[How-To] Configure OpenVPN Access Server First Time

Purpose

This document aims to walk through the initial confirmation of OpenVPN AS once OS is installed and up/running.

Prerequisites

List of prerequisites:

- Root user or sudo user
- OpenVPN AS

OpenVPN AS Configuration

Step 1: Log in with Default Credentials

If you don't have a public DNS record pointed to your OpenVPN Access Server, you can use its local IP address with port 943. Either way, you can browse to the login page and use the default OpenVPN username and the password generated during CLI installation. Once you've verified the default login works, add a /admin to the back of the URL at the base and login with the same default creds to get to the admin console.

Step 2: Licensing

Once logged in, you'll be presented with the Status Overview Page. Here, verify at the top that VPN Services are running. After you verify that, browse to configuration and then activation. Here is where you can apply for the license from your OpenVPN AS account. This isn't needed if you are using a free license but still good to apply for consistency's sake.

Step 3: Network Settings

Once your license is applied, browse down to the configuration and then the network settings section. Here we need to set a few things. First, change the Hostname/IP Address box from the server's local IP to the public DNS name for the website. If you don't have a public DNS record, use the local DNS record instead. But this should be set to what you want your VPN users to get redirected back to when connecting or having issues. Next, change the UDP port number to something that isn't he default 1194, like 1195 so that it's more secure. When finished, scroll to the bottom and click save settings. Then at the top after reloading, click Update running server.

Step 4: VPN Settings

In VPN Settings tab under Configuration, first change the network address settings under dynamic network address settings. Make this the IP range that you want users connecting to, like 102.168.10.0/24. Then, below see the section called routing. In the box with specify subnets accessible to VPN users section, add all subnets in the CIDR notation that you want accessible to the users when connected to this VPN. Enter down after each entry.

Step 5: Firewall Configuration

Now that the configuration section is done, log in to your network firewall solution and add a port forwarding nat rule on WAN to let in access to the port for your VPN and your web server on the local IP address of the server.

Step 6: Add Local User with 2FA

Now go to the user management and then the user permissions tab. This is where you'll need to change the default password for the OpenVPN user. Set it to something difficult as it has admin access. Save and update the running server. Then create a new local user with a strong password as well, allow it to admin access, and enable 2FA. Save and update the running server. Log out and log back in with the new local user. Add 2FA to your 2FA app on your phone and enter the code. Once working, go back to user permissions and enable 2fa for the OpenVPN user as well, and follow the same steps to add and test.

Step 7: Security Settings

As a final lockdown of security settings, you'll want to review all settings in the GUI as there are many related to security. The 2 we will focus on are allowing new users to auth for the first time and forcing 2FA on all users.

Revision #1
Created 3 November 2024 19:56:50 by Mike Leffring
Updated 3 November 2024 19:57:26 by Mike Leffring