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

**25. Windows Firewall in Windows Server:**

Role of Windows Firewall:

The Windows Firewall acts as a barrier, regulating incoming and outgoing network traffic.

It allows or blocks connections based on configured rules.

You can customize rules for inbound and outbound traffic.

Configuration Steps:

Step 1: Enable Windows Firewall

Open Server Manager:

Click on the Start button and search for Server Manager.

Launch Server Manager.

Access Windows Defender Firewall:

In the left pane of Server Manager, click on Tools.

Select Windows Defender Firewall with Advanced Security.

Create Inbound or Outbound Rules:

Choose either Inbound Rules or Outbound Rules.

Right-click and select New Rule.

Follow the wizard to create rules based on program path, port, protocol, or predefined services.

Step 2: Customize Rules

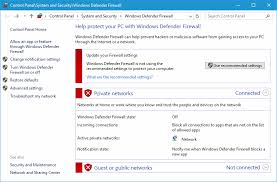
Configure Default Behavior:

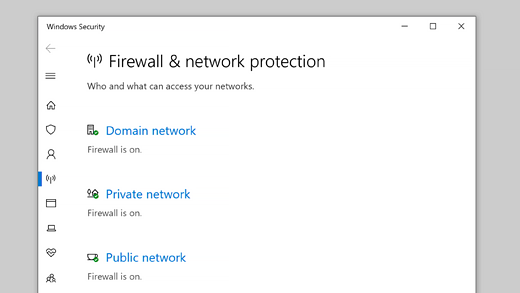
Decide whether inbound connections should be allowed or blocked by default.

Adjust outbound connection settings as needed.

Enable Logging (Optional):

For debugging purposes, consider enabling logging in the firewall rules.





**26. Network Address Translation (NAT):**

NAT in Windows Server:

NAT allows multiple devices within an internal network to share a single public IP address for internet access.

Configure NAT in Windows Server 2016 to enable this functionality.

Steps:

Step 1: Enable Routing and Remote Access

Install Routing and Remote Access Role:

Open Server Manager.

Add the Routing and Remote Access role.

Right-click the server and choose Configure and Enable Routing and Remote Access.

Select NAT:

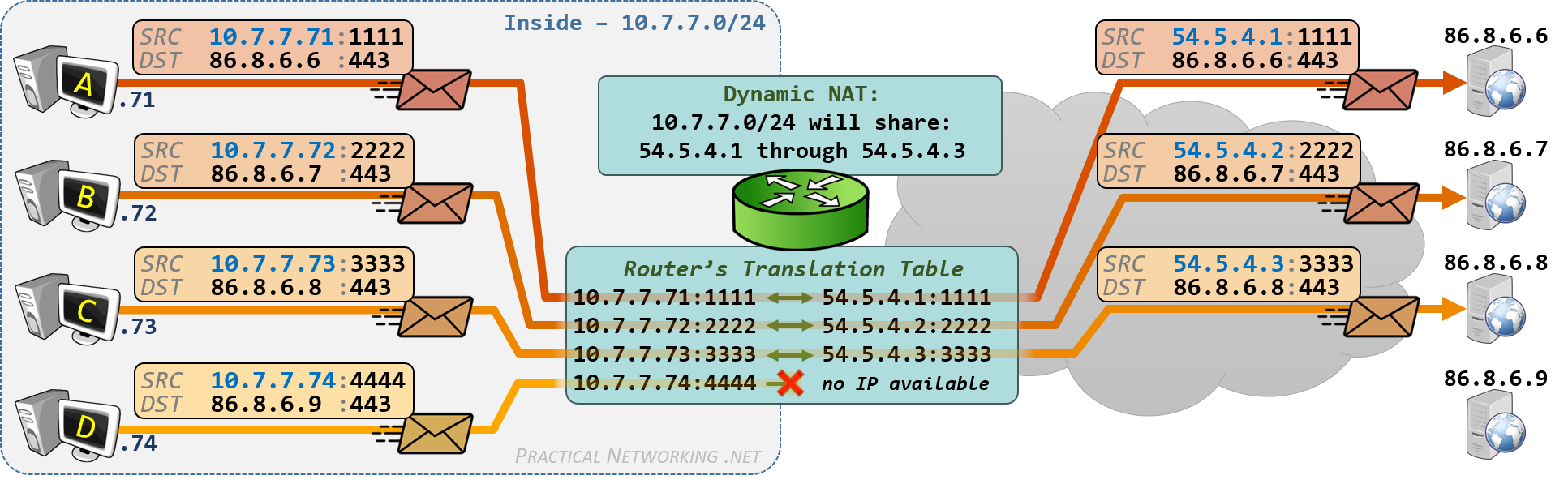
In the wizard, choose Network address translation (NAT).

