Website Firewall Readiness Audit Checklist

20-Point Firewall Deployment Audit

☐ Is a WAF or CDN firewall active?
☐ Are managed threat rules enabled?
☐ Are admin routes protected?
☐ Is wp-login or admin rate-limited?
☐ Are bots challenged?
☐ Are exploit payload signatures blocked?
☐ Are upload paths reviewed?
☐ Are checkout/account pages protected?
☐ Are geographic anomalies monitored?
☐ Are suspicious IPs blocked?
☐ Are alerts configured?
☐ Are firewall logs reviewed monthly?
☐ Are false positives reviewed?
☐ Are top blocked patterns analysed?
☐ Are plugin changes reflected in firewall rules?
☐ Is XML-RPC reviewed if WordPress?
☐ Are customer logins protected?
☐ Is DDoS filtering available?
☐ Is firewall tuning ongoing?
☐ Does the firewall create measurable friction?

Scoring:

17–20 = Strong perimeter defence maturity
12–16 = Moderate firewall effectiveness
0–11 = High avoidable exposure remains