推薦幾款實用的內網穿透工具

Java後端 Java後端 2022-01-25 14:43

收錄於話題
#內網穿透

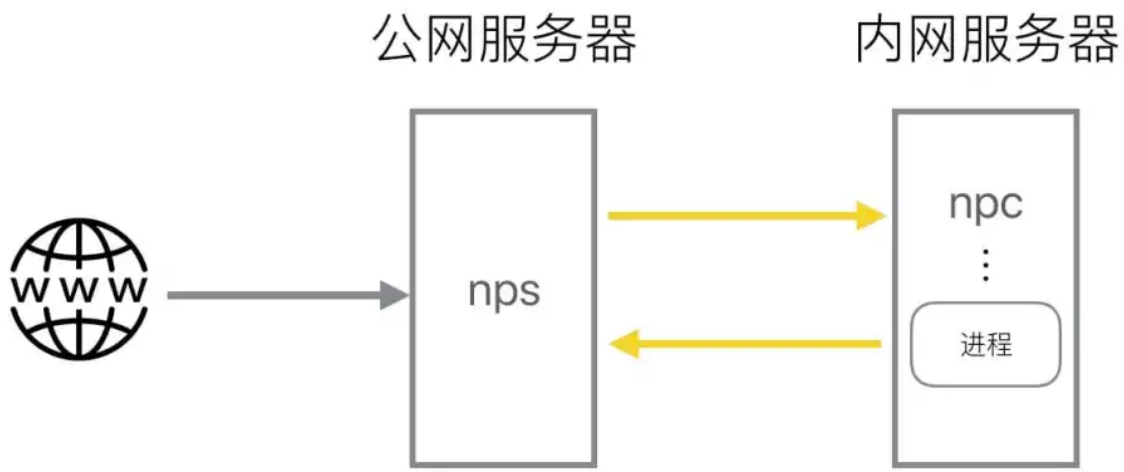
2個

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。

1.1 簡介

> nps是一款輕量級、高性能、功能強大的內網穿透代理服務器。目前支持tcp、udp流量轉發，可支持任何tcp、udp上層協議（訪問內網網站、本地支付接口調試、ssh訪問、遠程桌面，內網dns解析等等……），此外還支持內網http代理、內網socks5代理、p2p等，並帶有功能強大的web管理端。

- 一台有公網IP的服務器（VPS）運行服務端（NPS）
- 一個或多個運行在內網的服務器或者PC運行客戶端（NPC）



1.2 特點

1. Go語言編寫

2. 支持跨平台

3. 支持多種協議的代理

4. 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：

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

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

需要改一下#web下面的幾個參數，

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

修改#bridge 可以更改NPC的連接端口。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
bridge_type=tcp
bridge_port=443  # 修改连接端口
bridge_ip=0.0.0.0
```

啟動

```
#Mac/Linux
./nps test|start|stop|restart|status 测试配置文件|启动|停止|重启|状态

#Windows
nps.exe test|start|stop|restart|status 测试配置文件|启动|停止|重启|状态
```

NPC

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

新建好客戶端后，也可以在+中看到，詳細的客戶端連接命令：

web管理端

在客戶端界面可以通過新增的方式添加客戶端連接，每一個連接的vkey都是唯一區分的。

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。

	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	

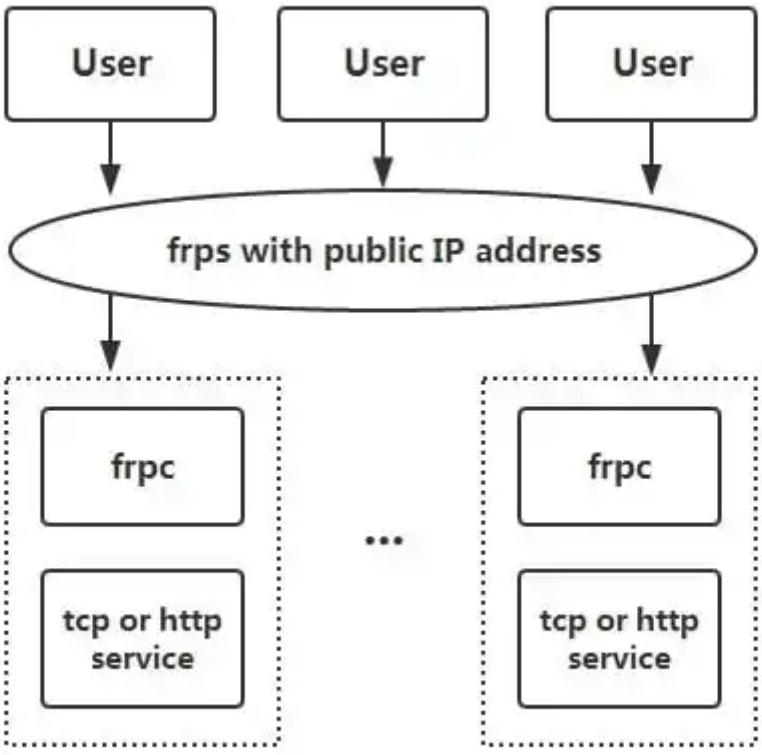
显示第 1 到第 2 条记录，总共 2 条记录

通過不同的協議和端口就可以連接代理的內網機器。

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. 通過rdp 訪問家裡的機器

1.修改frps.ini 文件，為了安全起見，這裡最好配置一下身份驗證，服務端和客戶端的common 配置中的 token 參數一致則身份驗證通過：

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

2. 啟動frps：

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

3. 修改frpc.ini 文件，假設frps 所在服務器的公網IP 為xxxx：

