https://github.com/EOFFULL/Detailed-tutorial-on-the-building-and-usage-of-Trojan
WinSCP 的一些使用方法在这篇教程里讲过了

进入 V2rayN 的这个界面，如何进入在基础版教程里讲了

点击，就会生成一个新的 UUID

复制这个 UUID

用 Notepad++打开这个配置文件

将这个 UUID 用刚才复制的 UUID 替换掉。保存并关闭文件。

打开这个文件

用你自己的域名将这个域名替换掉。保存并关闭文件。

在服务器上安装 V2ray 并启动的步骤和基础教程一样

安装完 V2ray 并启动之后，输入 apt-get -y install socat 敲回车。这是安装 acme 的一个依赖。

输入 curl https://get.acme.sh | sh 敲回车。这是安装 acme。

输入 source ~/.bashrc 敲回车。这是使安装 acme 时所做的一些更改生效。

输入 ~/.acme.sh/acme.sh --issue -d dskg.ml --standalone -k ec-256 敲回车（记得提前把 dskg.ml 改成你自己的域名）。这是给域名签发 ecc 证书。

输入　apt-get -y install nginx　　敲回车。这是安装 Nginx，用于实现网页伪装。

用 WinSCP 登录服务器
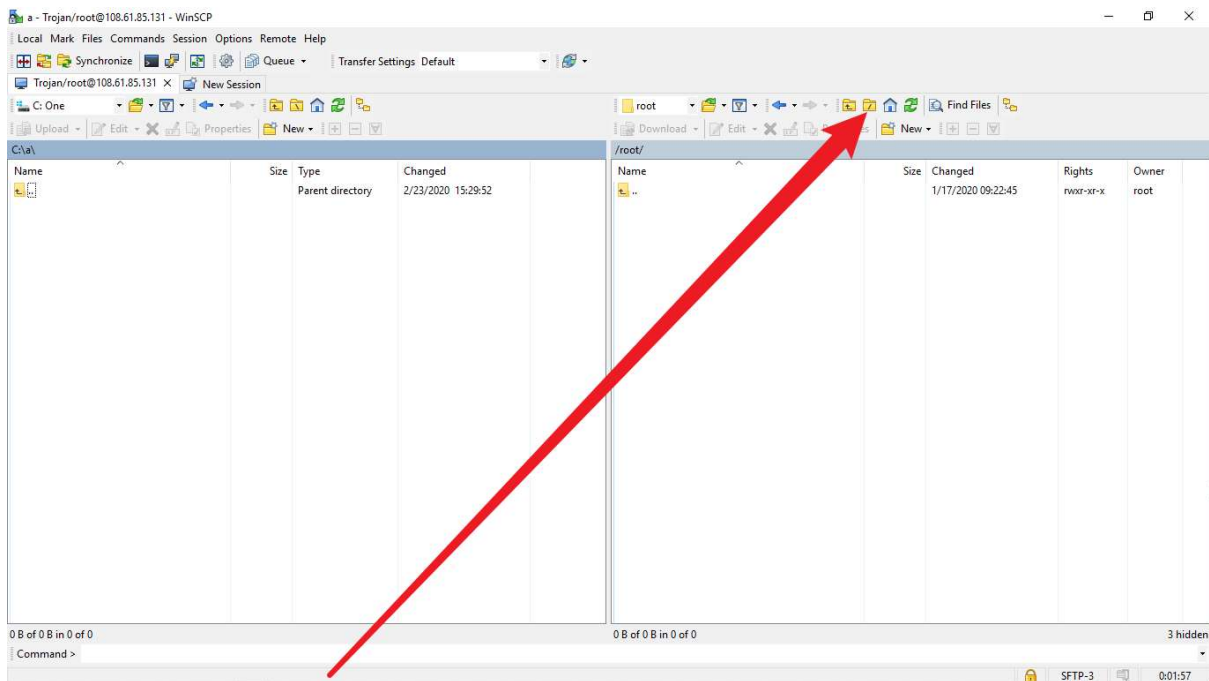
单击，就到了根目录
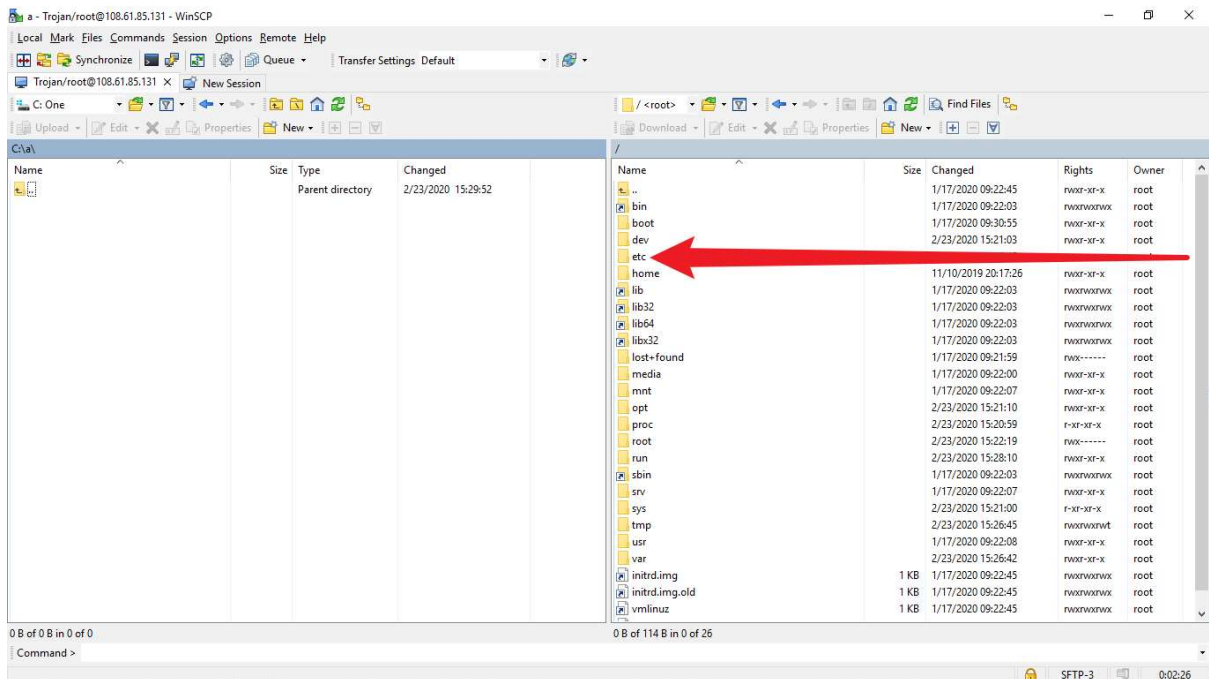
双击，就进入了/etc
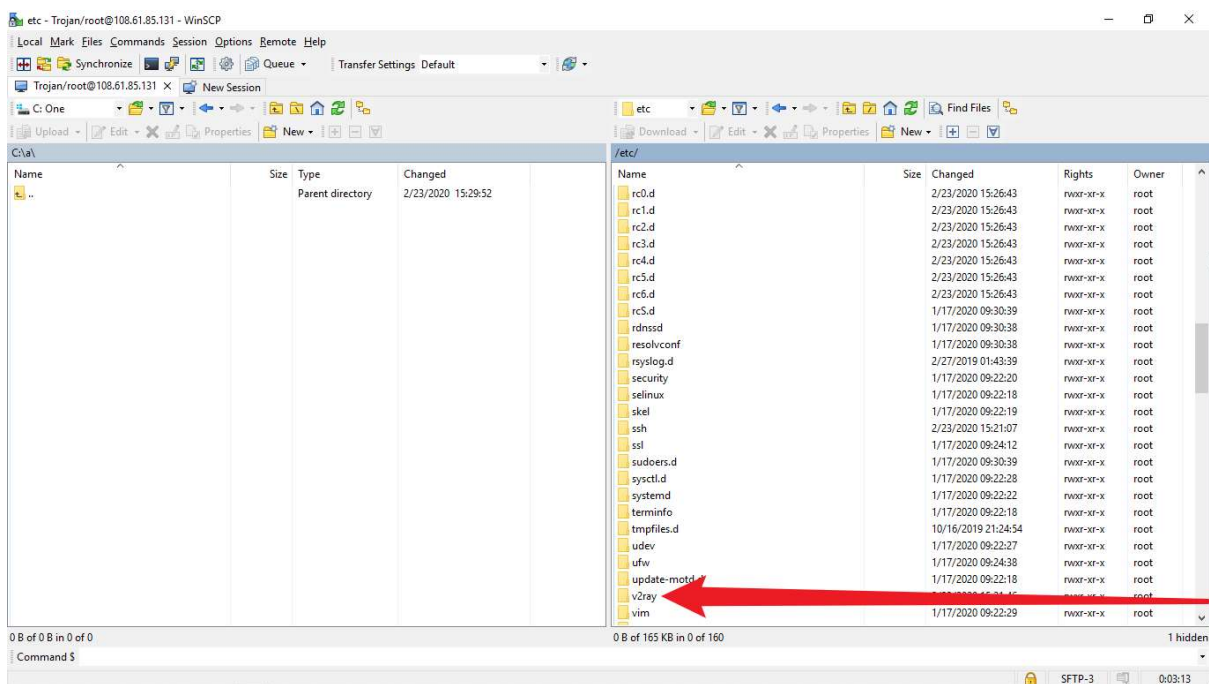
双击，就进入了/etc/v2ray。这是 V2ray 配置文件的文件夹。记住这种进入某个文件夹的方法，就是先进入根目录/，再一层层地双击进入子文件夹。
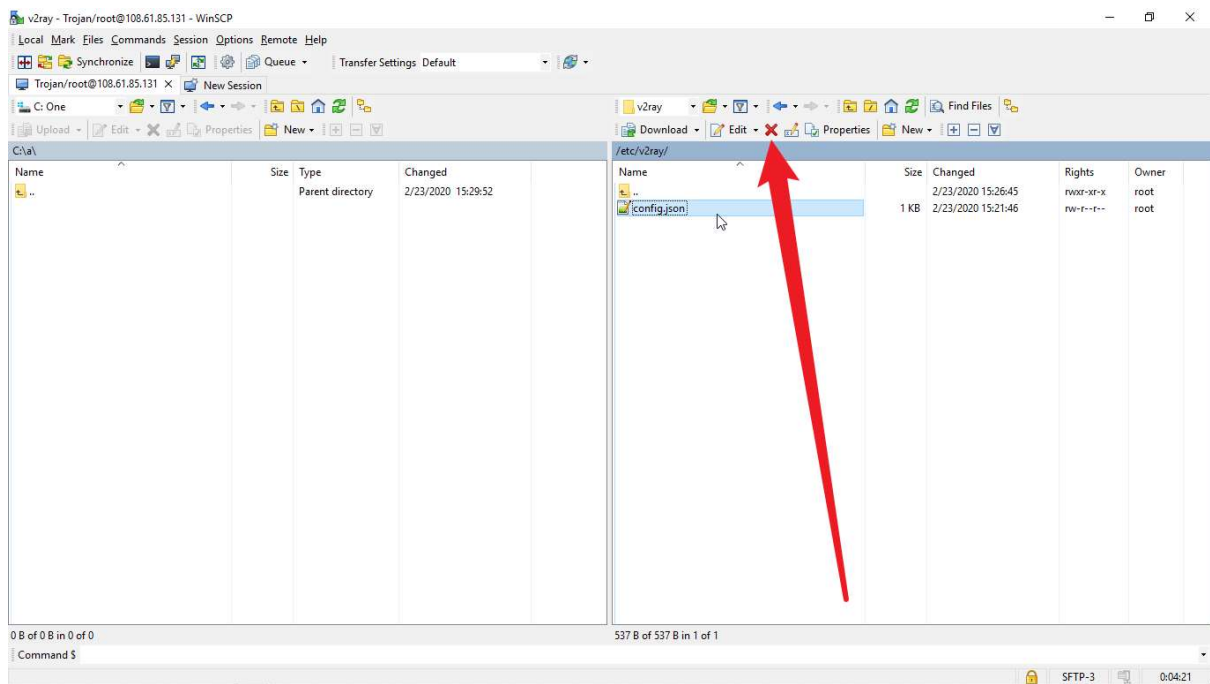
单击选中 config.json，然后点红色的×
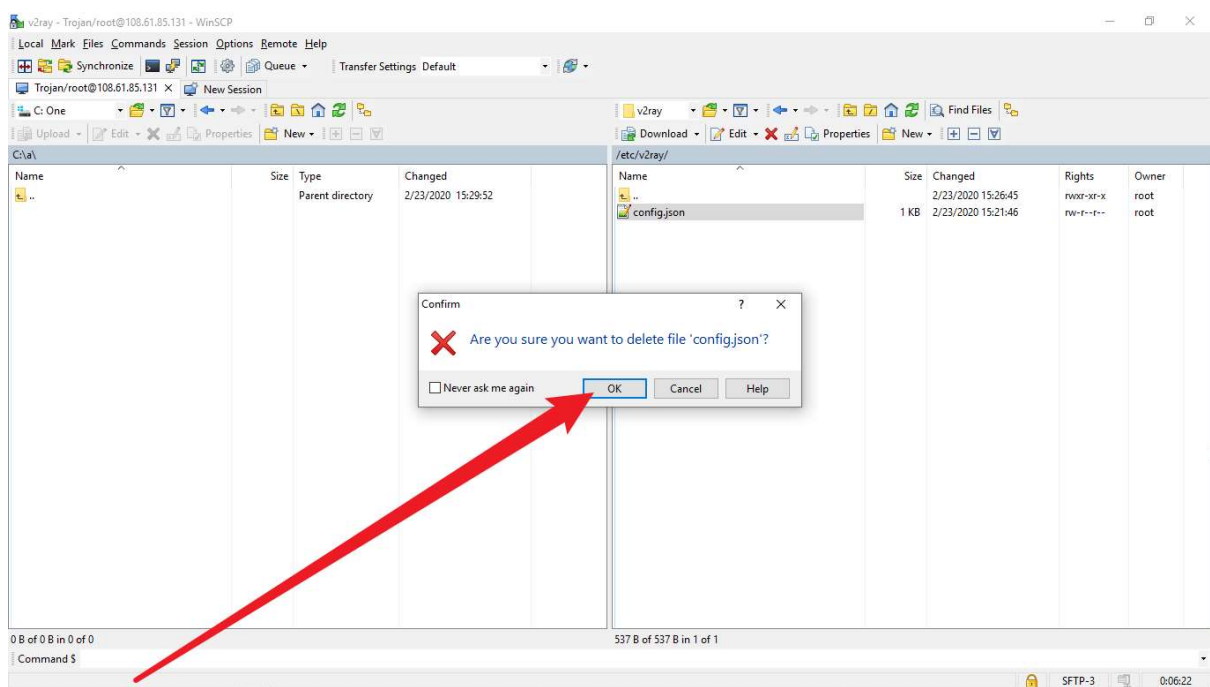
单击。就将这个文件删除了。记住这种删除文件的方法。

