





[原创]frida集群搭建，超详细

简单的人生



临时

1小时前

举报

65

介绍一下搭建中需要用到的nps服务器

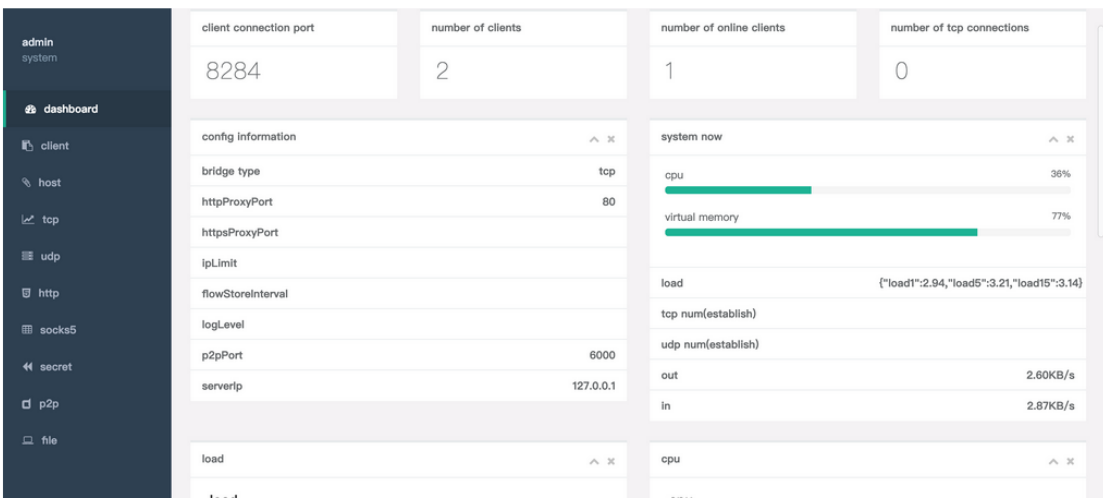
nps

stars 14k forks 2.4k chat on github build passing downloads 693k

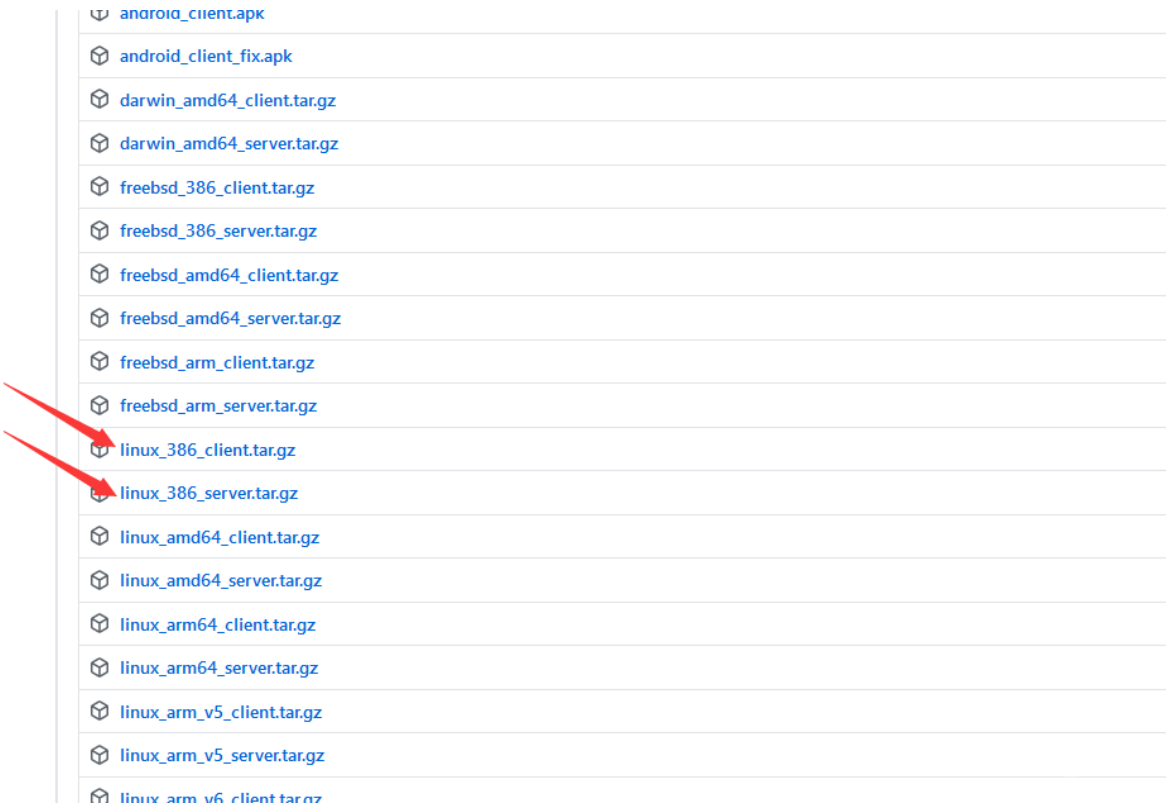
[README中文文档](#)