Select the network interface connected to the internet.

Step 2: Test NAT

Verify Connectivity:

Ensure that clients within your internal network can access the internet using the single public IP address.



**27. Dynamic Host Configuration Protocol (DHCP):**

DHCP Concept:

DHCP automatically assigns IP addresses and network settings to devices.

Configure DHCP in Windows Server 2016:

Configuration Steps:

Step 1: Install DHCP Server Role

Add DHCP Server Role:

Use Server Manager to add the DHCP Server role.

Configure the DHCP scope with an IP address range, lease duration, and other options.

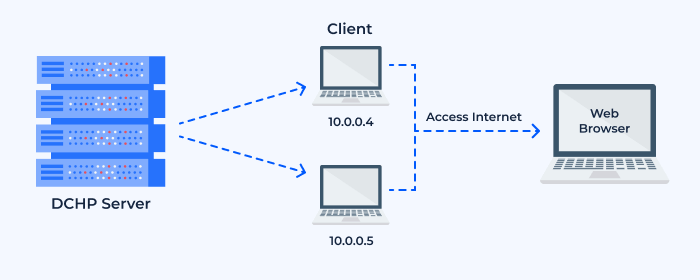
Step 2: Authorize DHCP Server (in a domain environment)

Authorize DHCP Server:

Run PowerShell as an administrator.

Execute the command: Add-DhcpServerInDC -DnsName DHCP1.corp.contoso.com -IPAddress 10.0.0.3.

Verify authorization using the same command.



**28. Configuring DNS (Domain Name System) in Windows Server:**

DNS (Domain Name System) is crucial for translating human-readable domain names (like “example.com”) into IP addresses. Here’s how to configure it:

Step 1: Install the DNS Server Role

Log on to the server where you want to install the DNS role (preferably a domain controller).

Open Server Manager.

Click Manage and select Add Roles or Features.

In the Add Role and Features Wizard, click Next.

Select Role-based or feature-based installation, and click Next.

Choose the appropriate destination server, and click Next.

Check the box next to DNS Server.

If prompted, add any required features for the DNS server.

Read the information about DNS, and click Next.

Finally, click Install.

Step 2: Configure the DNS Server Role

Open DNS Manager from Server Manager or by running dnsmgmt.msc.

Expand the DNS server, right-click Forward Lookup Zones, and click New Zone.

Follow the wizard to create a Forward Lookup Zone:

Choose the zone type (Primary or AD-integrated).

