WireGuard mit Windows 11 IIS

- Vorbereitungen:

  Im Router den Port 51820/UDP zur IP-Adresse des IIS-Server (lokale Netzwerk) freigeben (weiterleiten)

  In der Firewall des IIS-Servers eine Eingangsregel für Port 51820/UDP anlegen

  Am IIS-Server die „PowerShell" mit Administrator Rechten öffnen
  Den folgenden Befehl eingeben und Enter drücken:
  Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" -Name IPEnableRouter -Value 1

  Öffne "Dienste" oder mit Windows-Taste+R den Befehl „services.msc" ausführen:
  Dienst „Routing und RAS" (Routing and Remote Access) "Starten" und auf "Automatisch" stellen

  Den Windows 11 PC mit IIS-Server neu STARTEN

- Die Server Software „WS4WSetup-2.1.4.exe" downloaden und installieren

  LINK: https://github.com/micahmo/WgServerforWindows/releases/download/v2.1.4/WS4WSetup-2.1.4.exe

  Die Konfiguration von oben nach unten abarbeiten bis alle Icons grün sind.

  1) WireGuard.exe – Button „Install" drücken
     Fall noch nicht installiert wird „HyperV" installiert.

  2) Server Configuration – Button „Edit server configuration" drücken
     Name: Bezeichnung für den Server (z.B.: VPN)
     ListenPort: 51820 (Ist der Standard-Port in Windows)
     Allowed IPs: 0.0.0.0/0
     Endpoint (Public IP.Port): Button "Detect Public IP Address" drücken
     Address: IP-Adresse/24 Anm.: gibt die Software vor
     Private Key: Button „Generate" drücken
     Public Key: Button „Generate" drücken

  3) Client Configuration(s) – Button „Configure clien(s)" drücken
     Button „Add Client" für neuen Client drücken (es können natürlich mehrere Clients angelegt werden

Name: Bezeichnung des Client

Adresse: Button "Generate from Server" drücken

(falls am Ende der IP-Adresse /32 fehlt dann eintragen)

Allowed IPs: Button "Populate from Server" drücken

(falls am Ende der IP-Adresse /24 fehlt dann eintragen)

Private Key: Button „Generate" drücken

Public Key: Button „Generate" drücken

Persistent Keepalive: 25

Oben den Button "Export Configuration File" drücken

Für weitere Clients wieder mit Button „Add Client" den nächsten Client anlegen.

4) Tunnel Service – Button „Install" drücken

5) Private Network – Button "Make private Network" drücken

6) NAT Routing – Button "Enabled" drücken

- Im Ordner „C:\Users\Benutzername\AppData\Roaming\WS4W\server_wg"
  der Datei „wg_server.conf" im Abschnitt [Interface] folgende Zeilen hinzufügen:
  Die Adresse xx.xx.xx.xx/24 durch die richtige Adresse ersetzten

  PostUp = netsh interface ipv4 set int "wg_server" forwarding=enabled && powershell -Command "if (-not (Get-NetNat -Name 'WireGuardNAT' -ErrorAction SilentlyContinue)) { New-NetNat -Name 'WireGuardNAT' -InternalIPInterfaceAddressPrefix xx.xx.xx.xx/24 }"

  PostDown = netsh interface ipv4 set int "wg_server" forwarding=disabled && powershell -Command "if (Get-NetNat -Name 'WireGuardNAT' -ErrorAction SilentlyContinue) { Remove-NetNat -Name 'WireGuardNAT' }"

- Öffne "Dienste" oder mit Windows-Taste+R den Befehl „services.msc" ausführen:
  Den Dienst „WireGuard Tunnel: wg_server" neu starten und auf „Automatisch" stellen

- ANMERKUNG:
  Wenn ein Client ein Windows-PC ist, dann bei DNS „1.1.1.1" eintragen.
  Wenn Client ein Raspberry ist, dann keine DNS eintragen.

- TEST:

  Von einem der Clients in der Eingabeaufforderung einen anderen Client anpingen

  Ping „IP-Adresse des Clients im WireGuard"

  Öffne die „PowerShell" als Administrator und gebe den Befehl „Get -NetNat" ein

  Name: wg_server_nat

  InternalIPInterfaceAddressPrefix: IP-Adresse des Servers xx.xx.xx.xx/24

- BILDER: