

常見內網穿透工具使用總結

黑客技術和網絡安全 昨天



架構師大咖

架構師大咖，打造有價值的架構師交流平台。分享架構師乾貨、教程、課程、資訊。架構師大咖，每日推送。



公眾號



算法專欄

算法專欄，每日推送。算法是程序員內功，分享算法知識、文章、工具、算法題、教程等



公眾號

文章作者 | V0WKeep3r

原文鏈接 |

<http://v0w.top/2020/08/11/IntranetProxy/>

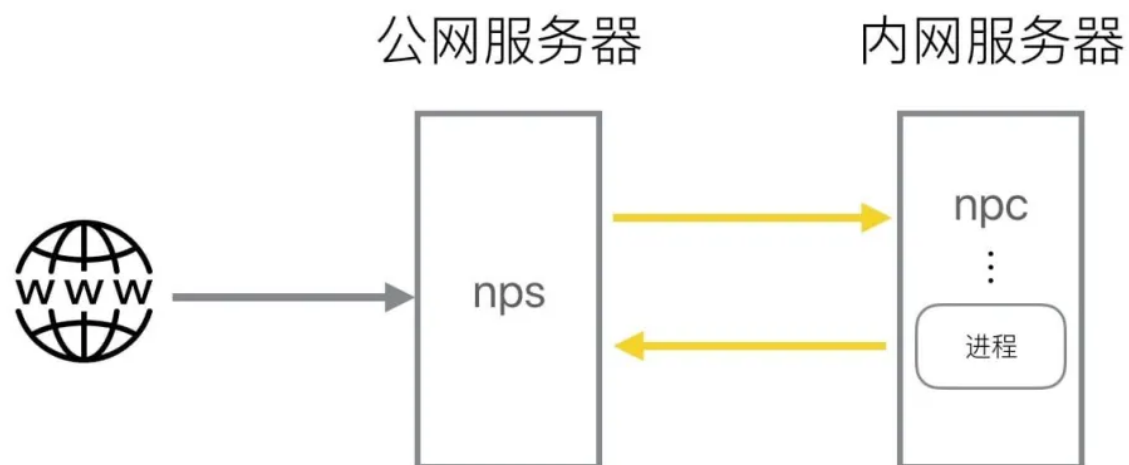
0x00 前言

本文以滲透的視角，總結幾種個人常用的內網穿透，內網代理工具，介紹其簡單原理和使用方法。

0x01 nps-npc

1.1 簡介

nps是一款輕量級、高性能、功能強大的 目前支持
一台有公網IP的服務器（VPS）運行服務端（
一個或多個運行在內網的服務器或者PC運行客戶端（



HACK之道

1.2 特點

- Go語言編寫
- 支持跨平台
- 支持多種協議的代理

- web管理端

1.3 使用方法

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

NPS

安裝配置

找到自己服務器相應版本的server:

```
1 cd ~
2 wget https://github.com/cnlh/nps/releases/download/v0.23.2/linux_amd64_server.tar.gz
3 tar xzvf linux_amd64_server.tar.gz
4 cd ~/nps
```

在nps目錄下面會有一個nps可執行文件、conf配置目錄和web網頁目錄，我們只需要修改 `conf/nps.conf`

```
1 vim conf/nps.conf
```

需要改一下 `#web`

```
1 web_host= 服务器IP或者域名
2 web_username= admin ( 登录用户名 )
3 web_password= 你的密码
4 web_port=8080 ( web管理端口 )
```

修改 比如我們拿到一台權限受限的服務器，有防火牆，可能只有部分端口（80，443）可以出網，就需要修改成出網端口。

#bridge

```
1 ##bridge
2 bridge_type=tcp
3 bridge_port=443      # 修改连接端口
4 bridge_ip=0.0.0.0
```

啟動

```
1 #Mac/Linux
2 ./nps test|start|stop|restart|status  测试配置文件|启动|停止|重启|状态
3
4 #Windows
5 nps.exe test|start|stop|restart|status 测试配置文件|启动|停止|重启|状态
```

