Module 6: Basic Security Essentials

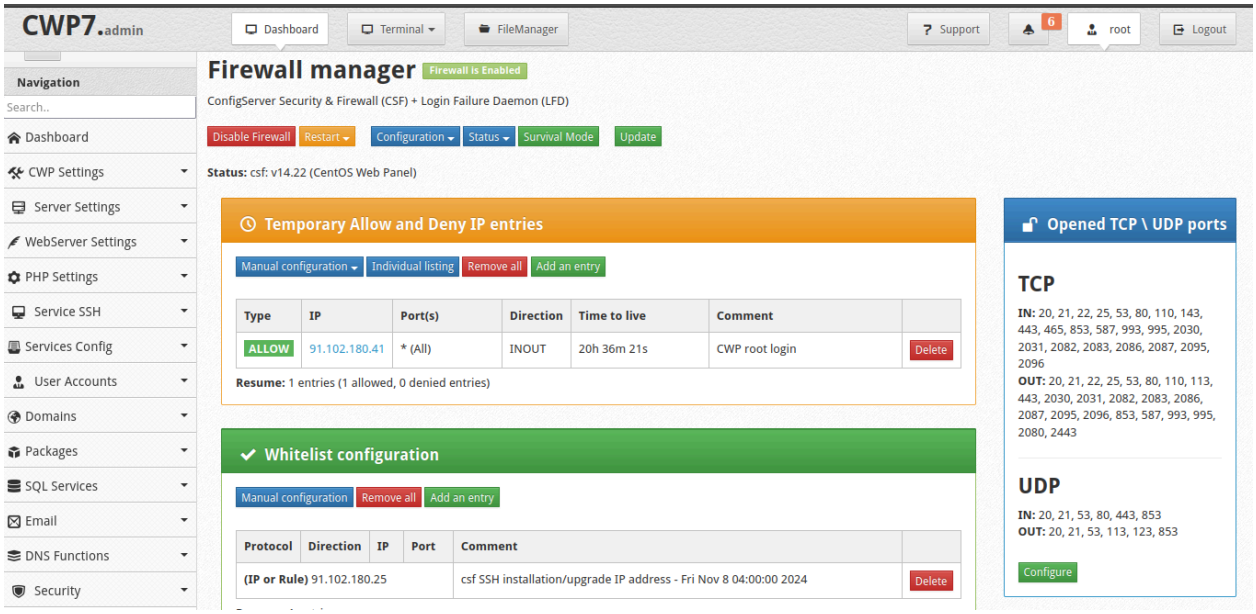
---

1. Setting Up Firewall and Basic Security Features

A firewall is essential for controlling incoming and outgoing network traffic based on security rules, helping protect the server from unauthorized access.

Setting Up the Firewall:

1. **Access the Firewall in CWP**:
    - Go to **Security > Firewall Manager** in the Admin Panel.
2. **Configuring Basic Firewall Rules**:
    - **Allow and Deny IPs**: Set specific IP addresses or ranges to be allowed or denied access.
    - **Port Management**: Only allow necessary ports (e.g., 80 for HTTP, 443 for HTTPS, 21 for FTP).
    - **Saving and Restarting the Firewall**: After making changes, click **Save** and **Restart** to apply new firewall rules.



---

2. Using CSF (ConfigServer Security & Firewall) for Security

CSF is an advanced firewall tool that adds additional layers of security and monitoring to your server. It integrates with CWP and is widely used to protect Linux-based servers.

Installing CSF in CWP:

1. **Install CSF**:
   - Go to **Security > CSF Firewall** in the CWP Admin Panel.
   - If CSF is not installed, click **Install CSF**.
2. **Basic CSF Configuration**:
   - **Access CSF Settings**: After installation, go to **Security > CSF Firewall** > **CSF Configuration**.
   - **Testing Mode**: Initially, CSF runs in “Testing” mode. Disable testing mode by setting `TESTING = 0` for full functionality.
   - **Whitelist and Blacklist**: Add trusted IPs to the whitelist and suspicious or known malicious IPs to the blacklist.

- **Port Configuration**: Open and close ports based on the services you need, such as:
  - **80 (HTTP)** and **443 (HTTPS)** for web traffic.
  - **21 (FTP)** if FTP is used.
  - **22 (SSH)** for secure shell access.

