19: Installing WireGuard - Secure VPN Access

WireGuard is a modern, fast, and secure VPN (Virtual Private Network) that lets you access your server and its services securely from anywhere. Once connected, you can access internal services, manage your server, and browse securely - all encrypted and protected!

For advanced features, API documentation, and technical details, see the official WireGuard documentation.

Why WireGuard?

- **Secure access** - Access your server and services securely from anywhere
- **Easy to use** - Web interface makes managing clients simple
- **Fast and modern** - Uses modern encryption (ChaCha20) for speed and security
- **Mobile-friendly** - QR codes for easy mobile device setup
- **Multiple devices** - Connect phones, laptops, tablets - all from one server
- **Split tunneling** - Only VPN traffic goes through VPN, rest uses normal internet
- **Low overhead** - Minimal impact on your internet speed

Prerequisites

- **Docker running** (from Chapter 3)
- **Linux kernel 5.6+** - Most modern Linux distributions have this
- **Optional: Traefik installed** (from Chapter 4) for HTTPS access with a domain
- **Optional: Subdomain** (from Chapter 4.5), e.g., `vpn.yourdomain.com`
- **Firewall access** - Ability to open UDP port (default: 51820)

Note: WireGuard works great with Traefik and a domain name. Having a friendly URL like `vpn.yourdomain.com` makes it easy to access the web management interface.

Step 1: Start Infinity Tools

```
sudo infinity-tools
```

Step 2: Install WireGuard

1. Go to □□ **APPLICATIONS**
2. Select **WireGuard**
3. Choose **Install WireGuard**

Using the Infinity Tools GUI

- Use ↑/↓ to move, **Enter** to select, **Esc** to go back
- Look for the **turquoise cursor** indicating the current selection
- Each screen shows a short description at the top explaining what's needed

Step 2.1: Network Configuration

You'll be asked to configure two networks:

VPN Network (Default: 10.13.13)

- **What it is:** The network used by WireGuard clients and Docker services
- **What you get:** Clients get IPs like 10.13.13.3, 10.13.13.4, etc.
- **Default:** 10.13.13 (usually fine to accept)
- **Pick this if:** You want the default setup (recommended)

Host Network (Default: 10.13.14)

- **What it is:** The network used for accessing host services (like Webmin, Apprise)
- **What you get:** Host services accessible at 10.13.14.1
- **Default:** 10.13.14 (usually fine to accept)
- **Pick this if:** You want the default setup (recommended)

□□ **Tip:** Unless you have a specific reason, accept the defaults (just press Enter).

Step 2.2: DNS Configuration

WireGuard will automatically detect your server's DNS settings. This ensures VPN clients use the same DNS as your server for consistency.

Usually, you can just accept the auto-detected DNS (press Enter).

Step 2.3: Choose SSL Mode

You'll see two options. Here's what each means:

- **Traefik (optional)**
  - **What it is:** Uses your domain name with a trusted HTTPS certificate from Let's Encrypt
  - **What you need:** A subdomain (e.g., `vpn.yourdomain.com`) pointing to your server (see Chapter 4.5)
  - **What you get:** Professional URL like `https://vpn.yourdomain.com` with trusted SSL
  - **Pick this if:** You want secure, easy access with a domain name
- **Standalone (recommended)**
  - **What it is:** Uses HTTPS with a self-signed certificate and direct port access
  - **What you need:** Just a free port (default: 8445)
  - **What you get:** URL like `https://SERVER_IP:8445` with a warning you must accept once
  - **Pick this if:** You don't have a domain or prefer direct access (recommended)

Simple rule of thumb: Use **Standalone** for most cases. Use **Traefik** if you have a domain and want trusted SSL.

