互联网生存指南-跨越高墙-Ⅰ

——借助Pritunl的VPN搭建

# 声明

本人坚决反对制作和售卖跨境VPN软件，坚决反对自行或帮助任何人进行不正当国际联网或提供国际出入口信道。

根据《中华人民共和国计算机信息网络国际联网管理暂行规定》第六条：任何计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道，任何单位和个人不得自行建立或使用其他信道进行国际联网。

望广大网友切莫以身试法，乃至追悔莫及。

# 前言

## 关于本文

本文可以说是笔者自己的学习笔记，尽可能详细介绍了借助Pritunl搭建VPN的过程。但是请务必注意，虽然在理想情况下你严格按照本文所述方法可以成功搭建VPN，但此方法并不向你保证其过程简洁、不出意外，如果你遇到任何问题，请自行尝试解决。

虽然本文已经尽可能详尽描述过程并作出大量解释，但是如果你依然有理解困难，那么这里提供你两个建议：你希望继续进行下去，并善于学习，请充分利用AI为您提供解答；如果您感到吃力和厌烦，不想继续进行，请考虑放弃。

如果您完全出于学习目的，可以严格按照本文条件进行一遍，这会对你的理解非常有帮助；但是如果您打算真正较长时间使用搭建出来的VPN，那么本文中使用的配置是不合理的，请自行选择适合自己的配置。

如开头所述，本文的过程仅仅是可行，但是并不简洁，如果您阅读本文后可以成功构建，那么在此后真正应用环境中，请参阅下面给出的链接提供的安装方式建议，相信这时你可以读懂：

* **这是Pritunl官方提供的安装指导文档：**[Installation (pritunl.com)](https://docs.pritunl.com/docs/installation)
* **这是MongoDB官方提供的安装指导文档：**[Install MongoDB - MongoDB Manual v7.0](https://www.mongodb.com/docs/manual/installation/)

## 事先准备

必须要说明的是，本次教程重点依然在如何安装和配置，但在这之前及过程中，会用到的部分资源是难以做详细讲解的，需要你提前准备。如果你已经拥有或者明白如何获取，这当然很好；如果还没有且不明白如何获取，那么请善用搜索引擎和AI进行学习。

具体来说，你最好提前准备好以下资源：

* **一台云服务器**（请相信，使用云服务器可以极大地方便操作，包括但不限于随时一键重装系统，提供固定的公网IP，方便设置登录密码或秘钥。比如下面使用的是阿里云平台99RMB/年的ECS云服务器，系统为Debian 12.5 x64，代号“书虫（bookworm·）”）
* **一个域名**（在哪里购买都是可以的，但是因为国内平台往往需要实名认证，并不推荐。比如下面使用的是Porkbun购买的域名，因为便宜）
* **SSH连接客户端**（选择自己喜欢的或者知名度高的，简单使用差别不大，比如下面我们使用的是Xshell）
* **一个浏览器**（在后面的配置环节，你主要需要通过浏览器完成操作。比如下面我使用Windows 11，那么直接用自带的Edge浏览器就是不错的选择）

## 知识储备

在必要的资源准备之外，你还需要一些相关知识储备，这部分内容只会简单描述，如果你对下面所述不了解，请自行搜索如何解决。

* **DNS的配置**（通常情况下，你购买域名的平台就会提供DNS，如果没有其他需求，本次教程中仅需要配置一次A记录）
* **远程登录服务器**（下面教程中假设你已经通过如Xshell的SSH连接客户端连接到了服务器，注意，大量指令都需要通过SSH下达和执行，请务必解决）
* **对云服务器提供商网站有一定了解**（云服务器在方便的同时也有一些限制，请确保在教程的部分简要描述步骤你能找到对应的操作在云服务器提供平台如何完成，比较重要的有获得IP、配置安全组、出现问题时重装系统）

# 步骤一：准备工作

## 云服务器基本配置

* 在阿里云平台购买云服务器（本次仅使用IPv4，如果没额外要求，阿里云不会分配IPv6）；
* 安装操作系统：系统选择页面设置好系统为Debian 12.5 x64，选择使用密码登录root账户并填写密码（你当然可以选择其他方式，但是本例会这样进行，因为只是测试，这样简单）；
* 本地安装Xshell客户端；
* 在阿里云平台获得当前服务器的公网IP，结合密码，用于在Xshell中登录。

## 更新和升级

这个命令组合用于在基于Debian的Linux发行版上更新软件包列表并升级所有已安装的软件包到最新版本：

1. sudo apt update && sudo apt upgrade

## 安装neofetch

Neofetch 的主要用途是生成一张显示系统信息的美观图片，通常用于社交媒体或论坛上分享系统配置。它支持多种操作系统，并且可以自定义显示的信息和样式。但是本次教程中使用它仅仅是为了获取当前使用系统的“代号”，如果你已经知道，那这一步不是必须的。

