pfSense 2.4.5

Michael B - 2021-08-16 - Guides and Articles (Other Language - 中国人))

本教程逐步引导您配置使用 pfSense 固件版本 2.4.5 的路由器。

开始之前，请确保您已下载了想要用于连接的连接地点。对于本指南来说，我们使用了加利福尼亚服务器以及标有 ***Default*** 的集合中的相关证书，请务必解压缩这个文件，以便能访问其内容。

* Default

* Strong

* Static IP

* TCP

* Strong TCP

此外，请决定适合您的需求的 DNS 服务器，共有四个选项：

* 10.0.0.241 — 这可提供以下所有三项的访问

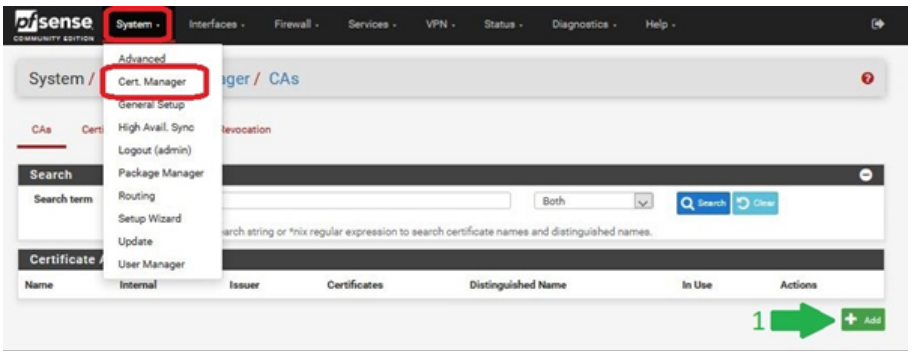
* 10.0.0.242 — 仅 DNS

* 10.0.0.243 — 将流媒体域转发到父代理，从而能访问一些流媒体服务

* 10.0.0.244 — MACE

第 1 步： 系统 – 证书管理器：在这个界面中，您可以添加 VPN 连接所需要的证书。点击顶栏中的 ***System***（系统）按钮，再点击下拉列表中的 ***Cert.Manager***（证书管理器）（下图用红色高亮显示）。

