CHECKLIST

# Windows Server 2022 Firewall Rules Secure Access Checklist

A practical checklist for planning, validating, and reviewing Windows Server 2022 firewall rules before production use.

## Windows Server 2022 Firewall Rules for Secure Access

## Production Readiness Checklist

Use this checklist to plan, validate, and review firewall rules on Windows Server 2022 before you expose a service to production traffic.

---

## 1) Define the business need

- [ ] Identify the exact service that must be reachable.
- [ ] Confirm why the service needs network access.
- [ ] Document the business owner for the exception.
- [ ] Confirm whether the access is temporary or permanent.
- [ ] Record the review date for the rule.

## 2) Identify the required traffic

- [ ] Determine whether the rule is inbound or outbound.
- [ ] Confirm the protocol required: TCP, UDP, or ICMP.
- [ ] Identify the local port or ports in use.
- [ ] Confirm whether the rule should be port-based or program-based.
- [ ] Verify the service or executable path if using a program rule.
- [ ] Check whether the application uses additional helper services or ports.

## 3) Confirm the network profile

- [ ] Check the active profile on the server: Domain, Private, or Public.
- [ ] Verify the rule applies only to the profiles that need it.
- [ ] Avoid enabling the rule on Public unless there is a clear business need.
- [ ] Confirm the server will not move to a less trusted profile unexpectedly.

## 4) Scope the allowed sources

- [ ] List the approved source IP addresses or subnets.
- [ ] Restrict remote IP scope to the smallest practical set.
- [ ] Prefer management subnets, jump hosts, load balancers, or application tiers over broad corporate ranges.
- [ ] Confirm any NAT, proxy, or relay systems that will appear as the source.
- [ ] Avoid ?Any? source unless the service is intentionally public.

## 5) Choose the least risky rule pattern

- [ ] Use the narrowest practical allow rule.
- [ ] Prefer deny-by-default with explicit exceptions.
- [ ] Choose a program rule only when the executable path is stable and well understood.

- [ ] Choose a port rule when the service is tied to a fixed port and needs simpler troubleshooting.
- [ ] Avoid overlapping rules that make the effective exposure difficult to understand.

## 6) Create or adjust the rule

- [ ] Name the rule clearly and consistently.
- [ ] Include the server role or service name in the rule name.
- [ ] Add a description with the justification and owner.
- [ ] Apply the correct direction, protocol, port, and action.
- [ ] Set the approved remote IP scope.
- [ ] Bind the rule to the correct profile(s).
- [ ] Confirm the rule is not broader than intended.

## 7) Check for conflicting policy or precedence

- [ ] Verify whether the rule is local or centrally managed.
- [ ] Check for existing rules that overlap or override the new rule.
- [ ] Review whether Group Policy or another central policy will supersede local settings.
- [ ] Confirm the final effective state, not just the rule entry itself.

## 8) Validate the service state

- [ ] Confirm the service is running.
- [ ] Verify the server is listening on the expected port.
- [ ] Check that the service is bound to the intended interface if relevant.
- [ ] Confirm there are no application-level errors preventing access.
- [ ] Validate any dependent services or certificates required for secure operation.

## 9) Test allowed access

- [ ] Test connectivity from an approved source.
- [ ] Confirm the intended protocol succeeds.
- [ ] Verify the expected response from the service.
- [ ] Check that the test behaves the same after a service restart.
- [ ] Repeat the test from each approved source category if needed.

## 10) Test denied access

- [ ] Test connectivity from a disallowed source.
- [ ] Confirm the connection is blocked as expected.
- [ ] Verify that only the intended source ranges can connect.
- [ ] Check for accidental exposure on alternate profiles or alternate ports.

## 11) Review logging and monitoring

- [ ] Confirm firewall logging is enabled if required by policy.
- [ ] Verify blocked and allowed traffic can be reviewed later.
- [ ] Check whether the service has its own access logs.
- [ ] Make sure alerts exist for unexpected exposure or access failures.

## 12) Document the change

- [ ] Record the change request or ticket number.
- [ ] Document the source addresses, ports, and profiles allowed.
- [ ] Note the reason the exception exists.

- [ ] Record the validation steps performed.
- [ ] Include rollback steps in case the rule must be removed.
- [ ] Save the date of implementation and the next review date.

## 13) Production sign-off check

- [ ] The rule is limited to the required service only.
- [ ] The rule is limited to approved sources only.
- [ ] The rule applies only to the required profile(s).
- [ ] The service works from approved sources.
- [ ] The service is blocked from unapproved sources.
- [ ] The rule is documented and assigned to an owner.
- [ ] The exposure level is acceptable for production.

---

## Quick decision checks

Use these questions before you approve a rule:

- [ ] Can I explain exactly why this rule exists?
- [ ] Do I know which system or subnet needs access?
- [ ] Do I know which port, protocol, or program is required?
- [ ] Have I limited the rule to the correct firewall profile?
- [ ] Have I tested both the allow path and the deny path?
- [ ] Would this rule still make sense in six months?

---

## Safe default reminders

- [ ] Deny by default and allow only what is required.
- [ ] Avoid broad source ranges when a smaller scope works.
- [ ] Avoid Public profile exposure unless it is intentional.
- [ ] Treat every exception as a risk decision.
- [ ] Revisit rules regularly and remove anything no longer needed.

---

## Example rule review summary

Service: Remote administration

Allowed from: Jump host subnet only

Protocol/Port: TCP 3389

Profiles: Domain only

Justification: Administrative access for operations staff

Validation: Connection succeeded from jump host; blocked from user subnet

Review date: _____

---

## Final approval

Before production use, confirm:

- [ ] The firewall rule is minimal.
- [ ] The scope is correct.
- [ ] The profile is correct.
- [ ] The service is validated.
- [ ] The denial behavior is confirmed.
- [ ] The rule is documented and approved.

Approved by: _____

Date: _____