OpenVPN (server) in Linux containers

This article describes how to setup a **Linux Container** to run **OpenVPN** in server mode for secure/private internet use. Doing so offers a distinct advantage over using full-blown virtualization like **VirtualBox** or **QEMU** in that the resource overhead is minimal by comparison and able to run on low powered devices.

Contents

Related articles

Easy-RSA

Linux Containers

OpenVPN

OpenVPN (client) in Linux containers

ufw

Host setup

1. The host OS needs a bridge ethernet setup to allow the container to run. Refer to **Linux Containers#Host network configuration** for this.
2. One needs to enable packet forwarding. Refer to **Internet sharing#Enable packet forwarding** for this.
3. Although not strictly required, a firewall is highly recommended.

Container setup

Basic setup and understanding of **Linux Containers** is required. This article assumes that readers have a base LXC setup operational. Newcomers to these are directed to the aforementioned article.

LXC config

The container's config should be modified to include several key lines in order run OpenVPN.

For the example, the lxc is named "playtime" and a full config is shown:

```
/var/lib/lxc/playtime/config
```

```
...
## for openvpn
```

```
lxc.mount.entry = /dev/net dev/net none bind,create=dir
lxc.cgroup.devices.allow = c 10:200 rwm
```

Needed packages within the container

In addition to the base system, **openvpn (https://www.archlinux.org/packages/?name=openvpn)** is required and available from the **official repositories**. A properly configured **firewall** to run within the container is *highly* recommended. This guide uses **ufw (https://www.archlinux.org/packages/?name=ufw)** which is very easy to configure, but other examples can certainly be used.

Package setup

OpenVPN

Refer to the **OpenVPN** article to properly setup the home server. Verify openvpn functionality within the container; **start** openvpn via `openvpn@myprofile.service` and once satisfied **enable** it to run at boot.

Note: Users running openvpn within an *unprivileged* container will need to create a custom systemd unit to start it within the container. Simply copy the package-provided `/usr/lib/systemd/system/openvpn-server@.service` to `/etc/systemd/system/openvpn-server@.service` and modify the new file commenting out the the line beginning with: `LimitNPROC...`

ufw

Refer to **OpenVPN#Firewall configuration** to setup the routes and firewall within the container. Failure to do so or to implement with an alternative will prevent openvpn from functioning properly in the container.

Start ufw and **enable** `ufw.service` to start at boot.

```
# ufw enable
```

Retrieved from "https://wiki.archlinux.org/index.php?title=OpenVPN_(server)_in_Linux_containers&oldid=491330"