CLOUDSWITCHED

FREE RESOURCE — GUIDE

Firewall Configuration Best Practices

Essential firewall rules, port management, zone-based policies, and maintenance procedures. Harden your network perimeter with these proven security practices for UK businesses.

6	Zero Trust	90 Days	Free
KEY PRACTICE AREAS	RECOMMENDED APPROACH	RULE REVIEW CYCLE	SECURITY GUIDE

Who This Guide Is For

This guide is written for IT managers and network administrators responsible for maintaining firewall security. It covers best practices applicable to all enterprise firewalls including Fortinet, Meraki, Palo Alto, SonicWall, and pfSense.

1 Rule Management Principles

Follow these fundamental principles when creating and maintaining firewall rules.

The principle of least privilege is the foundation of firewall security. Every rule should grant the minimum access required for a specific, documented business need. If you cannot justify why a rule exists, it should be removed.

- → **Default deny:** Start with a deny-all policy and add explicit allow rules. Never use a default-allow approach.
- → **Document every rule:** Each rule must have a description stating its purpose, who requested it, when it was created, and when it should be reviewed.
- → **Specific over broad:** Use specific IP addresses and ports rather than broad ranges. Avoid 'any' in source, destination, or service fields wherever possible.
- → **Rule ordering matters:** Place the most specific rules first and the most general last. Place frequently matched rules higher for performance.
- → **Separate inbound and outbound:** Manage ingress and egress rules independently. Many organisations focus on inbound but neglect outbound filtering.
- → **Log denied traffic:** Enable logging on deny rules to identify blocked legitimate traffic and potential attacks.

Common Mistake: Overly Permissive Rules

Rules using 'any' for source, destination, AND service are effectively disabling the firewall for that traffic flow. These rules are the most common cause of security breaches through firewalls. Audit for and eliminate any such rules immediately.

2 Zone-Based Security Architecture

Implement security zones to control traffic flow between different trust levels.

A zone-based architecture groups network interfaces and VLANs into security zones. Traffic between zones is controlled by inter-zone policies, creating a layered security model.

ZONE	TRUST LEVEL	CONTAINS	TYPICAL POLICY
WAN (Untrusted)	0 (Lowest)	Internet-facing interfaces	Deny all inbound except explicit allows
DMZ	25	Public-facing servers, web apps	Limited inbound from WAN, no direct access to LAN
Guest	30	Guest WiFi, visitor devices	Internet access only, no internal access
Corporate LAN	75	User workstations, printers	Full internal access, filtered internet
Server Zone	85	Production servers, databases	Restricted access from LAN, no direct WAN access
Management	100 (Highest)	Firewalls, switches, admin tools	Highly restricted, admin access only

Inter-Zone Policy Design

Define explicit policies for every zone-to-zone traffic flow. Traffic from lower trust zones to higher trust zones should be denied by default and allowed only for specific, documented requirements. Traffic from higher to lower zones can be more permissive but should still be logged and monitored.

3 Essential Port Management

Control which ports and services are accessible through the firewall.

Close everything by default and open only what is specifically required. Common ports that should be carefully managed:

PORT	SERVICE	RECOMMENDATION
22	SSH	Allow only from management zone to specific devices. Use key-based auth.
25	SMTP	Allow outbound to mail relay only. Block direct outbound from workstations.
53	DNS	Allow outbound to designated DNS servers only. Block other DNS for security.
80/443	HTTP/HTTPS	Allow outbound for users. Inbound only to DMZ web servers.
445	SMB	Never expose to WAN. Internal only within server and LAN zones.
3389	RDP	Never expose to WAN. Use VPN for remote access. Internal only with MFA.
1433/3306	SQL	Never expose to WAN. Restrict to application servers only.

Critical: Block RDP from the Internet

Remote Desktop Protocol (port 3389) exposed to the internet is one of the most exploited attack vectors. Ransomware groups actively scan for exposed RDP. Always require VPN or ZTNA for remote access. This single action prevents a significant percentage of attacks.

4 Maintenance & Review Schedule

Establish a regular maintenance and review cycle for firewall health and security.

TASK	FREQUENCY	OWNER	NOTES
Firmware update check	Monthly	Network Admin	Apply critical patches within 48 hours
Rule review and cleanup	Every 90 days	IT Manager + Admin	Remove unused rules, verify documentation
Log review for anomalies	Weekly	Security/SOC	Check for denied traffic patterns, port scans
Configuration backup	After every change	Network Admin	Store encrypted in version-controlled repository
Failover/HA test	Quarterly	Network Admin	Verify secondary firewall takes over cleanly
Full security audit	Annually	External auditor	Independent review of configuration and policies

Configuration Change Control

Every firewall change should follow a change management process: request, review, approve, implement, test, document. Maintain a changelog with dates, changes made, reasons, and the person responsible. Back up the configuration before and after every change.

Notes

Need Expert Firewall Management?

Our network engineers can audit, optimise, and manage your firewall infrastructure for maximum security.

info@cloudswitched.com
New London House, 6 London St, London EC3R 7LR

Prepared by: ________________________ Date: ________________________ Approved by: ________________________