NPC

```
1 ./npc -server=你的IP:8024 -vkey=唯一验证密码 -type=tcp
```

客戶端列表

+ 新增

搜索

ID	备注	版本	唯一验证密钥	客户端地址	入口流量	出口流量	网速	状态	连接	选项	查看
2	测试	0.26.8	14...	14...	0B	0B	0B/S	开放	离线	隧道 主机	隧道 主机
4			Playt...		0B	0B	0B/S	开放	离线	隧道 主机	隧道 主机
6	vuln...	2	V0V...		0B	0B	0B/S	开放	离线	隧道 主机	隧道 主机

显示第 1 到第 3 条记录, 总共 3 条记录

新建好客戶端后，也可以在 +

ID	备注	版本	唯一验证密钥	客户端地址	入口流量	出口流量	网速	状态	连接	选项	查看
4		0.26.8	Playt...	223...	0.15MB	0.23MB	0B/S	开放	离线	隧道 主机	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=182... -vkey=Pl... -type=tcp

web管理端

在客戶端界面可以通過 新增

每一個客戶端，在建立連接後，都可以建立多個不同協議的隧道，這一個個隧道就是不同的代理了。

+ 新增

搜索

🔄 列表

	ID	客户端 ID	备注	模式	端口	目标 (IP:端口)	唯一标识密钥	状态	运行状态	客户端状态	选项
+	2	4		SOCKS 代理	8024			开放	开放	在线	  
+	3	4		HTTP 代理	8848			开放	开放	在线	  

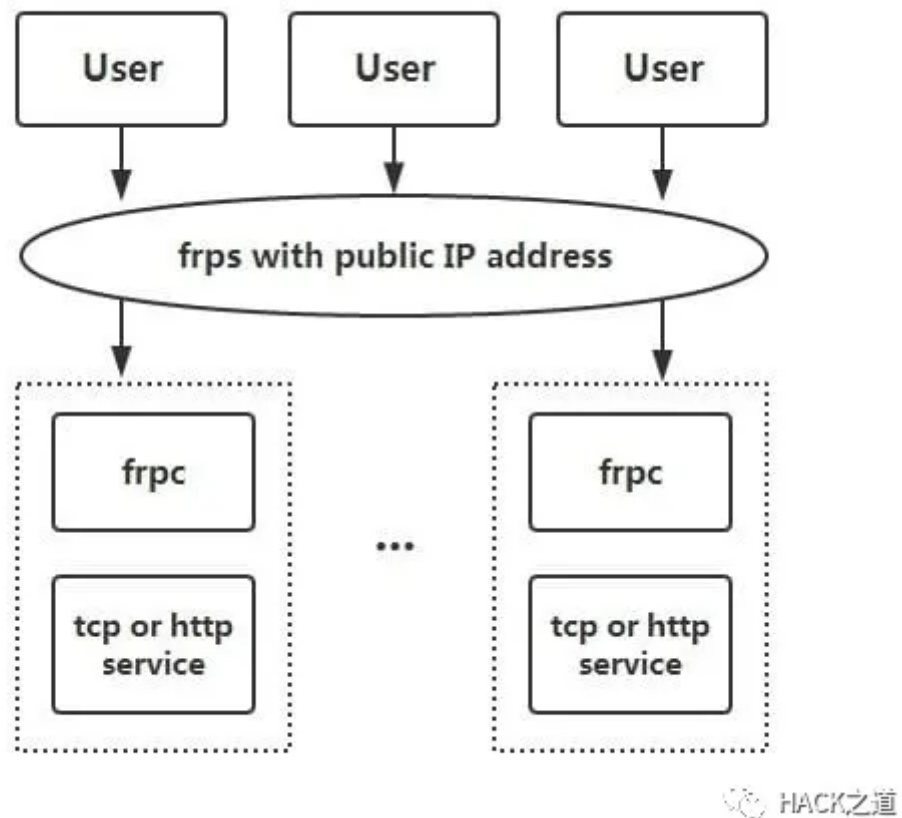
显示第 1 到第 2 条记录, 总共 2 条记录

通過不同的協議和端口就可以連接代理的內網機器。

0x02 frp

2.1 簡介

frp 是一個專注於內網穿透的高性能的反向代理應用，支持TCP、UDP、HTTP、HTTPS 等多種協議。可以將內網服務以安全、便捷的方式通過具有公網IP 節點的中轉暴露到公網。