要安装 Neofetch，只需在「终端」中执行以下命令：

1. sudo apt install neofetch

安装完成后，可以通过以下命令来查看版本：

1. neofetch *--version*

安装完成后，可以通过以下命令来查看基本系统信息，其中就包含我们需要的“代号”：

1. neofetch

执行此命令，你会看到类似下面的信息，其中的bookworm 就是我们需要的“代号”

1. \_,met$$$$$gg.          root@LT2H2G1Y
2. ,g$$$$$$$$$$$$$$$P.       -------------
3. ,g$$P"     """Y$$.".        OS: Debian GNU/Linux 12 (bookworm) x86\_64
4. ,$$P'              `$$$.     Host: Alibaba Cloud ECS pc-i440fx-2.1
5. ',$$P       ,ggs.     `$$b:   Kernel: 6.1.0-21-amd64
6. `d$$'     ,$P"'   .    $$$    Uptime: 18 hours, 37 mins
7. $$P      d$'     ,    $$P    Packages: 680 (dpkg)
8. $$:      $$.   -    ,d$$'    Shell: bash 5.2.15
9. $$;      Y$b.\_   \_,d$P'      Resolution: 1024x768
10. Y$$.    `.`"Y$$$$P"'         Terminal: /dev/pts/0
11. `$$b      "-.\_\_              CPU: Intel Xeon Platinum (2) @ 2.500GHz
12. `Y$$                        GPU: 00:02.0 Cirrus Logic GD 5446
13. `Y$$.                      Memory: 448MiB / 1725MiB
14. `$$b.
15. `Y$$b.
16. `"Y$b.\_
17. `"""

# 步骤二：安装MongoDB

关于MongoDB安装，大部分内容都是参照官方文档实现的。针对本次使用的操作系统，官方文档如下，但是你跟着本文进行就是可以的：

[Install MongoDB Community Edition on Debian - MongoDB Manual v7.0](https://www.mongodb.com/docs/manual/tutorial/install-mongodb-on-debian/" \l "std-label-install-mdb-community-debian)

## 安装gnupg和curl

其中gnupg 用于进行文件加密、解密，以及使用PGP密钥进行签名和验证；curl 用于从网络下载文件或通过命令行与Web服务进行交互。

使用以下命令完成安装：

1. sudo apt-get install gnupg curl

## 导入MongoDB公有 GPG 密钥

使用以下命令完成导入：

1. curl -fsSL https://www.mongodb.org/static/pgp/server-7.0.asc | \
2. sudo gpg -o /usr/share/keyrings/mongodb-server-7.0.gpg \
3. --dearmor

## 添加MongoDB软件源

这里就是需要用到“代号”的地方了，我们的系统代号为“bookworm”，所以执行下面命令，此命令将用于将MongoDB 7.0的官方APT软件源添加到Debian或Ubuntu系统的软件源列表中：

1. echo "deb [ signed-by=/usr/share/keyrings/mongodb-server-7.0.gpg ] http://repo.mongodb.org/apt/debian bookworm/mongodb-org/7.0 main" | sudo tee /etc/apt/sources.list.d/mongodb-org-7.0.list

## 重新加载本地包数据库

执行以下命令以重新装入本地包数据库：

1. sudo apt-get update

## 安装最新的稳定版本MongoDB

要安装最新的稳定版本，请使用以下命令：

1. sudo apt-get install -y mongodb-org

# 步骤三：安装Pritunl

关于Pritunl安装，大部分内容都是参考官方文档[Other Providers] Ubuntu 22.04部分实现的，官方文档地址如下：

[Installation (pritunl.com)](https://docs.pritunl.com/docs/installation)

## 导入Pritunl公有 GPG 密钥

使用以下命令完成导入：

1. curl https://raw.githubusercontent.com/pritunl/pgp/master/pritunl\_repo\_pub.asc | sudo apt-key add -

## 添加Pritunl软件源

这里也是需要用到“代号”的地方，我们的系统代号为“bookworm”，所以执行下面命令，此命令将用于在基于Debian的Linux发行版上添加Pritunl的稳定版APT软件源到您的系统的软件源列表中：

1. sudo tee /etc/apt/sources.list.d/pritunl.list << EOF
2. deb http:*//repo.pritunl.com/stable/apt bookworm main*
3. EOF

## 更新和升级

执行以下命令以更新软件包列表、升级所有已安装的软件包到最新版本以及在遇到选项时自动确认：

1. sudo apt update
2. sudo apt --assume-yes upgrade

## 安装Wireguard

Wireguard提供一种和常规VPN不同的方法/功能，但是其实本教程并没有用到Wireguard，安装它仅仅是因为官方教程中包含这一步，另一方面，如果后期想进阶学习，这也是方便的：

