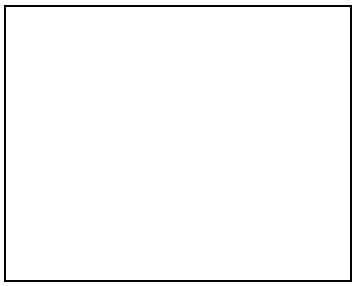
English • Deutsch • Español • Français • Italiano • ??? • Polski • Português • ??????? • Svenska • ???(????)? • ???(??)? •

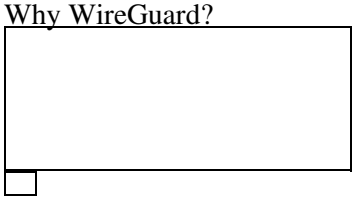
Contents

Introduction

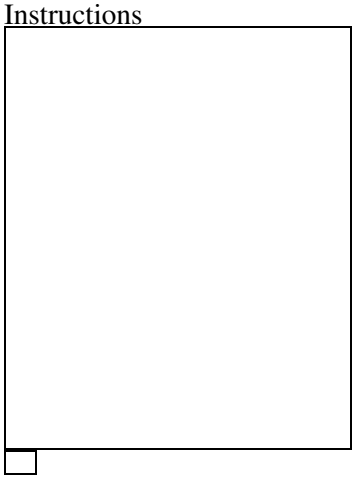
This Wireguard tutorial is for beginners, and therefore before proceeding make sure you have working reset button and have backed up you configuration (so you can reset your router and restore configuration if you stuck somewhere). This guide will show you the basics of creating tunnel from your Android/iOS device to dd-wrt unit in a secure way.



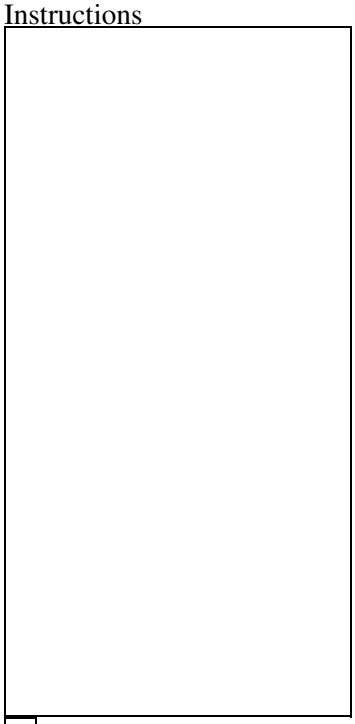
Why WireGuard?



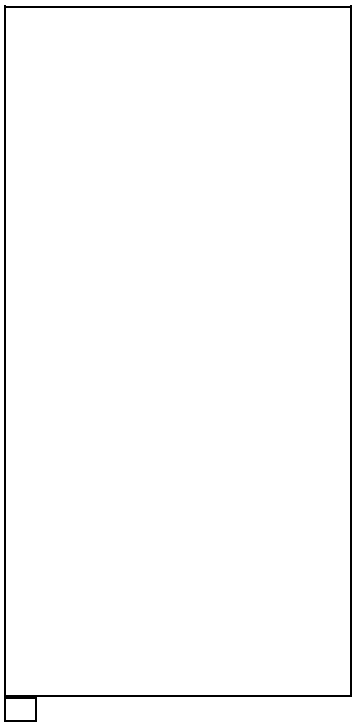
Instructions



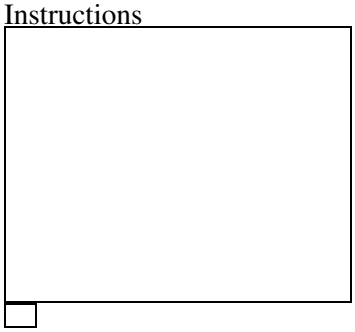
Instructions



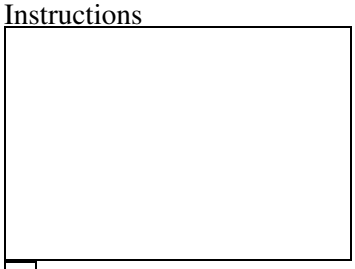
Instructions



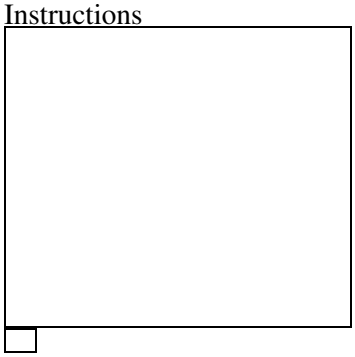
Instructions



Instructions



Instructions



Instructions

Why WireGuard?

WireGuard® is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN.

Why WireGuard + DD-WRT tunnel?

Starting from February 2019 and courtesy of BrainSlayer (Sebastian Gottschall, lead dd-wrt developer), a client config can be imported to Android/iOS in a very simple way using QR Code. No more complicated key generation, copy-paste and other headaches. The advantage of this approach is that there is no need to transfer sensitive information via data channels that can potentially be compromised and there is no need of any other supplementary software besides a WireGuard app (Android/iOS) and DD-WRT GUI.

What is a QR Code?

The QR Code is a two-dimensional version of the barcode, known from product packaging in the supermarket. Originally developed for process optimization in the logistics of the automotive industry, the QR Code has found its way into mobile marketing with the widespread adoption of smartphones. "QR" stands for "Quick Response", which refers to the instant access to the information hidden in the Code. QR Codes are gaining popularity because the technology is "open source", i.e. available for everyone. Significant advantages of QR Codes over conventional barcodes are larger data capacity and high fault tolerance.