Step 2.4: VPN Port Configuration

You'll be asked for the UDP port for VPN connections:

- **Default:** 51820
- **What it is:** The port clients will connect to
- **Important:** You must open this port in your firewall!
- **Pick this if:** Default is fine (recommended)

Step 2.5: Server Endpoint

You'll be asked for your server's public IP address or domain name:

- **What it is:** How clients will find your server
- **Examples:** `123.45.67.89` or `vpn.yourdomain.com`
- **Important:** This must be accessible from the internet!

What Happens During Installation

- WireGuard kernel module is installed (if needed)
- WireGuard container is created
- Web management interface is set up
- Random password is generated for web UI
- Host network interface is created
- Network routing is configured
- Service starts and becomes accessible

Step 3: Open Firewall Port

⚠ **CRITICAL:** You MUST open the VPN port in your firewall, or clients cannot connect!

Opening the Port

```
sudo ufw allow 51820/udp
```

Replace `51820` with your custom port if you chose a different one.

Why This Matters

- Without this, VPN clients cannot connect to your server
- The port must be UDP (not TCP)
- This is the ONLY port you need to open for VPN access

Step 4: Access WireGuard Web Interface

If Using Traefik

1. Wait 30-60 seconds for SSL certificate generation
2. Open `https://vpn.yourdomain.com` in your browser
3. You'll see the WireGuard login page

If Using Standalone

1. Open `https://SERVER_IP:8445` in your browser
2. You'll see a security warning (normal for self-signed certificates)
3. Click "Advanced" → "Proceed to site" to continue
4. You'll see the WireGuard login page

Step 5: Login to Web Interface

⚠ **CRITICAL:** During installation, a random password was generated and displayed. Save it immediately!

Default Credentials

- **Username:** `admin`
- **Password:** Randomly generated (shown during installation)

If You Lost the Password

You can retrieve it from:

```
cat /opt/speedbits/wireguard/web-password.txt
```

Login Steps

1. Enter username: `admin`
2. Enter the password shown during installation
3. Click "Login"
4. You'll see the WireGuard dashboard!

Step 6: Create Your First VPN Client

Now that you're logged in, let's create your first VPN client!

Adding a Client

1. Click **"Add Client"** or the **"+"** button
2. Enter a name for your device, e.g., "My Phone", "Laptop", "Work PC"
3. Configure settings (or use defaults):
   - **Allowed IPs:** Usually auto-filled (VPN network + Host network)
   - **Use Server DNS:** Usually enabled (recommended)
4. Click **"Save"** or **"Create"**
5. You'll see a QR code and download options!

What You'll Get

- □□ **QR Code** - Scan with mobile devices
- □□ **Config File** - Download for Windows/Linux
- □□ **Client Details** - IP address, public key, etc.

Step 7: Set Up WireGuard on Your Device

Windows

1. Install WireGuard from Microsoft Store
2. Open WireGuard app
3. Click **"Add Tunnel"** → **"Import from file"**
4. Select the downloaded .conf file
5. Click **"Activate"** to connect

Android/iOS/macOS

1. Install WireGuard app from Play Store/App Store
2. Open WireGuard app
3. Tap **"+"** → **"Create from QR code"**
4. Scan the QR code from the web interface
5. Tap **"Activate"** to connect

Linux

1. Install WireGuard: `sudo apt install wireguard`
2. Copy the .conf file to: `/etc/wireguard/wg0.conf`
3. Start WireGuard: `sudo wg-quick up wg0`
4. Enable auto-start: `sudo systemctl enable wg-quick@wg0`

Step 8: Understanding VPN Networks

WireGuard creates two networks for different purposes:

VPN Network (10.13.13.0/24)

This network is for WireGuard clients and Docker services:

- □□ **Your devices** - Get IPs like 10.13.13.3, 10.13.13.4, etc.
- □□ **Docker services** - Accessible via their container names
- □□ **Examples:**
  - Vaultwarden: `http://vaultwarden:80`
  - WordPress: `http://wordpress:80`

    - Apprise: `http://apprise:8000`

Host Network (10.13.14.0/24)

This network is for accessing host services (services running directly on the server):

- **Host services** - Accessible at 10.13.14.1
- **Examples:**
    - Webmin: `https://10.13.14.1:8443`
    - Apprise: `http://10.13.14.1:8444`
    - SSH: `ssh user@10.13.14.1`

What You Can Access via VPN

Docker Services (VPN Network)

- All your Infinity Tools applications
- Access via container names (e.g., `http://vaultwarden:80`)
- No need to expose ports publicly!

