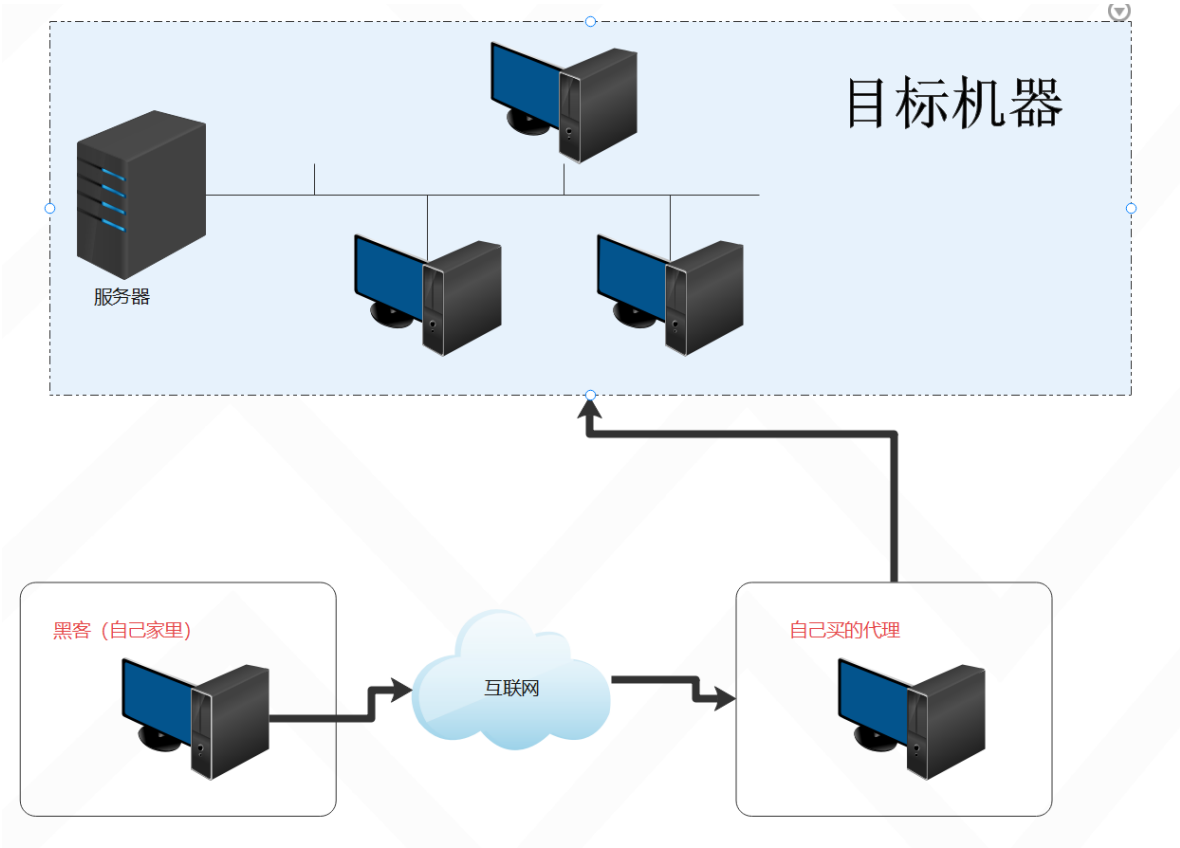


公网资产扫描-单代理配置

单代理介绍

平时在做渗透测试中我们需要对公网的资产进行扫描和探测，但是又害怕对方封掉你的IP地址，或者IP已经封了我们需要挂代理



单个代理

单个代理表示就一个IP代理机器，IP地址不会自动切换

IP	PORT	匿名度	类型	位置	响应速度	最后验证时间	付费方式
114.231.107.59	8888	高匿名	HTTP	中国 江苏 南通 电信	0.2秒	2023-07-06 14:31:01	免费代理ip
61.216.156.222	60808	高匿名	HTTP	中国 台湾 cht.com.tw	4秒	2023-07-06 13:31:01	免费代理ip
183.236.232.160	8080	高匿名	HTTP	中国 广东 江门 移动	6秒	2023-07-06 12:31:01	免费代理ip
114.231.46.123	8888	高匿名	HTTP	中国 江苏 南通 电信	0.3秒	2023-07-06 11:31:01	免费代理ip
183.64.239.19	8060	高匿名	HTTP	重庆市重庆市 电信	0.5秒	2023-07-06 10:31:01	免费代理ip
112.14.47.6	52024	高匿名	HTTP	浙江省宁波市 移动	8秒	2023-07-06 09:31:01	免费代理ip
183.247.211.41	30001	高匿名	HTTP	中国 浙江 台州 移动	4秒	2023-07-06 08:31:01	免费代理ip
60.170.204.30	8060	高匿名	HTTP	中国 安徽 蚌埠 电信	1秒	2023-07-06 07:31:01	免费代理ip
61.216.185.88	60808	高匿名	HTTP	中国 台湾 屏东县	0.7秒	2023-07-06 06:31:01	免费代理ip
222.74.73.202	42055	高匿名	HTTP	内蒙古自治区赤峰市 电信	1秒	2023-07-06 05:31:01	免费代理ip
183.236.123.242	8060	高匿名	HTTP	中国 广东 佛山 移动	0.4秒	2023-07-06 04:31:01	免费代理ip
112.244.148.228	9000	高匿名	HTTP	山东省潍坊市 联通	0.2秒	2023-07-06 03:31:01	免费代理ip

单个代理一般大家都用的免费的，这里告诉大家一个很残酷的事实

一般免费的这种单个代理有以下的弊端

- 1、使用人比较多网速比较慢，很多都用不了
- 2、有可能这些代理是有些公司主动放出的用来收集用户信息

