Firewall Rule Review Checklist

Version: 1.0 | **Author:** VarnaAI (varnaai.com) | **License:** Free for commercial use

---

Review Information

Field	Value
Review ID	FRR-**-**
Review Date	**/**/_____
Reviewer	
Firewall Name	
Firewall Platform	
Total Rules Reviewed	
Review Frequency	[ ] Quarterly [ ] Semi-Annual [ ] Annual

Per-Rule Review Checklist

For each rule, verify the following:

Rule Identification

#	Rule Name/ID	Source	Destination	Service	Action	Last Hit Date
1						
2						
3						
4						
5						

Rule Hygiene Checks

1. Unused Rules

Check	Status	Count	Action Required
Rules with zero hits in 90+ days	[ ] Checked		
Rules with zero hits in 180+ days	[ ] Checked		
Rules with zero hits in 365+ days	[ ] Checked		
Disabled rules still in policy	[ ] Checked		

Recommendation: Rules unused for 90+ days should be disabled. Rules unused for 180+ days should be removed.

2. Overly Permissive Rules

Check	Status	Count
Rules with "Any" as source	[ ] Checked	
Rules with "Any" as destination	[ ] Checked	
Rules with "Any" as service/port	[ ] Checked	
Rules allowing "Any/Any/Any"	[ ] Checked	
Rules with port ranges > 100 ports	[ ] Checked	
Rules allowing all outbound traffic	[ ] Checked	

3. Shadowed and Redundant Rules

Check	Status	Count
Rules shadowed by earlier rules (never matched)	[ ] Checked	
Duplicate rules (identical source/dest/service)	[ ] Checked	
Rules that can be consolidated into groups	[ ] Checked	
Contradicting rules (allow + deny same traffic)	[ ] Checked	

4. Compliance Checks

Check	Status	Notes
No rules allowing direct internet access to cardholder data (PCI 1.3)	[ ] Pass [ ] Fail	
Explicit deny-all at end of each zone pair (PCI 1.2.1)	[ ] Pass [ ] Fail	
No rules with "Any" service to DMZ (ISO 27001 A.13.1)	[ ] Pass [ ] Fail	
All management access restricted to jump hosts (CIS 9.2)	[ ] Pass [ ] Fail	
Logging enabled on all deny rules	[ ] Pass [ ] Fail	
Logging enabled on all cross-zone allow rules	[ ] Pass [ ] Fail	
Temporary rules within expiry date	[ ] Pass [ ] Fail	

5. Documentation Checks

Check	Status	Notes
Every rule has a description/comment	[ ] Pass [ ] Fail	
Every rule links to a change request (FCR)	[ ] Pass [ ] Fail	
Rule owner is documented and still employed	[ ] Pass [ ] Fail	

Business justification is still valid	[ ] Pass [ ] Fail	

6. Object/Group Hygiene

Check	Status	Count
Unused address objects	[ ] Checked	
Unused service objects	[ ] Checked	
Unused address groups	[ ] Checked	
Objects with overlapping IPs	[ ] Checked	
Objects with stale DNS entries	[ ] Checked	

Summary

Metric	Count
Total rules reviewed	
Rules to remove (unused)	
Rules to tighten (overly permissive)	
Rules to consolidate	
Shadowed rules found	
Compliance violations	
Undocumented rules	

Risk Score

Rating	Criteria
A (Excellent)	0 compliance violations, <5% unused rules, all rules documented
B (Good)	0-2 compliance violations, <10% unused rules
C (Needs Work)	3-5 compliance violations, 10-20% unused rules
D (Poor)	5+ compliance violations, >20% unused rules, "Any/Any" rules present
F (Critical)	Active compliance violations, uncontrolled "Any/Any" rules, no documentation

This Review Grade: ____

Sign-Off

Role	Name	Signature	Date

Reviewer			
Security Manager			
Compliance Officer			