2.2 特點

- 客戶端服務端通信支持TCP、KCP 以及Websocket 等多種協議。
- 端口復用，多個服務通過同一個服務端端口暴露。
- 跨平台，但是支持的比nps少一點
- 多種插件，提供很多功能

2.3 使用方法

下載: <https://github.com/fatedier/frp/releases>

以下內容摘自: <https://segmentfault.com/a/1190000021876836>

1. 通过 rdp 访问家里的机器

修改 frps.ini 文件, 为了安全起见, 这里最好配置一下身份验证, 服务端和客户端的 common 配置中的 token 参数一致则身份验证通过:

```
1 # frps.ini
2 [common]
3 bind_port = 7000
4 # 用于身份验证, 请自行修改, 要保证服务端与客户端一致
5 token = abcdefgh
```

启动 frps:

```
./frps -c ./frps.ini
```

修改 frpc.ini 文件, 假设 frps 所在服务器的公网 IP 为 x.x.x.x:

```
1 # frpc.ini
2 [common]
3 server_addr = x.x.x.x
4 server_port = 7000
5 # 用于身份验证, 请自行修改, 要保证服务端与客户端一致
6 token = abcdefgh
7
8 [rdp]
9 type = tcp
10 local_ip = 127.0.0.1
```



```
11 local_port = 3389
12 remote_port = 6000
```

启动 frpc:

```
./frpc -c ./frpc.ini
```

通过 rdp 访问远程的机器，地址为：

```
x.x.x.x:6000
```

开机自启

针对 Windows 系统，为了便于使用，可以配置一下开机的时候静默启动。

在 frpc.exe 的同级目录创建一个 start_frpc.vbs:

```
1 'start_frpc.vbs
2 '请根据实际情况修改路径
3 CreateObject("WScript.Shell").Run ""D:\Program Files\frp_windows_amd64\frpc.exe"" & "-c" &
  ""D:\Program Files\frp_windows_amd64\frpc.ini"",0
```

复制 start_frpc.vbs 文件，打开以下目录，注意将

```
1 <USER_NAME>
```

改为你的用户名：

```
C:\Users\<USER_NAME>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
```

鼠标右击，粘贴为快捷方式即可。

2. 通过 SSH 访问公司内网机器

frps 的部署步骤同上。

启动 frpc，配置如下：

```
1 # frpc.ini
2 [common]
3 server_addr = x.x.x.x
4 server_port = 7000
5 # 用于身份验证，请自行修改，要保证服务端与客户端一致
6 token = abcdefgh
7
8 [ssh]
9 type = tcp
10 local_ip = 127.0.0.1
11 local_port = 22
12 remote_port = 6000
```

通过 SSH 访问内网机器，假设用户名为 test：

```
ssh -oPort=6000 test@x.x.x.x
```

3. 通过自定义域名访问部署于内网的 Web 服务

有时想要让其他人通过域名访问或者测试我们在本地搭建的 Web 服务，但是由于本地机器没有公网 IP，无法将域名解析到本地的机器，通过 frp 就可以实现这一功能，以下示例为 http 服务，https 服务配置方法相同，vhost_http_port 替换为 vhost_https_port，type 设置为 https 即可。

修改 frps.ini 文件，设置 http 访问端口为 8080：

```
1 # frps.ini
2 [common]
3 bind_port = 7000
4 vhost_http_port = 8080
5 # 用于身份验证，请自行修改，要保证服务端与客户端一致
6 token = abcdefgh
```

