Module 10: CyberPanel Security Essentials

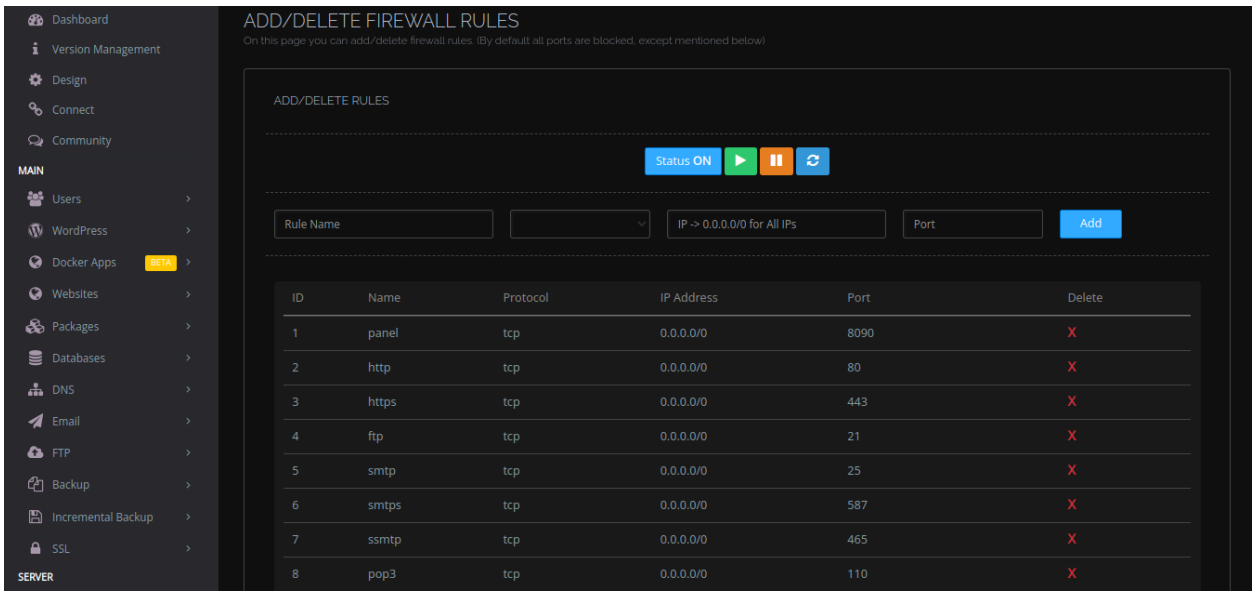
10.1 Firewall Setup: Configuring CyberPanel's Default Firewall

A firewall is one of the first lines of defense in protecting your server from unauthorized access and malicious traffic. CyberPanel offers a built-in firewall configuration that is easy to use and effective.

10.1.1 Configuring the Default Firewall

1. **Access the Firewall Settings**:
    - Navigate to **"Security"** → **"Firewall"** in the CyberPanel dashboard.
2. **Enable the Firewall**:
    - Ensure that the firewall is enabled for the server. If it's not enabled, toggle the switch to **"Enable"**.
3. **Configure Rules**:
    - You can configure inbound and outbound rules to control the traffic. Some basic rules might include:

        - Allowing traffic on ports **80 (HTTP)**, **443 (HTTPS)**, and **22 (SSH)**.
        - Blocking specific IP addresses or IP ranges that you suspect are malicious.
4. **Firewall Settings**:
    - Set up rules for:
        - **Allowing** or **blocking IPs** based on country, region, or specific IP addresses.
        - **Rate limiting** requests to certain services (e.g., limiting SSH access attempts).
5. **Saving Firewall Configurations**:
    - Once you've configured the firewall rules, save the settings, and restart the firewall to apply changes.



