Firewall basics cheat sheet

Vendor-neutral. The same ideas apply to Fortinet, Palo Alto, Cisco, Sophos, pfSense and cloud security groups.

Firewall types

Type	What it checks
Packet filter (ACL)	Source/destination IP, protocol, port; no memory of connections
Stateful	Tracks connections, so replies are allowed back automatically
NGFW	Adds application ID, user ID, IPS, URL filtering, TLS inspection
WAF	Protects web apps (SQL injection, XSS) at Layer 7
Host firewall	On the device itself (Windows Defender Firewall, ufw, iptables/nftables)
Cloud	Security groups / NSGs and cloud firewalls around workloads

How rules are processed

1. Rules are read **top to bottom**; the **first match** wins.
2. Anything that matches nothing hits the **default deny**.
3. Put specific rules above general ones.
4. Stateful firewalls allow the reply traffic of an allowed session.

Zones and DMZ

Zone	Typical trust
Inside / LAN	Trusted users and devices
DMZ	Public servers (web, mail relay): reachable from outside, limited inside
Outside / WAN	Internet: untrusted
Guest, IoT, servers	Separate zones, only the access they need

> Default flows: inside → outside allowed (with inspection); outside → inside denied; outside → DMZ only to published services.

NAT in one table

Kind	Use
Source NAT / PAT	Many inside users share one public IP
Destination NAT (port forward / VIP)	Publish an inside server on a public IP and port
Static 1:1 NAT	One private IP always maps to one public IP

Writing a good rule

- **Least privilege:** exact source, destination and service; avoid "any any".
- Use named **address and service objects**, not raw numbers.
- Give every rule a **name, owner, ticket number and review date**.
- Turn on **logging** for allow and deny rules that matter.
- Never expose RDP, SMB, databases or admin pages to the internet: use a VPN.
- Admin access: separate management network, MFA, no shared accounts.
- Review rules regularly; remove unused and duplicate ones.

Troubleshooting blocked traffic

1. Get the exact flow: source IP, destination IP, port, time.
2. Search the **traffic log** for it: denied, allowed or not seen at all?
3. **Not seen:** routing problem, or traffic never reached the firewall.
4. **Denied:** which rule matched? Check order, objects, zones.
5. **Allowed but fails:** check NAT, the return route, the host firewall and the app itself.
6. Use the vendor's policy lookup / packet tracer tool to test.

Useful tests

Command	What it does
`Test-NetConnection host -Port 443`	Windows: is the port reachable?
`nc -zv host 443`	Linux/macOS: quick TCP port test
`curl -v https://host`	Full HTTPS handshake and response
`traceroute / tracert host`	Where does the path stop?

© 2026 FM TecHub · Free to print and share for personal study. Please don't sell or republish.