启动 frps:

```
./frps -c ./frps.ini
```

修改 frpc.ini 文件，假设 frps 所在的服务器的 IP 为 x.x.x.x，local_port 为本地机器上 Web 服务对应的端口，绑定自定义域名 `www.yourdomain.com`:

```
1 # frpc.ini
2 [common]
3 server_addr = x.x.x.x
4 server_port = 7000
5 # 用于身份验证，请自行修改，要保证服务端与客户端一致
6 token = abcdefgh
7
8 [web]
9 type = http
10 local_port = 80
11 custom_domains = www.yourdomain.com
```

启动 frpc:

```
./frpc -c ./frpc.ini
```

将 `www.yourdomain.com` 的域名 A 记录解析到 IP `x.x.x.x`，如果服务器已经有对应的域名，也可以将 CNAME 记录解析到服务器原先的域名。

通过浏览器访问 `http://www.yourdomain.com:8080` 即可访问到处于内网机器上的 Web 服务。

4. 对外提供简单的文件访问服务

通过 `static_file` 插件可以对外提供一个简单的基于 HTTP 的文件访问服务。

frps 的部署步骤同上。

启动 frpc，启用 `static_file` 插件，配置如下：

```
1 # frpc.ini
2 [common]
3 server_addr = x.x.x.x
4 server_port = 7000
5 # 用于身份验证，请自行修改，要保证服务端与客户端一致
6 token = abcdefgh
7
8 [test_static_file]
9 type = tcp
10 remote_port = 6000
11 plugin = static_file
12 # 要对外暴露的文件目录
13 plugin_local_path = /tmp/file
14 # 访问 url 中会被去除的前缀，保留的内容即为要访问的文件路径
15 plugin_strip_prefix = static
16 plugin_http_user = abc
17 plugin_http_passwd = abc
```

通过浏览器访问 `http://x.x.x.x:6000/static/` 来查看位于 `/tmp/file` 目录下的文件，会要求输入已设置好的用户名和密码。

2.4 常用功能

1. 统计面板 (Dashboard)

通过浏览器查看 frp 的状态以及代理统计信息展示。

注：Dashboard 尚未针对大量的 proxy 数据展示做优化，如果出现 Dashboard 访问较慢的情况，请不要启用此功能。

需要在 frps.ini 中指定 dashboard 服务使用的端口，即可开启此功能：

```
1 [common]
2 dashboard_port = 7500
3 # dashboard 用户名密码，默认都为 admin
4 dashboard_user = admin
5 dashboard_pwd = admin
```

打开浏览器通过 `http://[server_addr]:7500` 访问 dashboard 界面，用户名密码默认为 `admin`。

2. 加密与压缩

这两个功能默认是不开启的，需要在 frpc.ini 中通过配置来为指定的代理启用加密与压缩的功能，压缩算法使用 snappy：

```
1 # frpc.ini
2 [ssh]
3 type = tcp
4 local_port = 22
5 remote_port = 6000
```

```
6 use_encryption = true
7 use_compression = true
```

如果公司内网防火墙对外网访问进行了流量识别与屏蔽，例如禁止了 SSH 协议等，通过设置 `use_encryption = true`，将 frpc 与 frps 之间的通信内容加密传输，将会有效防止流量被拦截。

如果传输的报文长度较长，通过设置 `use_compression = true` 对传输内容进行压缩，可以有效减小 frpc 与 frps 之间的网络流量，加快流量转发速度，但是会额外消耗一些 CPU 资源。

TLS

从 v0.25.0 版本开始 frpc 和 frps 之间支持通过 TLS 协议加密传输。通过在 `frpc.ini` 的 `common` 中配置 `tls_enable = true` 来启用此功能，安全性更高。