用 WinSCP 将这个文件上传。这是服务器端 V2ray 的配置文件。
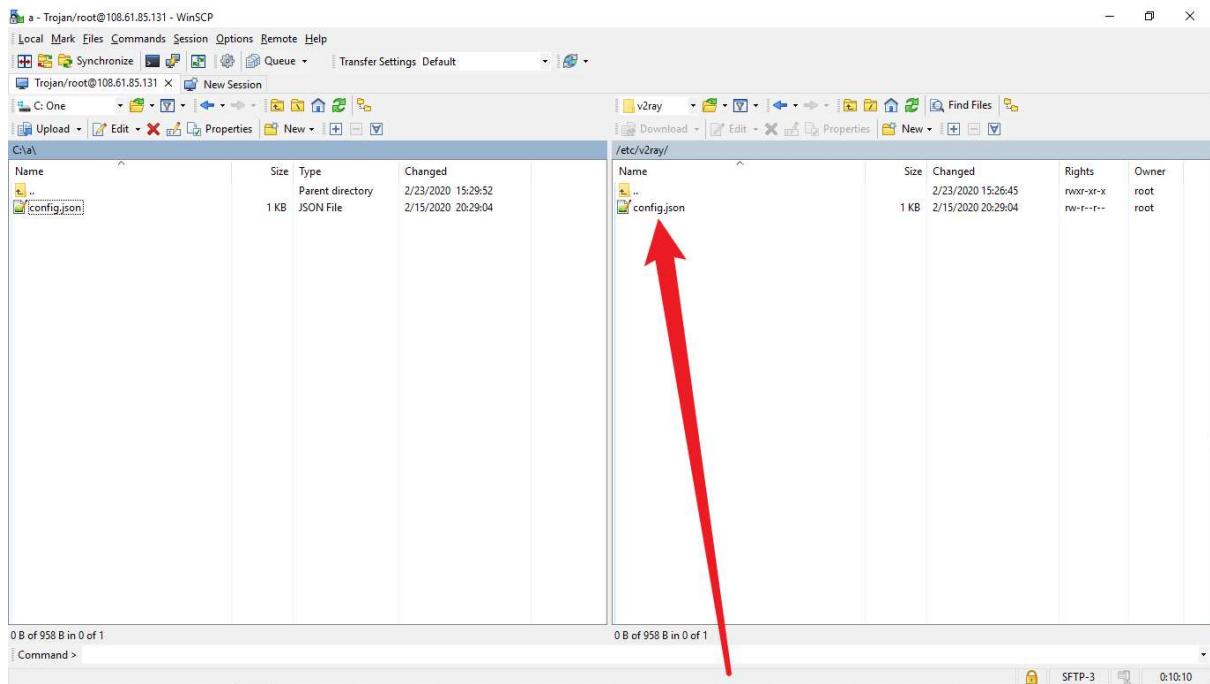
这是上传完成之后的截图
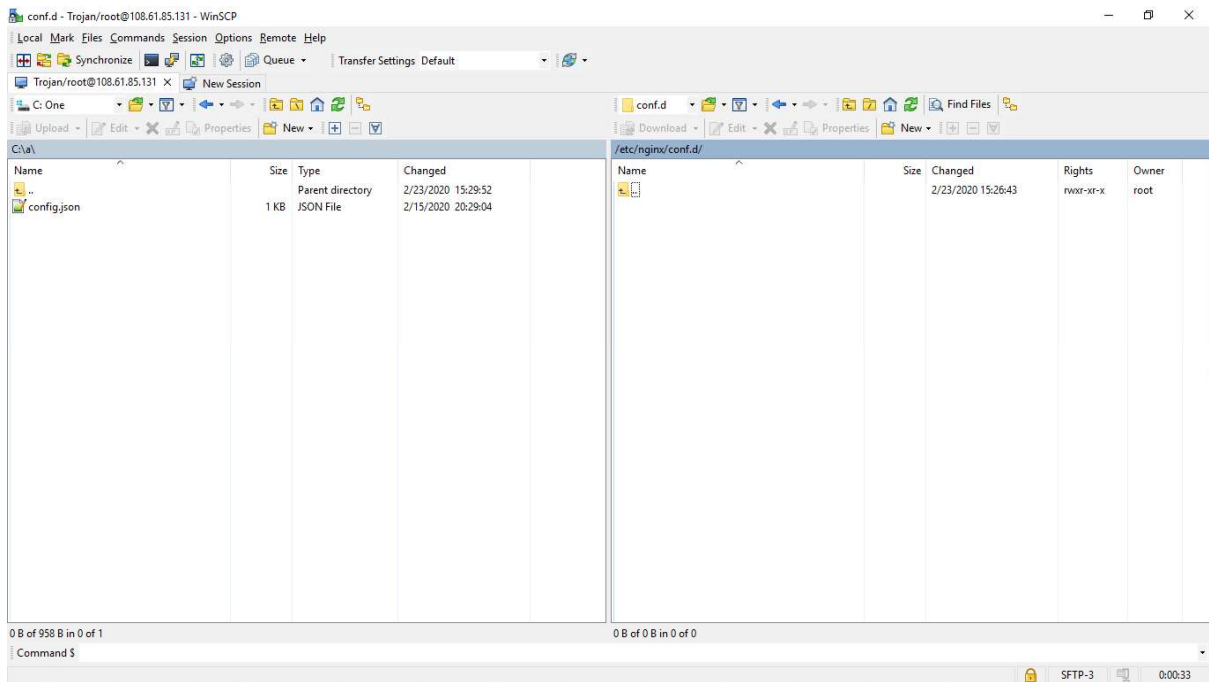
进入 /etc/nginx/conf.d

