cPanel Mail Server Hardening Checklist

The steps I run on every server before it touches a customer's domain.

1. Anti-spam engine

- [ ] Enable Apache SpamAssassin — Forced Global ON
  WHM › Email › Apache SpamAssassin
- [ ] Set Spam Threshold Score to 10 ("Passive – Only Very Obvious Spam") to avoid false positives
  cPanel › Spam Filters

2. Blocklists & DNS resolver

- [ ] Enable Spamhaus (zen) and SpamCop blocklists (RBLs)
  WHM › Exim Configuration Manager › RBLs
- [ ] Run a local DNS resolver, point the server at itself, then lock the file

```
rm -f /etc/resolv.conf
echo "nameserver 127.0.0.1" > /etc/resolv.conf
chattr +i /etc/resolv.conf
```

- [ ] Verify the blocklist actually answers (should return a result)

```
dig @127.0.0.1 2.0.0.127.zen.spamhaus.org +short
```

3. Authenticate incoming mail

- [ ] Enable DKIM verification for incoming messages
  WHM › Exim Configuration Manager › Basic Editor

4. Antivirus

- [ ] Install ClamAV antivirus / anti-malware
  WHM › cPanel › Manage Plugins

5. Outbound abuse controls (protect your IP reputation)

- [ ] Cap the maximum hourly emails per account
  WHM › Tweak Settings
- [ ] Reject undeliverable mail instead of silently discarding it
- [ ] Fail immediately instead of queueing
- [ ] Enable outbound rate-limiting / sender tracking

6. Server identity & deliverability

- [ ] Set a proper hostname (e.g. your-host.example.com)
- [ ] Configure matching reverse DNS (PTR) — ask your datacenter
- [ ] Install a fresh SSL certificate
  cPanel › SSL

- [ ] Set the correct server time / timezone
- [ ] Create DNS records: A (root, www, mail, webmail) and MX
- [ ] Publish SPF, DKIM and DMARC records
- [ ] Reject remote mail sent to the server's own hostname
  WHM › Exim

7. Firewall & admin access

- [ ] Web (ports 80, 443): allow from Cloudflare IP ranges only
- [ ] Mail (ports 25, 465, 587, 993, 995): allow from all
- [ ] cPanel 2083 / WHM 2087 / SSH 22: restrict to admin IP <ADMIN_IP> only
- [ ] Default-deny everything else; allow all outbound
- [ ] Enable Two-Factor Authentication (MFA) for WHM
  WHM › Security Center › Two-Factor Authentication

8. Performance tuning

- [ ] Dovecot: disable IPv6 (if unused); spare auth 10 / max auth 100; tune LMTP concurrency & cache; balanced compression
- [ ] PHP: max execution 300s, memory 512 MB, upload & POST 100 MB
- [ ] Email-only box: stop cPanel PHP-FPM for a lighter Roundcube
  WHM › Service Manager

9. Network edge (the silent mail-killer)

- [ ] Ask your datacenter / NOC to whitelist inbound SMTP (port 25) for the server IP
- [ ] Check the mail log for SMTP data-timeouts / dropped connections

```
grep -i "data timeout" /var/log/exim_mainlog | tail -10
```

10. Update & verify

- [ ] Force a full cPanel update so every component is patched

```
/usr/local/cpanel/scripts/upcp --force
```

- [ ] Confirm the automatic-update cron job is scheduled

```
grep -R "upcp" /etc/cron* /var/spool/cron* 2>/dev/null
```