



## Firewall Security Audit Checklist

Score each item:

- Yes = 2 points
  - Partially = 1 point
  - No = 0 points
- 

### Perimeter Rule Security

- 1. Only business-critical services are publicly exposed.
  - 2. Old inbound ports are reviewed and removed regularly.
  - 3. Broad “allow all” style rules have been eliminated.
  - 4. Vendor access exceptions are documented and limited.
- 

### Outbound Traffic Control

- 5. Suspicious outbound traffic is monitored.
  - 6. Unnecessary outbound destinations or categories are restricted.
  - 7. DNS anomalies are reviewed when possible.
- 

### Administrative Console Protection

- 8. Firewall admin accounts are unique and named.
  - 9. MFA protects firewall management access.
  - 10. Firewall management portals are not openly exposed.
  - 11. Admin rights are reviewed periodically.
- 

### VPN and Remote Connectivity

- 12. VPN accounts are individually assigned.
- 13. Dormant VPN users are removed promptly.
- 14. Remote sessions require MFA.
- 15. Remote users receive only necessary internal access.

---

## Logging and Visibility

- 16. Firewall logs are centrally retained.
- 17. Repeated denied inbound attempts are reviewed.
- 18. Administrative changes are logged and attributable.
- 19. Security alerts have assigned human review.

---

## Governance and Lifecycle

- 20. Firewall rules are documented with business purpose.
- 21. Quarterly or periodic rule cleanup is performed.
- 22. Firmware updates are maintained.
- 23. Configuration backups exist before major changes.
- 24. Firewall ownership is clearly assigned.
- 25. Leadership receives periodic perimeter risk summaries.

---

## SCORING RESULTS

### 40–50 Points — Strong Maturity

Your firewall is being managed as an intentional perimeter security asset.

### 22–39 Points — Moderate Exposure

Key protections exist, but historical drift or inconsistent review leaves meaningful risk.

### 0–21 Points — High Vulnerability

Your firewall may be functioning operationally while still permitting significant avoidable perimeter exposure.