FTP Server & Firewall Configuration

Introduction to FTP Server

What is an FTP Server?

FTP (File Transfer Protocol) is a protocol used to transfer files between computers over a network, such as the internet or a local LAN.

An FTP Server is a software/service that uses FTP to allow clients to:

- Upload files to the server
- Download files from the server

How FTP Works

Connection Process:

- Client initiates a connection to the FTP server on port 21 (control port).
- Client authenticates using a username and password (or anonymously).
- A data connection is opened for transferring files.
- File operations (upload/download) are performed.

Two Connection Modes:

- Active Mode: Server connects back to client for data transfer.
- Passive Mode: Server tells client which port to connect to (better with firewalls).

Types of FTP Access

Type	Description
Anonymous FTP	No login needed. Used for public file sharing.
Authenticated FTP	Requires username & password. Private & secure.
FTPS (FTP Secure)	FTP with SSL/TLS encryption.
SFTP (SSH File Transfer Protocol)	Not FTP! Runs over SSH, more secure.

Common FTP Server Software

OS	FTP Server Software
Windows	FileZilla Server, IIS FTP
Linux	vsftpd, ProFTPD, Pure-FTPd

FTP Server Setup Example (Windows with FileZilla Server)

Steps to Install & Configure FileZilla Server:

- Download and install FileZilla Server from official website.
- Open FileZilla Server Interface.
- Create a user account:
- Go to Edit > Users.
- Click “Add”, set username.
- Set password and permissions (read/write).
- Add a shared folder:
- Select "Shared Folders".
- Click "Add" to choose a directory.
- Configure Firewall to allow port 21.
- Start the server and test connection using FileZilla Client.

FTP Client Connection (Example):

Host: 192.168.1.100

Port: 21

Username: ftpuser

Password: mypassword

FTP Server Use Cases

Use Case	Example
Backup	Store daily backups from remote clients
File Sharing	Internal file exchange in organizations
Website Hosting	Uploading files to web hosting services
IoT Devices	Devices uploading logs or data to central FTP

Server Backup Using Server

What is a Backup?

A backup is a copy of your important files and data saved in another place so that you don't lose it if something goes wrong (like system crash, virus, hardware failure, etc.).

What is Server Backup?

Server backup means saving a copy of files, folders, databases, or even the whole system from one server to:

- Another server
- External drive
- Cloud storage

This helps protect important data and keeps your work safe.

Real-Life Example

Let's say:

- You have a company server called "MainServer".
- It stores all employee documents, reports, and project files.
- You also have another server called "BackupServer".

Backup Process:

- Every night at 2 AM, MainServer sends a copy of its files to BackupServer.
- This is done using a backup script or software.
- If the MainServer crashes, you can recover your files from the BackupServer.

Ways to Do Server Backup

1. Manual Backup:

- You copy files from one server to another manually.
- Not suitable for large data or daily tasks.

2. Automated Backup (Best Way):

You schedule automatic backups using scripts or backup software.

Example: Windows Backup Using FTP

You can back up your server files to an FTP Server (remote server that stores files).

Why Backups Are Important

- Prevents data loss due to system failure or hacking.
- Helps in disaster recovery (getting data back after a crash).
- Keeps your business running smoothly.

Tips for Good Backup Strategy

Tip	Why It's Good
Daily Backups	Always have fresh data
Store on Different Server	Safe even if one server fails
Secure Backups	Use passwords and encryption
Test Restores	Make sure backups actually work

Summary

Server backup means making a safe copy of important data from one server to another so you can restore it if anything goes wrong.

FIREWALL CONFIGURATION

What is a Firewall?

A firewall is a security system that controls what network traffic is allowed or blocked from entering or leaving a computer or server.

It acts like a security guard between your computer/server and the outside world (internet or local network).

Why is Firewall Important?

- Stops hackers from accessing your system.
- Blocks unwanted traffic.
- Allows only trusted connections like FTP, HTTP, Remote Desktop, etc.
- Can limit access by port number, IP address, or protocol (TCP/UDP).

Types of Firewall:

Type	Description
Software Firewall	Installed on the OS (like Windows Firewall).
Hardware Firewall	A physical device (like Cisco ASA) placed between network and internet.

Where is Firewall Used?

- On servers (to protect services like FTP, Web, Email).
- On client machines (to protect from malware or intrusions).
- In networks (router/firewall appliance).

Example: Firewall in Windows Server 2016

- Windows has a built-in firewall called:
- Windows Defender Firewall with Advanced Security.

To access it:

Go to Control Panel > System and Security > Windows Defender Firewall > Advanced Settings

Rajkot-Morbi Highway, Rajkot-360003, Gujarat, India
www.marwadiuniversity.ac.in
For Admission Enquiries, Call or WhatsApp:
8980030090
Scan for 360° Campus View

What You Can Do with Firewall Configuration:

- Create Inbound Rules (Allow/block incoming traffic).
- Create Outbound Rules (Control outgoing traffic).
- Specify IP address, Port number, Protocols (TCP/UDP).
- Enable or Disable firewall profiles:

1. Domain (work network)
2. Private (home network)
3. Public (public Wi-Fi)

INBOUND RULE USING ADVANCED FIREWALL CONFIGURATION

What is an Inbound Rule?

An Inbound Rule is a firewall rule that controls incoming traffic to your computer or server.

For example: If you're running an FTP server, you need to allow port 21.

If this rule is not set, clients can't connect to your server.

When Do You Need Inbound Rules?

Service	Port	Inbound Rule Needed?
FTP	21	✓ Yes
HTTP (Web Server)	80	✓ Yes
Remote Desktop (RDP)	3389	✓ Yes
MySQL	3306	✓ Yes

Steps to Create an Inbound Rule (in Windows Server 2016)

Let's say you want to allow FTP traffic (port 21).

Step-by-Step:

Open:

Control Panel > Administrative Tools > Windows Defender Firewall with Advanced Security

Click on:

Inbound Rules > New Rule (Right-hand side)

Choose Rule Type:

✓ Select Port, then click Next

Protocol & Ports:

- Select TCP
- Type 21 in Specific Local Ports
- ➞ (This is the FTP port)

Action: ✓ Choose Allow the connection

Profile: ✓ Select when this rule applies:

- Domain
- Private
- Public

(Select all if you're unsure, or choose based on your network type)

Name the Rule:

➞ Example: Allow FTP Port 21

Finish

Rajkot-Morbi Highway, Rajkot-360003, Gujarat, India
www.marwadiuniversity.ac.in
For Admission Enquiries, Call or WhatsApp:
8980030090
Scan for 360° Campus View

Now your server will allow FTP connections on port 21.

Summary

Topic	Key Points
Firewall	Blocks/Allows network traffic based on rules
Inbound Rule	Lets you allow specific types of incoming traffic
When to Use	When hosting services like FTP, HTTP, RDP, etc.
How to Create	Use Advanced Firewall > Inbound Rules > New Rule