Syntho Quest

FIREWALL VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

Scope: Perimeter / edge / next-gen / virtual firewalls (stateful, NGFW, cloud firewalls, web application firewalls). Test config, rules, management plane, logging, NAT/port-forwarding, VPN, IDS/IPS features, updates/firmware, and high-risk policies.

Core goals

- Verify rule correctness (least-privilege), detect overly permissive rules, broken NAT/port-forwards.
- Find management/remote access weaknesses (default creds, exposed consoles).
- Identify bypass paths (VPN, proxy, tunnels, application layer).
- Test logging/alerting and firmware/backdoor issues.
- Produce prioritized, actionable remediation + retest plan.

Top test areas (must cover)

1. Rulebase review — redundant/overlapping rules, ANY/0.0.0.0/0 allowances, overly broad source/destination/service.
2. NAT & Port-Forwarding — exposed services, public-to-private mappings, hairpinning issues.
3. Management plane — admin interface exposure, default creds, weak auth (HTTP vs HTTPS), MFA absence.
4. VPN & Remote Access — misconfigured tunnels, split-tunneling risks, weak crypto, auth bypass.
5. Application inspection / NGFW features — incorrect app signatures, SSL inspection gaps, bypassable IPS rules.
6. Bypass & Tunneling — DNS/HTTP/ICMP tunneling, proxy chains, IPv6 misconfig, VLAN hopping.
7. Logging & Monitoring — insufficient logs, missing outbound/inbound alerts, log tampering risk.
8. Firmware & Supply Chain — outdated firmware, unsigned images, known CVEs, hidden accounts.
9. High availability & failover — insecure sync channels, cleartext replication of configs/secrets.
10. Cloud & Virtual Firewalls — cloud security groups vs firewall rules mismatches, API permissions.