为了端口复用，frp 建立 TLS 连接的第一个字节为 0x17。

注意：启用此功能后除 `xtcp` 外，不需要再设置 `use_encryption`。

3. 代理限速

目前支持在客户端的代理配置中设置代理级别的限速，限制单个 proxy 可以占用的带宽。

```
1 # frpc.ini
2 [ssh]
3 type = tcp
4 local_port = 22
5 remote_port = 6000
6 bandwidth_limit = 1MB
```

在代理配置中增加 `bandwidth_limit` 字段启用此功能，目前仅支持 `MB` 和 `KB` 单位。

4. 范围端口映射

在 frpc 的配置文件中可以指定映射多个端口，目前只支持 tcp 和 udp 的类型。

这一功能通过 `range:` 段落标记来实现，客户端会解析这个标记中的配置，将其拆分成多个 proxy，每一个 proxy 以数字为后缀命名。

例如要映射本地 6000-6005, 6007 这 6 个端口，主要配置如下：

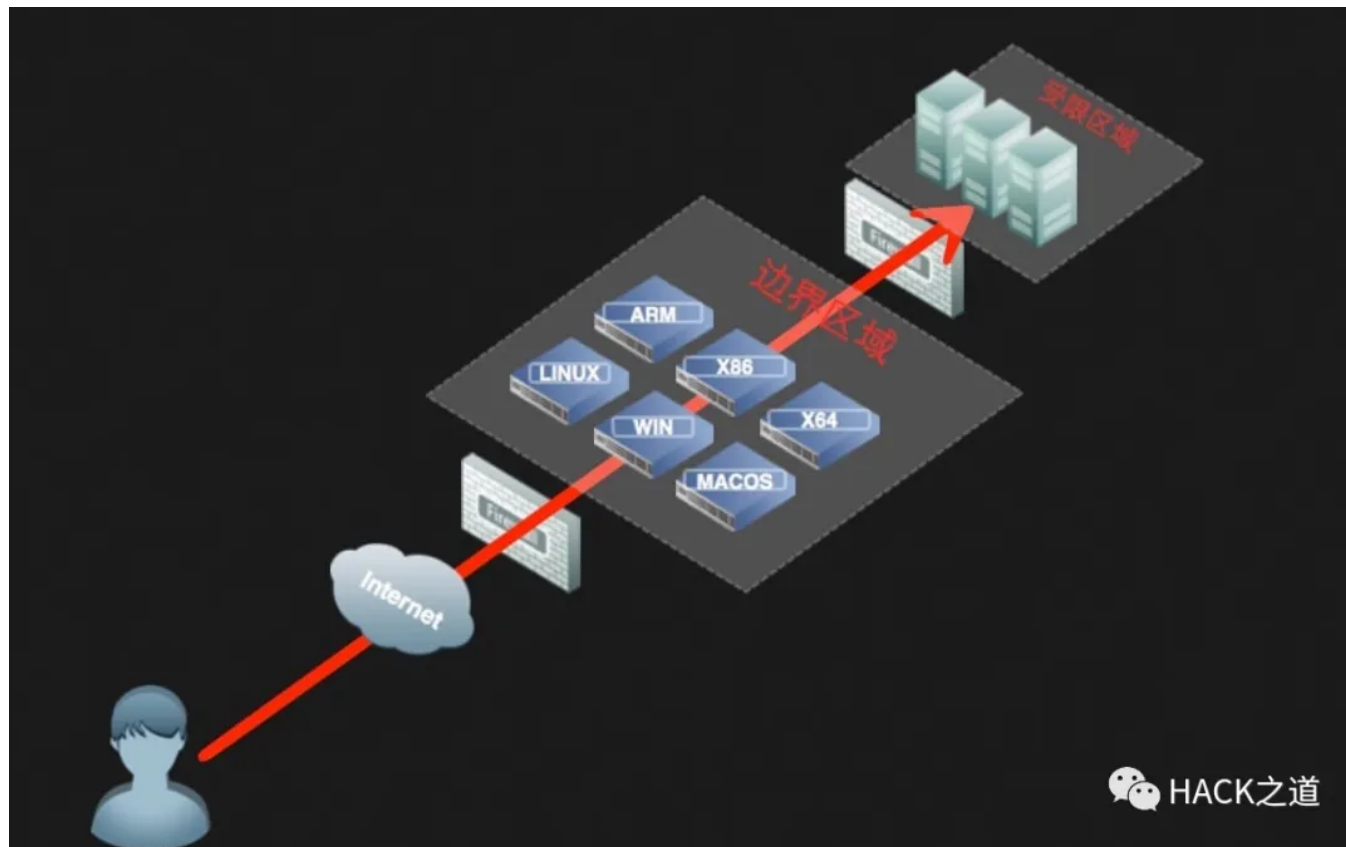
```
1 # frpc.ini
2 [range:test_tcp]
3 type = tcp
4 local_ip = 127.0.0.1
5 local_port = 6000-6006,6007
6 remote_port = 6000-6006,6007
```

