Firewall Migration Project Plan

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

---

Project Information

Field	Value
Project Name	
Project Manager	
Start Date	**/**/_____
Target Completion	**/**/_____
Source Platform	[ ] Cisco ASA [ ] Check Point [ ] Juniper SRX [ ] Fortinet [ ] Other: ____
Target Platform	[ ] Palo Alto [ ] Fortinet [ ] Cisco FTD [ ] Check Point [ ] Other: ____
Number of Firewalls	
Total Rules to Migrate	

Phase 1: Discovery and Assessment (Weeks 1-2)

#	Task	Owner	Status	Due Date
1.1	Inventory all firewalls in scope (hostname, model, version, location)		[ ] Done	
1.2	Export current rulebase from each firewall		[ ] Done	
1.3	Document current network topology		[ ] Done	
1.4	Map all zones, interfaces, and routing		[ ] Done	
1.5	Identify NAT rules and translations		[ ] Done	
1.6	Identify VPN tunnels (site-to-site and remote access)		[ ] Done	
1.7	Document all address objects and groups		[ ] Done	
1.8	Document all service objects and groups		[ ] Done	
1.9	Collect traffic logs (minimum 30 days recommended)		[ ] Done	
1.10	Identify unused rules via log analysis		[ ] Done	
1.11	Identify application-level policies (L7)		[ ] Done	
1.12	Document management access methods and users		[ ] Done	
1.13	List all integrations (SIEM, RADIUS, SNMP, syslog)		[ ] Done	
1.14	Create stakeholder contact list		[ ] Done	

Phase 1 Deliverables:

- [ ] Firewall inventory spreadsheet
- [ ] Current rulebase exports
- [ ] Network topology diagram
- [ ] Integration dependency map
- [ ] Unused rule report

Phase 2: Rule Cleanup and Optimization (Weeks 2-3)

#	Task	Owner	Status	Due Date
2.1	Remove unused rules (zero-hit for 180+ days)		[ ] Done	
2.2	Remove disabled/expired rules		[ ] Done	
2.3	Consolidate duplicate rules		[ ] Done	
2.4	Resolve shadowed rules		[ ] Done	
2.5	Tighten overly permissive rules (Any/Any)		[ ] Done	
2.6	Standardize object naming convention		[ ] Done	
2.7	Document business owner for each rule		[ ] Done	
2.8	Get sign-off from rule owners on cleanup		[ ] Done	

Phase 2 Deliverables:

- [ ] Cleanup report (rules removed, consolidated, tightened)
- [ ] Optimized rulebase (pre-migration baseline)
- [ ] Rule owner sign-off

Rule Count Tracking:

Metric	Count
Original rule count	
Rules removed (unused)	
Rules consolidated	
Rules tightened	
Final rule count for migration	

Phase 3: Translation and Configuration (Weeks 3-5)

#	Task	Owner	Status	Due Date
3.1	Translate address objects to target platform format		[ ] Done	

3.2	Translate service objects to target platform format		[ ] Done	
3.3	Translate security rules (with zone mapping)		[ ] Done	
3.4	Translate NAT rules		[ ] Done	
3.5	Configure VPN tunnels on target platform		[ ] Done	
3.6	Configure routing (static, OSPF, BGP)		[ ] Done	
3.7	Configure management access (SSH, HTTPS, SNMP)		[ ] Done	
3.8	Configure logging and SIEM integration		[ ] Done	
3.9	Configure authentication (RADIUS/TACACS+)		[ ] Done	
3.10	Configure HA pair (if applicable)		[ ] Done	
3.11	Enable application-level inspection (L7) where applicable		[ ] Done	
3.12	Peer review of all translated rules		[ ] Done	

Phase 3 Deliverables:

- ☐ Target platform configuration (staged, not deployed)
- ☐ Translation mapping document (source rule → target rule)
- ☐ Peer review sign-off

Phase 4: Testing (Weeks 5-6)