nps是一款轻量级、高性能、功能强大的内网穿透代理服务器。目前支持tcp、udp流量转发，可支持任何tcp、udp上层协议（访问内网网站、本地支付接口调试、ssh访问、远程桌面，内网dns解析等等.....），此外还支持内网http代理、内网socks5代理、p2p等，并带有功能强大的web管理端。

背景



nps分为服务器端和客户端，针对不同的架构有区分，分别下载不同的压缩包部署即可。
实验中我使用的是云服务器和模拟器，所以选择了386的版本



在服务器端，启动之前确保服务器的 80，443，8080，8024端口都没有被占用，如果启动失败，可以查看在/var/log/nps.log中的日志找出问题出在哪里并且解决。云服务器还要记得将这些端口放进安全组。

- 1

解压
- 2

tar zxvf linux_386_server.tar.gz
- 3

安装
- 4

sudo ./nps install
- 5

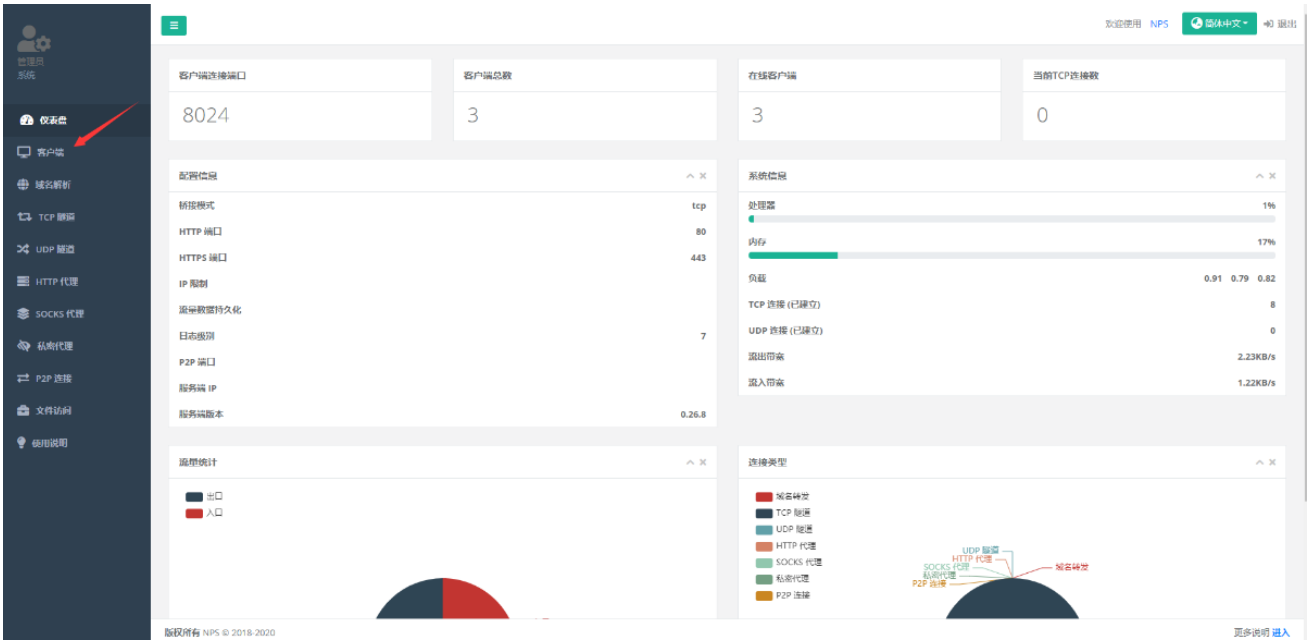
启动
- 6

sudo nps start

启动之后，直接访问服务器的8080端口，就可以进入web管理界面， 默认的账号密码为admin， 123， 生产环境中一定要记得更改。



登录后，进入客户端管理界面，



点击新增，（图中是我已经配置好的三台手机模拟器）



简单的添加一个备注

新增客户端

备注

模拟器4

Basic 认证用户名

留空表示不受限制

仅限Socks5、Web、HTTP转发代理

Basic 认证密码

留空表示不受限制

仅限Socks5、Web、HTTP转发代理

唯一验证密钥

留空表示不受限制

唯一值，不填将自动生成

允许客户端通过配置文件连接

是

压缩

否

加密

否

新增

点击左上角的+号就可以看到在客户端运行的命令。

5

模拟器4