```
# frpc.ini
[common]
server_addr = x.x.x.x
server_port = 7000
# 用于身份验证，请自行修改，要保证服务端与客户端一致
token = abcdefgh

[rdp]
type = tcp
local_ip = 127.0.0.1
```

```
local_port = 3389
remote_port = 6000
```

4. 啟動frpc：

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

5.通過rdp 訪問遠程的機器，地址為：

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

開機自啟

針對Windows 系統，為了便於使用，可以配置一下開機的時候靜默啟動。

1.在frpc.exe 的同級目錄創建一個start_frpc.vbs：

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

2.複製start_frpc.vbs 文件，打開以下目錄，注意將

```
<USER_NAME>
```

改為你的用戶名：

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

3.鼠標右擊，粘貼為快捷方式即可。

2. 通過SSH 訪問公司內網機器

frps 的部署步驟同上。

1.啟動frpc，配置如下：

```
# frpc.ini
[common]
server_addr = x.x.x.x
server_port = 7000
# 用于身份验证，请自行修改，要保证服务端与客户端一致
token = abcdefgh

[ssh]
type = tcp
local_ip = 127.0.0.1
local_port = 22
remote_port = 6000
```

2.通過SSH 訪問內網機器，假設用戶名為test：

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

3. 通過自定義域名訪問部署於內網的Web 服務

有時想要讓其他人通過域名訪問或者測試我們在本地搭建的Web 服務，但是由於本地機器沒有公網IP，無法將域名解析到本地的機器，通過frp 就可以實現這一功能，以下示例為http 服務，https 服務配置方法相同， vhost_http_port 替換為vhost_https_port， type 設置為https 即可。

1.修改frps.ini 文件，設置http 訪問端口為8080：

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

2.啟動frps：

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

3.修改frpc.ini 文件，假設frps 所在的服務器的IP 為xxxx，local_port 為本地機器上Web 服務對應的端口， 綁定自定義域名 www.yourdomain.com:

```
# frpc.ini
[common]
server_addr = x.x.x.x
server_port = 7000
# 用于身份验证，请自行修改，要保证服务端与客户端一致
token = abcdefgh

[web]
type = http
local_port = 80
custom_domains = www.yourdomain.com
```

4.啟動frpc:

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

5.將 www.yourdomain.com 的域名A 記錄解析到IP x.x.x.x，如果服務器已經有對應的域名，也可以將CNAME 記錄解析到服務器原先的域名。

6.通過瀏覽器訪問 http://www.yourdomain.com:8080 即可訪問到處於內網機器上的Web 服務。

4. 對外提供簡單的文件訪問服務

通過 static_file 插件可以對外提供一個簡單的基於HTTP 的文件訪問服務。

frps 的部署步驟同上。

1.啟動frpc，啟用 static_file 插件，配置如下:

