Creating an ad-blocking VPN using Pi-hole and OpenVPN

Reviewed on 07 March 2023 • Published on 09 December 2020

compute **firewall** **Pi-hole** **pihole** **vpn** **OpenVPN** **ad-block**

Pi-hole and VPN - Overview

Pi-hole® is a **DNS sinkhole (https://en.wikipedia.org/wiki/DNS_sinkhole)** that protects your devices from unwanted content, such as advertisements, without installing any client-side software. It comes with an easy-to-use interactive installer and is even able to block content in non-browser locations, such as mobile apps and smart TVs. This can help to reduce data consumption on mobile plans.

To secure the connection, we use the PiVPN tool to install an **OpenVPN (https://openvpn.net/community/)** virtual Private Network that routes all traffic over a Scaleway Virtual Cloud Instance.

Security & Identity (IAM): You may need certain IAM permissions to carry out some actions described on this page. This means:

- you are the Owner of the Scaleway Organization in which the actions will be carried out, or
- you are an IAM user of the Organization, with a policy granting you the necessary permission sets

Requirements:

- You have an account and are logged into the **Scaleway console (https://console.scaleway.com)**
- You have configured your SSH Key

Deploying the Instance

1. Log in to your Scaleway Console and **create a new Instance (https://console.scaleway.com/instance/servers/create)**. For this tutorial we use a `DEV1-S` instance running on Ubuntu Focal Fossa (20.04 LTS).
2. Log into the newly created instance using SSH.
3. Update the cache of the apt package manager and upgrade the software already installed on the server:

```
apt update && apt upgrade -y
```

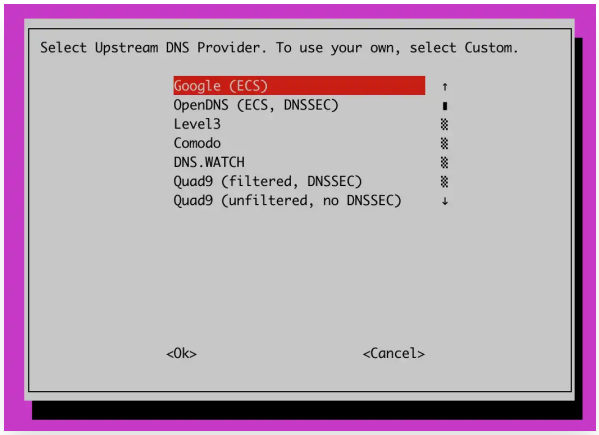
Installing Pi-hole VPN

1. Download the **Pi-hole** **(https://pi-hole.net)** installer and run it:

   ```
   curl -sSL https://install.pi-hole.net | bash
   ```

   The installer does some checks, and then gives you a series of prompt questions to answer. Choose OK or answer positively to all of them, until you are being asked choose an upstream DNS provider.

2. Select one of the proposed upstream DNS servers from the list or specify a custom DNS server. Once selected, use the `TAB` key to move to the OK button and confirm by pressing `ENTER`.



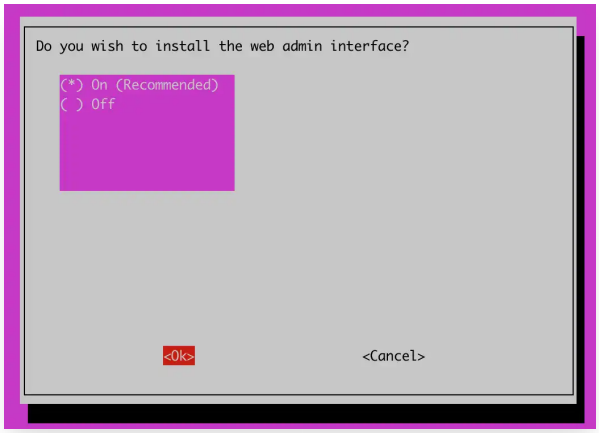
3. Pi-hole uses third party filter lists. Select the list you want to use and confirm by pressing the OK button:

4. Choose whether you want to filter both IPv6 and IPv4 traffic and confirm by pressing the OK button.

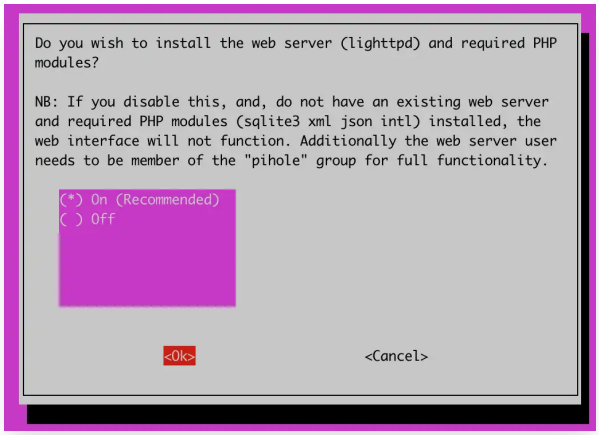
5. Confirm the network settings by navigating to the YES button. You will be guided

through two more network prompts. Confirm them by pressing the OK button.