将 v2ray.conf 上传。这是 Nginx 用于 V2ray 的配置文件。
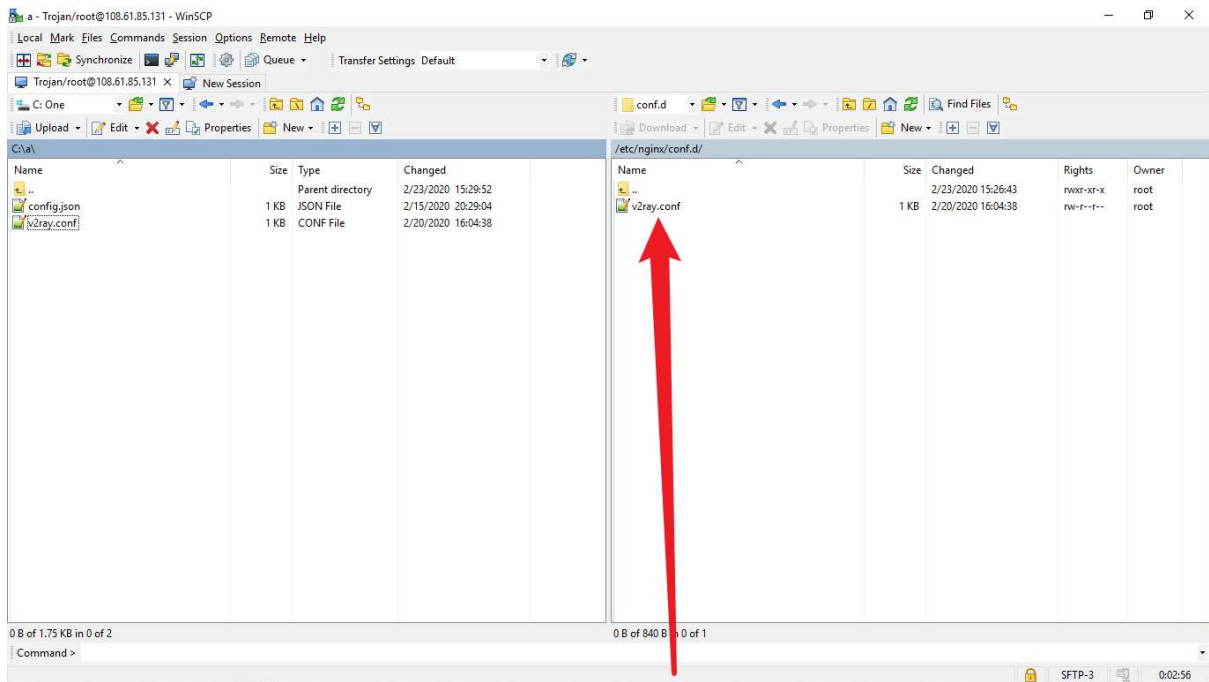
这是上传完成之后的截图
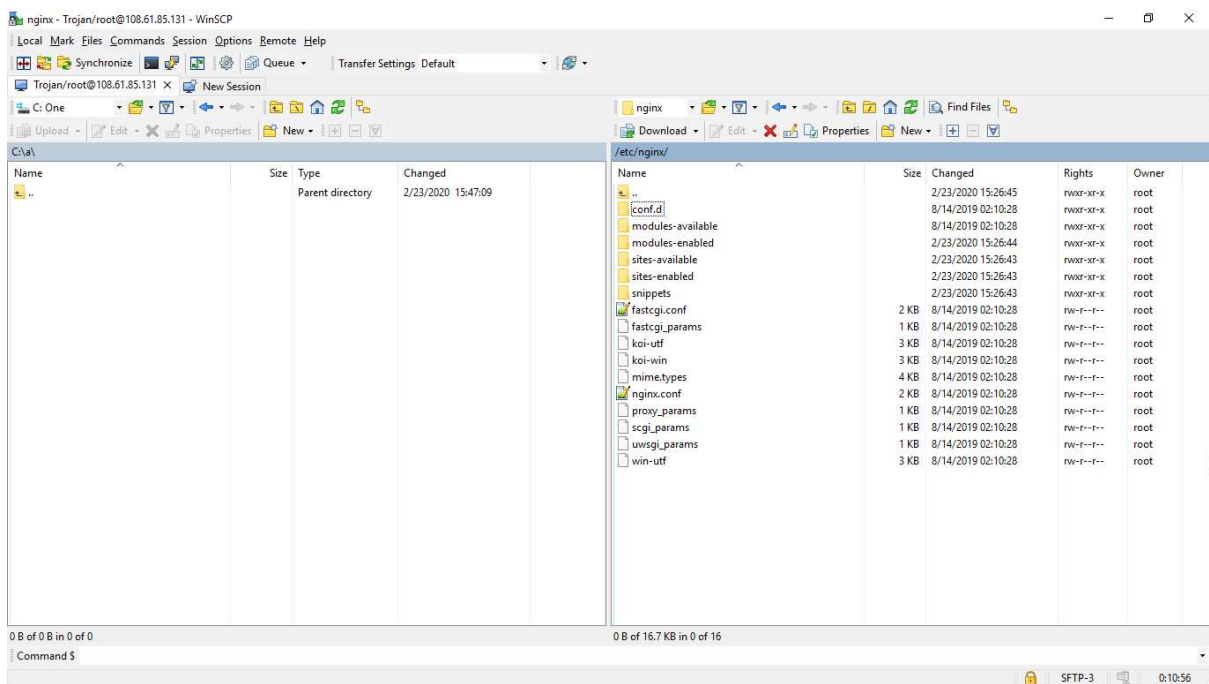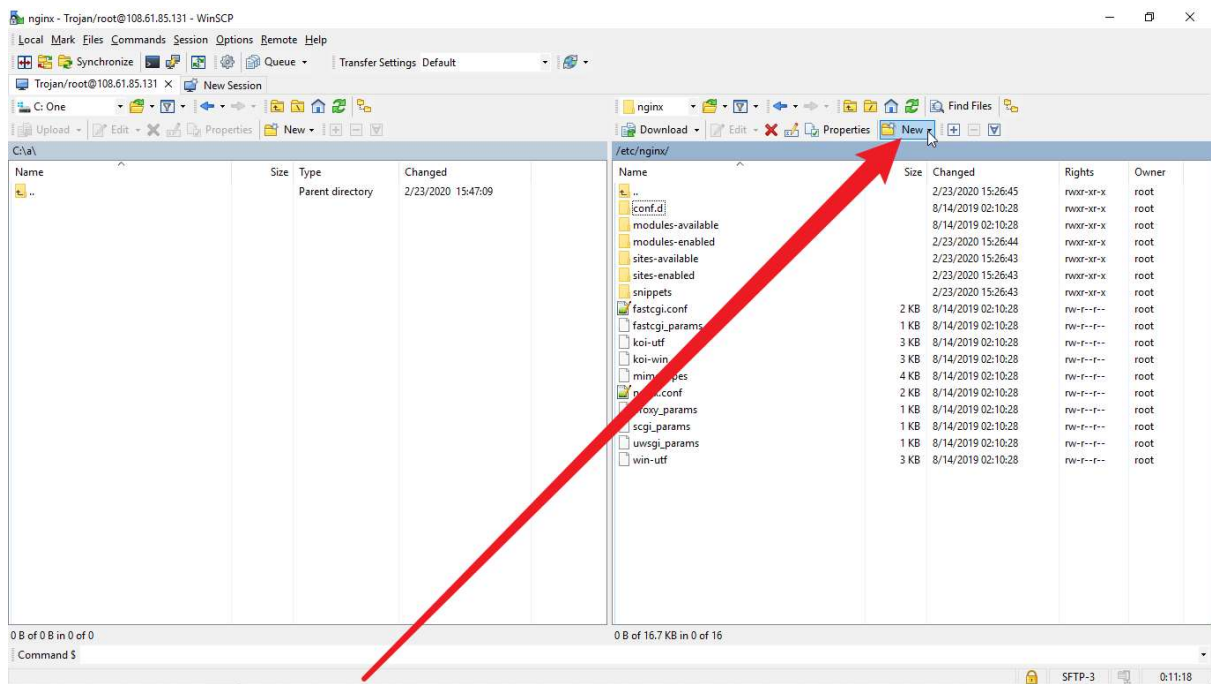
进入 /etc/nginx

