ECHELON
RISK +
CYBER

# Managed Firewall Security Checklist

Firewalls are a critical component of your network's first line of defense. This checklist offers a comprehensive guide to optimizing firewall security, from deploying next-generation firewalls to implementing geo-restriction rules. By maintaining up-to-date configurations and leveraging advanced features, you can reduce the attack surface and protect against potential threats.

□ Deploy next-generation firewalls to provide both traffic filtering and intrusion prevention.

□ Regularly review firewall rules to ensure they follow the principle of least privilege.

□ Use network segmentation to isolate critical assets and minimize the attack surface.

□ Implement intrusion detection/prevention systems (IDS/IPS) to detect and block malicious traffic.

□ Enable threat detection policies

□ Ensure VPNs are encrypted and use strong authentication for secure remote access.

□ Enable logging for all firewall events and send logs to a centralized logging platform for analysis.

□ Configure access control lists (ACLs) to limit inbound and outbound traffic to only necessary sources.

□ Implement geo-restriction rules for enhanced control.

□ Maintain a documented change management process for firewall rules.

□ Enable automatic updates for firewall signatures and firmware to keep protections up to date.

**Strengthen your firewall defenses—connect with Echelon Risk + Cyber to explore our Managed Firewall Security solutions.**

We defend the basic human right to security and privacy. echeloncyber.com