1. 点击 ***Add+***（添加+）按钮，以创建一个新的证书条目。

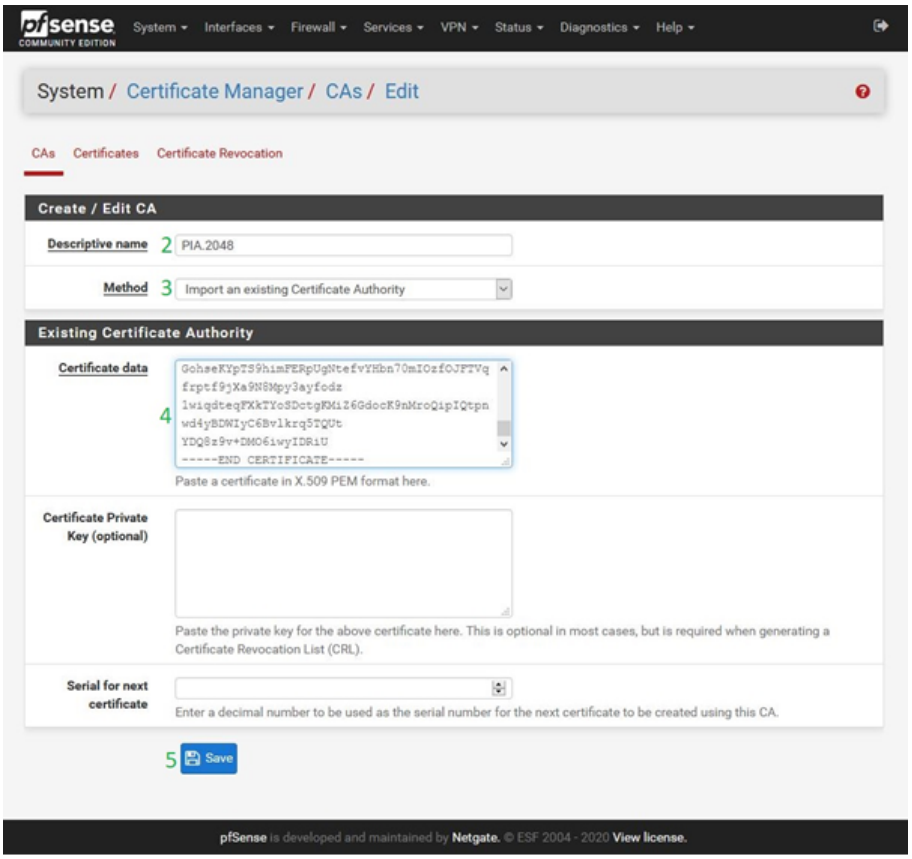


2. 将 ***Descriptive name***（描述性名称）设为易于识别的名称，我们使用的是 ***PIA.2048***

3. 在 ***Method***（方式）下拉列表中，选择 ***Import an existing Certificate Authority***（导入现有证书颁发机构）

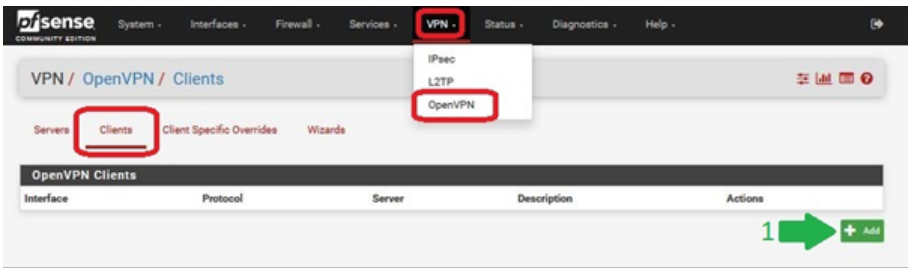
4. 您需要复制特定于所用加密设置的安全证书的内容，这可在您开始之前下载的文件中找到。在文本编辑器中打开证书，再将其内容复制到***Certificatedata***（证书数据）字段中。（注意：此字段的内容也必须包含 *begin* 和 *end* 证书行，请务必复制完整的内容。）

5. 点击 ***Save***（保存）。



第 2 步： VPN - OpenVPN - 客户端：在这个界面中，您可以输入 OpenVPN 连接需要的所有配置详情。前往顶部导航栏中的***VPN***，点击 ***OpenVPN***，然后在出现的界面中选择所示选项中的***Clients***（客户端）（这几项在下图中都用红色高亮显示）。

1. 点击 ***Add+***（添加+）以创建新的 VPN 客户端配置。



2. 设置您想要用于连接的 ***Protocol***（协议），您可以选择 ***UDP on IPv4 only***（UDP 仅限 IPv4）或 ***TCP on IPv4 only***（ TCP 仅限 IPv4）。这个决定基于您在本指南开头部分选择的文件中使用的设置。（注意：这里提供了许多设置，但只提及了需要从默认值更改的那一些。如果您遇到问题，请确保未提到的设置与本指南中提供的屏幕截图相符。）

3. 对于***Server host or address***（服务器主机或地址），您要输入想要连接的 PIA 服务器，您在开头时下载的文件集合中可以找到适用于您要连接的服务器代次的服务器地址。您要寻找的信息可在 OpenVPN 配置文件的第四行找到，本例中为“remote ***us-california.privacy.network****1198*”。文本“us-california.privacy.network”是输入的服务器地址，而“1198”则是下一步中要输入的服务器端口。

4. 对于 ***Server port***（服务器端口）设置，您需要为所选的配置输入必要的端口，即上一步中的 1198。

5. 在 ***Description***（描述）中，您可以为此 VPN 配置指定一个易于识别的名称。

6. 在 ***Username***（用户名）字段中，输入您的 PIA 用户名，其格式始终为 p1234567而且无法替换为其他信息。

7.**Password**（密码）字段中需要输入您的 PIA 帐户密码，系统为您分配了密码，但您可以在客户端控制面板中进行自定义。界面中会要求您输入这个密码两次，以防输错密码。

8.***Use a TLS key***（使用 TLS 密钥）复选框默认为选中，请***取消选中***这项。

9. 在 ***Peer Certificate Authority***（对等方证书颁发机构）下拉列表中，选择您在***第 2 步***中创建的安全证书的 ***Descriptive name***（描述性名称）。