点击
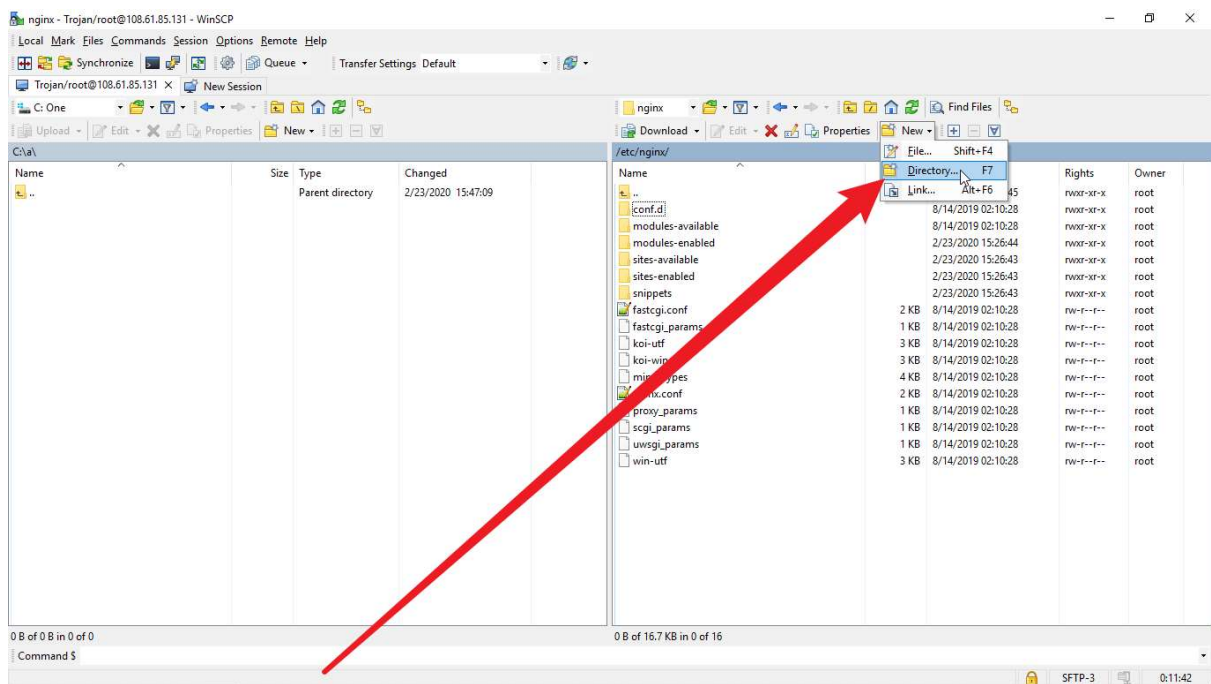
点击
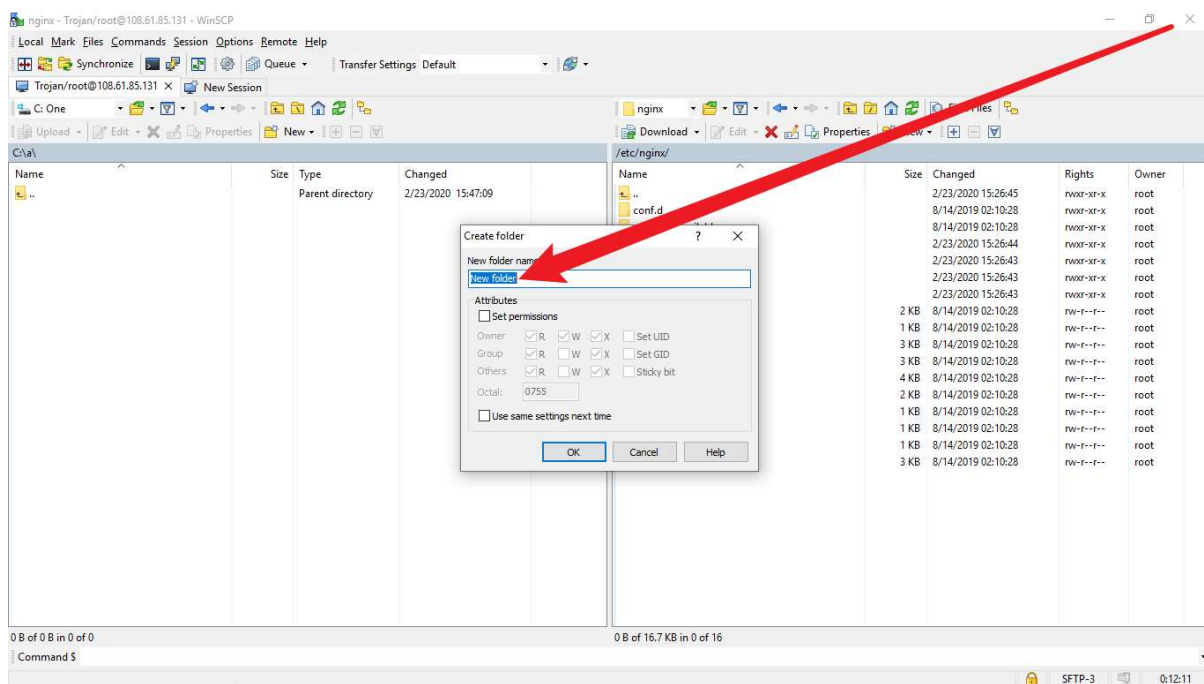
这里改成 ssl