6 Choose whether you want to enter the Pi-hole web interface and confirm by pressing the OK button:



7 The Pi-hole installer proposes the automatic installation of a webserver and its dependencies. If you are not using another web server, select to install it and confirm by pressing the OK button:



8 Choose whether you want to log queries and confirm by pressing the OK button:

9 Select a privacy mode for FTL and confirm by pressing the OK button:

The Pi Hole installer proceeds with the automatic installation of the required software. Once the installation is complete, the URL to the admin interface and your password are displayed in a prompt. Take a note of the password and leave the prompt by pressing the OK button. 10. Set the listener of the Pi-hole web interface to `local` to avoid it being accessible from the public Internet:

```
pihole -a -i local
```

1 Optionally, you can customize the password of your Pi-hole's web interface, run the following command:

```
pihole -a -p
```

Installing PiVPN

To direct Internet traffic via our Pi-hole Instance, we install OpenVPN using the **PiVPN (https://pivpn.io/)** project. It provides a very easy way to install OpenVPN and Wireguard on the Instance. In this tutorial we are using OpenVPN.

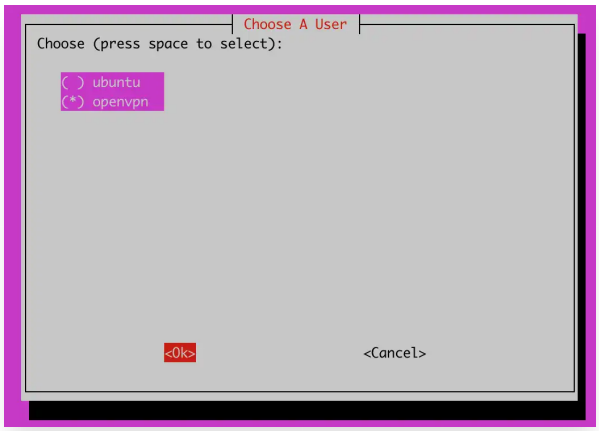
1 Create a new non-root user for OpenVPN:

```
adduser openvpn
```

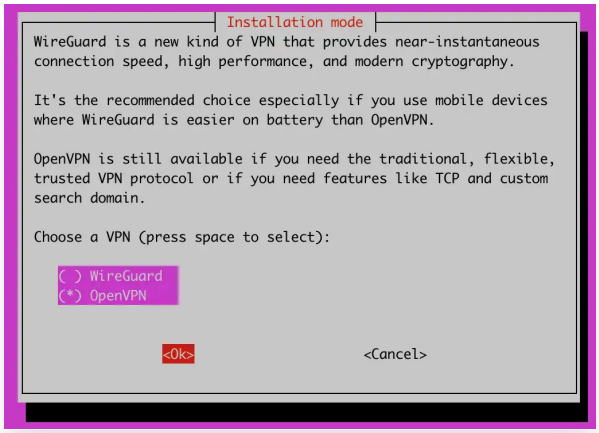
2 Run the following command from a SSH shell on your instance to download and launch the PiVPN installer:

```
curl -L https://install.pivpn.io | bash
```

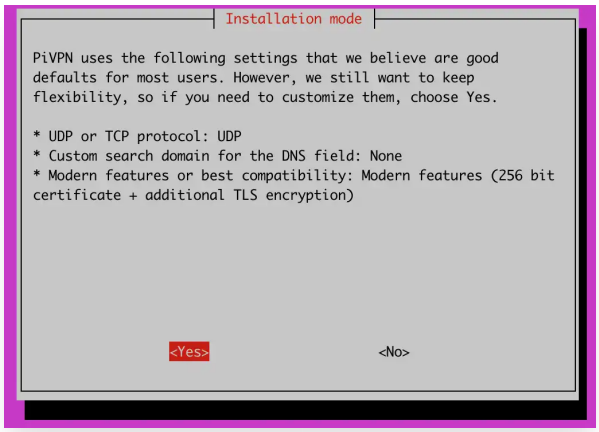
3 A series of prompts displays. Validate them by pressing the OK button until you are asked under which user the OpenVPN application should run. Select the previously created `openvpn` user and validate by pressing the OK button:



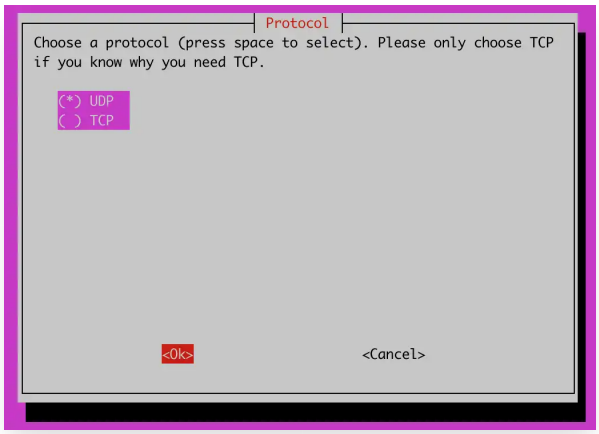
4 Choose the OpenVPN protocol in the prompt and validate by pressing the OK button:



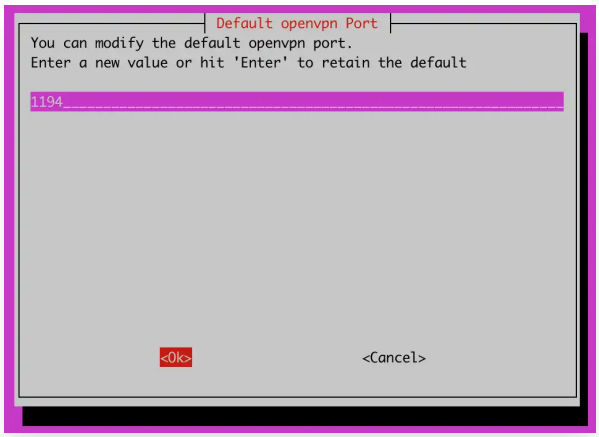
5 PiVPN provides a default configuration, accept it by pressing **Yes**:



6 Keep the value for the UDP transport protocol unless you have specific requirements and validate by pressing the OK button:

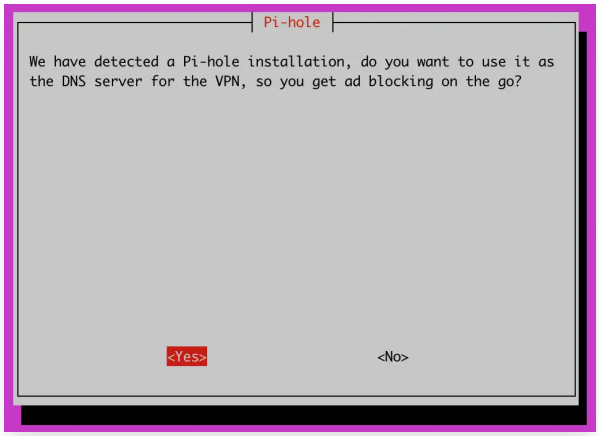


7 You can leave the default OpenVPN port `1194` unless your network configuration requires another port. Confirm by pressing the OK button:



8 The PiVPN installer automatically detects the presence of Pi-hole and asks to use it.

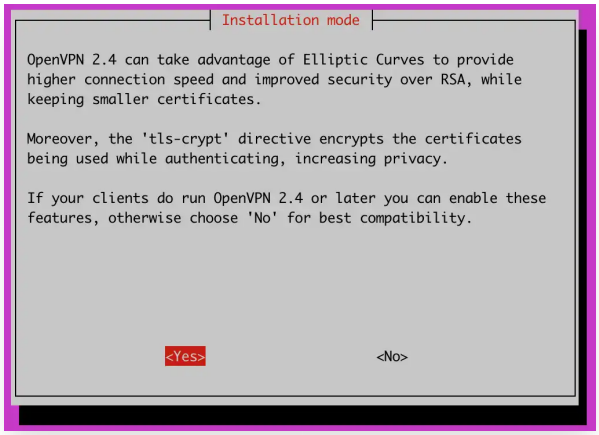
Validate the prompt by confirming with the **Yes** button:



9 The Pi-hole installer asks you if you want to use a custom search domain. Keep the default value and press the **No** button unless you have specific requirements:

10 The following prompt asks you if you want to use the instance's IP address or a custom domain name to connect to your VPN. Keep the default setting, using the public IP address of your instance and validate by pressing the OK button.