qn21vhjju651u9mz

0B

0B

16MB/s

开放

删除

编辑

隧道

主机

最大连接数: 0

当前连接数: 0

流量限制: 0m

带宽限制: 0kb/s

最大隧道数: 0

Web登陆用户名:

Web登陆密码:

Basic 认证用户名:

Basic 认证密码:

加密: 否

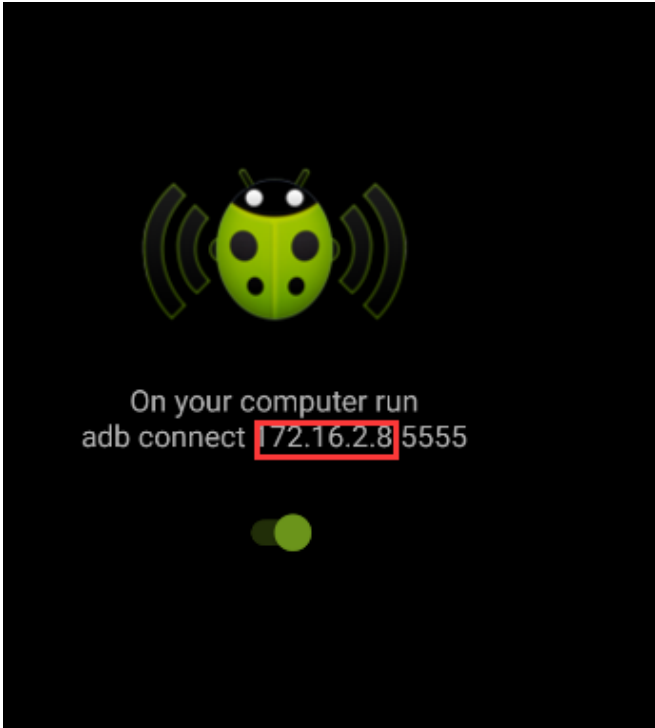
压缩: 否

允许客户端通过配置文件连接: 是

客户端命令: ./npc -server=62.234.132.155:8024 -vkey=qn21vhjju651u9mz -type=tcp

显示第 1 到第 4 条记录，总共 4 条记录

模拟器端，需要启动wifiadb，查看该手机模拟器的内网端口



```
1 | 启动frida，
2 | adb -s emulator-5554 shell './data/local/tmp/fs -l 0.0.0.0:1111'
3 | 启动nps客户端
4 | adb -s emulator-5554 shell './data/local/tmp/npc -server=62.234.132.155:8024 -vkey=fqclv2e4kqv4xf6f -type=tcp'
```

服务端还需要最后一步，新建隧道，服务端端口可以随便填没有被占用的端口，目标的ip端口需要填写模拟器所在的内网ip，和frida监听的端口。知道这个内网ip后，关闭wifiadb后好像也没影响，在模拟器上是这样，手机没试过，但估计必须要打开吧！



新增

模式

使用场景: 通过公网服务器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。

TCP 隧道

客户端 ID

5

备注

留空表示不受限制

服务端端口

5555

目标 (IP:端口)

