SAFEDNS

Linux Server Security Checklist

The information in this checklist is intended only for general informational purposes. You should consult with a specialist regarding your own circumstances.

Securing the Operating System

- **Restrict the core dumps**

Core dumps can serve as useful debugging aids, it allows a user to save a crash for later or off-site analysis, or comparison with other crashes. But they may contain sensitive or confidential data from memory. It is recommended that core dumps be disabled or restricted.

- **Enable an Network Time Protocol (NTP) service to ensure clock accuracy**

Accurate time keeping facilitates analysis of system logs when needed.

- **Disable or remove server services that are not going to be utilized**

(e.g., FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.)

- **Ensure syslog (rsyslog, syslog, syslogng) service is running.**

- **Remove legacy services**

Services that provide or rely on unencrypted authentication should be disabled unless there are grounds for an exception. These include telnet server; rsh, rlogin, rcp; ypserv, ypbind; tftp, tftpserver; talk and talk server.

- **Restrict the use of the cron services**

These can be used to run commands on the system and should only be allowed to accounts which need this access.

- **Use Linux security extensions**

If possible, use SELinux and other Linux security extensions to set restrictions for the network and other programs.

- **Disable unwanted Linux services**

User Access & Passwords

- **Enforce the use of strong passwords**

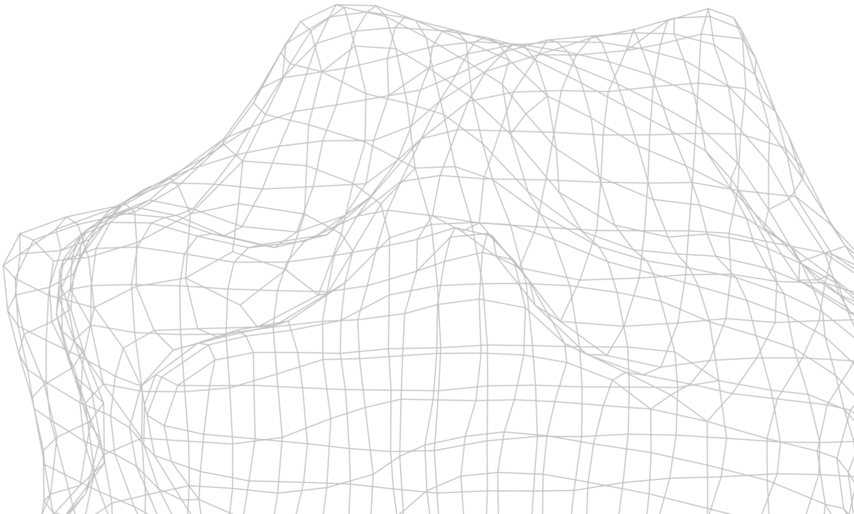
A strong password should consist of at least 8 characters and a combination of letters, numbers, special characters, uppercase and lowercase letters, etc.

- **Create an account for each user who should access the system**

Avoiding shared accounts/passwords makes it easier to keep an audit trail and remove access when no longer needed.

- **Use sudo to delegate admin access**

The sudo command allows for fineg rained control of rights to run commands as root (or other user).



Network Security & Remote Access

- **Encrypt the transmitted data whenever possible**

Data transmitted over a network, whether wired or wireless, is susceptible to passive monitoring. Whenever practical solutions for encrypting such data exist, they should be applied.

- **Limit connections to services running on the host to authorized users of the service**

via firewalls and other access control technologies.

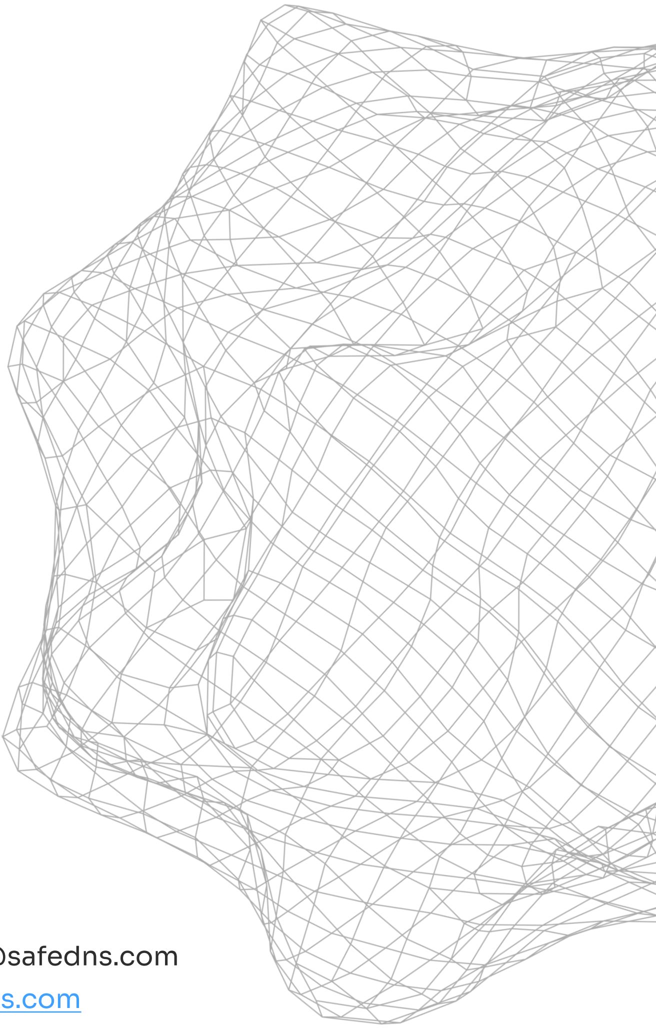
- **Deploy an Intrusion Prevention System (IPS) such as fail2ban**

fail2ban uses the iptables firewall to block remote systems generating many authentication failures as a way to combat brute force password attempts.

- **Disable IPv6 if not using it**

Network Security & Remote Access

- **If possible, use public key-based authentication only**
- **Disable empty password authentication**
- **Disable root login**



Contacts

+ 1 800.820.2530 (US)
+ 1 571.421.2990 (Outside US)

sales@safedns.com
safedns.com