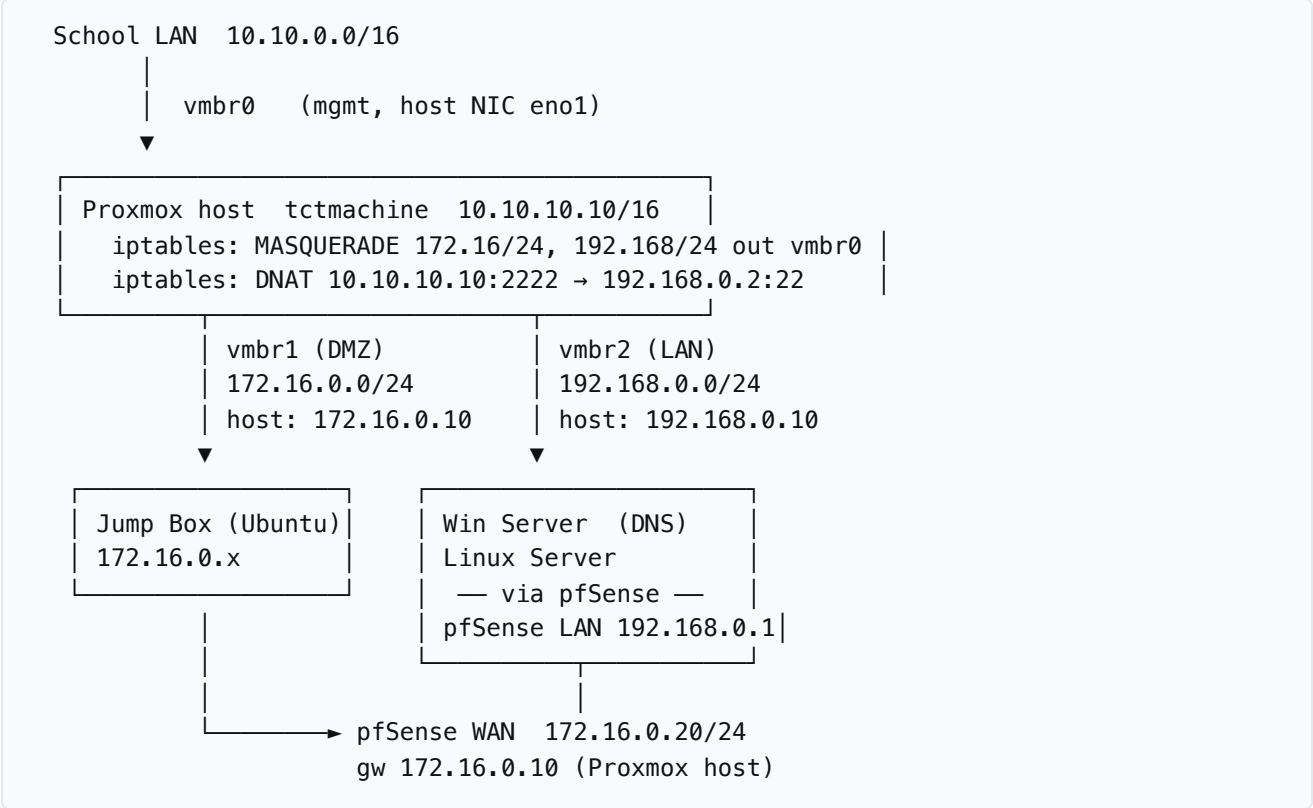
pfSense Setup — Capstone Week 2

HPE ProLiant ML350p Gen8 · Proxmox VE 8.2 host `tctmachine` (10.10.10.10/16) · pfSense CE on Netgate installer 1.1.1-RELEASE
Generated 2026-04-28 · for Hak (Cybertex Server+ capstone, instructor: Anthony Pena)

> **Important context.** The newer Week 1–5 ODT guide does *not* use pfSense — it puts NAT/PAT on the Proxmox host itself and uses a Linux Jump Box. You are deliberately blending the two: pfSense as the LAN-side router (DMZ → LAN), with host iptables MASQUERADE as the upstream path to the school network. Keep both layers consistent or you'll chase asymmetric-routing ghosts.