Instructions

Creating tunnel

First, enable the tunnel on the DD-WRT EOP Tunnel page (http://your_router_ip/eop-tunnel.asp). From the *Protocol Type* drop-down menu, choose WireGuard. Generate Key and enter IP Address (this will be oet1 interface ip and must be out of your local lan range, on a separate network. E.g. if your router LAN IP is 192.168.2.1, for an IP address of oet1 put 10.10.0.1.

Adding Peer

For a simple configuration you just need to enter Peer Tunnel IP within oet1 interface ip range (e.g. 10.10.0.2) and Peer Tunnel DNS (8.8.8.8). Peer Tunnel MTU will be calculated automatically (WAN mtu-40) but can then be edited. Click Save. Generate QR-Code by pressing QR-Code button.

Masquerading tunnel

The disadvantage of Wireguard is that you cannot bridge anything. You always have to forward and do nat. No other way! So, head to Networking.asp and unbridge oet1 interface and enable Masquerade / NAT. Apply. This way, you'll have internet on other side of your tunnel.

Note for Access Point mode

Add the following firewall rule under Administration/Commands and save as firewall then reboot:

```
iptables -t nat -I POSTROUTING -o br0 -j SNAT --to $(nvram get lan_ipaddr)
```

Importing config to Android/iOS

Start your WireGuard app. In lower right corner press "+" and select "Create from QR code", scan QO-Code within DD-WRT GUI (peer section). After transferring config file from dd-wrt you will be prompted to name your tunnel. Go to whats is my ip to check you public IP. Android Apple iOS (iOS 12.0 or later)

Importing config to desktop (ArchLinux)

First of all, we'll need some packages to be installed.

- networkmanager-wireguard-git (dkms)
- **qtqr** - A Graphical interface QRCode decoder
- flameshot

You can use console or Pamac. It's your choice:) Go to the eop-tunnel.asp of you router, and use flameshot to select area of qrcode and grab screenshot. Save it but remember location and name of png file. Open **qtqr** and add png file (choose Decode from file). You will be prompted with decoded txt config file. Use it to populate wireguard client side config in network manager.

Importing config to desktop (Windows)

You'll need some additional softwares.

- Windows.msi
- CodeTwo QR Code Reader

This Windows Pre-alpha is in testing phase see Announce If you find any bugs write report back to team@wireguard.com

Troubleshooting

Dynamic WAN IP on router

After importing configs from ddwrt to Android/iOS app you can edit peer section (tap on pencil in upper right corner) - Endpoint. Enter something like this Endpoint = my.ddns.address.com:51820. This way you will be able to access your router even after reboot and changing IP.

Adding a second peer breaks the first

You cannot use allowed ips of 0.0.0.0/0 for both peer. This causes a collision. What works is setting of 10.10.0.2/32 and 10.10.0.3/32. The allowed ip's feature is for crypto routing. The key is valid for the allowed ip space. So, one single key is valid for the whole space.

Resolving local hostnames accross wg tunnel with dnsmasq

First of all you need to enable "Local DNS" and disable "No DNS Rebind" options on DNSMasq section of Services.asp site. Then, on eop-tunnel.asp site for Peer Tunnel DNS field enter your router/local DNS ip (e.g. 192.168.1.1). Repeat it for every peer. As we mentioned before wireguard cannot be bridged. So you need to specify the wireguard interface or local ip of the interface in dnsmasq as additional binding interface / listener (interface=oet1). There is also a nvram var "dnsmasq_addif" which allows you to specify custom additional interfaces (nvram set dnsmasq_addif=oet1). But, the easiest way is to simply add a dhcp interface at networking.asp (bottom of the page). Since the client is not requesting any ip nothing special will happen. Dhcp is present and reachable, but unused.

Persistent Keep Alive

This is optional, it's seconds between keep alive messages. Default is 0 (Disabled). Recommended value for NATed devices is 25.

Allowed IPs

This is required. Represent IP addresses that this peer is allowed to use inside the tunnel. Usually the peer's tunnel IP addresses and the networks the peer routes through tunnel. Outgoing packets will be sent to the peer whose AllowedIPs contain the destination address (If there are multiple matches, the one with the longest matching prefix is chosen). Incoming packets are only accepted if traffic to their source IP would be sent to the same peer. May be specified multiple times.

Preshared Key

A base64 preshared key generated by wg genpsk. Optional, and may be omitted. This option adds an additional layer of symmetric-key cryptography to be mixed into the already existing public-key cryptography, for post-quantum resistance.

to check if tunnel is active

```
wg

interface: oet1
  public key: blablaPyAN3eOyINB5JKNu4mHyKwrg3Mblabla=
  private key: (hidden)
  listening port: 51820

peer: BLABLAT3TQJwIE0OYx2qeZWYystRb9BLABLAbla=
  endpoint: 212.200.181.116:9208
  allowed ips: 0.0.0.0/0
  latest handshake: 7 seconds ago
  transfer: 14.11 KiB received, 39.85 KiB sent
```

to check if you nat-ed your oet1 network

```
iptables -t nat -v -n -L

Chain POSTROUTING (policy ACCEPT 75 packets, 5466 bytes)
 pkts bytes target     prot opt in     out     source               destination
   71 14687 SNAT       0    --  *      ppp0    192.168.2.0/24       0.0.0.0/0           to:your_r
   38  2381 SNAT       0    --  *      ppp0    10.0.0.0/24          0.0.0.0/0           to:your_r
```

Useful console directives

```
ip addr

ip route show

ifconfig

traceroute

ping
```

Reference

Conceptual Overview
Git Repository
WireGuard Mailing Lists
Changeset
Forum