实际连接成功后会创建 8 个 proxy，命名为 `test_tcp_0`, `test_tcp_1` ... `test_tcp_7`。

0x03 ew

3.1 简介

EW 是一套便携式的网络穿透工具，具有 SOCKS v5 服务架设和端口转发两大核心功能，可在复杂网络环境下完成网络穿透。但是，现在工具已经不更新了。。。



3.2 特点

- 轻量级，C语言编写
- 可以设置多级代理
- 跨平台
- 但是只支持Socks5代理

3.3 使用方法

以下使用方法均摘自：<http://rootkiter.com/EarthWorm/>

以下所有样例，如无特殊说明代理端口均为1080，服务均为SOCKSv5代理服务。

该工具共有 6 种命令格式 (ssocksd、rcsocks、rssocks、lcx_slave、lcx_listen、lcx_tran)。

1. 正向 SOCKS v5 服务器

```
1 $ ./ew -s ssocksd -l 1080
```

2. 反弹 SOCKS v5 服务器

这个操作具体分两步：

a) 先在一台具有公网 ip 的主机A上运行以下命令：

```
1 $ ./ew -s rcsocks -l 1080 -e 8888
```

b) 在目标主机B上启动 SOCKS v5 服务 并反弹到公网主机的 8888端口

```
1 $ ./ew -s rssocks -d 1.1.1.1 -e 8888
```

成功。

3. 多级级联

工具中自带的三条端口转发指令， 它们的参数格式分别为：

```
1 $ ./ew -s lcx_listen -l 1080 -e 8888
2 $ ./ew -s lcx_tran -l 1080 -f 2.2.2.3 -g 9999
3 $ ./ew -s lcx_slave -d 1.1.1.1 -e 8888 -f 2.2.2.3 -g 9999
```

通过这些端口转发指令可以将处于网络深层的基于TCP的服务转发至根前,比如 SOCKS v5。首先提供两个“二级级联”本地SOCKS测试样例:

a) `lcx_tran` 的用法

```
1 $ ./ew -s ssocksd -l 9999
2 $ ./ew -s lcx_tran -l 1080 -f 127.0.0.1 -g 9999
```

b) `lcx_listen`、`lcx_slave` 的用法

```
1 $ ./ew -s lcx_listen -l 1080 -e 8888
2 $ ./ew -s ssocksd -l 9999
3 $ ./ew -s lcx_slave -d 127.0.0.1 -e 8888 -f 127.0.0.1 -g 9999
```

再提供一个“三级级联”的本地SOCKS测试用例以供参考

```
1 $ ./ew -s rcsocks -l 1080 -e 8888
2 $ ./ew -s lcx_slave -d 127.0.0.1 -e 8888 -f 127.0.0.1 -g 9999
3 $ ./ew -s lcx_listen -l 9999 -e 7777
4 $ ./ew -s rssocks -d 127.0.0.1 -e 7777
```