1. Where pfSense sits in the topology



2. VM specs (Proxmox)

Field	Value
Name	`pfsense`
VM ID	(next free, e.g. 100)
OS / ISO	Netgate pfSense CE installer (downloaded ISO uploaded to `local` storage)
BIOS	SeaBIOS (default)
Machine	q35
SCSI controller	VirtIO SCSI single
Disk	20 GB, `local-lvm`, format raw, Discard ✓, SSD emulation off
CPU	2 vCPU, type `host` (single-socket box, conserve cores)
Memory	2048 MB (no ballooning)
Network 1 (WAN)	Bridge `vmbr1`, Model **Intel E1000**, firewall off
Network 2 (LAN)	Bridge `vmbr2`, Model **Intel E1000**, firewall off
Start at boot	Yes, boot order 1 (so LAN is up before downstream VMs)

E1000 is required because pfSense expects `em0` / `em1` device names. VirtIO works but renames the interfaces and breaks the rest of the guide's assumptions.

3. Install pfSense

1. Upload ISO: Proxmox GUI → `local` → ISO Images → Upload.
2. Create the VM with the specs above; attach the ISO to `ide2` as CD-ROM.
3. Start the VM and open the noVNC console.
4. Accept the copyright notice → **Install**.
5. Keymap: default (US) unless you've changed it.
6. Partitioning: **Auto (ZFS)** → **stripe** (single disk) → select `da0` (or `vtbd0`) → confirm wipe.
7. Wait for the install to finish, decline the manual config shell, **Reboot**.
8. Detach the ISO from `ide2` before the reboot completes (Hardware → CD/DVD → Edit → Do not use any media).

4. Console interface assignment

On first boot pfSense lands at the console menu. Pick option `1` (Assign Interfaces).

```
Should VLANs be set up now [y|n]?          n
Enter the WAN interface name:              em0
Enter the LAN interface name (or nothing): em1
Enter the Optional 1 interface name:       (blank, press Enter)
Do you want to proceed [y|n]?              y
```

Confirm the summary shows `WAN → em0`, `LAN → em1`.

5. Set IPs from the console

From the console menu pick `2` (Set interface(s) IP address).

WAN (em0)

```
Enter the number of the interface:                  1   (WAN)
Configure IPv4 address WAN interface via DHCP?      n
Enter the new WAN IPv4 address:                     172.16.0.20
Subnet bit count:                                   24
Upstream gateway:                                   172.16.0.10
Should this be the default gateway?                 y
Configure IPv6 via DHCP6?                           n
New WAN IPv6 address (blank for none):              (Enter)
Revert to HTTP for webConfigurator?                 n
```

LAN (em1)

```
Enter the number of the interface:                  2   (LAN)
Enter the new LAN IPv4 address:                     192.168.0.1
Subnet bit count:                                   24
Upstream gateway (LAN):                             (blank, press Enter)
Configure IPv6:                                     n
Enable DHCP server on LAN?                          y
  Start address:                                    192.168.0.100
  End address:                                      192.168.0.200
Revert to HTTP for webConfigurator?                 n
```

> After this step you can manage pfSense from any LAN VM at `https://192.168.0.1` (default creds `admin` / `pfsense`). From the Proxmox host you can also reach it temporarily by adding a route, but the cleanest test is to bring up the Linux Server VM on vmbr2 and curl it.

6. Web UI — initial setup wizard

1. Browse to `https://192.168.0.1`, log in `admin` / `pfsense`.

2. Wizard → General Information:
    - Hostname: `pfsense`
    - Domain: `capstone.local`
    - Primary DNS: `192.168.0.2` (Windows Server, once it exists). Until then: `1.1.1.1`.
    - Override DNS: leave checked for now.
3. Time server: `pool.ntp.org`, Timezone: `America/Chicago`.
4. WAN config:
    - Type: **Static IPv4**
    - IP: `172.16.0.20/24`, Gateway: `172.16.0.10`
    - **Uncheck** "Block RFC1918 private networks"
    - **Uncheck** "Block bogon networks"

> These two boxes are the #1 reason a capstone pfSense looks installed but won't pass traffic. WAN here lives in 172.16/12 — that *is* RFC1918, so the default rule drops everything.

5. LAN config: `192.168.0.1/24` (already set).
6. Set a new admin password. Record it somewhere durable (you will be asked at the demo).
7. Reload, finish wizard.