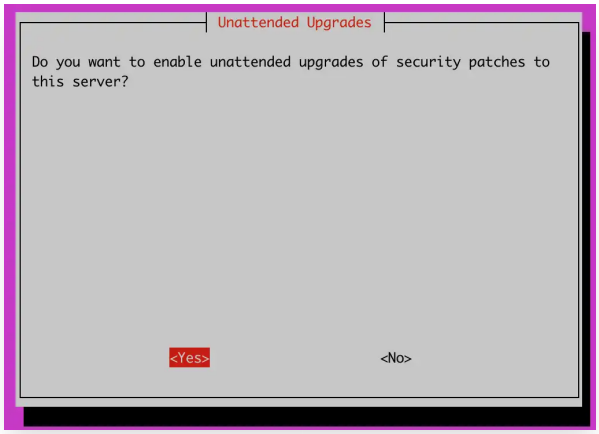
11 During the installation, PiVPN prompts you if you want to use Elliptic Curves to provide higher connection speed and improved security over RSA. Confirm by pressing the **Yes** button. If you are using some devices using legacy OpenVPN clients not supporting this feature, select **No**.



12 Select the desired key size for the certificate. In this tutorial we use the recommended size of 256 bit. Confirm by pressing the OK button:

13 The following prompt informs you that the server key and HMAC key are now being generated. Confirm by pressing the OK button.

14 The installer now prompts you to enable unattended upgrades, which allow to update the software on your server automatically to make sure it is using the latest version of the software available in the repository. Validate by pressing the **Yes** button.



15 The installation of PiVPN is now complete. You can reboot your instance as suggested by the installer by pressing the Yes button.

Adding VPN users

You can now add users to your filtered VPN service. It is recommended to create a user profile for each device you want to connect to the VPN. Sharing profiles between devices is not recommended for security reasons.

1 Run the `pivpn add` command to launch the interactive user creation wizard.

2 Enter each parameter of the user and validate by pressing the Enter key on your keyboard:

```
Enter a Name for the Client:  client <- the identifier of yo
How many days should the certificate last?  1080 <- the vali
Enter the password for the client: <- a secret password for
Enter the password again to verify: <- enter the password ag
```

The certificate and user profile is now generated and once it is ready, the following message displays:

```
============================================================
Done! client.ovpn successfully created!
client.ovpn was copied to:
  /home/openvpn/ovpns
for easy transfer. Please use this profile only on one
device and create additional profiles for other devices.
============================================================
```

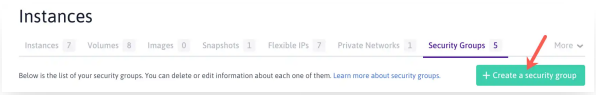
1. Download the generated `*.ovpn` configration file on your device and import it into your OpenVPN client.
2. Connect to your VPN to use your secure and filtered Internet connection.
3. Open the following URL in your web browser to connect to the Pi-hole webinterface: `http://10.8.0.1/admin/`. The web interface allows you to further configure Pi-hole and to view statistics about your DNS requests:

Lightbox src="scaleway-pihole_17.webp" alt="" />

Blocking unwanted traffic

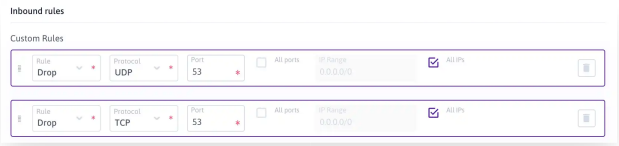
To avoid keeping an open DNS resolver on the Intenet, we restrict the requests from outside of our infrastructure. This is very important, as unprotected DNS servers can be abused and participate in
DNS Amplification attacks (https://en.wikipedia.org/wiki/Denial-of-service_attack#Amplification)
.

1. From your Scaleway console, click **Instances** in the **Compute** section of the side menu.
2. Click the **Security Groups** tab. A list of your existing security groups displays.
3. Click **Create a security group** to go the security group creation page:



4. Enter the details for your new security group:
   - **Security group Name:** a friendly name for your security group, (e.g. `block-remote-dns`)
   - **Description:** An optional description for your security group
   - **Available Zone:** Choose the geographic region in which your security group will be deployed. The region must match the region of your Instance.
   - **Rules:** Configure rules in your security group to block incoming traffic on Port 53 (DNS) to block external requests to your PiHole instance:
     1 . Click **Add inbound rule**
     2 . Select the rule `Drop`, the Protocol `TCP`, untick the box `All Ports` and enter the Port number `53`.
     3 . Click **Add inbound rule**
     4 . Select the rule `Drop`, the Protocol `UDP`, untick the box `All Ports` and enter the Port number `53`.

Your configuration should look like the following example:



- Click **Add an instance** and select your Pi-hole instance from the drop down list.
- Click **Create a new security group** to launch the creation of the security group.

You instance is now protected against requests to the DNS server running on it from external hosts. For more information about Security Groups, refer to our dedicated documentation.

Conclusion

You now have configured a secure and filtered OpenVPN connection to the Internet. Pi-hole automatically filters unwanted advertisings and and helps to save bandwidth on metered plans. The web interface allows you to view detailed statistics about the DNS requests made and you can white or blacklist additional entries.