3. **CSF Features for Added Security**:
   - **Login Failure Daemon (LFD)**: LFD monitors login attempts and blocks IPs after too many failed attempts, reducing brute-force attacks.
   - **Firewall Deny IPs**: Set rules to block known malicious IP addresses.
   - **Alerts and Notifications**: Configure CSF to send alerts for suspicious activity, such as login attempts or port scans.

---

3. Introduction to SSL Certificates and Basic Setup

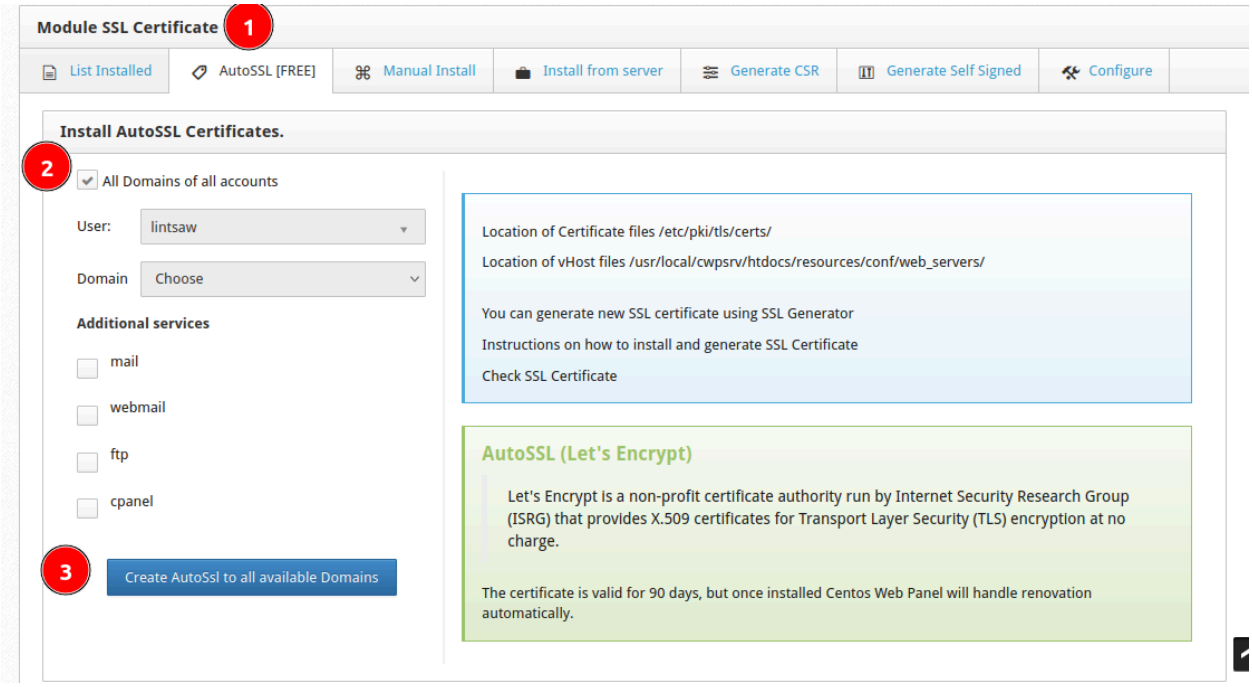
SSL (Secure Sockets Layer) certificates secure data transmitted between the server and users by encrypting the data, which is crucial for protecting sensitive information and building trust with website visitors.

Types of SSL Certificates:

- **Self-Signed SSL**: Free but not trusted by browsers.
- **Let's Encrypt**: A widely used free certificate provider supported by CWP.
- **Paid SSL Certificates**: Offer higher validation levels and warranties, generally purchased from certificate authorities.