10. 对于 ***Encryption Algorithm***（加密算法），请选择适合您的配置的选项。通常，我们建议使用 GCM 而非 CBC

11. 对于 ***Auth digest algorithm***（验证摘要算法），请选择适合您的配置的选项，如*依赖项表格*中所示。

12. 将 ***Compression***（压缩）下拉菜单设为 ***Adaptive LZO Compression***（自适应 LZO 压缩）。

13.***Custom options***（自定义选项）部分需要输入多个特定的文本行；请将以下几行复制并粘贴到这个字段中：

```
persist-key

persist-tun

remote-cert-tls server

reneg-sec 0

auth-retry interact

dhcp-option DNS 10.0.0.241

dhcp-option DNS 10.0.0.243
```

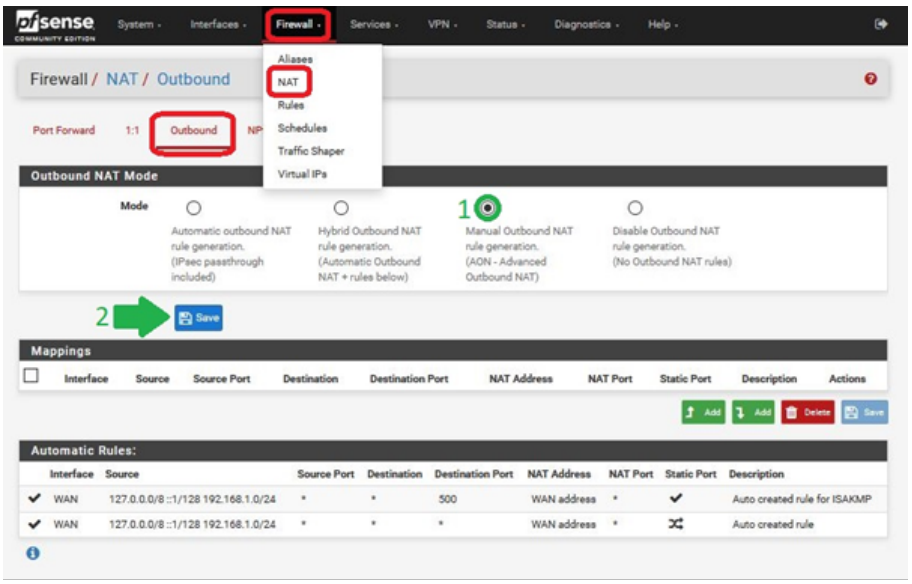
14. 对于 ***Gateway Creation***（网关创建）设置，请选择 ***IPv4 only***（仅 IPv4单选按钮。

15. 点击 ***Save***（保存）。

第 3 步： 防火墙 — NAT — 出站：在这个界面中，您可以手动创建出站 NAT 规则来利用您创建的 OpenVPN 配置。点击顶部导航栏中的 ***Firewall***（防火墙），从出现的选项中选择 ***NAT***，然后在加载的页面中选择顶部选项中的 ***Outbound***（出站）；这几项已在下图中用红色高亮显示。

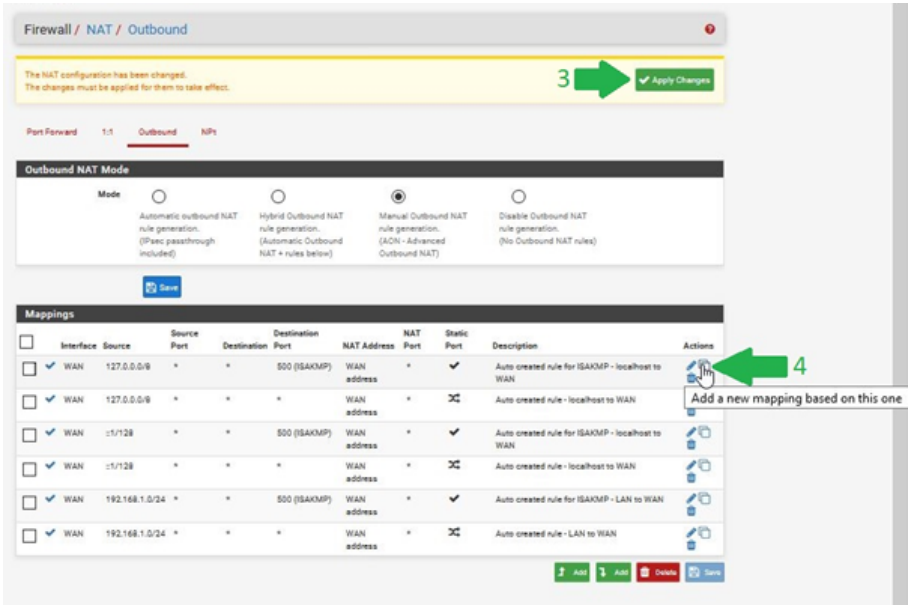
1. 点击 ***Manual Outbound Rule Generation***（手动生成出站规则）单选按钮。