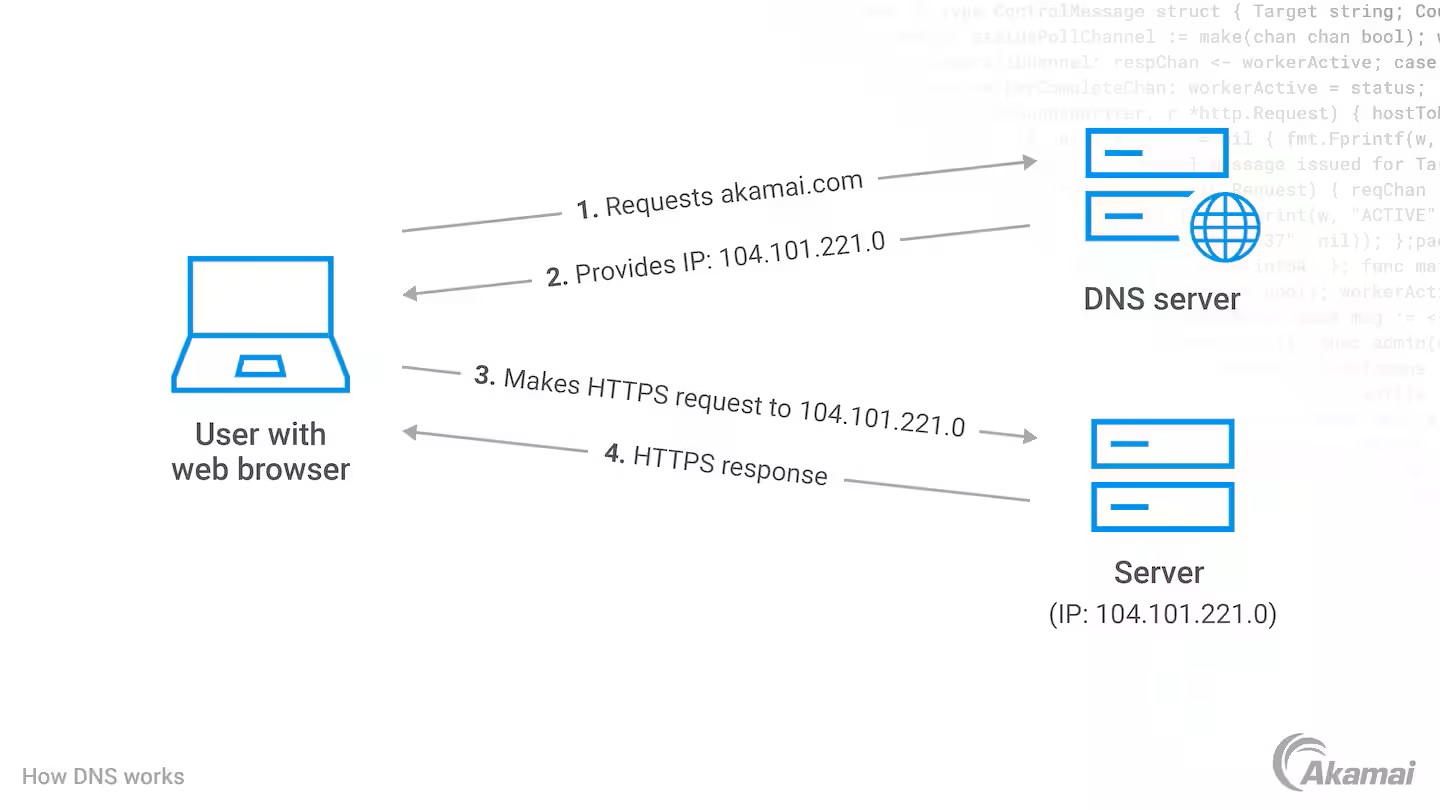
Specify the zone name.

Configure dynamic updates.

Create a Reverse Lookup Zone:

Right-click Reverse Lookup Zones and select New Zone.

Follow the wizard to create a reverse lookup zone (usually for IPv4 addresses).



**29. Server Manager in Windows Server:**

Server Manager is a management console that helps IT professionals provision and manage both local and remote Windows-based servers. Here’s how to use it:

Adding Servers:

Open Server Manager.

Click Manage and select Add Servers.

Add the servers you want to manage (local or remote).

Roles and Features:

Click Add Roles and Features.

