Screened Subnet (DMZ) Firewall - what it is, why it helps, and how to set it up safely

Gridinsoft Help Center

What it is

A screened subnet (also called a DMZ) is a simple layout with three areas: the internet, a small "buffer" network for public stuff (DMZ), and your private home/office network (LAN). People on the internet can only reach the DMZ (like your website or mail gateway). Your private network stays hidden behind the firewall, and DMZ machines can’t freely reach into it.

Why it matters

If a public server gets hacked, the damage is contained in the DMZ instead of spilling into your private devices. It keeps risky traffic at arm’s length and makes problems easier to spot and fix.

How it works

- Three zones: Internet -> Firewall -> DMZ -> Firewall -> Private network.

- Publish safely: put public-facing services in the DMZ.

- Tight rules: only the ports you need are opened; direct internet -> private network is blocked.

- Limited reach-back: DMZ can talk to the private network only on specific, logged ports (if needed).

- Outbound control: traffic leaving the DMZ/private network is filtered and monitored.

Red flags

- Any rule that lets the internet talk straight to your private network.

- DMZ servers using admin accounts that can control your private devices.

- "Side doors" that bypass the firewall (a second, forgotten internet connection).

- Over-broad rules like "allow everything out from everywhere."

Do it right

- Start with "block by default," then allow only what’s required.

- Keep origins private; use a reverse proxy/WAF in the DMZ if you host sites.

- Use a VPN or jump host for admin access - never open raw RDP/SSH to the internet.

- Log and alert on rule changes and denied traffic; keep DMZ systems lean and updated.