2. 点击 ***Save***（保存）。



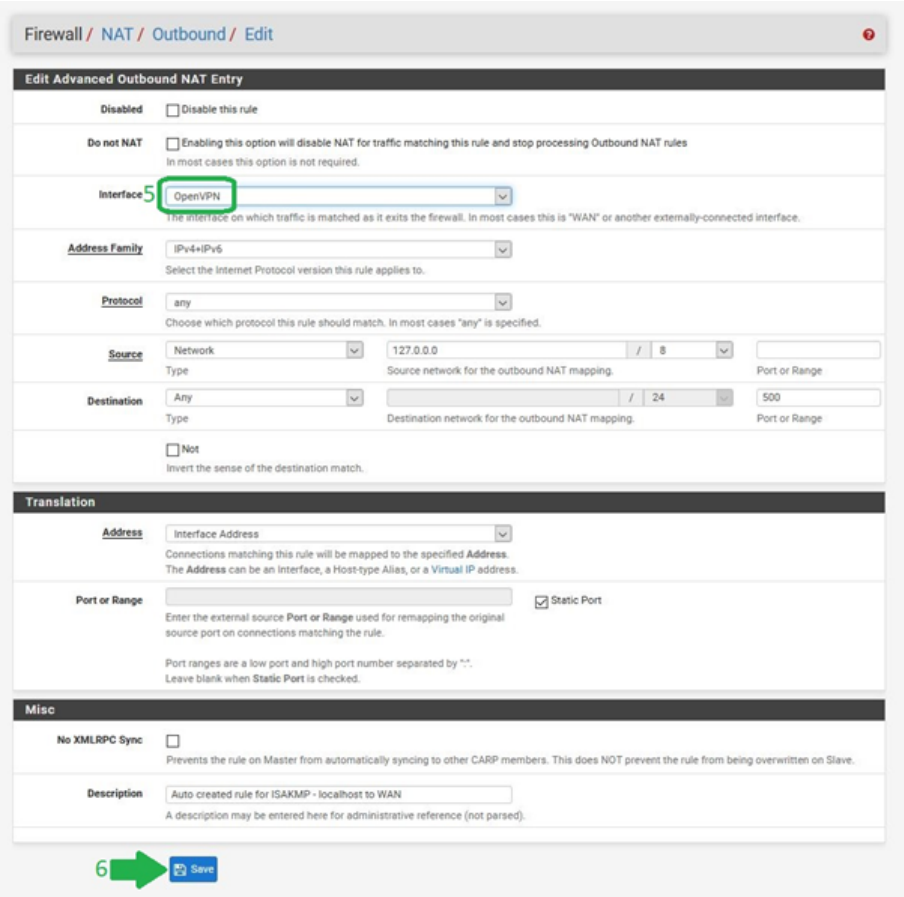
3. 点击 ***Apply Changes***（应用更改），以便让系统使用您创建的新规则。

4. 您需要重复默认显示的各个界面，其第一步就是点击 ***Actions***（操作）列中的 ***Add a new mapping based on this one***（根据此项添加新映射）。