10.1.2 Using Custom Firewall Rules

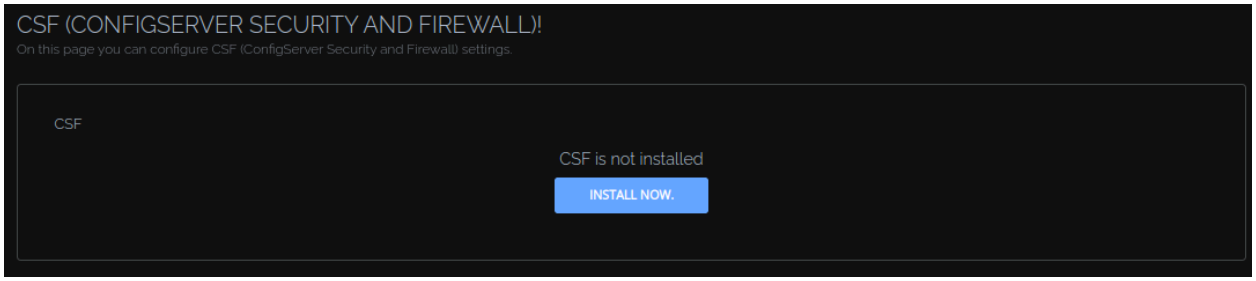
- For advanced users, CyberPanel allows you to add custom firewall rules by directly editing the configuration file (e.g., `iptables` or `firewalld`). This is useful for more complex setups.

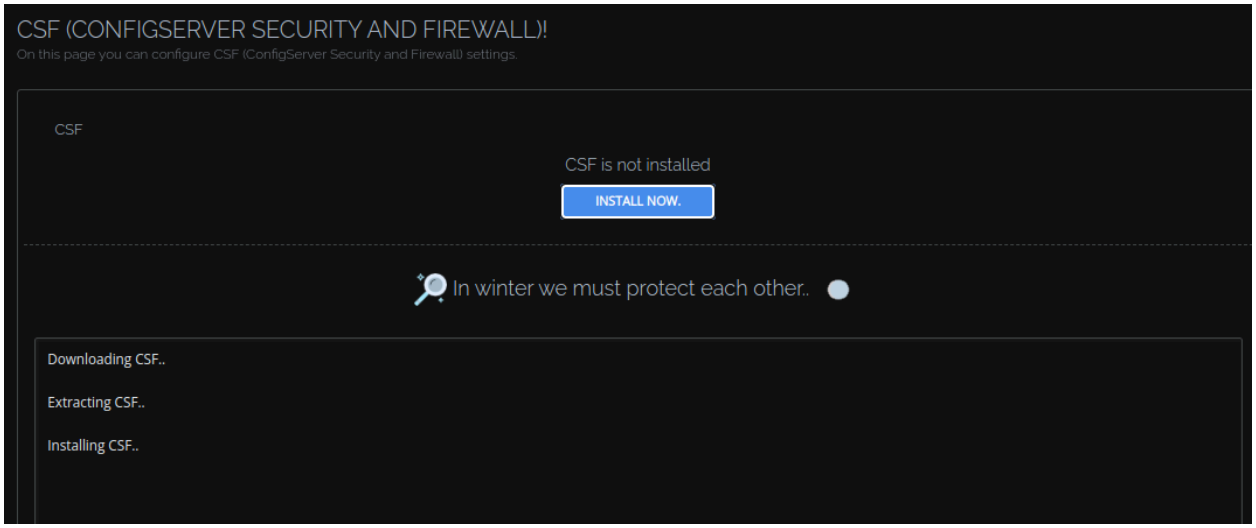
10.2 CSF (ConfigServer Security & Firewall): Installation and Basic Configuration

CSF is a powerful firewall and security tool for Linux servers. It provides enhanced protection through advanced security options, including login tracking, rate-limiting, and more.

10.2.1 Installing CSF on CyberPanel

1. Navigate to **"Security"** → **"CSF"** in the CyberPanel dashboard.
2. **Click install**





10.2.2 Basic Configuration of CSF

1. **Access CSF Settings**:
    - Go to **"Security"** → **"CSF Firewall"** in CyberPanel to manage CSF settings.
2. **Configure CSF Rules**:
    - Enable the firewall and configure basic settings, such as:
        - **Port Configuration**: Ensure that required ports (e.g., 80, 443, 22) are open.
        - **Login Tracking**: Set thresholds for login attempts to prevent brute-force attacks.
        - **SMTP Protection**: Protect against abuse of email services by configuring the SMTP settings.

