CHECKLIST

CentOS 7 SELinux and Firewalld Hardening Checklist

A practical checklist for validating SELinux and Firewalld together on CentOS 7 before production, with clear steps to confirm exposure, enforcement, and common hardening pitfalls.

CentOS 7 SELinux and Firewalld Hardening Checklist

Use this checklist to confirm that a CentOS 7 host is hardened with SELinux and Firewalld working together, not as separate afterthoughts.

1) Scope the host and service

- [ ] Identify the exact service or services that must be reachable.
- [ ] Document the business purpose of each exposed service.
- [ ] List the approved client hosts, source networks, or VPN ranges.
- [ ] Confirm whether the host is general-purpose, DMZ, shared, or disposable.
- [ ] Record whether inbound access is required at all.

2) Verify SELinux status

- [ ] Confirm SELinux is enabled.
- [ ] Confirm SELinux is set to enforcing, not permissive.
- [ ] Check for recent SELinux denials during normal operation.
- [ ] Verify that denials are understood, not ignored.

- [ ] Confirm the service runs with the expected SELinux context.

Validation questions:

- [ ] Is SELinux enforcing after reboot?
- [ ] Are expected file paths labeled correctly?
- [ ] Are any SELinux booleans required and intentionally set?
- [ ] Are denials caused by bad labels, bad paths, or bad policy assumptions?

3) Verify Firewalld status and zone design

- [ ] Confirm Firewalld is installed and running.
- [ ] Identify the active zone for each network interface.
- [ ] Confirm the active zone matches the intended trust level.
- [ ] Review all allowed services and ports in the active zone.
- [ ] Remove any broad rules that were added only for troubleshooting.
- [ ] Prefer source-limited rules when only a small set of clients should connect.

Validation questions:

- [ ] Is the service open only where it needs to be?
- [ ] Are port rules narrower than necessary?
- [ ] Are source restrictions in place for administrative or internal access?
- [ ] Does the zone assignment survive restart and reboot?

4) Confirm the service is exposed only as intended

- [ ] Test reachability from an approved client network.
- [ ] Test that the service is not reachable from an unapproved network.
- [ ] Confirm localhost testing is not being mistaken for external access.
- [ ] Verify the application only listens on required interfaces.
- [ ] Check that no extra ports are listening on the host.

Remember: a service that works locally may still be blocked externally by Firewalld or denied by SELinux.

5) Validate SELinux and Firewalld together

- [ ] Start with SELinux enforcing and Firewalld enabled.
- [ ] Exercise the service from an approved client.
- [ ] Review logs for SELinux denials during the test.
- [ ] Review firewall logs or counters if traffic is unexpectedly blocked.
- [ ] Confirm the service works without disabling security controls.
- [ ] Confirm access is successful only through approved paths.

Pass criteria:

- [ ] The service is reachable from approved sources.
- [ ] The service is blocked from unapproved sources.
- [ ] No unexpected SELinux denials remain.
- [ ] No broad firewall exceptions are required.

6) Check for common hardening mistakes

- [ ] SELinux is not left in permissive mode.
- [ ] Firewalld rules are not overly broad.
- [ ] Temporary troubleshooting exceptions have been removed.
- [ ] SELinux was not disabled just to make the service work.
- [ ] File labels, contexts, or booleans were checked before weakening policy.
- [ ] The service was tested from a real client, not only from localhost.
- [ ] Exception ownership is documented and reviewable.

7) Confirm persistence after restart

- [ ] Reboot the host or restart key services.
- [ ] Confirm SELinux remains enforcing.
- [ ] Confirm the Firewalld configuration persists.
- [ ] Confirm zone assignments are still correct.
- [ ] Re-test from approved and unapproved sources.
- [ ] Recheck logs for new or repeated denials.

8) Production readiness review

- [ ] Can you explain why the service is reachable?
- [ ] Can you explain who is allowed to reach it?
- [ ] Can you explain what the process is allowed to do after connection?
- [ ] Are both controls documented and auditable?
- [ ] Would a misconfigured application be contained by SELinux?
- [ ] Would Firewalld prevent unnecessary external exposure?

9) Decision check

Proceed to production only if all of the following are true:

- [ ] The host accepts traffic only from intended sources.
- [ ] The application functions without broad firewall exceptions.
- [ ] SELinux is enforcing and any denials are understood.
- [ ] No temporary workaround is still in place.
- [ ] The configuration remains correct after reboot.

Quick remediation guide

If a check fails, use this order of operations:

- [ ] Confirm the failure is not caused by a mislabeled file or incorrect path.
- [ ] Confirm the service actually needs the access it is requesting.
- [ ] Confirm the Firewalld zone and source rules are correct.
- [ ] Confirm SELinux is enforcing and that any denials are expected.
- [ ] Remove temporary exceptions and retest.

Final sign-off

- [ ] Reviewed by: _____
- [ ] Date: _____
- [ ] Hostname / Asset ID: _____
- [ ] Service owner: _____
- [ ] Production approved: Yes / No

Notes

Use this checklist as a repeatable validation step any time a CentOS 7 service is added, changed, or returned to production.