1. sudo apt -y install wireguard wireguard-tools

## 安装Pritunl

使用以下命令完成安装：

1. sudo apt -y install pritunl

# 步骤四：必要的配置

## 禁用简单防火墙

目的在于避免和Pritunl的冲突：

1. sudo ufw disable

## 增加打开文件限制

运行以下命令以增加服务器上的打开文件限制。这将防止高负载服务器上的连接问题：

1. sudo sh -c 'echo "\* hard nofile 64000" >> /etc/security/limits.conf'
2. sudo sh -c 'echo "\* soft nofile 64000" >> /etc/security/limits.conf'
3. sudo sh -c 'echo "root hard nofile 64000" >> /etc/security/limits.conf'
4. sudo sh -c 'echo "root soft nofile 64000" >> /etc/security/limits.conf'

## 配置MongoDB和Pritunl的自启动

此命令用于在使用systemd作为初始化系统的Linux发行版上配置MongoDB和Pritunl服务的开机自启动：

1. sudo systemctl enable mongod pritunl

### 提示：关于初始化系统

要运行和管理MongoDB的mongod进程，您将使用操作系统的内置初始化系统。最新版本的 Linux 倾向于使用systemd （使用systemctl命令），而旧版本的 Linux 倾向于使用System V init （使用service命令）。本次使用的Debian 12 采用的就是systemd，这很重要，将影响相当一部分操作。然而，如果您不确定您的平台使用的是哪个初始化系统，请运行以下 命令：

1. ps --no-headers -o comm 1

## 阿里云控制台中为服务器开放80、443端口

这一步是否存在存疑，因为我自己也忘了默认安全组是不是开放这两个端口的，但检查一下总是好的。

## 在你的域名的DNS服务商处添加一条A记录

这不是必要的，但是重要的，请最好完成。此条A记录将建立你选择的域名和我们现在使用的服务器的IP地址之间的指向关系，如果你不了解如何操作，请自行搜索，如果有不了解的名词，请善用AI进行学习。

# 步骤五：启动和Web界面为主的配置

## 正常启动MongoDB和Pritunl

如果不出意外，执行以下命令就可以正常完成启动：

1. sudo systemctl start mongod pritunl

## 验证是否正常启动

验证MongoDB是否正常启动使用：

1. sudo systemctl status mongod

验证Pritunl是否正常启动使用：

1. sudo systemctl status pritunl

以上两步如果没有问题，你应该会看到类似下面的输出（以MongoDB为例），大部分终端如Xshell的会将running和enable等高亮显示：

1. ● mongod.service - MongoDB Database Server
2. Loaded: loaded (/lib/systemd/system/mongod.service; enabled; preset: enabled)
3. Active: active (running) since Sat 2024-06-15 21:48:08 CST; 18h ago
4. Docs: https://docs.mongodb.org/manual
5. Main PID: 5660 (mongod)
6. Memory: 264.8M
7. CPU: 11min 44.527s
8. CGroup: /system.slice/mongod.service
9. └─5660 /usr/bin/mongod --config /etc/mongod.conf
10. Jun 15 21:48:08 LT2H2G1Y systemd[1]: Started mongod.service - MongoDB Database Server.
11. Jun 15 21:48:08 LT2H2G1Y mongod[5660]: {"t":{"$date":"2024-06-15T13:48:08.726Z"},"s":"I",  "c":"CONTROL",  "id":7484500, "ctx":"main","msg":"Environment variable MONGODB\_CONFIG\_OVERRIDE\_NOFORK == 1, overriding>

### 可能的问题

你不应该直接来看这一步，如果上一步没有问题，下一步操作也没有问题，那么这里应该跳过，如果你遇到了问题，那么看下去：

#### 启动mongod时收到类似以下内容的错误

1. Failed to start mongod.service: Unit mongod.service not found.

首先运行以下命令：

1. sudo systemctl daemon-reload

然后重新执行之前的start命令：

1. sudo systemctl start mongod

#### 进行下一步无法打开页面

请务必检查是否开放了80和443端口，请务必思考之前有没有误操作可能修改了默认服务端口，如果是，请尝试执行下面命令，这将让Pritunl 更新其配置文件（通常是 /etc/pritunl.conf），并将 HTTP/HTTPS 服务端口设置为 443，同时禁用重定向服务器：