```
# frpc.ini
[common]
server_addr = x.x.x.x
server_port = 7000
```

```
# 用于身份验证，请自行修改，要保证服务端与客户端一致
token = abcdefgh

[test_static_file]
type = tcp
remote_port = 6000
plugin = static_file
# 要对外暴露的文件目录
plugin_local_path = /tmp/file
# 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
plugin_strip_prefix = static
plugin_http_user = abc
plugin_http_passwd = abc
```

2.通過瀏覽器訪問 `http://x.x.x.x:6000/static/` 來查看位於 `/tmp/file` 目錄下的文件，會要求輸入已設置好的用戶名和密碼。

常用功能

統計面板（Dashboard）

通過瀏覽器查看frp 的狀態以及代理統計信息展示。

注：Dashboard 尚未針對大量的proxy 數據展示做優化，如果出現Dashboard 訪問較慢的情況，請不要啟用此功能。

需要在frps.ini 中指定dashboard 服務使用的端口，即可開啟此功能：

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

打開瀏覽器通過 `http://[server_addr]:7500` 訪問dashboard 界面，用戶名密碼默認為 `admin`。

加密與壓縮

這兩個功能默認是不開啟的，需要在frpc.ini 中通過配置來為指定的代理啟用加密與壓縮的功能，壓縮算法使用snappy：

```
# frpc.ini
[ssh]
type = tcp
local_port = 22
remote_port = 6000
use_encryption = true
use_compression = true
```

如果公司內網防火牆對外網訪問進行了流量識別與屏蔽，例如禁止了SSH 協議等，通過設置 use_encryption = true，將frpc 與frps 之間的通信內容加密傳輸，將會有效防止流量被攔截。

如果傳輸的報文長度較長，通過設置 use_compression = true 對傳輸內容進行壓縮，可以有效減小frpc 與frps 之間的網絡流量，加快流量轉發速度，但是會額外消耗一些CPU 資源。

[TLS

從v0.25.0 版本開始frpc 和frps 之間支持通過TLS 協議加密傳輸。通過在 frpc.ini 的 common 中配置 tls_enable = true 來啟用此功能，安全性更高。

為了端口復用，frp 建立TLS 連接的第一個字節為0x17。

注意：啟用此功能後除xtcp 外，不需要再設置use_encryption。

代理限速

目前支持在客戶端的代理配置中設置代理級別的限速，限制單個proxy 可以佔用的帶寬。

```
# frpc.ini
[ssh]
type = tcp
local_port = 22
```

```
remote_port = 6000
bandwidth_limit = 1MB
```

在代理配置中增加 bandwidth_limit 字段啟用此功能，目前僅支持 MB 和 KB 單位。

範圍端口映射

在frpc 的配置文件中可以指定映射多個端口，目前只支持tcp 和udp 的類型。

這一功能通過 range：段落標記來實現，客戶端會解析這個標記中的配置，將其拆分成多個proxy，每一個proxy 以數字為後綴命名。

例如要映射本地6000-6005, 6007 這6 個端口，主要配置如下：