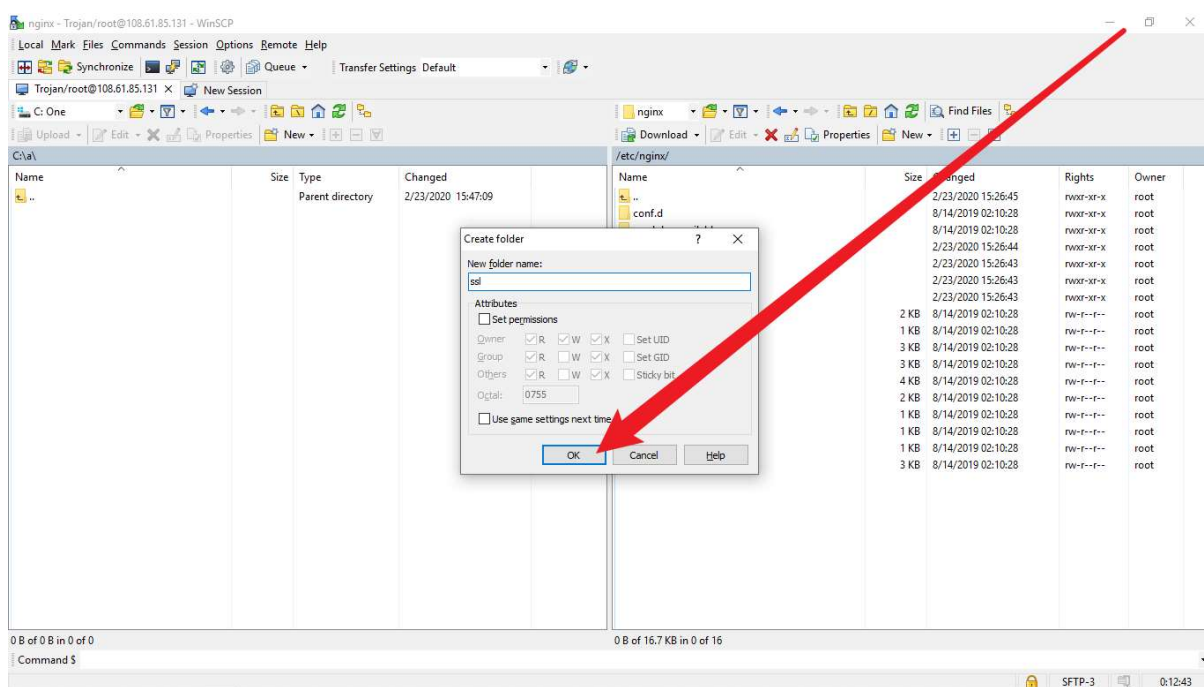
点击
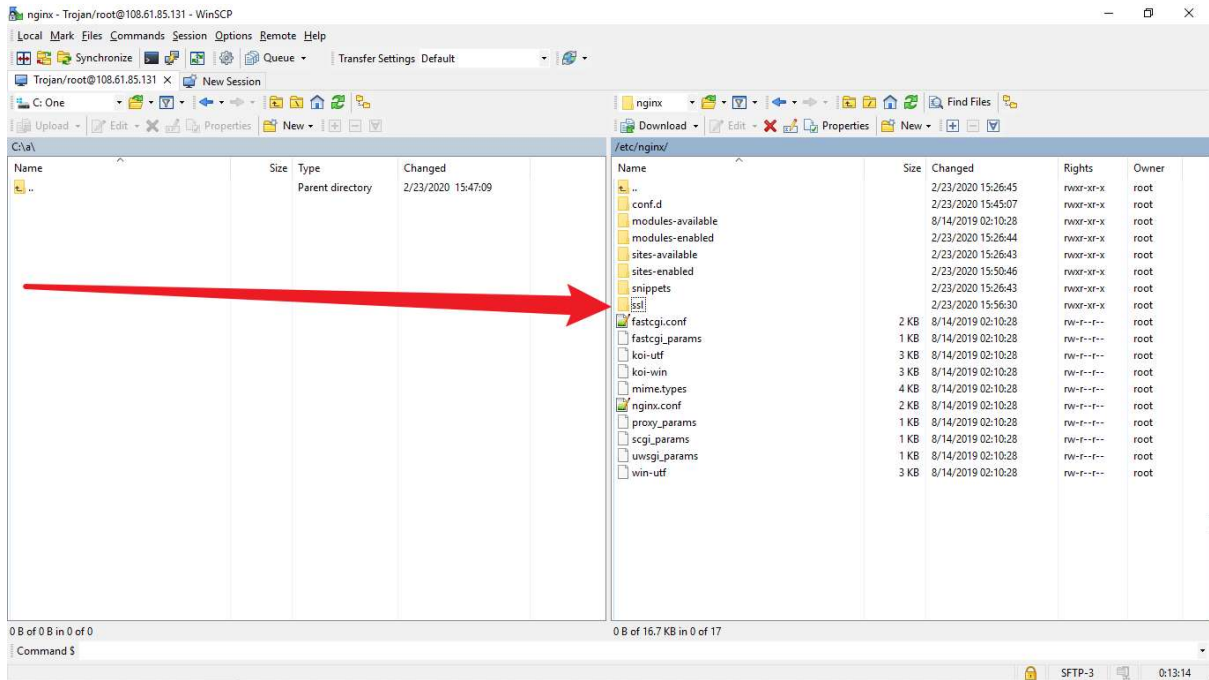
一个名为 ssl 的文件夹就新建好了。稍后我们会通过命令将刚才申请好的证书安装到这个文件夹。

