一、使用说明

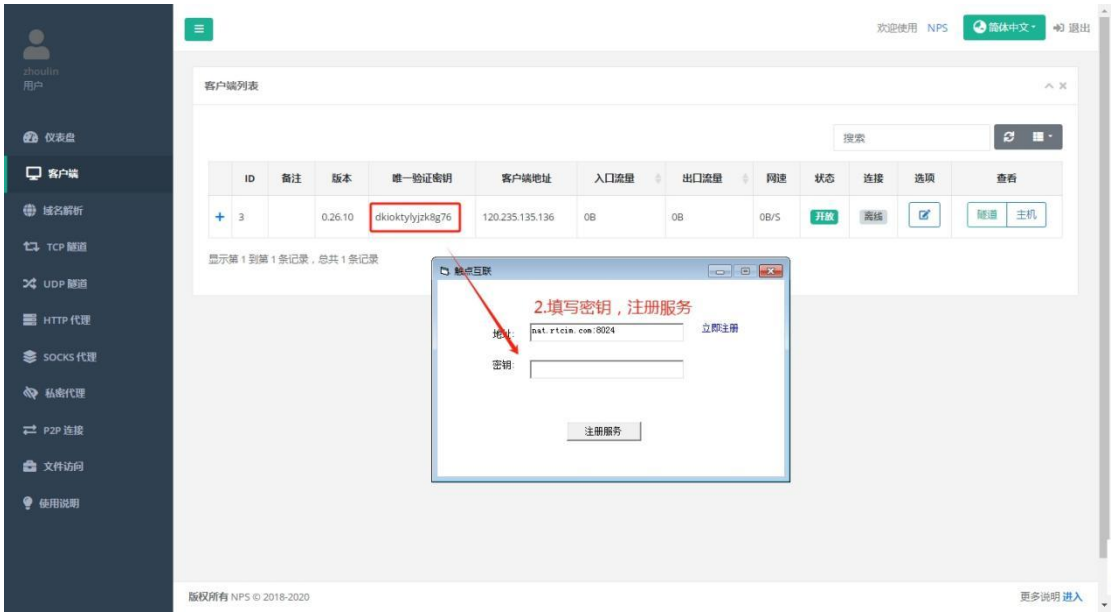
1. 退出 360 等防护软件。

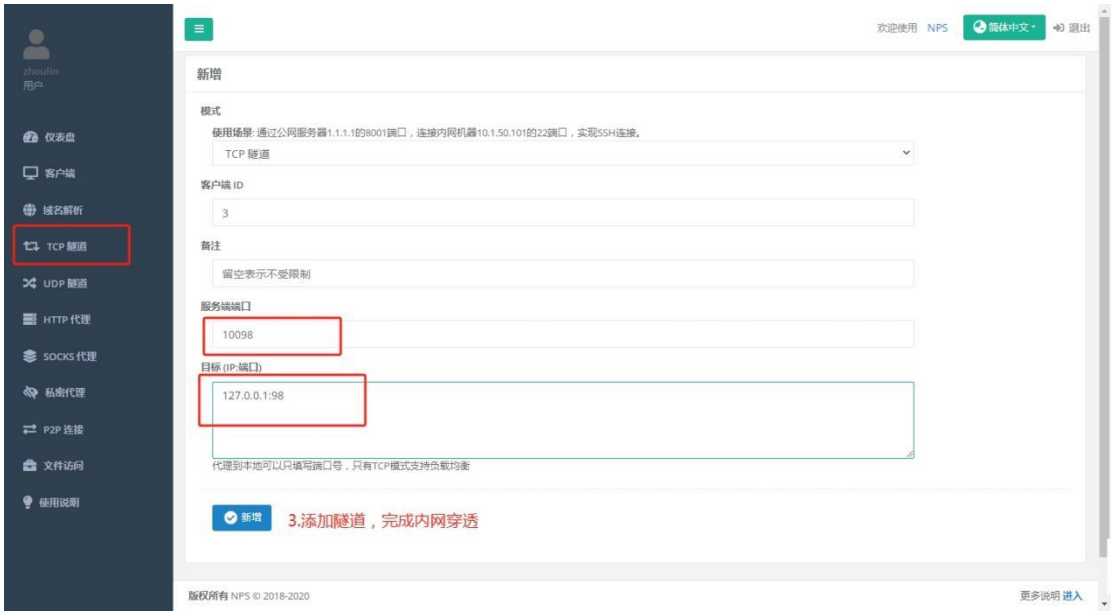
2. 页面右上角点击“客户端下载”，解压缩 RTCNAT.zip，双击 RTCNAT.exe。

3. 注册一个账号登陆进入后台，填写客户端密钥，注册服务。

4. 添加隧道，完成内网穿透。

5. 打开 http://nat.rtcim.com:隧道端口，即可打开公司内网 erp/crm/oa/nas 等系统。





二、域名解析

适用范围： 小程序开发、微信公众号开发、产品演示

注意：域名解析模式为 http 反向代理，不是 dns 服务器，在 web 上能够轻松灵活配置

假设场景：

- 有一个域名 proxy.com，有一台公网机器 ip 为 1.1.1.1
- 两个内网开发站点 127.0.0.1:81，127.0.0.1:82
- 想通过（http|https://）a.proxy.com 访问 127.0.0.1:81，通过（http|https://）b.proxy.com 访问 127.0.0.1:82

