Firewall Rule Creation Guide

Step-by-Step Guide to Create Firewall Outbound Rule (Windows)

Outbound Rule Creation:

1. Open Windows Defender Firewall with Advanced Security.

2. Click on "Outbound Rules" in the left panel.

3. Click "New Rule..." on the right panel.

4. Select "Port" and click "Next".

5. Choose "TCP".

6. Under "Specific remote ports", enter: 80,443

7. Click "Next", then select "Block the connection".

8. Click "Next", under Profile, check all three checkboxes: Domain, Private, and Public.

9. Click "Next", give the rule a name: Block Website

10. Click "Finish".

Verification (Optional):

1. Open Command Prompt (CMD).

2. Type: ping demo.testfire.net

This tests if the rule blocks traffic to the site.

FTP Server Setup on Windows Server 2022

1. Open Server Manager:

   - Click Start > Search 'Server Manager' > Open it.

2. Add Roles and Features:

   - Click 'Add roles and features'.

   - Click 'Next' on the 'Before you begin' screen.

3. Server Selection:

   - Choose the default local server.

   - Click 'Next'.

4. Server Roles:

   - Check 'Web Server (IIS)'.

   - Click 'Add Features' when prompted.

   - Click 'Next'.

5. Features:

   - Check 'FTP Server'.

   - Click 'Next', then click 'Install'.

6. Open IIS Manager:

   - Start > Search 'Windows Administrative Tools' > Open 'Internet Information Services (IIS) Manager'.

7. Add FTP Site:

   - Expand the server name > Right-click 'Sites' > Add FTP Site.

   - FTP Site Name: Wipro.local

   - Physical Path: C:/Documents

   - Click 'Next'.

8. Binding and SSL:

- Use port 21 and select 'No SSL'.

- Click 'Next'.

9. Authentication and Authorization:

- Authentication: Basic

- Allow access to: All Users

- Permissions: Read and Write

- Click 'Finish'.

10. Configure Windows Firewall:

- Open Windows Defender Firewall > Advanced Settings.

- Inbound Rules > New Rule.

- Rule Type: Port > Protocol: TCP > Specific local port: 21

- Click Next > Allow Connection > Next

- Name: 'FTP Allow' > Finish.

11. Create User Account:

- Start > Search 'Computer Management'

- Go to Local Users and Groups > Users > Right-click > New User.

- Username: aman | Full name: Aman K

- Check 'Password never expires' > Create.

12. Set Folder Permissions:

- Go to File Explorer > Documents > Right-click > Properties > Security tab.

- Click 'Edit' > Add > Type 'aman' > Check Names > OK > Grant full control.

13. Test FTP Connection:

- Open CMD > Type 'ftp'

- Enter IP address > Enter username and password.

14. Check FTP Sessions:

- Open IIS Manager > Sites > Click on 'Wipro.local'

- Double-click 'FTP Current Sessions'.

Burp Suite & Firefox Proxy Setup Guide

Step 1: Configure Burp Suite

1. Open Burp Suite -> Proxy tab -> Options

2. Note IP address (usually 127.0.0.1) and Port (usually 8080)

Step 2: Firefox Proxy Settings

1. Open Firefox -> Settings -> Network Settings

2. Select "Manual proxy configuration"

3. Enter Burp's IP and Port (e.g., 127.0.0.1 : 8080)

4. Check "Also use this proxy for HTTPS"

Step 3: Install CA Certificate

1. In Firefox address bar, visit: http://burp

2. Click "CA Certificate" to download cert

3. Go to Firefox Settings -> Privacy & Security -> Certificates -> View Certificates

4. In "Authorities" tab -> Import -> Select downloaded .cer file

5. Check both trust boxes when prompted

Step 4: Verify Setup

1. Keep Burp running -> Ensure "Intercept is on" (Proxy -> Intercept)

Burp Suite & Firefox Proxy Setup Guide

2. Visit Google.com in Firefox

3. Observe traffic in Burp's "HTTP History" tab

Day 10: Palo Alto Firewall & Cloudflare Warp Practical

Practical 1: Palo Alto Firewall in VM

1. Installation & Login

1.1 Install Palo Alto Firewall on the VM.

1.2 Login via browser or CLI:

- Username: admin
- Password: admin

2. Basic Configuration

1.3 Enter device configuration mode:

```
configure
```

1.4 Disable HTTP service:

```
set deviceconfig system service disable-http yes
commit
```

1.5 Disable HTTPS service:

- Use the arrow key up arrow to recall the previous command.
- Replace disable-http with disable-https:

```
set deviceconfig system service disable-https yes
commit
```

3. Set Permitted IP

1.6 Set a specific management IP:

```
set deviceconfig system permitted-ip 172.20.0.11/32
commit
```

Practical 2: Cloudflare Warp & Traffic Testing

1. Cloudflare Warp Setup

Day 10: Palo Alto Firewall & Cloudflare Warp Practical

2.1 Open Cloudflare dashboard.

2.2 Go to Settings > Teams.

2.3 Copy your Team Name.

2. SysTracer Configuration

2.4 Open SysTracer or client software.

2.5 Paste the Team Name into the designated field.

3. Enable Warp

2.6 Open Cloudflare Warp client.

2.7 Login and paste your Team Name.

2.8 Connect to establish the secure tunnel.

4. Generate Traffic for Testing

Option 1: Browser

- Visit websites like https://example.com or https://speed.cloudflare.com

Option 2: Command Line (Windows)

```
curl https://example.com
ping 1.1.1.1
```

Option 3: Command Line (Linux)

```
wget https://example.com
ping 1.1.1.1
```