数据流向: SOCKS v5 -> 1080 -> 8888 -> 9999 -> 7777 -> rssocks

0x04 ngrok

4.1 简介

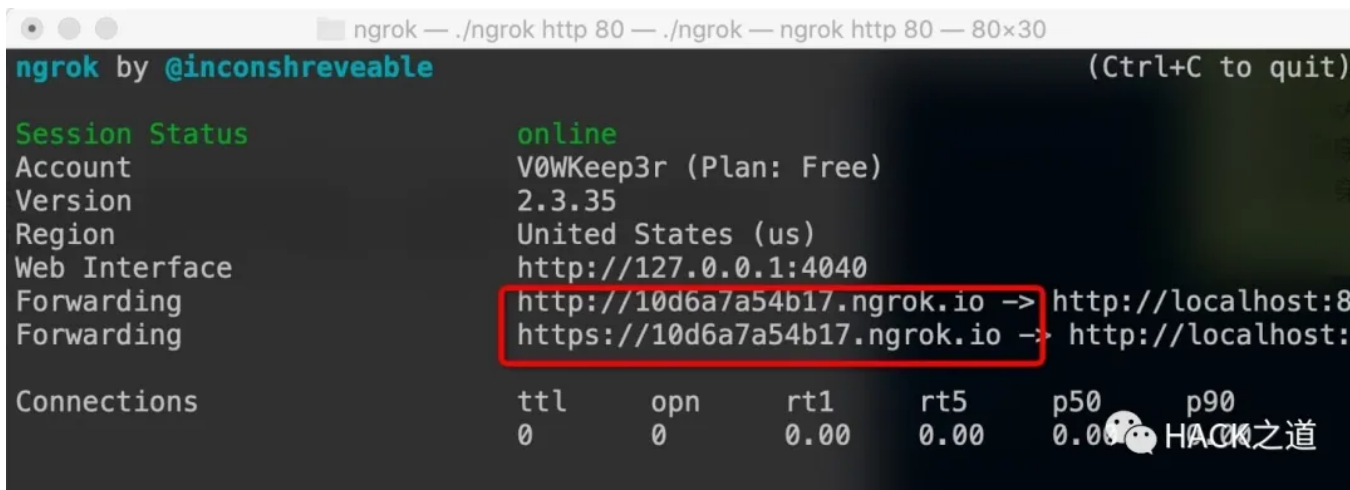
ngrok 是一个反向代理，通过在公共端点和本地运行的 Web 服务器之间建立一个安全的通道，实现内网主机的服务可以暴露给外网。ngrok 可捕获和分析所有通道上的流量，便于后期分析和重放，所以ngrok可以很方便地协助服务端程序测试。

4.2 特点

- 官方维护，一般较为稳定
- 跨平台，闭源
- 有流量记录和重发功能

4.3 使用方法

- 进入ngrok官网 (<https://ngrok.com/>)，注册ngrok账号并下载ngrok；
- 根据官网给定的授权码，运行如下授权命令；
- `./ngrok authtoken 1hAotxhm0RtzCYvUc3BsxDBPh1H_*****`
- `./ngrok http 80` 即可将机器的80端口http服务暴露到公网，并且会提供一个公网域名。



```
ngrok — ./ngrok http 80 — ./ngrok — ngrok http 80 — 80x30
ngrok by @inconshreveable (Ctrl+C to quit)

Session Status      online
Account             V0WKeep3r (Plan: Free)
Version             2.3.35
Region              United States (us)
Web Interface        http://127.0.0.1:4040
Forwarding           http://10d6a7a54b17.ngrok.io -> http://localhost:8
Forwarding           https://10d6a7a54b17.ngrok.io -> http://localhost:

Connections         ttl    opn    rt1    rt5    p50    p90
                   0      0      0.00   0.00   0.00   0.00
```

可以通过官网的UI界面查看数据包和流量等等（但是要付费 ==、）

Clear

200 OK	26.58ms
200 OK	4.05ms
404 NOT FOUND	25.77ms
200 OK	33.18ms

5 minutes ago

🕒 Duration 26.58ms

👤 IP 192

GET /headers


Summary Headers Raw Binary

200 OK

Summary Headers Raw Binary

```
HTTP/1.1 200 OK
Server: gunicorn/18.0
Date: Tue, 16 Dec 2014 07:10:56 GMT
Connection: close
Content-Type: application/json
Content-Length: 620
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true

{
  "headers": {
```

