CLOUDSWITCHED

FREE RESOURCE — BEST PRACTICES 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.

4	Zero Trust	90d	Free
PRACTICE AREAS COVERED	RECOMMENDED APPROACH	RULE REVIEW CYCLE	SECURITY GUIDE

RULE MANAGEMENT · ZONE ARCHITECTURE · PORT HYGIENE · MAINTENANCE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Read-only PDF

01

Rule management principles

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. The principles below apply to every enterprise firewall, including Fortinet, Meraki, Palo Alto, SonicWall, and pfSense.

Deny	90 d	Log
DEFAULT POLICY FOR EVERY ZONE	MAXIMUM GAP BETWEEN RULE REVIEWS	EVERY DENY RULE — NOT JUST THE ALLOWS

Six rules to live by when writing firewall policy

Default deny. Start with a deny-all policy and add explicit allow rules. Never use a default-allow approach — if the firewall fails open, anything reachable is reachable.

Document every rule. Each rule must carry a description stating its purpose, who requested it, when it was created, and when it should next be reviewed. Undocumented rules become un-removable rules.

Specific over broad. Use specific IP addresses, ports, and services 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 — a top-N hit count is your friend.

Separate inbound and outbound. Manage ingress and egress rules independently. Most organisations focus on inbound but neglect outbound filtering — that is how data leaves the network.

Log denied traffic. Enable logging on deny rules to identify blocked legitimate traffic, misconfigured services, and active reconnaissance against the perimeter.

COMMON MISTAKE — OVERLY PERMISSIVE RULES

Rules using `any` for source, destination, AND service are effectively disabling the firewall for that traffic flow. These are the single most common cause of breaches through a firewall. Audit for them and eliminate them immediately — if a business owner cannot describe what the rule should allow, it should not exist.

02

Zone-based security architecture

A zone-based architecture groups interfaces and VLANs into **security zones** controlled by inter-zone policies, so compromise of one segment does not automatically expose the rest.

The six standard zones for a UK SME network

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 Wi-Fi, 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

Lower-to-higher is deny by default. Traffic from a less trusted zone to a more trusted one is denied unless documented — the rule that stops the DMZ becoming a pivot into the LAN.

Management is an island. Reachable only from named admin workstations or a jump host — never from the user LAN at large, and never from the WAN.

Guest never touches internal. Guest Wi-Fi routes straight to the internet; no visitor device should ever reach a production server.

DOCUMENT THE ZONE MAP

Maintain a zone-and-policy diagram alongside the configuration: which VLANs sit in each zone, which interface terminates each zone, and which inter-zone policies exist. Otherwise the model lives only in the head of whoever last touched the firewall.

03

Essential port management

Close everything by default and open only what is specifically required. The ports below cause the majority of real-world incidents on UK SME networks — either because they were left exposed to the internet, or because outbound traffic on them was never restricted.

Ports that need careful management

PORT	SERVICE	RECOMMENDATION
`22`	SSH	Allow only from the management zone to specific devices. Key-based auth, no passwords.
`25`	SMTP	Allow outbound to the mail relay only. Block direct outbound SMTP from workstations.
`53`	DNS	Allow outbound to designated DNS servers only. Block other DNS to stop tunnelling.
`80 / 443`	HTTP / HTTPS	Allow outbound for users. Inbound only to DMZ web servers, never to the LAN.
`445`	SMB	Never expose to the WAN. Internal only within the server and LAN zones.
`3389`	RDP	Never expose to the WAN. VPN or ZTNA for remote access. Internal only with MFA.
`1433 / 3306`	SQL	Never expose to the WAN. Restrict to application servers only.

Outbound is just as important as inbound

Block outbound SMB and RDP to the internet. A workstation should never need to speak these to a public address — if it does, that is almost certainly malware or exfiltration in progress.

Restrict outbound DNS to your resolvers. Forcing all DNS through your own resolvers blocks DNS tunnelling and gives visibility into the hosts each device is trying to reach.

CRITICAL — BLOCK RDP FROM THE INTERNET

Remote Desktop Protocol (port `3389`) exposed to the internet is one of the most exploited attack vectors today. Ransomware groups actively scan for exposed RDP and chain it with credential stuffing. Always require VPN or ZTNA in front of RDP — this single change prevents a significant percentage of attacks on UK SMEs.

04

Maintenance & review schedule

A firewall is not a one-off project — it is an ongoing operating discipline. Establish a regular cadence for firmware, rules, logs, and configuration backups, and assign every task to a named owner. Without an owner, every task drifts.

Recommended cadence

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 a version-controlled repository
Failover / HA test	Quarterly	Network admin	Verify the 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, the reason, and the person responsible. Back up the configuration before and after every change — rollback is only available if you took the backup.

CLOUDSWITCHED

NETWORK SECURITY & FIREWALL MANAGEMENT

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom