CHECKLIST

Ubuntu AppArmor and UFW Hardening Checklist

A practical checklist for validating AppArmor and UFW on Ubuntu before production use. Covers network exposure, application confinement, enforcement mode, and operational verification.

Ubuntu AppArmor and UFW Hardening Checklist

Use this checklist to confirm that AppArmor and UFW are doing real work on an Ubuntu host before you rely on them in production.

1) Scope the host and its exposure

- [ ] Identify the host?s purpose and the services that must remain reachable.
- [ ] List every listening port and map each port to a service.
- [ ] Identify approved source networks, admin networks, VPN ranges, and any public-facing endpoints.
- [ ] Confirm whether the host must enforce its own firewall policy, even if upstream security groups exist.
- [ ] Confirm whether each service handles untrusted input or business-critical data.

2) Set a minimal network policy with UFW

- [ ] Confirm UFW is installed.
- [ ] Confirm UFW is enabled.

- [ ] Verify the default inbound policy is deny.
- [ ] Verify the default outbound policy matches your operational needs.
- [ ] Allow only the ports required for the host to function.
- [ ] Restrict sensitive services to approved source ranges whenever possible.
- [ ] Avoid broad rules such as allow from any unless the service is intentionally public.
- [ ] Remove unused or temporary rules.
- [ ] Confirm the final rule set is understandable and auditable.

UFW verification checks

- [ ] ufw status verbose shows UFW active.
- [ ] Default inbound policy is deny.
- [ ] Only expected inbound ports appear in the rule list.
- [ ] Restricted-source rules match the intended networks.
- [ ] No duplicate or stale rules remain.

3) Confirm AppArmor coverage

- [ ] Confirm AppArmor is installed and active.
- [ ] Identify the AppArmor profile for each exposed service.
- [ ] Confirm the profile exists for the service you want to confine.
- [ ] Confirm the profile is loaded at boot or during service start.
- [ ] Confirm the profile is in enforce mode for production use.
- [ ] Note any services that do not have a profile and decide whether that exception is acceptable.

AppArmor verification checks

- [ ] aa-status shows AppArmor loaded.
- [ ] The target service appears in the list of loaded profiles.
- [ ] The target profile is in enforce mode, not complain mode.
- [ ] There are no unexplained denials during normal service operation.
- [ ] If denials exist, they are reviewed and understood before production use.

4) Test the service under normal conditions

- [ ] Start or restart the service after policy changes.
- [ ] Access the service from an approved client.
- [ ] Confirm the service still performs its required function.
- [ ] Confirm the service can read only the files and directories it needs.
- [ ] Confirm the service can write only to the locations it requires.
- [ ] Confirm the service can use only the capabilities it needs.
- [ ] Confirm expected network access succeeds and unauthorized access fails.

5) Validate deny behavior intentionally

- [ ] Test a connection from a disallowed source network.
- [ ] Confirm UFW blocks the connection.
- [ ] Attempt a request that should trigger AppArmor restrictions.
- [ ] Confirm the application is blocked or logged as expected.
- [ ] Review logs to ensure denies align with policy, not with broken service behavior.
- [ ] Differentiate between a useful block and an accidental outage.

6) Review logs and monitoring

- [ ] Review UFW logs for denied inbound traffic.

- [ ] Review AppArmor logs for denied file, capability, or path access.
- [ ] Confirm the denials are expected and manageable.
- [ ] Confirm log volume is not excessive.
- [ ] Set up alerting or periodic review for repeated denies that may indicate misuse or attack.

7) Check production readiness

- [ ] The allowed network surface is minimal and documented.
- [ ] The service runs with an enforcing AppArmor profile.
- [ ] The service has been tested under normal production-like traffic.
- [ ] No unexpected denials appear in logs.
- [ ] Exceptions are documented with a reason and an owner.
- [ ] Rules and profiles are captured in configuration management or change control.
- [ ] A rollback plan exists in case the policy is too restrictive.
- [ ] Ownership for future maintenance is clear.

8) Common red flags

- [ ] UFW is installed but inactive.
- [ ] Default inbound policy is not deny.
- [ ] A critical port is open to all sources without a clear reason.
- [ ] AppArmor is enabled but the target service has no profile.
- [ ] The profile is in complain mode for production.
- [ ] Denials are present but unreviewed.
- [ ] Firewall rules exist only in upstream tooling, with no local host policy.
- [ ] The service was hardened without a validation test from an approved client.

Quick pass/fail summary

- [ ] Network exposure is minimal.
- [ ] Only intended sources can reach the service.
- [ ] AppArmor is enforcing for the target service.
- [ ] Normal traffic works.
- [ ] Unauthorized access is blocked.
- [ ] Denials are understood and acceptable.
- [ ] The host is ready for production use.

Notes

- Document any exceptions clearly.
- Re-check AppArmor and UFW after package upgrades, service changes, or new listeners.
- Re-validate after any change to cloud firewall rules, load balancers, VPN access, or service configuration.