Host Services (Host Network)

- Webmin (if installed)
- Apprise (if installed)
- SSH access
- Any other services running on the host

Security Recommendations

- **Open only VPN port** - Close other public ports (Webmin, Apprise, etc.)
- **Use strong password** - The generated password is strong, keep it safe!
- **Store password securely** - Use a password manager (Vaultwarden recommended!)
- **Limit client access** - Only create clients for trusted devices
- **Disable unused clients** - Turn off clients you're not using
- **Keep WireGuard updated** - Re-run install script periodically for updates
- ⚠ **Protect web interface** - The web UI manages all VPN clients - keep it secure!

Firewall Best Practices

After setting up WireGuard, you can close other public ports:

```
# Close Webmin public access (access via VPN instead)
sudo ufw delete allow 8443

# Close Apprise public access (access via VPN instead)
sudo ufw delete allow 8444

# Close WireGuard web UI public access (access via VPN instead)
sudo ufw delete allow 8445
```

Now access everything securely via VPN!

Troubleshooting

Can't Connect to VPN

- **Check firewall:** Make sure UDP port 51820 (or your custom port) is open
- **Check server endpoint:** Verify the IP/domain is correct and accessible
- **Check client config:** Make sure you're using the correct .conf file
- **Check WireGuard status:** Run `docker logs wireguard` to see errors

Can't Access Web Interface

- **Traefik mode:** Wait 30-60 seconds after installation for SSL certificate generation
- **Standalone mode:** Accept the self-signed certificate warning
- **Check container:** Run `docker ps | grep wireguard` to see if it's running
- **Check logs:** Run `docker logs wireguard` to see error messages

Can't Access Services via VPN

- **Check VPN connection:** Make sure WireGuard is connected on your device
- **Check IP address:** Verify you're using the correct IPs (10.13.13.x or 10.13.14.1)
- **Check Allowed IPs:** Make sure client config includes both VPN and Host networks
- **Check routing:** Verify network routing is configured correctly

Lost Web UI Password

- View saved password: `cat /opt/speedbits/wireguard/web-password.txt`
- If file doesn't exist, you'll need to reinstall WireGuard

Where to Find WireGuard After Install

- On the finish screen, Infinity Tools prints the web interface URL and password
- You can also see it in □□ **STATUS & HEALTH → STATUS**
- Check the installation directory: `/opt/speedbits/wireguard`
- Password saved in: `/opt/speedbits/wireguard/web-password.txt`
- Client configs: `/opt/speedbits/wireguard/data/` (managed via web UI)

Managing VPN Clients

Adding More Clients

Simply repeat Step 6 for each device you want to connect. Each device gets its own unique IP address.

Disabling Clients

In the web interface, you can disable clients without deleting them. This is useful if you temporarily don't want a device to connect.

Viewing Connection Stats

The web interface shows connection statistics for each client, including data transferred and connection time.

You're Ready!

WireGuard is now installed and ready to use! Remember:

- □□ Open the firewall port (UDP 51820) - critical for connections!
- □□ Save your web UI password securely
- □□ Create clients via the web interface
- □□ Close other public ports and access everything via VPN
- □□ Use VPN network (10.13.13.x) for Docker services
- □□ Use Host network (10.13.14.1) for host services

Next steps: Create your first client, set up WireGuard on your device, test the connection, and start accessing your services securely from anywhere!

Revision #2
Created 17 November 2025 17:30:32 by bjoern

Updated 11 December 2025 15:58:29 by bjoern