Wireguard Server auf OpnSense einrichten

Achtung: die vielen Tutorials im Internet beschreiben diesen Vorgang nur sehr lückenhaft. Es muss aber ALLES stimmen, sonst klappt das nicht!

Diese Beschreibung geht davon aus, dass man vom lokalen Netz auf den Client Zugriff hat, der Client aber keinen Zugriff auf das lokale Netz hat. Das ist aber nur eine Sache welche Regeln man aufstellt.

Man kann also vom lokalen Netz aus die Tunnel-IP Adresse des Clients erreichen und sich z.B. mit SSH in den Client einloggen. Der Client hat von sich aus keinen Zugriff auf das lokale Netz. Diese Konfiguration wird z.B. für Remote Sensoren oder ähnliches benutzt.

Wireguard konfigurieren

Wireguard ist bei aktuellen Versionen von OpnSense standardmäßig installiert. Ansonsten als Plugin installieren.

Instance ... Konfiguration der lokalen Seite
Peer ... Konfiguration der Remote Seite

Instance

Name: beliebiger Name
auf das Zahnrad-Symbol klicken: Public und Private Key werden erzeugt
Listen Port: 51820
Tunnel Address: 10.0.0.1/24 ... das ist die IP Adresse der lokalen Seite des Tunnels

Peer

Name: beliebiger Name
Public Key: das ist der public key der Remote Station (dort erzeugen und dann hierher übertragen)
Allowed IPs: Netzwerke die durch den Tunnel dürfen: 10.0.0.0/24
Endpoint address und port können frei bleiben
Instance: die zuvor erzeugte Instance

jetzt nochmal zurück zur Instance, und dort den, gerade erstellten, Peer angeben.

Wireguard einschalten

Enable Wireguard ankreuzen und APPLY drücken

VPN Interface wg0 zuweisen

Beim aktivieren von wireguard wurde das neue Interface wg0 erstellt. Dieses muss noch zugewiesen werden in
Interfaces - Assignments
+Assign a new interface: hier wg0 auswählen und ADD drücken. Jetzt erscheint es in der Liste der zugewiesenen Interfaces

Gateway erstellen

Wird im lokalen Netz auf das Tunnel-Netzwerk zugegriffen, so sollen diese Pakete in den Tunnel geleitet werden. Dazu brauchen wir ein passendes Gateway:

System - Gateways - Configuration:

Neues Gateway **+**:
beliebigen Namen und Beschreibung eintragen
Interface: das zuvor zugewiesene Interface auswählen
Address Family: üblicherweise IPv4
IP address: IP Adresse der lokalen Seite des Tunnels (die IP Adresse von OpnSense im Tunnelnetzwerk)
alle weiteren Angaben nicht auswählen
Monitor IP: Tunnel IP Adresse der Remote Station. Wiregard pingt dorthin um zu sehen ob eine Verbindung besteht.

Route erstellen

damit Pakete aus dem lokalen Netz durch den Tunnel geleitet werden, braucht man eine neue Route.

System - Routes - Configuration:

Network Address: Netzwerk des Tunnels, z.B.: 10.0.0.0/24
Gateway: das zuvor erstellte Gateway
beliebige Beschreibung

Regeln erstellen

Regeln für den Aufbau des Tunnel über Port 51820:

Firewall - Rules - WANinterface:

eine neue Regel erstellen mit:

Action: Pass
Interface: WANinterface

Direction: in
TCP/IP Version: IPv4
Protocol: UDP
Destination: WANinterface-address
Destination port range: (other) 51820

outbound NAT erstellen

die lokalen IP Adressen müssen in Tunnel IPs umgesetzt werden.

Firewall - NAT - outbound:

eine neue Regel erstellen **+**:

Interface: das zuvor zugewiesene Tunnelinterface
TCP/IP Version: IPv4
Protocol: any
Source address: any
Destination address: Single host or Network, z.B.: 10.0.0.2/32 (in diesem Fall die IP der Remote Station)
Translation/target: <Interface>-address des zuvor zugewiesenen Tunnelinterfaces

Normalization erstellen

das korrekte einstellen der Normalization ist Voraussetzung dafür dass TCP Pakete korrekt übertragen werden, ansonsten könnten sie durch Fragmentierung verloren gehen.

Firewall - Settings - Normalization:

ein neue erstellen **+**:

Interface: WireGuard(Group)
Description: Beispiel: „Wireguard MSS Clamping IPv4“
Max mss: 1200 (oder ein Wert der für die Fragmentierung passend ist, meist geht es noch bis 1360 oder 1400, mit einem kleineren Wert ist man auf der sicheren Seite)

Tunnel prüfen

Wireguard neu starten durch enable entfernen, Apply, enable setzen, Apply.

Der Client muss jetzt laufen, dann in

VPN - WireGuard - Status

prüfen ob der Tunnel aktiv ist.