输入 rm /etc/nginx/sites-enabled/default ，敲回车。这是删除 Nginx 的无用配置，防止和上传的配置冲突。

输入 ~/.acme.sh/acme.sh --installcert -d dskg.ml --fullchainpath /etc/nginx/ssl/site.crt --keypath /etc/nginx/ssl/site.key --ecc ，敲回车。记得提前把 dskg.ml 改成你自己的域名。这是安装证书到刚才新建的 ssl 文件夹。

输入 systemctl restart nginx ，敲回车。这是重启 Nginx，因为刚才上传了新配置文件。

输入 systemctl restart v2ray ，敲回车。这是重启 V2ray，因为刚才上传了新配置文件。

这里输入你的域名。V2ray 客户端会根据域名找到服务器。

这里输入 443   。这是要连接到的服务器的端口。

这里输入前面复制的 UUID

这里改成数字 0

点击

点击。这是将传输协议设置成 Websocket。

输入几个英文字母作为这个配置的名字

```
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    ssl_certificate        /etc/nginx/ssl/site.crt;
    ssl_certificate_key    /etc/nginx/ssl/site.key;
    ssl_protocols         TLSv1.3;
    ssl_prefer_server_ciphers on;
    add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload" always;
    server_name dskg.ml;
    location / {
        proxy_pass https://www.ietf.org;
    }
    location /pojfpoiehrgipwgfedhpotjknopffapqpejriwehgsfehgfrjphognmxspvgsojouegefdnhptihosug
    {
    proxy_redirect off;
    proxy_pass http://127.0.0.1:51337;
    proxy_http_version 1.1;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
    proxy_set_header Host $http_host;
    }
}
```

复制

粘贴到这里。这是 V2ray 的真实路径，设置得如此复杂无序是防止被 GFW 主动探测。

点击

点击。这是用 TLS 加密传输。

Edit or add a [VMess] server
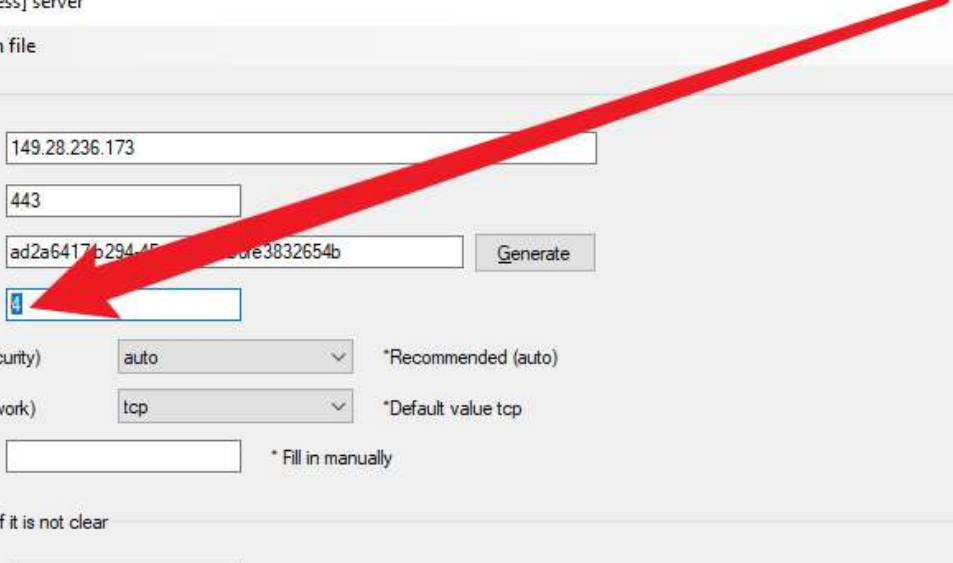
Import configuration file