```
# frpc.ini
[range:test_tcp]
type = tcp
local_ip = 127.0.0.1
local_port = 6000-6006,6007
remote_port = 6000-6006,6007
```

實際連接成功後會創建8 個proxy，命名為 test_tcp_0, test_tcp_1 ... test_tcp_7。

ew

3.1 簡介

> EW 是一套便攜式的網絡穿透工具，具有SOCKS v5服務架設和端口轉發兩大核心功能，可在復雜網絡環境下完成網絡穿透。但是，現在工具已經不更新了。。。

特點

1. 輕量級，C語言編寫

2. 可以設置多級代理

3. 跨平台

4. 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/

以下所有樣例，如無特殊說明代理端口均為1080，服務均為SOCKSv5代理服務.

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

1. 正向SOCKS v5 服務器

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

2. 反彈SOCKS v5 服務器

這個操作具體分兩步：

a) 先在一台具有公網ip 的主機A上運行以下命令：

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

b) 在目標主機B上啟動SOCKS v5 服務並反彈到公網主機的8888端口

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

成功。

3. 多級級聯

工具中自帶的三條端口轉髮指令， 它們的參數格式分別為：

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

通過這些端口轉髮指令可以將處於網絡深層的基於TCP的服務轉發至根前,比如SOCKS v5。首先提供兩個“二級級聯”本地SOCKS測試樣例：

a) `lcx_tran` 的用法

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

b) `lcx_listen`、`lcx_slave` 的用法

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

再提供一個“三級級聯”的本地SOCKS測試用例以供參考

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

數據流向: `SOCKS v5 -> 1080 -> 8888 -> 9999 -> 7777 -> rssocks`

ngrok

4.1 簡介

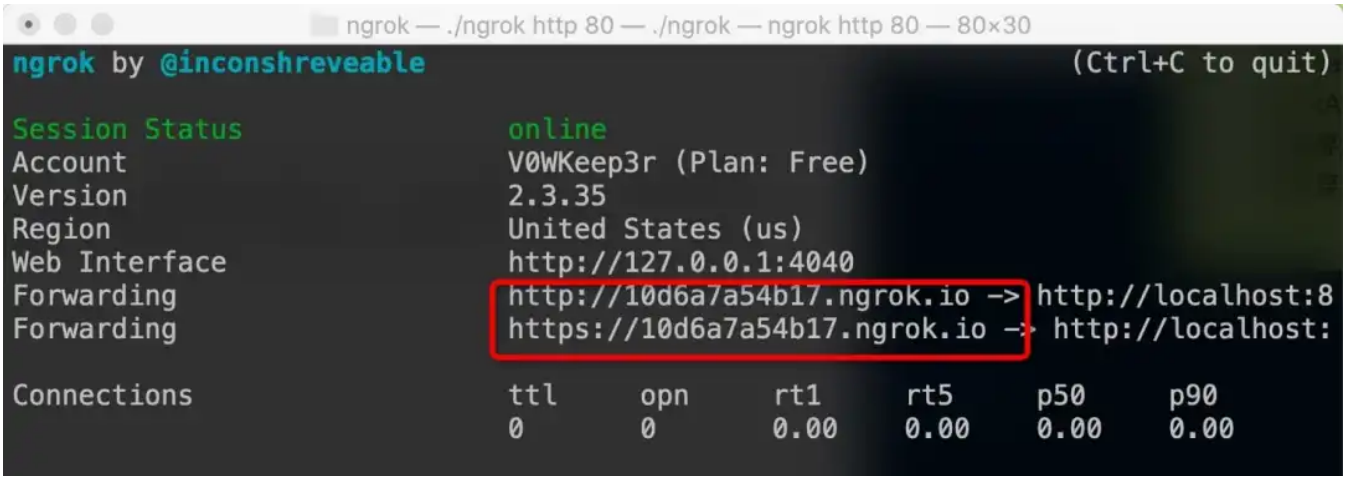
> ngrok 是一個反向代理，通過在公共端點和本地運行的Web 服務器之間建立一個安全的通道，實現內網主機的服務可以暴露給外網。ngrok 可捕獲和分析所有通道上的流量，便於後期分析和重放，所以ngrok可以很方便地協助服務端程序測試。

4.2 特點

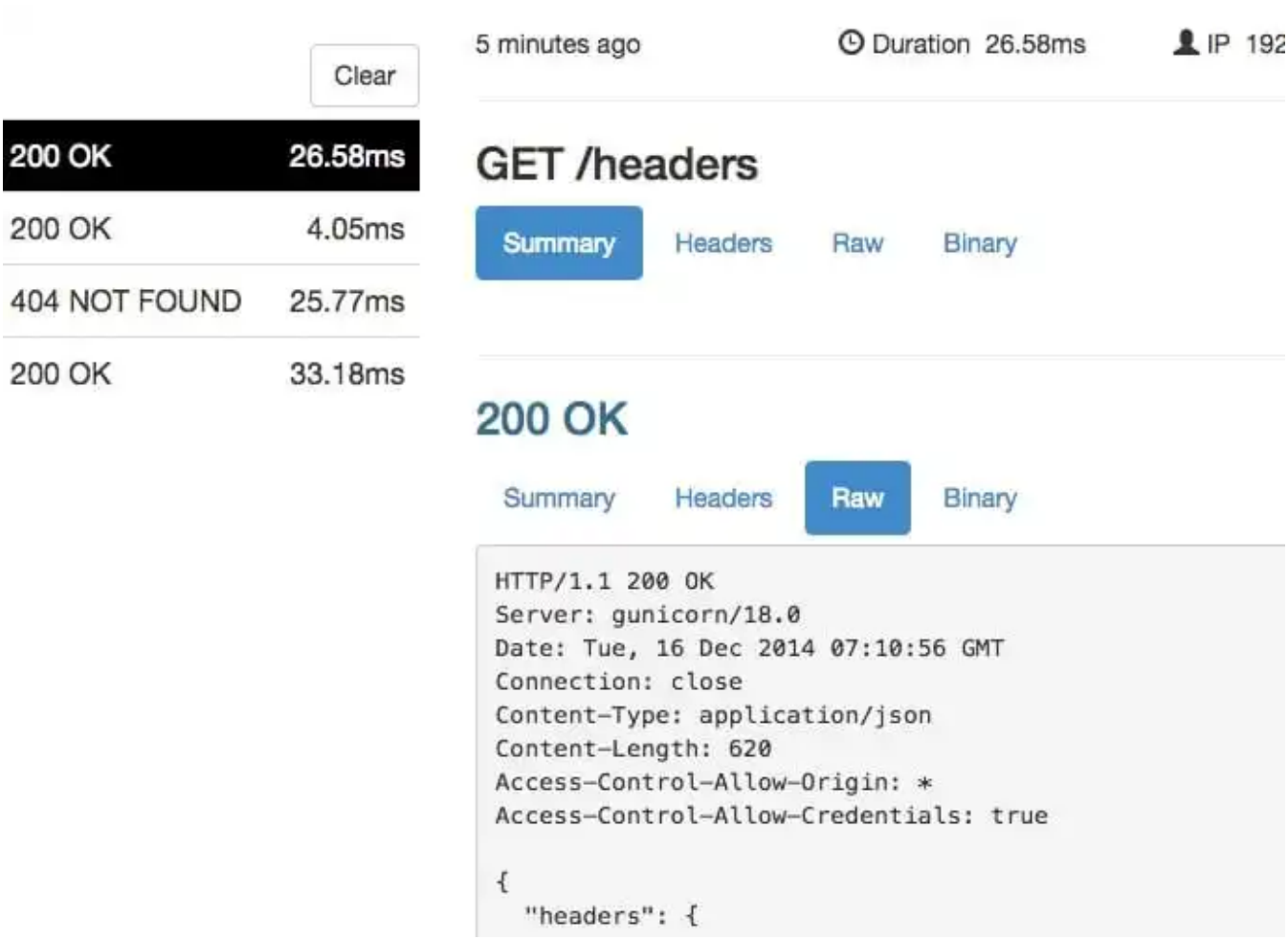
1. 官方維護，一般較為穩定
2. 跨平台，閉源
3. 有流量記錄和重發功能

4.3 使用方法

1. 進入ngrok官網（https://ngrok.com/），註冊ngrok賬號並下載ngrok；
2. 根據官網給定的授權碼，運行如下授權命令；
3. `./ngrok authtoken 1hAotxhmORtzCYvUc3BsxDBPh1H_******************`
4. `./ngrok http 80`即可將機器的80端口http服務暴露到公網，並且會提供一個公網域名。



可以通過官網的UI界面查看數據包和流量等等（但是要付費==、）



還可以通過一些命令將內網的文件和其他TCP服務暴露到公網中。

有授權的設置文件共享

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

無授權的設置文件共享

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

將主機的3389的TCP端口暴露到公網