例如

10.1.50.203:80

10.1.50.202:80

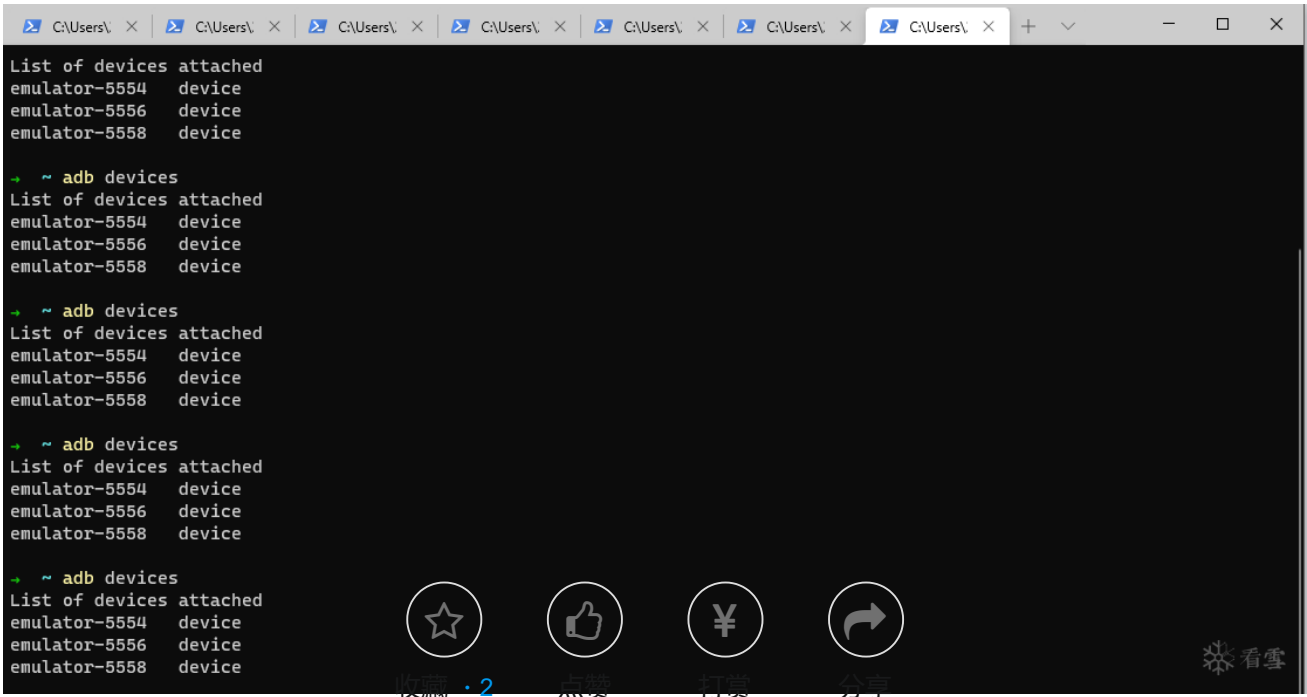
代理到本地可以只填写端口号，只有TCP模式支持负载均衡

✓ 新增

这样一个最重要的公网访问frida-server的部分就完成了，要想搭建集群，只要多添加几个手机客户端就可以了。

```
1  这段代码的目的就是，挨个启动手机中的设置，也可以自己再使用frida-rpc调用主动调用app中的函数，只要hook好，什么都跑不掉^_^，
2  device_list = ["服务器ip:1111", "服务器ip:2222", "服务器ip:3333"]
3  for device in device_list:
4      time.sleep(2)
5      device = frida.get_device_manager().add_remote_device(device)
6      print(device.get_frontmost_application())
7
8      pid = device.spawn("com.android.settings")
9      device.resume(pid)
10
11     print(pid)
12     time.sleep(1)
13     device.attach(pid)
14     session = device.attach(pid)
15     with open("demo.js") as f:
16         script = session.create_script(f.read())
17     script.load()
```

但是这种frida-server集群的方法不是很方便，每个手机客户端都要开两个命令行窗口，但是应该可以做一个py脚本批量运行命令，要不然一个一个的启动实在太过麻烦。我三台模拟器就开了6个窗口。还有多台设备管理的问题，需要在python中将每台设备主动调用函数的次数做到限制，使用类似负载均衡中用到的方法？（轮询？随机？大佬做过的可以讲讲，谢谢）并且对外做成一个web服务，这样别人不用管内部具体实现，直接调用接口即可。



nps地址 <https://github.com/ehang-io/nps>

最新回复 (0)



wx_nu无情

内容

回帖

表情

高级回复



2

©2000-2020 看雪学院 | Based on [Xiuno BBS](#)
域名：加速乐 | SSL证书：[亚洲诚信](#) | [安全网易易盾](#)| [同盾反欺诈](#)| 服务器：绿盟科技

看雪APP | 公众号：ikanxue | [关于我们](#) | [联系我们](#) | [企业服务](#)
Processed: **0.030**s, SQL: **18** / [京ICP备10040895号-17](#)



首页



论坛



课程



招聘



发现