


WPF NetSec	VPN	
7.2.2022	Wireguard mit OPNsense	

## WireGuard Road Warrior Setup

Um eine Remote-Access-VPN-Verbindung (z.B. Homeoffice PC zum Server in der Firmenzentrale) mit Wireguard aufzubauen werden ein Endpunkt (z.B. Firewall, öffentlich erreichbar) und ein Client benötigt.

Neben vielen Technologien steht eine rel. neue Art zur Verfügung: Wireguard. Sie ist neben IPSec und OpenVPN u.a. eine Möglichkeit, einen sicheren VPN Tunnel zwischen zwei Punkten aufzubauen.

Aufgabe:

Laden Sie sich die neueste OPNsense Firewall runter, und installieren Sie diese in einer VM. Stellen Sie die Netzwerkkarte der VM auf bridged, host-only oder internal.

Virtualbox: [https://www.thomas-krenn.com/de/wiki/Netzwerkkonfiguration\\_in\\_VirtualBox](https://www.thomas-krenn.com/de/wiki/Netzwerkkonfiguration_in_VirtualBox)

OPNsense FW: [https://www.thomas-krenn.com/de/wiki/OPNsense\\_installieren](https://www.thomas-krenn.com/de/wiki/OPNsense_installieren)

Aktivieren Sie das Wireguard Plugin innerhalb der Plugin Verwaltung von OPNsense.

Befolgen Sie folgende Schritte, um ein VPN Zugangspunkt mit Wireguard aufzubauen:

<https://docs.opnsense.org/manual/how-to/wireguard-client.html>

Um das Setup zu testen installieren Sie in einer weiteren VM ein Client Betriebssystem ihrer Wahl (Windows 10, LinuxMint 20.3 etc.)

Installieren Sie dort einen Wireguard Client und bauen Sie eine Verbindung zu Ihrem Wireguard Server auf. [Link](#).

Sobald die Verbindung steht, versuchen Sie eine SSH-Verbindung zur OPNsense herzustellen. Sollte dies funktionieren steht der VPN Tunnel.

Alternativ:

Siehe auch: <https://www.ionos.de/digitalguide/server/tools/wireguard-vpn-grundlagen/>

und <https://www.linode.com/docs/guides/set-up-wireguard-vpn-on-ubuntu/>