使用步骤

- 将*.proxy.com 解析到公网服务器 1.1.1.1
- 点击刚才创建的客户端的域名管理，添加两条规则规则：1、域名：`a.proxy.com`，内网目标：`127.0.0.1:81`，2、域名：`b.proxy.com`，内网目标：`127.0.0.1:82`

现在访问（http|https://）`a.proxy.com`，`b.proxy.com` 即可成功

三、tcp 隧道

适用范围： ssh、远程桌面等 tcp 连接场景

假设场景： 想通过访问公网服务器 1.1.1.1 的 8001 端口，连接内网机器 10.1.50.101 的 22 端口，实现 ssh 连接

使用步骤

- 在刚才创建的客户端隧道管理中添加一条 tcp 隧道，填写监听的端口（8001）、内网目标 ip 和目标端口（10.1.50.101:22），保存。
- 访问公网服务器 ip（1.1.1.1）,填写的监听端口(8001)，相当于访问内网 ip(10.1.50.101):目标端口(22)，例如：`ssh -p 8001 root@1.1.1.1`

四、udp 隧道

适用范围： 内网 dns 解析等 udp 连接场景

假设场景： 内网有一台 dns（10.1.50.102:53），在非内网环境下想使用该 dns，公网服务器为 1.1.1.1

使用步骤

- 在刚才创建的客户端的隧道管理中添加一条 udp 隧道，填写监听的端口（53）、内网目标 ip 和目标端口（10.1.50.102:53），保存。
- 修改需要使用的 dns 地址为 1.1.1.1，则相当于使用 10.1.50.102 作为 dns 服务器

五、socks5 代理

适用范围： 在外网环境下如同使用 vpn 一样访问内网设备或者资源

假设场景： 想将公网服务器 1.1.1.1 的 8003 端口作为 socks5 代理，达到访问内网任意设备或者资源的效果

使用步骤

- 在刚才创建的客户端隧道管理中添加一条 socks5 代理，填写监听的端口（8003），保存。
- 在外网环境的本机配置 socks5 代理(例如使用 proxifier 进行全局代理)，ip 为公网服务器 ip（1.1.1.1），端口为填写的监听端口(8003)，即可畅享内网了

注意 经过 socks5 代理，当收到 socks5 数据包时 socket 已经是 accept 状态。表现是扫描端口全 open，建立连接后短时间关闭。若想同内网表现一致，建议远程连接一台设备。

六、http 正向代理

适用范围： 在外网环境下使用 http 正向代理访问内网站点

假设场景： 想将公网服务器 1.1.1.1 的 8004 端口作为 http 代理，访问内网网站

使用步骤

- 在刚才创建的客户端隧道管理中添加一条 http 代理，填写监听的端口（8004），保存。
- 在外网环境的本机配置 http 代理，ip 为公网服务器 ip（1.1.1.1），端口为填写的监听端口(8004)，即可访问了

注意：对于私密代理与 p2p，除了统一配置的客户端和服务端，还需要一个客户端作为访问端提供一个端口来访问

七、私密代理

适用范围： 无需占用多余的端口、安全性要求较高可以防止其他人连接的 tcp 服务，例如 ssh。

假设场景： 无需新增多的端口实现访问内网服务器 10.1.50.2 的 22 端口

使用步骤

- 在刚才创建的客户端中添加一条私密代理，并设置唯一密钥 secrettest 和内网目标 10.1.50.2:22
- 在需要连接 ssh 的机器上以执行命令

```
./npc -server=1.1.1.1:8024 -vkey=vkey -type=tcp -password=secrettest -local_type=secretCopy to clipboardErrorCopied
```

如需指定本地端口可加参数`-local_port=xx`，默认为 2000

注意： password 为 web 管理上添加的唯一密钥，具体命令可查看 web 管理上的命令提示

假设 10.1.50.2 用户名为 root，现在执行 `ssh -p 2000 root@127.0.0.1` 即可访问 ssh

八、p2p 服务

适用范围： 大流量传输场景，流量不经过公网服务器，但是由于 p2p 穿透和 nat 类型关系较大，不保证 100%成功，支持大部分 nat 类型。

假设场景：

想通过访问使用端机器（访问端，也就是本机）的 2000 端口---->访问到内网机器 10.2.50.2 的 22 端口

使用步骤

- 在 `nps.conf` 中设置 `p2p_ip`（nps 服务器 ip）和 `p2p_port`（nps 服务器 udp 端口）

  注：若 `p2p_port` 设置为 6000，请在防火墙开放 6000~6002(额外添加 2 个端口)udp 端口

- 在刚才刚才创建的客户端中添加一条 p2p 代理，并设置唯一密钥 p2pssh
- 在使用端机器（本机）执行命令

```
./npc -server=1.1.1.1:8024 -vkey=123 -password=p2pssh -target=10.2.50.2:22Copy to clipboardErrorCopied
```

如需指定本地端口可加参数`-local_port=xx`，默认为 2000

注意： password 为 web 管理上添加的唯一密钥，具体命令可查看 web 管理上的命令提示

假设内网机器为 10.2.50.2 的 ssh 用户名为 root，现在在本机上执行 `ssh -p 2000 root@127.0.0.1` 即可访问机器 2 的 ssh，如果是网站在浏览器访问 127.0.0.1:2000 端口即可。