or Block Connection** as per requirement.
   * Apply rule to **Domain, Private, or Public** profiles.
   * Name the rule and finish the setup.
3. **Create an Outbound Rule**
   * Similar to inbound rules but applies to outbound traffic.
4. **Enable or Disable Windows Firewall**
   * Open **Windows Defender Firewall** → Click **Turn Windows Defender Firewall on or off**.
   * Choose settings for different network profiles.
5. **Configure via PowerShell**

powershell

CopyEdit

# Enable Windows Firewall

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

# Allow inbound traffic on port 443 (HTTPS)

New-NetFirewallRule -DisplayName "Allow HTTPS" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow

**2. Network Address Translation (NAT) in Windows Server and How to Configure It**

**ANS: What is NAT in Windows Server?**

Network Address Translation (NAT) is a networking technique used to allow multiple devices on a private network to access the internet using a single public IP address. NAT is essential for:

* **IP Address Conservation**: Reduces the need for multiple public IP addresses.
* **Security**: Hides internal network structure from the internet.
* **Routing and Connectivity**: Helps servers in different subnets communicate.

**How to Configure NAT in Windows Server**

1. **Install Remote Access Role**
   * Open **Server Manager** → Click **Add roles and features**.
   * Select **Remote Access** → Choose **Routing**.
   * Click **Next** and **Install**.
2. **Configure NAT**
   * Open **Routing and Remote Access** (RRAS) from **Server Manager**.
   * Right-click on the server name and select **Configure and Enable Routing and Remote Access**.
   * Choose **NAT** and click **Next**.
   * Select the **network interface** connected to the internet.
   * Enable **Basic Firewall** if needed.
   * Finish the wizard.
3. **Enable NAT on an Interface**
   * In **RRAS**, expand the server node → Right-click **IPv4** → Choose **New Interface**.
   * Select the public-facing network adapter → Choose **NAT**.
   * In **Address Assignment**, enable **DHCP Relay Agent** if needed.
   * Click **OK** to save settings.
4. **Verify NAT Configuration**
   * Run ipconfig on a client machine and check the gateway.
   * Use tracert google.com to confirm routing.

**3. Dynamic Host Configuration Protocol (DHCP) and How to Configure It in Windows Server 2016**

**ANS: What is DHCP?**

DHCP (Dynamic Host Configuration Protocol) is a network management protocol that dynamically assigns **IP addresses, subnet masks, default gateways, and DNS settings** to devices. This prevents manual IP configuration and ensures efficient IP address management.

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

1. **Install DHCP Role**
   * Open **Server Manager** → Click **Add roles and features**.
   * Select **DHCP Server** → Click **Next** and install.
2. **Authorize the DHCP Server**
   * Open **DHCP Manager**.
   * Right-click on the **server name** → Select **Authorize**.
3. **Create a New DHCP Scope**
   * Expand the DHCP server node.
   * Right-click **IPv4** → Choose **New Scope**.
   * Enter a **Scope Name** (e.g., Office LAN).
   * Define the **IP address range** (e.g., 192.168.1.10 – 192.168.1.100).
   * Configure **Exclusions** if necessary.
   * Set **Lease Duration** (default: 8 days).
   * Add **Default Gateway, DNS, and WINS**.
   * Activate the scope.
4. **Verify DHCP Lease**
   * Run ipconfig /renew on a client machine.
   * Check assigned IP using ipconfig /all.

**4. Configuring DNS in Windows Server**

**ANS: What is DNS?**

DNS (Domain Name System) resolves domain names into IP addresses, allowing users to access websites and services using human-readable names.

**Steps to Configure DNS in Windows Server**

1. **Install DNS Server Role**
   * Open **Server Manager** → Click **Add roles and features**.
   * Select **DNS Server** → Click **Next** and install.
2. **Configure a Forward Lookup Zone**
   * Open **DNS Manager**.
   * Right-click **Forward Lookup Zones** → Click **New Zone**.
   * Choose **Primary Zone** → Enter domain name (e.g., mycompany.local).
   * Choose **Allow dynamic updates** if required.
   * Click **Finish**.
3. **Create DNS Records**
   * Right-click on the zone → Choose **New Host (A or AAAA)**.
   * Enter **hostname** (e.g., webserver) and **IP address** (e.g., 192.168.1.10).
   * Click **OK**.
4. **Configure Reverse Lookup Zone (Optional)**
   * Used for IP-to-name resolution.
   * Similar steps as forward lookup zone.

**5. What is Server Manager and How to Use It?**

**AMS: Server Manager** is a centralized console in Windows Server used to manage local and remote servers.

**Key Features:**

* **Role & Feature Management**: Install or remove server roles.
* **Remote Management**: Monitor multiple servers.
* **Event Logging**: View logs for troubleshooting.
* **Performance Monitoring**: CPU, RAM, and disk usage statistics.

**How to Use:**

* Open **Server Manager**.
* Click **Manage** → Add Servers for remote management.
* Use **Tools** to open various administrative consoles.

**6. Role of Remote Desktop Services (RDS) in Windows Server 2016/2019 and How to Configure It**

**ANS: Role of RDS**

Remote Desktop Services (RDS) allows users to remotely access Windows applications and desktops over a network. Benefits include:

* **Secure Remote Access**: Uses RDP protocol.
* **Centralized Application Hosting**: Reduces the need for local software installations.
* **Load Balancing**: Supports multiple sessions on a single server.

**Configuring RDS**

1. **Install RDS Role**
   * Open **Server Manager** → Click **Add roles and features**.
   * Select **Remote Desktop Services** → Click **Next**.
2. **Configure RDS Deployment**
   * Choose **Quick Start** (for single server) or **Standard Deployment**.
   * Select **Session-based or Virtual Desktop**.
3. **Add RDS Licensing**
   * Open **Remote Desktop Licensing Manager** → Activate License Server.
4. **Allow Remote Access**
   * Right-click **This PC** → Click **Properties** → Enable **Remote Desktop**.
5. **Test RDS**
   * Use **Remote Desktop Connection (mstsc)** to connect