3. **Testing CSF**:

- After configuration, test the firewall settings by running:

```
csf -t
```

  - This will verify the configuration and ensure that the firewall is functioning properly.

4. **Some common CSF commands.**

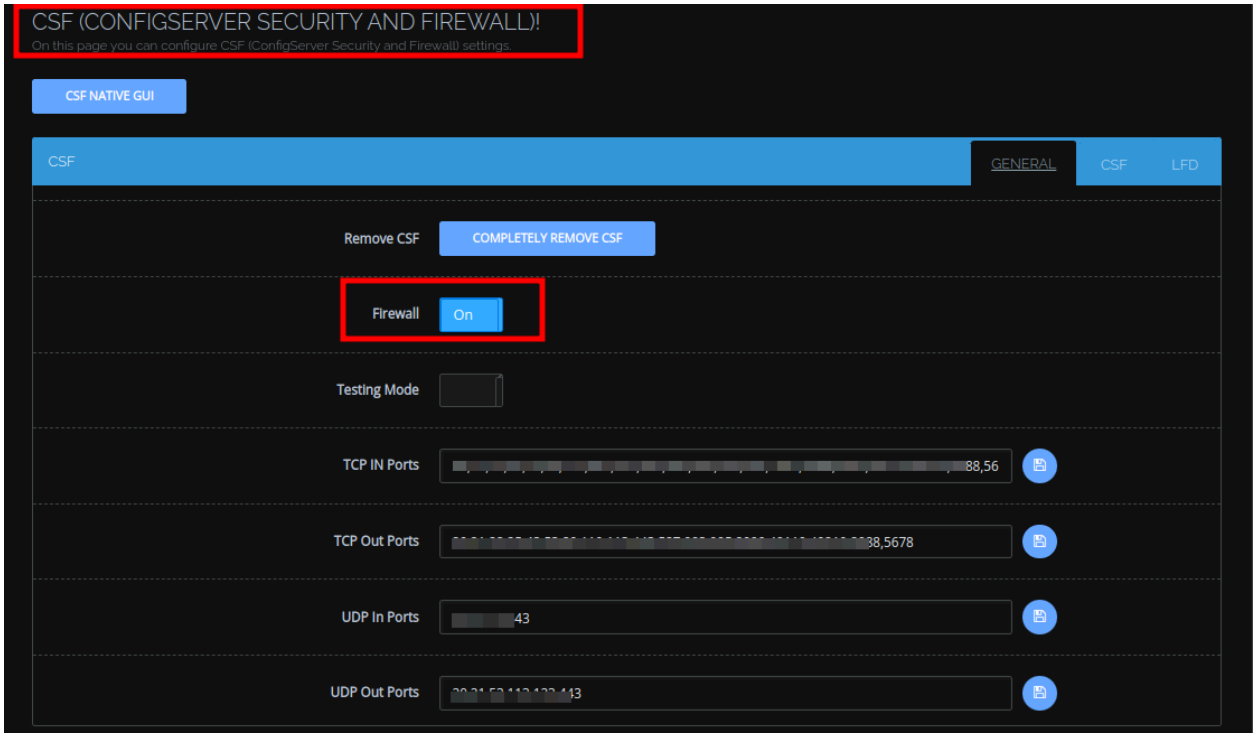
Here is a list of a few very useful CSF commands covering some of the most common tasks when managing CSF on your server.