筛选代理

1、购买或者使用免费的单个代理IP

网站：<https://www.kuaidaili.com>

快代理提供了免费的单个代理IP,也可以花钱购买自己独有的IP

购买独享代理

产品选择

隧道代理

私密代理

独享代理

独享类型

☐ IP共享型

☒ IP独享型

完全独享所购买的IP、并发量和带宽，更专业的选择

选择带宽

☒ 1Mb/s

☐ 2Mb/s

☐ 4Mb/s

☐ 6Mb/s 新

☐ 10Mb/s 新

选择城市

随机分配

▼

随机分配会排除一线城市

购买IP量

1

—

1

个

+

授权IP白名单

300 个 ⓘ

下单备注

选填，100字以内

购买时长

1天

1周

1个月

3个月

半年

1年 8.6折

其他时长

有效期至：2023-08-06 17:09:08

价格

180.00元

144.00元

8折优惠

提交订单

产品规格

- 完全独享所购买的IP
- IP固定，长期有效
- 高品质IP，极速响应
- 高匿名；支持HTTP/HTTPS/Socks5
- 选择城市：**随机分配**
- 购买IP量：**1个**
- 带宽：**1Mb/s**
- 并发请求量：**1000次/s**
- 授权IP白名单：**300个**
- 若所选产品规格无法满足您的需求，
请[联系客服](#)进行专属定制

免费的有很多，百度搜索下

- 2、将IP地址整理然后进行测试，看一下那个可以用
- 可以使用代理检测工具检测一下

<http://www.leishenhttp.com/index/check/index.html>

<https://www.zdaye.com/ip/CheckHttp/>

IP地址	端口	匿名等级	地理位置	https	post	响应时间
112.14.47.6	52024		浙江省温州市 移动			
183.247.211.41	30001	普匿	浙江省台州市 移动			62
60.170.204.30	8060		安徽省蚌埠市 电信			
222.74.73.202	42055	待验证	内蒙古赤峰市 电信	待验证	待验证	待验证
183.236.123.242	8060	待验证	广东省广州市 移动	待验证	待验证	待验证
112.244.148.228	9000	待验证	山东省潍坊市 联通	待验证	待验证	待验证

导出有效代理IP

使用代理

1、浏览器

设置

界面

通用

导入/导出

情景模式

HTTP代理

burp

burp1

proxy

auto switch

新建情景模式...