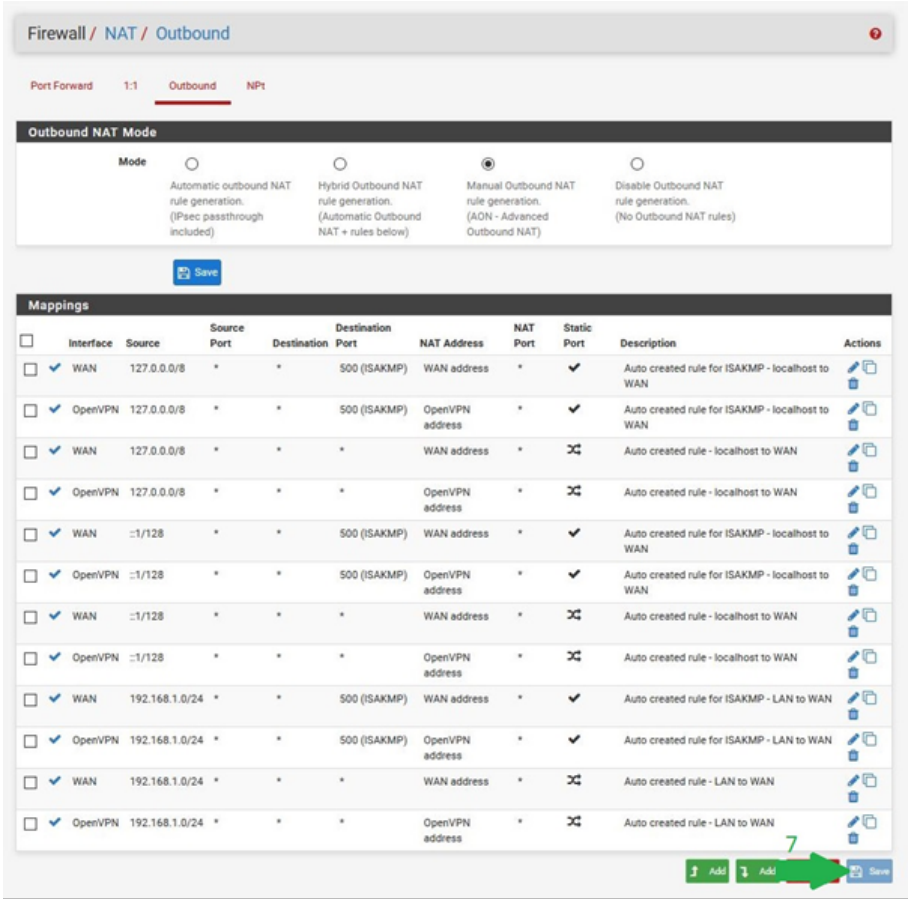
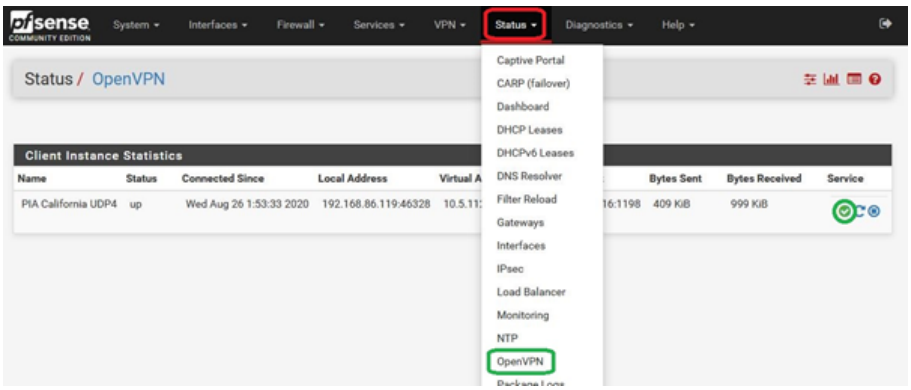


5. 将新配置使用的 ***Interface***（接口）更改为使用 ***OpenVPN***

6. 点击 ***Save***（保存）



7.*为六个连接逐一重复前面三项操作（3.4、3.5 和 3.6）。*重复了所有接口并设为使用 OpenVPN 后，点击 ***Save***（保存）



您已成功完成了 pfSense 的 OpenVPN 设置。您可以在 ***Status - OpenVPN***（ 状态 - OpenVPN界面中确认连接状态。