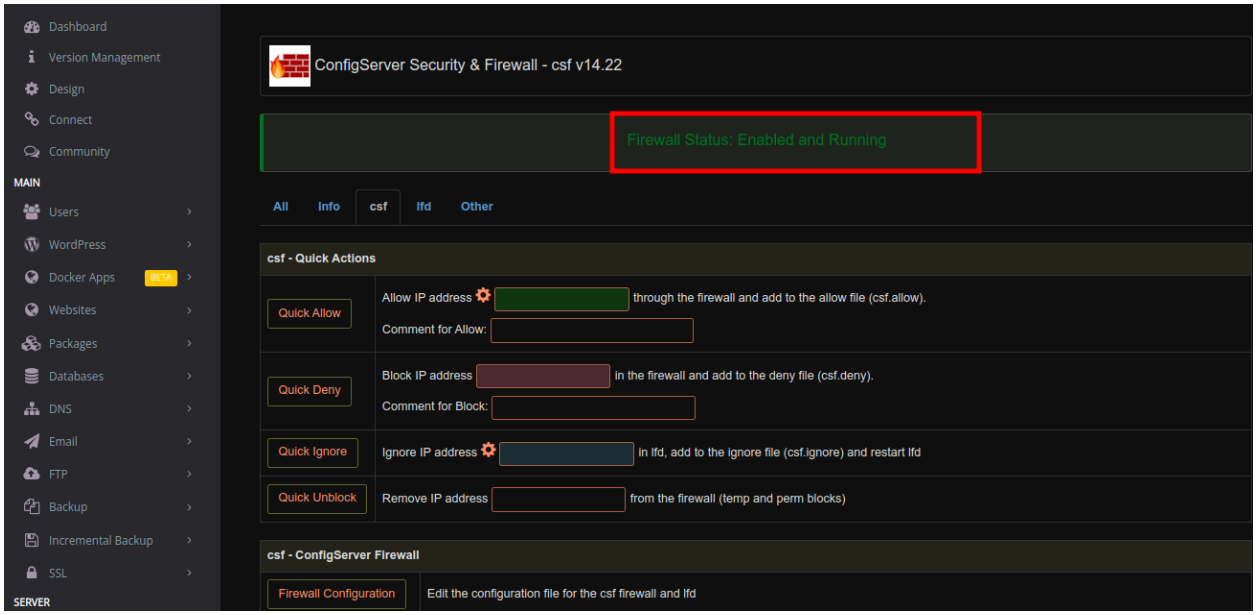
Command	Description	Example
csf -e	**Enable CSF**	**root@server[~]# csf -e**
csf -x	**Disable CSF**	**root@server[~]# csf -x**
csf -s	***Start the firewall rules***	**root@server[~]# csf -s**

csf -f	***Flush/Stop firewall rules (note: lfd may restart csf)***	**root@server[~]# csf -f**
csf -r	***Restart the firewall rules***	**root@server[~]# csf -r**
csf -a [IP] [Optional comment]	***Allow an IP and add to /etc/csf/csf.allow***	**root@server[~]# csf -a 187.33.3.3**
csf -td [IP] [Optional comment]	**Place an IP on the temporary deny list in /var/lib/csf/csf.tempban**	**root@server[~]# csf -td 55.55.55.55 Odd traffic patterns**
csf -tr [IP]	***Remove an IP from the temporary IP ban or allow list.***	**root@server[~]# csf -tr 66.192.23.1**

csf -tf	***Flush all IPs from the temporary IP entries***	**root@server[~]# csf -tf**
csf -d [IP] [Optional comment]	***Deny an IP and add to /etc/csf/csf.deny***	**root@server[~]# csf -d 66.192.23.1 Blocked This Guy**
csf -dr [IP]	***Unblock an IP and remove from /etc/csf/csf.deny***	**root@server[~]# csf -dr 66.192.23.1**
csf -df	***Remove and unblock all entries in /etc/csf/csf.deny***	**root@server[~]# csf -df**
csf -g [IP]	***Search the iptables and ip6tables rules for a match (e.g.***	**root@server[~]# csf -g 66.192.23.1**

	IP, CIDR, Port Number)	
csf -t	**Displays the current list of temporary allow and deny IP entries with their TTL and comments**	**root@server[~]# csf -t**





10.3 Managing IP Whitelisting and Blacklisting

IP whitelisting and blacklisting are critical for controlling access to your server. By allowing only trusted IPs and blocking suspicious ones, you can greatly reduce the risk of unauthorized access.