1. pritunl set app.server\_port 443
2. pritunl set app.redirect\_server false

### 你还想知道

#### 如何重启？

你可以通过发出以下命令来分别重新启动mongod和Pritunl进程：

1. sudo systemctl restart mongod
2. sudo systemctl restart pritunl

#### 如何停止？

你可以通过发出以下命令来分别停止mongod和Pritunl进程：

1. sudo systemctl stop mongod
2. sudo systemctl stop pritunl

## 进入Web界面并安装

验证两个核心程序都正常启动后，就可以来到Web配置界面了。在本地浏览器地址栏输入你的云服务器IP地址，回车，即可进入登录页面，界面为英文，如果有理解困难请自行翻译。

不出意外，你会看到两栏内容需要填写，分别为Setup Key和MongoDB URI，后者已自动填写，仅需要填写前者。Setup Key获取方法为回到Xshell，在终端输入：

1. pritunl setup-key

获得Setup Key后，复制，粘贴填入，点击SAVE按钮即可进入安装，请等待几分钟。

### 注意

如果你的浏览器设置安全级别较高，可能会提示http连接不安全，这是正常的，无须理会，请选择禁用警告、继续进入。

## 修改临时信息和重要配置

如果不出意外，根据网络上其他教程所言，安装完成后会自己跳转到修改临时信息页面。各项参数填写说明如下：

* Username：请填写你喜欢的名字作为你的管理员账户，root和Admin是常见的选择；
* Newpassword：请填写你能记住的、足够安全的密码取代默认的密码；
* Public Address：公网地址，你的IP，已自动填写；
* Public IPv6 Address：公网地址，IPv6，如果没有，留空；
* Web Console Port：Web控制台端口，默认443，你可以修改为你喜欢的数字；
* Lets Encrypt Domain：这里填入你之前已经在DNS服务商处指向本IP地址的域名即可，Pritunl会自动为你配置SSL/TLS证书并更新；
* 最下面几个勾选框：可以自己看看什么意思，这里我选择不管，用默认。

### 如果超时

如果你感觉几分钟太长，离开去完成别的事情，而这花了太长时间，那么你可能会看到提示登录的界面，不用担心，Pritunl给出了红色警示提示，通过在终端输入以下指令获得当前的默认账户和密码：

1. sudo pritunl default-password

完成登录，就可以正常进行本环节的配置修改。

## 添加组织、添加用户、添加服务

到了这里其实就已经很简单了，虽然是英文界面，但是单词没有太大难度，再不济可以使用翻译软件，同时Pritunl在一些容易存在误解的地方给出了详细的说明。

### 添加组织

不出所料，你将默认进入Dashboard（仪表盘），接下来请分别点击顶栏User-点击Add Organization-填写组织名称-确认添加。

### 添加用户

现在已经拥有了一个组织，接下来请分别点击Add User-填写各项信息-保存。注意，填写信息的部分如果有不合规的地方会给出提示的。

### 添加服务

现在点击顶栏Servers，进入服务页面，点击Add Servers-依次填写各项信息-确认添加。注意，填写信息的Port和Protocol可以自由选择，但是为了避免冲突，Port一般会设置很大，比如22333，而Protocol也是随便的，但是选择了哪一种类型记得去云服务提供商处配置安全组，开放对应端口、对应连接类型的入方向连接。至于其他勾选框，默认即可，如果有兴趣可以了解分别提供什么功能，这不是本篇应该讲解的。

### 绑定组织

服务需要绑定组织才能运行，服务页面点击Attach Organization绑定组织和服务-确认绑定。注意，一个服务可以绑定多个组织，多个组织也可以绑定一个服务，但是无论哪一种，都需要服务处于Offline状态才可以，也就是，如果服务是开启的，那么要先停止。

### 开始运行

点击Start Server，开始运行服务吧！

# 步骤六：连接

## 安装客户端

安装OpenVpn Connect客户端，手机电脑都有对应客户端，自行搜索安装，不赘述。下面的内容同样简略，一方面写了一天，现在已经累了，另一方面，能看到这里的人想必是有能力理解下面描述并完成的。

## 通过URL连接

由于未知问题，我无法连接，此条目待补充。

## 通过配置文件

在控制台User界面可以看见每个用户，点击右侧的小小蓝色下载按钮即可下载一个.tar文件，解压即可获得.ovpn文件，导入OpenVPN客户端，填写必要的信息即可连接。

# 尾声

相信通过仔细阅读本文档，加上一定程度的学习能力，在看的你一定是可以完成搭建全过程的。感谢看到这里所有人。

最后，我也必须承认，本文档仍然有大量不足之处，包括但不限于越往后介绍越简略，还有没弄明白的问题，以及本文档格式并不相当规范，埋了不少暗雷……如果有时间，或许会考虑继续细化和补充吧。这里还要说明，不要试图用于不法目的，已经有很多博主告诉你VPN特征有多明显了。