#	Task	Owner	Status	Due Date
4.1	Lab/staging environment prepared		[ ] Done	
4.2	Deploy configuration in lab environment		[ ] Done	
4.3	Test connectivity for each zone pair		[ ] Done	
4.4	Test all NAT translations		[ ] Done	
4.5	Test all VPN tunnels		[ ] Done	
4.6	Test management access (SSH, HTTPS)		[ ] Done	
4.7	Test SIEM/syslog integration		[ ] Done	
4.8	Test HA failover		[ ] Done	
4.9	Run compliance scan against new configuration		[ ] Done	
4.10	Performance/throughput testing		[ ] Done	
4.11	Application team validation (critical apps)		[ ] Done	
4.12	Document test results		[ ] Done	

Phase 4 Deliverables:

- [ ] Test plan with results
- [ ] Application team sign-off
- [ ] Go/No-Go decision

Phase 5: Migration Execution (Week 6-7)

Pre-Migration Checklist (Day of Migration)

#	Check	Status
5.1	Change request approved	[ ] Done
5.2	Rollback plan documented and tested	[ ] Done
5.3	All stakeholders notified of maintenance window	[ ] Done
5.4	Backup of current firewall configuration	[ ] Done
5.5	War room / bridge call established	[ ] Done
5.6	Monitoring dashboards open	[ ] Done
5.7	Application support teams on standby	[ ] Done

Migration Steps

#	Step	Time	Owner	Status
5.8	Take final backup of source firewall	T+0		[ ] Done
5.9	Deploy target firewall in parallel (if applicable)	T+__		[ ] Done
5.10	Switch traffic to target firewall	T+__		[ ] Done
5.11	Verify connectivity — zone by zone	T+__		[ ] Done
5.12	Verify NAT translations	T+__		[ ] Done
5.13	Verify VPN tunnels	T+__		[ ] Done
5.14	Verify logging/SIEM	T+__		[ ] Done
5.15	Application team smoke tests	T+__		[ ] Done
5.16	Confirm stable — end maintenance window	T+__		[ ] Done

Rollback Triggers

- [ ] Critical application unavailable for >15 minutes
- [ ] VPN tunnel failure affecting remote sites
- [ ] Packet loss >1% on production traffic
- [ ] Security monitoring blackout >30 minutes

Rollback Procedure: Switch traffic back to source firewall within ____ minutes.

Phase 6: Post-Migration (Weeks 7-8)

#	Task	Owner	Status	Due Date
6.1	Monitor for 7 days — track dropped/denied traffic		[ ] Done	
6.2	Resolve any false positives from new ruleset		[ ] Done	
6.3	Validate all compliance requirements still met		[ ] Done	
6.4	Update network topology documentation		[ ] Done	
6.5	Update CMDB/asset inventory		[ ] Done	
6.6	Decommission source firewall		[ ] Done	
6.7	Archive source firewall configuration		[ ] Done	
6.8	Lessons learned session		[ ] Done	
6.9	Final project report		[ ] Done	

Risk Register

Risk	Impact	Likelihood	Mitigation
Rule translation error causes outage	High	Medium	Peer review + lab testing
VPN re-establishment takes longer than window	High	Low	Pre-negotiate with remote site contacts
Application breaks due to L7 inspection	Medium	Medium	Whitelist known apps before cutover
HA failover fails on new platform	High	Low	Test failover in lab and during migration
Rollback exceeds maintenance window	High	Low	Practice rollback in lab, keep source hot

---

RACI Matrix

Activity	PM	Network	Security	App Teams	Management
Discovery	A	R	C	C	I
Rule Cleanup	A	R	R	C	I
Translation	A	R	C	I	I
Testing	A	R	R	R	I
Migration	A	R	C	C	I
Post-Migration	A	R	C	C	I

R = Responsible, A = Accountable, C = Consulted, I = Informed

---

Sign-Off

Milestone	Approver	Signature	Date
Phase 1 Complete			
Phase 2 Complete			
Phase 4 Go/No-Go			
Migration Complete			
Project Closed			