```
ngrok tcp 3389
```

更多使用方法參考：https://ngrok.com/docs

參考鏈接

1. 內網滲透之內網穿透

2. 開源內網穿透工具frp 簡單使用教程

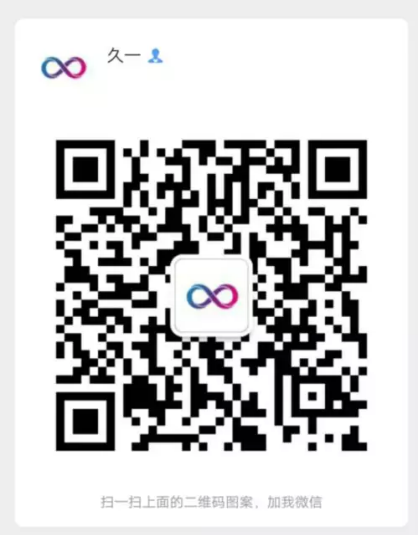
3. http://rootkiter.com/EarthWorm/

來源：v0w.top/2020/08/11/IntranetProxy

【END】

如果看到這裡，說明你喜歡這篇文章，請**轉發、點贊**。微信搜索「web_resource」，關注後回复「進群」或者掃描下方二維碼即可進入無廣告交流群。

↓掃描二維碼進群↓



閱讀原文