

Lessons learned & gotchas

- **The single-MAC rule is the gotcha that catches everyone.** A VM that "has no network" on a public IP is, nine times out of ten, a VM whose MAC was never reserved upstream. The symptom looks like a broken VM; the cause is the provider dropping unknown-MAC frames. Check the reservation first, always.
- **Graduate to a routed subnet or vSwitch sooner than you think.** The per-IP MAC reservation is fine for one or two addresses and tedious for more. If you can already see yourself wanting several public IPs, skip ahead.
- **Keep the private side genuinely private.** VMs should default-route out through pfSense (NAT), exposing nothing except what you deliberately publish through it. The gateway is also your firewall — use it.
- **Write down which method a given host uses.** The three approaches look similar once running but are configured very differently. Future-you, debugging at midnight, will be grateful to know whether this box uses a reserved MAC, a routed block, or a vSwitch.

“ **Lesson in one line:** on this kind of hosting, "the VM can't reach the internet" is almost always an upstream MAC/routing rule, not a problem inside the VM. Learn the provider's rule first; debug the guest second.

Revision #1

Created 2026-04-13 10:43:02 UTC by Eslam Shapsough

Updated 2026-04-13 10:52:02 UTC by Eslam Shapsough