 HACK之道

还可以通过一些命令将内网的文件和其他TCP服务 暴露到公网中。

有授权的设置文件共享

```
1 ngrok http -auth="user:password" file:///Users/alan/share
```

无授权的设置文件共享

```
1 ngrok http "file:///C:\Users\alan\Public Folder"
```

将主机的3389的TCP端口暴露到公网

```
1 ngrok tcp 3389
```

更多使用方法参考：<https://ngrok.com/docs>

0xFF 参考链接

内网渗透之内网穿透

-<https://xz.aliyun.com/t/7701>

开源内网穿透工具 frp 简单使用教程

-<https://segmentfault.com/a/1190000021876836>

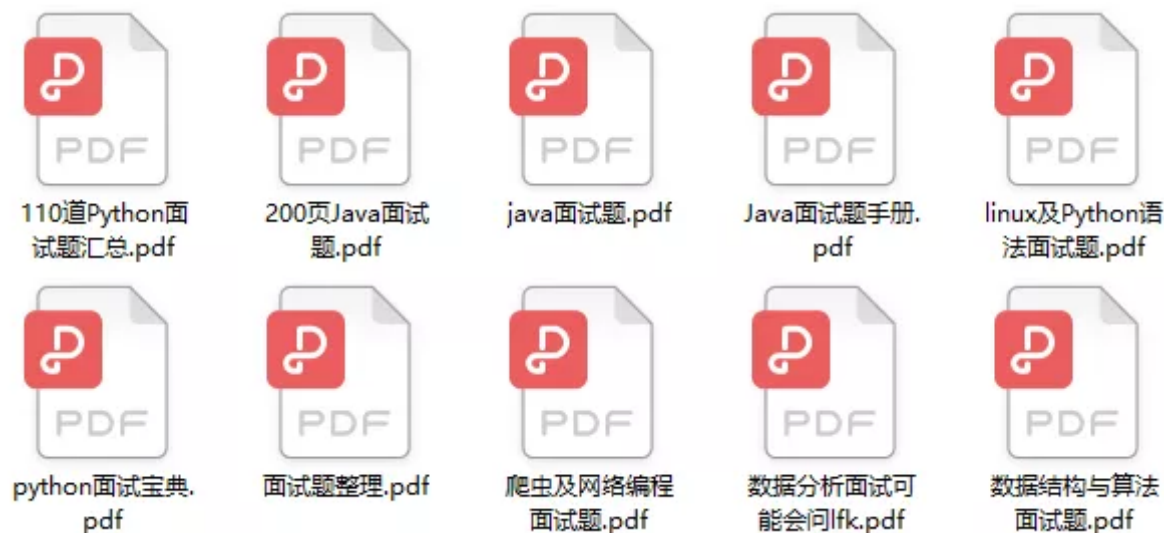
<http://rootkiter.com/EarthWorm/>

文章作者:: V0WKeep3r

文章鏈接:: <http://v0w.top/2020/08/11/IntranetProxy/>

-End-

最近有一些小伙伴，讓我幫忙找一些 面試題 資料，於是我翻遍了收藏的5T 資料後，匯總整理出來，可以說是程序員面試必備！所有資料都整理到網盤了，歡迎下載！



程序員直聘

程序員直聘，一個程序員找工作平台。

21篇原創內容



公眾號

點擊👉卡片，關注後回復【面試題

在看點這裡

[閱讀原文](#)

喜歡此內容的人還喜歡

知乎高讚：從源碼層，拆解OracleJDK和OpenJDK有什麼區別？ 網友：不愧是大神的回答~

朱小廝的博客



如何遠程登錄開發板？

嵌入式資訊精選