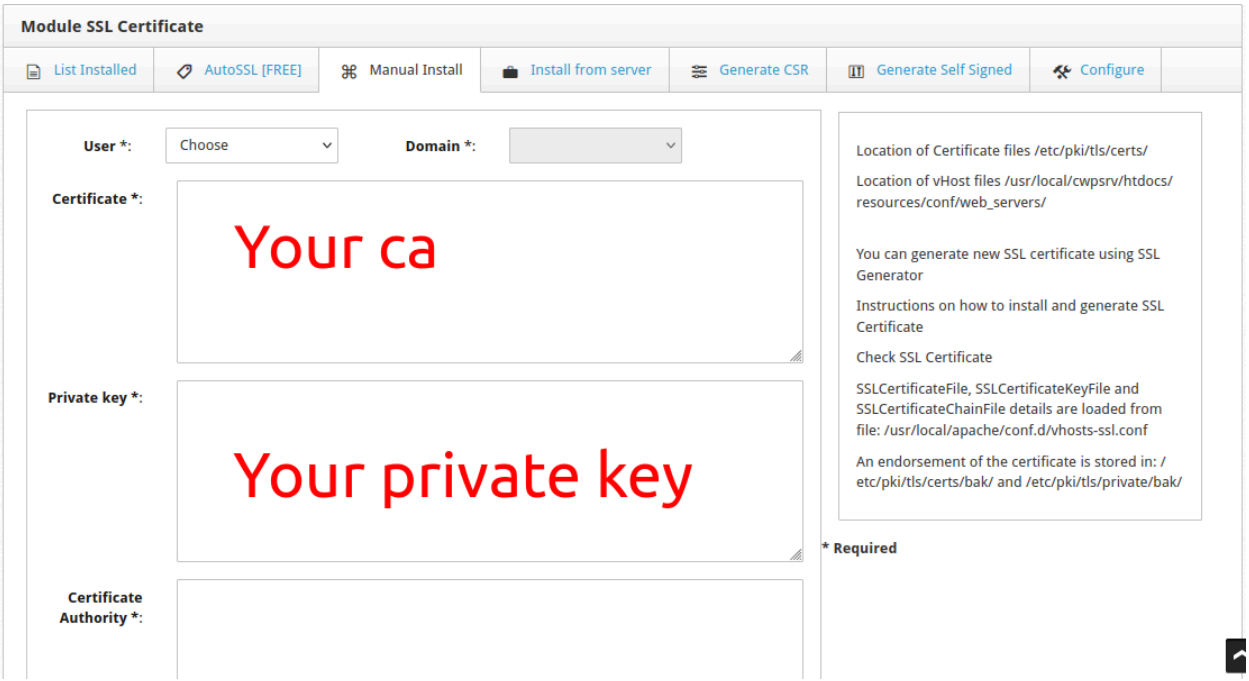
Installing an SSL Certificate in CWP:

1. **Navigate to SSL Settings**:
    - Go to **WebServer Settings > SSL Certificates** in the Admin Panel.
2. **Generate or Install a Certificate**:
    - **Let's Encrypt**: CWP offers easy integration with Let's Encrypt.
        - Choose **Let's Encrypt** in the SSL options, select the domain, and click **Install**. Let's Encrypt will generate and install the SSL certificate for your domain.



    - **Manual Certificate Installation**:

- For custom certificates, you need the **Certificate (CRT)**, **Private Key (KEY)**, and optionally, a **CA Bundle**.
- Copy and paste these into the respective fields and click **Install Certificate**.



3. **Verify SSL Installation**:
   - After installation, check your site using a tool like **SSL Labs SSL Test** or confirm by accessing your site via `https://your-domain.com`.

---

4. Basic Security Best Practices for Beginners

Following best practices helps strengthen your server's security and minimize vulnerabilities.

Basic Security Best Practices:

- **Regular Software Updates**:
  - Always keep CWP, the operating system, and other software up to date to protect against vulnerabilities.

- **Strong Password Policies**:
  - Use complex, unique passwords for all accounts. Avoid reusing passwords and regularly change them.
  - Enforce a password policy for all user accounts in CWP.
- **Disable Root Login**:
  - Disable direct root login for SSH. Instead, create an admin user with sudo privileges. This prevents attackers from targeting the root account.
- **Use SSH Key Authentication**:
  - For SSH access, use key-based authentication rather than passwords. This adds a layer of security and helps prevent brute-force attacks.
- **Limit Login Attempts**:
  - Configure tools like CSF to limit login attempts, making it harder for attackers to brute-force credentials.
- **Disable Unused Services**:
  - Disable or remove any unused services to minimize the number of possible entry points.
- **Regular Backups**:
  - Schedule automatic backups of files and databases. Store backups securely off-site to prevent data loss in case of a breach or server failure.
- **Monitor Logs**:
  - Regularly review logs in CWP under **Logs** or **Security** sections for any suspicious activity, such as repeated failed logins or unexpected IP addresses.

The END.