**[一、使用说明](https://ehang-io.github.io/nps/" \l "/example?id=%e5%9f%9f%e5%90%8d%e8%a7%a3%e6%9e%90)**

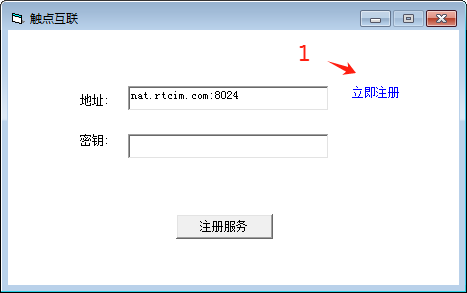
1.退出360等防护软件。

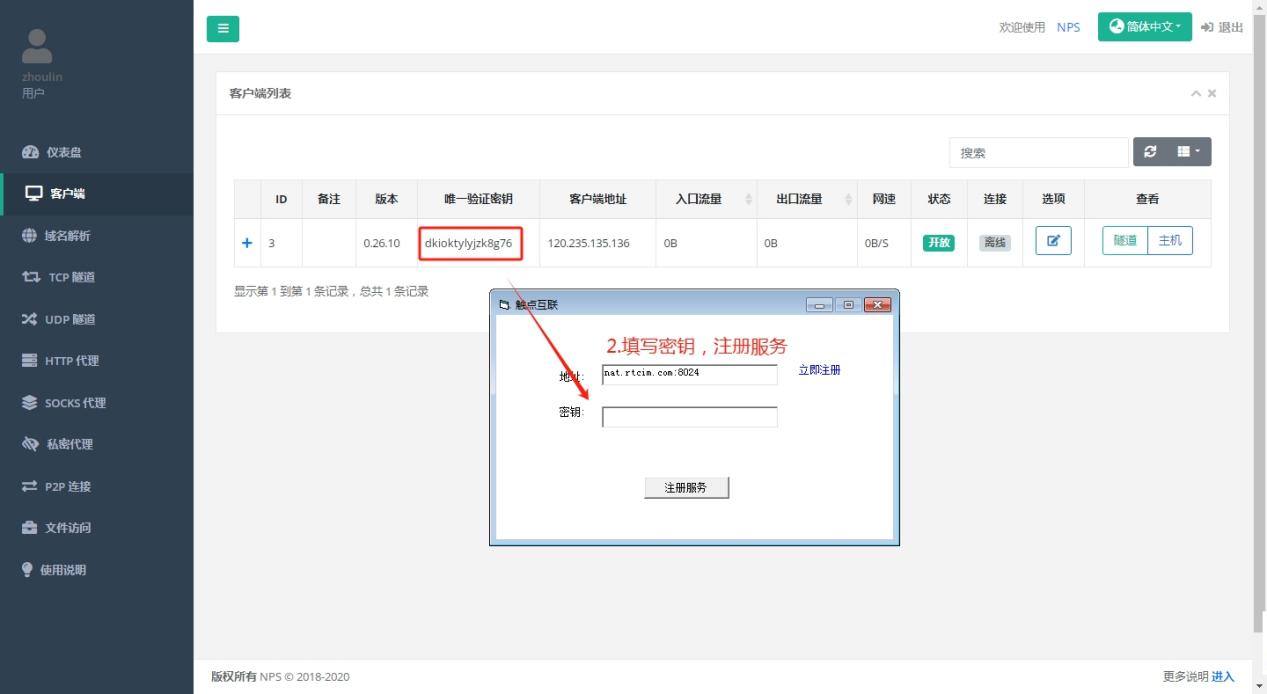
2.页面右上角点击“客户端下载”,解压缩RTCNAT.zip,双击RTCNAT.exe。

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](https://ehang-io.github.io/nps/" \l "/example?id=%e5%9f%9f%e5%90%8d%e8%a7%a3%e6%9e%90)**

****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](https://ehang-io.github.io/nps/" \l "/example?id=tcp%e9%9a%a7%e9%81%93)**

****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](https://ehang-io.github.io/nps/" \l "/example?id=udp%e9%9a%a7%e9%81%93)**

****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](https://ehang-io.github.io/nps/" \l "/example?id=socks5%e4%bb%a3%e7%90%86)**

****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](https://ehang-io.github.io/nps/" \l "/example?id=http%e6%ad%a3%e5%90%91%e4%bb%a3%e7%90%86)**

****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](https://ehang-io.github.io/nps/" \l "/example?id=%e7%a7%81%e5%af%86%e4%bb%a3%e7%90%86)**

****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](https://ehang-io.github.io/nps/" \l "/example?id=p2p%e6%9c%8d%e5%8a%a1)**

****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。