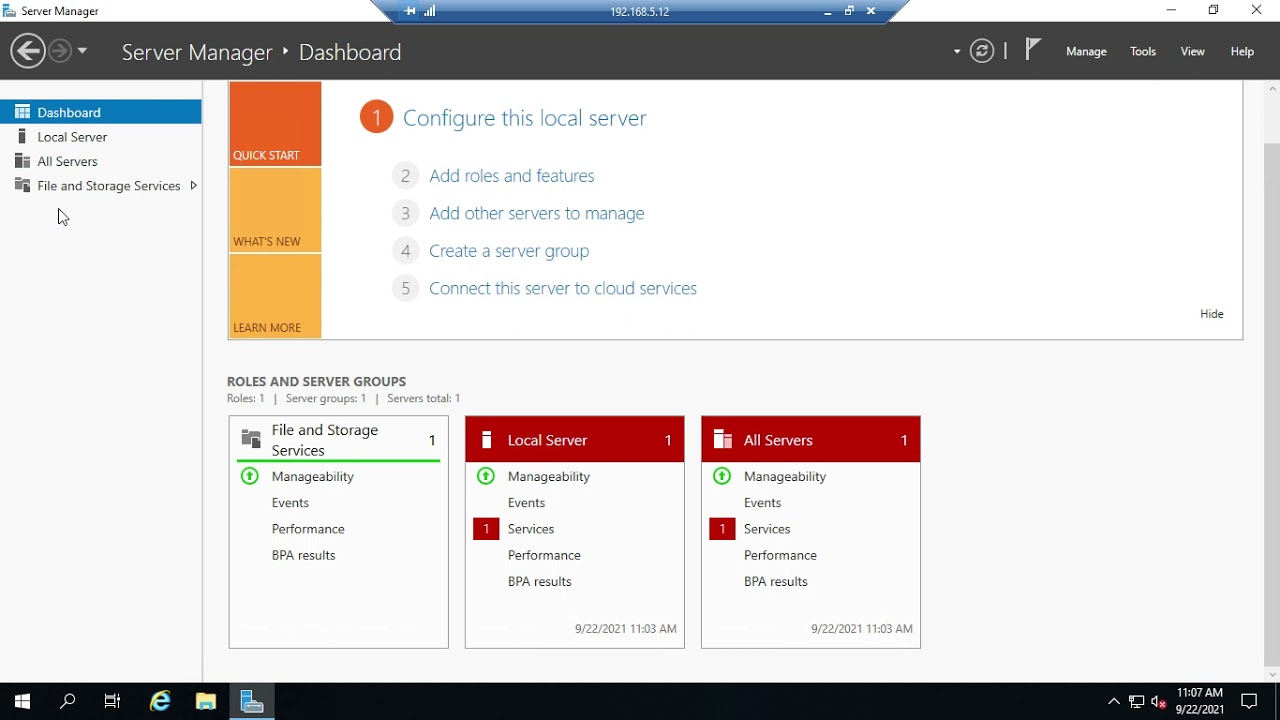
Install or remove server roles and features.

Configure services and manage server roles.

Remote Management:

By default, remote management is enabled on servers running Windows Server 2016.

Add servers to the Server Manager server pool to manage them remotely.



**30. Role of Remote Desktop Services (RDS) in Windows Server:**

RDS allows:

Delivering virtualized applications.

Providing secure mobile and remote desktop access.

Running business-critical applications from the cloud.

Configuration Steps for RDS:

Deploy RDS Servers:

RDS allows:

Delivering virtualized applications.

Providing secure mobile and remote desktop access.

Running business-critical applications from the cloud.

Configuration Steps for RDS:

Deploy RDS Servers:

Install the RDS roles (RD Connection Broker, RD Web Access, RD Session Host).

Use physical or virtual machines based on your environment.

Add RD License Server:

Open Server Manager.

Click Remote Desktop Services > +RD Licensing.

Select the virtual machine for the RD license server.

Activate the RD License Server.

Configure RD Gateway:

Open Server Manager.

Click Remote Desktop Services > +RD Gateway.

Specify the virtual machine for the RD Gateway server.

Enter the SSL certificate name (external FQDN).