ACTIONS

应用选项

代理服务器

网址协议	代理协议	代理服务器	代理端口	
(默认)	HTTP	60.170.204.30	8060	

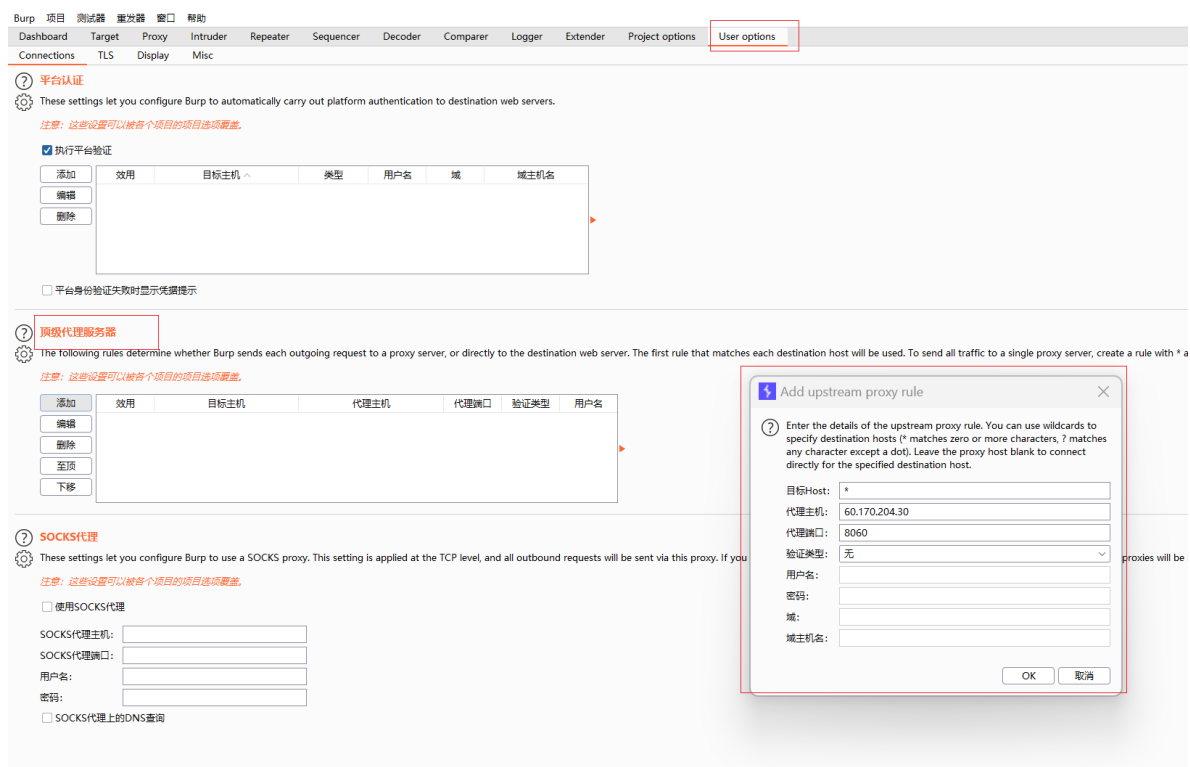
显示高级设置

不代理的地址列表

不经过代理连接的主机列表: (每行一个主机)

(可使用通配符等匹配规则...)

2、burp



3、工具有些扫描工具是支持代理的可以查看工具的具体命令看看用法

Connection Settings:

```
--timeout=TIMEOUT    Connection timeout
--delay=DELAY         Delay between requests
-p PROXY, --proxy=PROXY
                     Proxy URL (HTTP/SOCKS), can use multiple flags
--proxies-file=PATH
                     File contains proxy servers
--proxy-auth=CREDENTIAL
                     Proxy authentication credential
--replay-proxy=PROXY
                     Proxy to replay with found paths
--tor
                     Use Tor network as proxy
--scheme=SCHEME
                     Scheme for raw request or if there is no scheme in the
                     URL (Default: auto-detect)
--max-rate=RATE
                     Max requests per second
--retries=RETRIES
                     Number of retries for failed requests
--ip=IP
                     Server IP address
```