CHECKLIST

CentOS 7 FirewallD Secure Service Exposure Checklist

A practical checklist for safely exposing services with FirewallD on CentOS 7, including zone validation, runtime vs permanent rules, source scoping, and production verification.

CentOS 7 FirewallD Secure Service Exposure Checklist

Use this checklist before exposing any new service or changing firewall policy on a CentOS 7 host.

---

1) Define the exposure requirement

- [ ] Identify the exact service being exposed.
- [ ] Confirm the listening port and protocol.
- [ ] Determine whether a named FirewallD service exists for it.
- [ ] Confirm the minimum source scope required:
- [ ] Single IP
- [ ] Source subnet
- [ ] Internal segment
- [ ] Specific interface
- [ ] Dedicated zone
- [ ] Confirm whether the service must be reachable from:
- [ ] Only internal clients

- [ ] Only a management network
- [ ] Only a reverse proxy
- [ ] A broader trusted network
- [ ] Verify that opening the service is necessary and not avoidable by another control.

---

2) Confirm the correct zone model

- [ ] Identify which interface is assigned to which zone.
- [ ] Identify which source networks are assigned to which zone.
- [ ] Verify the active zone bindings before making changes.
- [ ] Confirm the service belongs in the intended trust zone, not a public or default zone.
- [ ] Check whether the host has multiple NICs, tunnels, VPNs, or overlay networks that could alter traffic paths.
- [ ] If the host is multi-homed, validate every path that could reach the service.

---

3) Choose the simplest correct rule type

- [ ] Use a named FirewallD service if it accurately matches the application.
- [ ] Use an explicit port rule if the service uses a nonstandard port or protocol.
- [ ] Use a source restriction if only specific clients should connect.
- [ ] Use a rich rule only when zones, services, or simple source rules are not enough.
- [ ] Avoid broad rules when a narrower rule expresses the real requirement.

---

4) Apply the change safely

- [ ] Make the runtime change first.
- [ ] Keep the rule as narrow as possible.
- [ ] Avoid opening the same service in multiple zones unless there is a clear reason.
- [ ] If using a source-based rule, confirm the source is exact and not overly broad.
- [ ] Document the change while it is fresh:
- [ ] Service or port
- [ ] Zone
- [ ] Source scope
- [ ] Runtime or permanent
- [ ] Reason for the exception

---

5) Validate reachability immediately

- [ ] Test connectivity from an approved source only.
- [ ] Confirm the service responds on the intended port.
- [ ] Confirm the service is unreachable from a disallowed source.
- [ ] Confirm the rule does not expose unrelated ports.
- [ ] Check whether the service behavior matches the expected zone.
- [ ] If validation fails, stop and review zone assignment before broadening the rule.

---

6) Make the configuration persistent when needed

- [ ] Mirror the runtime change into the permanent configuration.
- [ ] Confirm the permanent rule matches the runtime rule.
- [ ] Reload FirewallD carefully.
- [ ] Retest from the same approved source after reload.

- [ ] Confirm the result is unchanged after reload.
- [ ] If the service must survive reboot, verify persistence explicitly.

---

7) Verify production readiness

- [ ] The approved source can connect.
- [ ] An unapproved source cannot connect.
- [ ] The rule is in the correct zone.
- [ ] The runtime and permanent policies are aligned.
- [ ] The change is documented for future operators.
- [ ] A rollback method is defined and tested.
- [ ] Monitoring or logging is available if the service is critical.

---

8) Watch for common mistakes

- [ ] Do not allow a service in the wrong zone.
- [ ] Do not confuse runtime changes with permanent changes.
- [ ] Do not open a port globally when only one subnet needs access.
- [ ] Do not rely on the service responding locally as proof of network exposure correctness.
- [ ] Do not assume one interface-to-zone mapping covers every path on a multi-homed server.
- [ ] Do not use a richer rule than necessary if a simpler zone or source rule is sufficient.
- [ ] Do not leave troubleshooting rules in place after the issue is resolved.

---

9) Quick approval questions

Before you approve the firewall change, answer these four questions:

- [ ] Which service is being exposed?
- [ ] Which zone controls the traffic path?
- [ ] Which callers must succeed?
- [ ] Which callers must fail?

If any answer is unclear, pause and redesign the rule.

---

10) Rollback checklist

- [ ] Know the exact rule to remove.
- [ ] Know the exact zone to revert.
- [ ] Know whether the change exists in runtime, permanent configuration, or both.
- [ ] Confirm how to reload safely after rollback.
- [ ] Verify the service becomes unavailable from unauthorized sources after rollback.
- [ ] Record the rollback result.

Example review standard

A secure FirewallD change on CentOS 7 should be:

- Specific: only the required service or port
- Scoped: only the intended source or zone
- Verified: tested from allowed and disallowed sources
- Persistent: saved if it must survive reloads and reboots

- Documented: easy for the next operator to understand

Final sign-off

- [ ] I have confirmed the service requirement.
- [ ] I have validated the zone and source scope.
- [ ] I have tested the runtime rule.
- [ ] I have aligned the permanent configuration.
- [ ] I have verified allowed and denied access paths.
- [ ] I have documented rollback steps.

Do not approve the change until every item that applies has been checked.