Firewall Setup and Configuration

This checklist is designed to guide you in adding and configuring a new firewall instance for your network.

By following these steps, you can ensure robust network protection and minimize vulnerabilities to cyber threats.

# 1. Initial Setup and Access Control

☐ Unbox and physically connect the firewall to your network (if hardware-based).
☐ Connect to the firewall management interface (via browser, console, or CLI).
☐ Change the default admin credentials to a strong, unique password.
☐ Enable Multi-Factor Authentication (MFA) for all administrative accounts.
☐ Limit management access to trusted IP addresses or subnets.

# 2. Network Configuration

☐ Configure interfaces (e.g., WAN, LAN, DMZ) with appropriate IP addresses.
☐ Define VLANs and segment the network for better isolation and security.
☐ Set up DHCP if needed or ensure proper IP addressing within your network.
☐ Enable routing protocols if required (e.g., OSPF, BGP) for network connectivity.

# 3. Firewall Rules and Policies

☐ Implement a default deny rule for inbound and outbound traffic.
☐ Create allow rules only for required traffic based on business needs.
☐ Restrict administrative access to the firewall (e.g., allow only from internal network).
☐ Define policies for specific traffic types (e.g., HTTP/HTTPS, email, DNS).
☐ Regularly review and optimize firewall rules to minimize unnecessary exposure.

# 4. Threat Protection and Logging

☐ Enable Intrusion Detection/Prevention System (IDS/IPS) features to detect and block malicious traffic.
☐ Configure anti-virus, anti-spam, and malware filtering if supported.
☐ Enable logging for all critical activities and traffic.
☐ Forward logs to a centralized logging server or SIEM for analysis and compliance.

# 5. VPN Setup for Remote Access

☐ Configure site-to-site VPN or remote-access VPN as required.
☐ Use strong encryption protocols (e.g., AES-256, IPsec, or TLS).
☐ Enforce Multi-Factor Authentication (MFA) for VPN access.
☐ Set up split tunneling or full tunneling based on your security requirements.

# 6. Security Hardening

☐ Disable unused services and interfaces to reduce the attack surface.
☐ Update the firewall firmware/software to the latest version.
☐ Enable secure management protocols (e.g., HTTPS, SSH) and disable insecure ones (e.g., HTTP, Telnet).
☐ Create backup configurations and store them securely.
☐ Schedule regular updates and security patching.

# 7. Monitoring and Maintenance

☐ Set up email or SMS alerts for critical events.
☐ Use a dashboard or monitoring tool to track firewall performance and threat statistics.
☐ Conduct regular firewall policy audits to ensure compliance with security standards.
☐ Schedule penetration testing to validate firewall effectiveness.

Need a hand with the next step?

If you have a question about any of these steps, or need help setting up a more advanced or tailored solution, we're here for you!

Feel free to send us an email at contact@403bits.com.

For simpler queries, we'll gladly share advice or point you in the right direction — free of charge!

And if you're facing a more complex challenge or want to save time, our experts can take over and deliver a comprehensive setup that perfectly fits your needs.

We're here to help you build security and efficiency
so you can focus on growing your business!

If you liked this checklist or have improvement suggestions, - let us know contact@403bits.com.