Firewall Basics Guide

Ports, protocols, rule anatomy, and reachability testing without treating memorization as the whole skill.

Ports are labels for conversations. Firewalls make decisions using direction, zone, source, destination, service, identity, state, and policy order.

COMMON PORTS

SERVICE	PORT	NOTES
SSH	TCP/22	Encrypted remote shell. Prefer over Telnet.
DNS	UDP/TCP 53	UDP is common. TCP is normal for large answers, zone transfer, and some resolver behavior.
DHCP	UDP 67/68	Broadcast or relay-assisted client addressing.
HTTP	TCP/80	Cleartext web traffic.
HTTPS	TCP/443, UDP/443	TCP for traditional TLS. UDP/443 is common for QUIC and HTTP/3.
NTP	UDP/123	Time sync. Critical for logs, certs, auth, and troubleshooting.
RDP	TCP/3389	Restrict heavily. Use VPN, ZTNA, or jump hosts.

Rule Anatomy

- Source zone and address.
- Destination zone and address.
- Application or service.
- User or identity context.
- Action: allow, deny, reject, inspect.
- Logging and hit count.

Stateful Means

The firewall tracks sessions. Return traffic for an allowed session is usually permitted without a separate reverse rule. Asymmetric routing can break that assumption.

TEST REACHABILITY

NEED	BETTER TOOL	WHY
Is TCP open?	`nc -vz host 443`	Simple connect test on macOS/Linux.
Windows TCP test	`Test-NetConnection host -Port 443`	Built-in PowerShell test.
Web app behavior	`curl -vk https://host/path`	Shows HTTP status, TLS behavior, redirects.
TLS details	`openssl s_client -connect host:443 -servername host`	Shows cert and handshake details.
UDP service	App-specific test or packet capture	UDP has no simple universal open or closed result.

Allow vs Reject vs Drop

Reject is useful inside controlled networks because it fails fast. Drop is common at untrusted edges. Choose intentionally, not by habit.

Log What Matters

Log denies during build and troubleshooting. Tune noisy rules later. A firewall without usable logs becomes a guessing machine.

TROUBLESHOOTING FLOW

1. Confirm source IP, destination IP, protocol, and port.
2. Confirm route and NAT before blaming policy.
3. Check rule order and shadowed rules.
4. Check whether the firewall sees both directions.
5. Check session table and deny logs.
6. Test from the same source network as the failing client.

Beginner Mistakes

- Opening TCP when the service uses UDP.
- Testing by hostname while DNS is broken.
- Forgetting NAT changes the address the policy sees.
- Allowing the port but blocking the app dependency.
- Assuming ping proves the application works.

Canonical Lookup

Use this guide for firewall concepts and testing workflow. Use the HTML Common Ports sheet for the fast Packet Life-style port lookup.