10.3.1 Whitelisting IPs

1. **Add Trusted IPs**:
    - Navigate to **"Security"** → **"Firewall"** or **"CSF Firewall"**.
    - Under the **"IP Allow/Deny"** section, add the IP addresses you want to whitelist (trusted IPs that need access to the server).

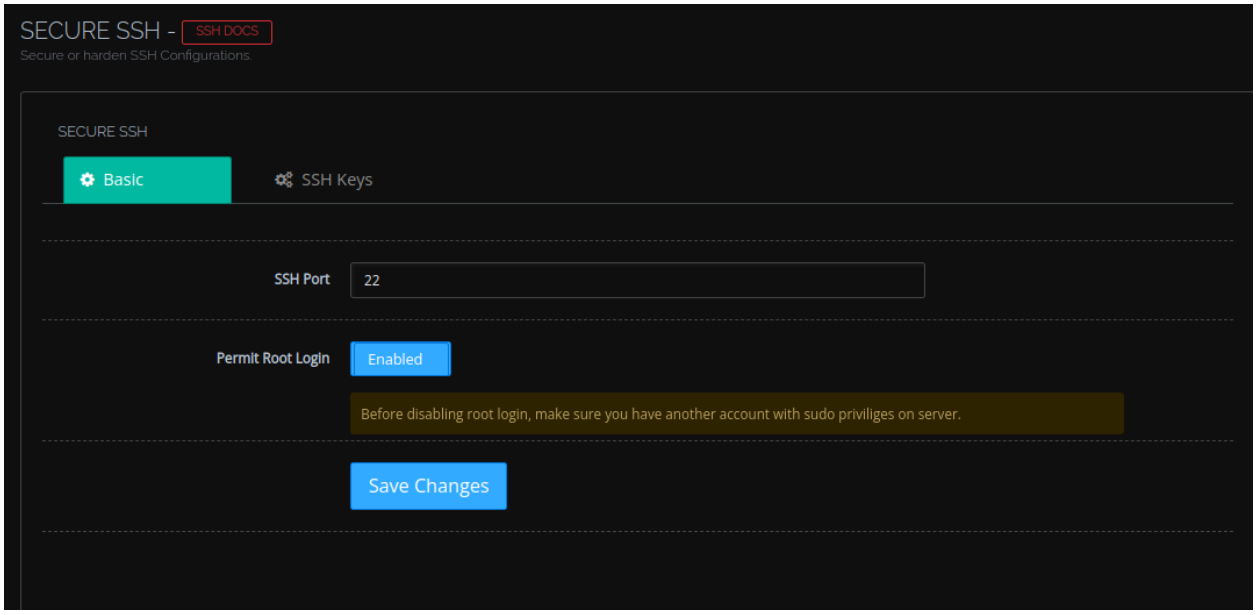
- You can whitelist IPs for services like SSH, Web, and Mail.

10.3.2 Blacklisting IPs

1. **Block Suspicious IPs**:
   - Add any malicious or suspicious IP addresses to the blacklist in the same **"IP Allow/Deny"** section.
   - CSF provides automatic blocking for repeated failed login attempts, but you can manually add IPs if needed.
2. **Check for Attackers**:
   - CyberPanel will log suspicious activity, such as multiple failed login attempts. Review these logs regularly to block any IPs that show repeated malicious behavior.

More security Measures.

- **Install Fail2Ban**: Fail2Ban is another tool that can automatically block IP addresses after a specified number of failed login attempts. It works with various services like SSH, FTP, and SMTP.
- **SSH Key Authentication**: Instead of using passwords for SSH access, switch to SSH key authentication, which is more secure and resistant to brute-force attacks.
- Navigate to **Security -> Secure SSH**


SECURE SSH - SSH DOCS
Secure or harden SSH Configurations.
SECURE SSH
Basic
SSH Keys
SSH Port
22
Permit Root Login
Enabled
Before disabling root login, make sure you have another account with sudo priviliges on server.
Save Changes

‘

The END.