# pfSense

- IPv6 deaktivieren
- Konsole Tastaturlayout ändern
- QEMU Guest Agent installieren
- Virtualisierung mit Proxmox
- Anleitung: WireGuard VPN Site-to-Site (S2S) und Point-to-Site (P2S)

# IPv6 deaktivieren

## How to disable Ipv6 on pFsense

IPv6 is the future of internet protocol. It offers several benefits.

How to disable Ipv6 on pFsense

However, there are cases where disabling IPv6 becomes necessary. For instance, like simplifying network management or addressing specific issues.

Today, we are going to take a look at how to disable IPv6 on pfSense.

1. 1. First, we have to head to System > Advanced > Networking.
   2. Then, we have to uncheck the “Allow IPv6” checkbox.
   3. Next, it is time to turn on Logging for PFsense Default Blocks. We can do this by heading to Rules under Firewalls.
   4. Now, click the icon to view the logs in the top right corner.
   5. Then, click Settings and check the boxes next to “Log firewall default blocks.”

      This will give us access to IPv6 traffic in our logs.
   6. Next, we have to make sure DHCPv6 Relay is disabled. We do this by heading to Services > DHCPv6 Relay and unchecking “Enable.”
   7. Then, save and apply the settings.
   8. Furthermore, we have to disable IPv6 on each Interface individually.
      - First, head to Interfaces and review the list of interfaces on the firewall.
      - Then, start with the WAN interface and click it.
      - After that, we have to set the configuration type for each interface to “None.”

- Next, save and apply our changes.
- We have to repeat this process for all other interfaces.

9. Finally, head to Routing under System and set “Default gateway IPv6” to “none.” Then click Save.
10. Additionally, we can create firewall rules to block IPv6 to help identify potential misconfigurations or issues. This step is optional but can be useful for monitoring.

After the above steps, we will no longer see IPv6 traffic in our logs.

https://bobcares.com/blog/pfsense-disable-ipv6/

# Konsole Tastaturlayout ändern

https://blogmotion.fr/internet/pfsense-clavier-azerty-16564

https://forum.netgate.com/topic/148227/change-keyboard-layout-permanently/6

# QEMU Guest Agent installieren

The scripts in this repo have been collected and tweaked from various places.

The instructions and scripts have been tested, but there is no guarantee they will work in your situation. Make appropriate backups before using.

As with all scripts you download from the internet, inspect them and **kiddy scriptor usus cautela** .

---

# install-qemu-guest-agent.sh

If you are using pfSense in Proxmox Virtual Environment (PVE), running this script from the pfSense command line will install the QEMU guest agent and set it to run on boot.

## Enable QEMU Guest Agent in Proxmox VE

When creating your pfSense virtual machine (VM), set Options > QEMU Guest Agent to `enabled` when you create your VM.

If you enable the QEMU Guest Agent while the VM is running, you will need to reboot it.

## Usage

1. Log into the pfSense command line as `root`
2. Run `curl -LJO https://raw.githubusercontent.com/Weehooey/pfSense-scripts/main/install-qemu-guest-agent.sh`
3. READ THE DOWNLOADED FILE! You should never blindly run scripts from the internet.
4. Make the file executable `chmod +x install-qemu-guest-agent.sh`
5. Run the installation script `./install-qemu-guest-agent.sh`
6. You should now see the IP addresses for the interfaces on the VMs summary page (click the More button to see all of them)

# Tested On

- pfSense CE
  - 2.5.2
  - 2.6.0
  - 2.7.0
  - 2.7.2
  - 2.8.0 (thank you to bhenstra)
  - 2.8.1
- pfSense Plus
  - 23.05
  - 23.05.1

Thanks to contributors on this Netgate forum post. You can also find some troubleshooting tips on the same forum post.

https://github.com/Weehooey/pfSense-scripts

# Virtualisierung mit Proxmox

# □□ Optimierung einer pfSense-VM auf Proxmox VE

Dieser Artikel beschreibt Best Practices zur Performance-Optimierung einer pfSense-VM in einer Proxmox-Umgebung, insbesondere in Kombination mit VirtIO-Netzwerkadaptern (vtnet), Intel-CPUs und fortgeschrittenen CPU-Tunings.

---

## □ Systemvoraussetzungen und Ausgangslage

- Hypervisor: Proxmox VE 8.x
- VM: pfSense CE oder pfSense+ (FreeBSD-basiert)
- CPU: z. B. Intel Core i7-10710U (Comet Lake, 6C/12T, AVX2)
- Netzwerk: VirtIO (`vtnet`) mit VLANs und Bridge-Setup
- Zugriffe: Nur von fixer externer IP via WireGuard, restlicher Verkehr wird geblockt
- Weitere VMs auf demselben Host vorhanden (Multi-VM-Umgebung)

---

## □□ Ziele

- Netzwerk- und CPU-Leistung der pfSense-VM maximieren
- Stabilität und Latenz verbessern
- Sicherheits-Risiko durch Mitigation-Abschaltung bewusst abwägen
- CPU-spezifische VM-Features korrekt konfigurieren

---

# □□ Virtuelle Hardware-Empfehlung

| Komponente | Einstellung |
|---|---|
| CPU | `host` oder `x86-64-v3` |
| vCPUs | 2–4 vCPUs |
| RAM | mind. 2 GB (mehr bei Suricata etc.) |
| Netzwerk (NIC) | `VirtIO (vtnet)` |
| Multiqueue | `queues = Anzahl vCPUs` |
| Storage | `VirtIO SCSI`, `writeback`, `ssd=1` |
| Ballooning | **Deaktivieren** |
| IOThreads | Aktivieren (`io_thread: 1`) |
| NUMA | Aktivieren (`numa: 1`) |

---

# ⚙ CPU-Features & Level (für CPU-Typ-Auswahl)

**CPU:** Intel Core i7-10710U (Comet Lake, 2019)
**Unterstützt:** `x86-64-v3` (inkl. AVX2, FMA3, SSE4.2)
**Nicht unterstützt:** `x86-64-v4` (kein AVX-512)

# Empfehlung:

```
cpu: host
```

# Anleitung: WireGuard VPN Site-to-Site (S2S) und Point-to-Site (P2S)

## Einleitung

WireGuard ist ein leichtgewichtiges und leistungsstarkes VPN-Protokoll, das sich durch einfache Konfiguration und hohe Sicherheit auszeichnet. Diese Anleitung beschreibt, wie Sie WireGuard auf pfSense einrichten und sowohl eine Site-to-Site (S2S) Verbindung als auch eine Point-to-Site (P2S) Verbindung für Windows und Android konfigurieren.

## Vorraussetzungen

- pfSense-Firewall: Installiert und konfiguriert mit Zugang zur Web-Oberfläche.
- WireGuard-Paket: Auf pfSense installiert.
- Installieren Sie es über System > Package Manager > Available Packages.
- Kenntnis der Netzwerkkonfiguration: IP-Bereiche, Gateways, etc.

## Site-to-Site VPN

## Point-to-Site VPN

### Windows Client

### Android Client