7. Verify and harden

Connectivity tests

From	To	Expected
pfSense Diagnostics → Ping	`172.16.0.10` (host vmbr1)	Reply
pfSense Diagnostics → Ping (source: WAN)	`1.1.1.1`	Reply (proves host MASQUERADE works)
LAN VM (Linux/Win)	`192.168.0.1`	Reply, web UI loads
LAN VM	`1.1.1.1`	Reply
LAN VM	`google.com`	Resolves + replies (only after DNS is set)

Default firewall posture

- **LAN → any:** allow (default rule, keep).
- **WAN → LAN:** deny (default, keep). The Jump Box reaches the LAN servers *only* via the reverse-route + host DNAT path.
- Disable the anti-lockout rule only after you have a tested admin password and a console fallback.

Reverse routes on internal VMs (so they can reach Jump Box at 172.16.0.x)

```
# Linux Server (192.168.0.x)
sudo ip route add 172.16.0.0/24 via 192.168.0.1
# Persist in /etc/netplan/<file>.yaml under routes: - to: 172.16.0.0/24 via: 192.168

# Windows Server (admin PowerShell)
route -p add 172.16.0.0 mask 255.255.255.0 192.168.0.1
```

Backup the config

Diagnostics → Backup & Restore → Download configuration as XML. Save it to `~/Capstone-Guide/pfsense-config-YYYYMMDD.xml` and to your USB drive. Do this *after* every meaningful change.

8. Where you left off & what's next

> **Done:** Proxmox install, vmbr0/1/2 bridges, host IP forwarding, MASQUERADE NAT for both internal subnets, pfSense VM created with E1000 NICs.

1. Finish pfSense console interface assignment + IP setup (sections 4–5 above).
2. Run the web wizard, uncheck the two "Block …" boxes, set admin password.
3. Build the Jump Box VM on vmbr1 (Ubuntu Server, 2/2/25, static `172.16.0.x` gw `172.16.0.1`). Harden SSH, ufw allow 22 from the three subnets.
4. Add the host DNAT rule for the Jump Box and persist it:

   ```
   iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 2222 \
     -j DNAT --to-destination 192.168.0.2:22
   iptables -A FORWARD -p tcp -d 192.168.0.2 --dport 22 -j ACCEPT
   apt install iptables-persistent
   netfilter-persistent save
   ```

   If the Jump Box stays on vmbr1 you'll DNAT to `172.16.0.x:22` instead — the ODT guide assumes the Jump Box landed on the LAN side. Pick one and document it.
5. Build Windows Server on vmbr2, promote to DNS for `capstone.local`, point pfSense + every VM at it.
6. Build the Linux Server on vmbr2.
7. Take screenshots for the Week 2 report: pfSense dashboard, Interfaces page, Firewall → Rules WAN/LAN, successful ping from a LAN VM to `1.1.1.1`.
8. Export pfSense config XML to your guide folder.

9. Troubleshooting quick reference

Symptom	First thing to check
pfSense WAN ping fails to `172.16.0.10`	vmbr1 bridge is wrong NIC; em0 didn't get assigned to the vmbr1 vNIC. Confirm in Proxmox VM → Hardware that net0 is vmbr1.
pfSense WAN ping works to .10 but not 1.1.1.1	Host iptables MASQUERADE missing or IP forwarding off. `sysctl net.ipv4.ip_forward` should be `1`; `iptables -t nat -L POSTROUTING -nv` should show the two MASQ rules.
LAN VM gets DHCP but can't reach internet	Either pfSense WAN gateway isn't marked default, or the two "Block private/bogon" boxes are still checked.
Can ping IPs but not hostnames	DNS. Until Windows Server exists, set pfSense System → General to `1.1.1.1` and tick "Allow DNS server list to be overridden".
LAN VM can't SSH to Jump Box at 172.16.0.x	Reverse static route missing on the LAN VM, or pfSense WAN→LAN rule blocking return traffic. Add the `ip route add 172.16.0.0/24 via 192.168.0.1`.
Web UI unreachable after wizard	You probably re-checked "Block RFC1918" with the laptop on the wrong side. Console menu → option 11 (Restart webConfigurator) and re-verify Interfaces → WAN.

10. Files and references

- `~/Capstone-Guide/Capstone-Config-Guide-Week1-5.odt` — instructor master guide (pfSense-less variant).
- `~/Capstone-Guide/index.html` — local guide hub.
- `~/Capstone-Guide/week2.html` — Week 2 walkthrough.
- `~/Capstone-Guide/ML350p-Gen8-User-Guide.pdf` — HPE 139-page service manual.
- pfSense docs: `docs.netgate.com/pfsense/` (offline copy not stored locally).