Server

Address	149.28.236.173
Port	443
UUID(id)	ad2a6417-b294-45e7-9309-b0fe3832654b Generate
AlterId	0
Encryption method (security)	auto *Recommended (auto)
Transport protocol(network)	ws *Default value tcp
Alias (remarks)	aabbcc * Fill in manually

Keep the default value if it is not clear

Camouflage type   none   *tcp or kcp or QUIC camouflage type, default none

Camouflage domain(host)
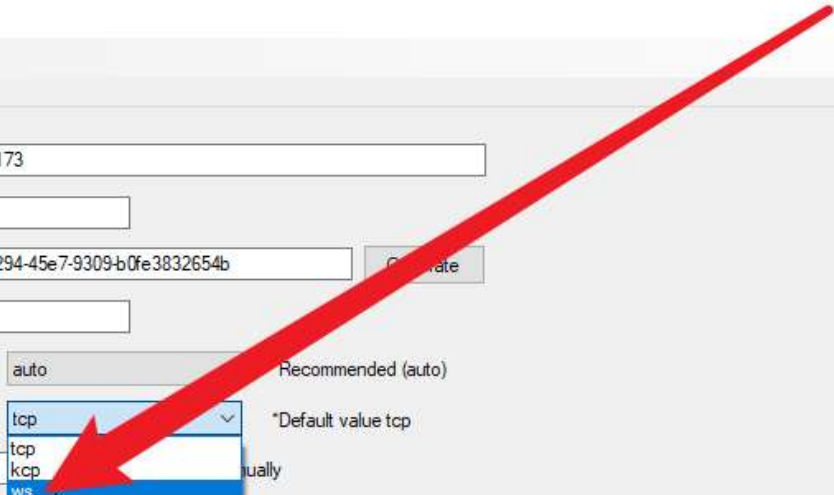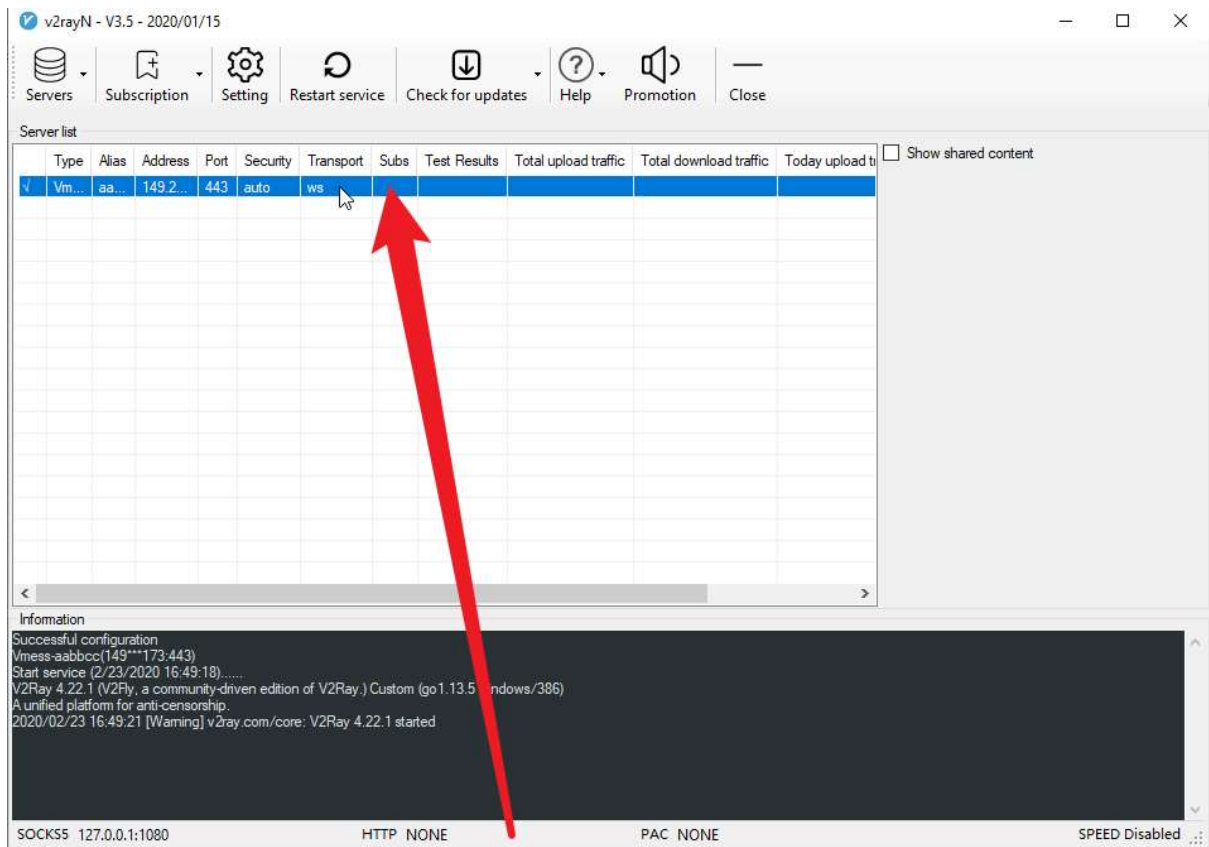1)http host Separated by commas (,)
2) ws host
3) h2 host Separated by commas (,)
4) QUIC securty

Path   /pojfpoiehrgipwgfedhpotjknopffapqpejriwehgsfehgfrjphognmxspvgsojc efdnhpti hosug
1)ws path
2)h2 path
3)QUIC key

TLS   tls   allowInsecure   Default value true

OK   Cancel

点击

点击。这是验证证书的安全性。

点击。这个配置就添加了。

单击新添加的配置，敲回车，这个配置就开始运行了

在任何地方提任何问题之前首先要确保自己已经仔细研读过下面这篇文章至少三遍：
https://github.com/ryanhanwu/How-To-Ask-Questions-The-Smart-Way/blob/master/README-zh_CN.md