FortiGate Hardening Checklist

BLACKHAWK DATA

Administrative Access

- [ ] Default admin password changed
- [ ] Trusted hosts configured for admin access
- [ ] HTTPS-only admin access (HTTP disabled)
- [ ] Admin session timeout configured (max 15 min)
- [ ] Two-factor authentication for admin accounts
- [ ] Login banner configured
- [ ] Admin profiles with least privilege

Network Security

- [ ] Unused interfaces disabled
- [ ] Management interface on dedicated VLAN
- [ ] DNS set to trusted resolvers (not ISP defaults)
- [ ] NTP configured with authentication
- [ ] SNMP community strings changed from defaults
- [ ] SNMPv3 used instead of v1/v2c

Firewall Policy

- [ ] Deny-all default policy in place
- [ ] No any/any allow rules
- [ ] Unused policies removed
- [ ] Policy logging enabled for all rules
- [ ] IPS profiles applied to relevant policies
- [ ] Application control enabled
- [ ] SSL deep inspection configured where appropriate

Logging & Monitoring

- [ ] FortiAnalyzer or syslog configured
- [ ] Log all traffic (or at minimum denied traffic)
- [ ] Alert thresholds configured
- [ ] Firmware on vendor-recommended version
- [ ] Automatic signature updates enabled