应用层代理

应用层代理介绍

应用层代理是我们最常用的代理，平时在进行内网渗透，或者扫描的时候经常需要这个代理，根据协议不同大体有以下的分类

1、http代理

2、socks代理

3、SSH代理

4、DNS代理

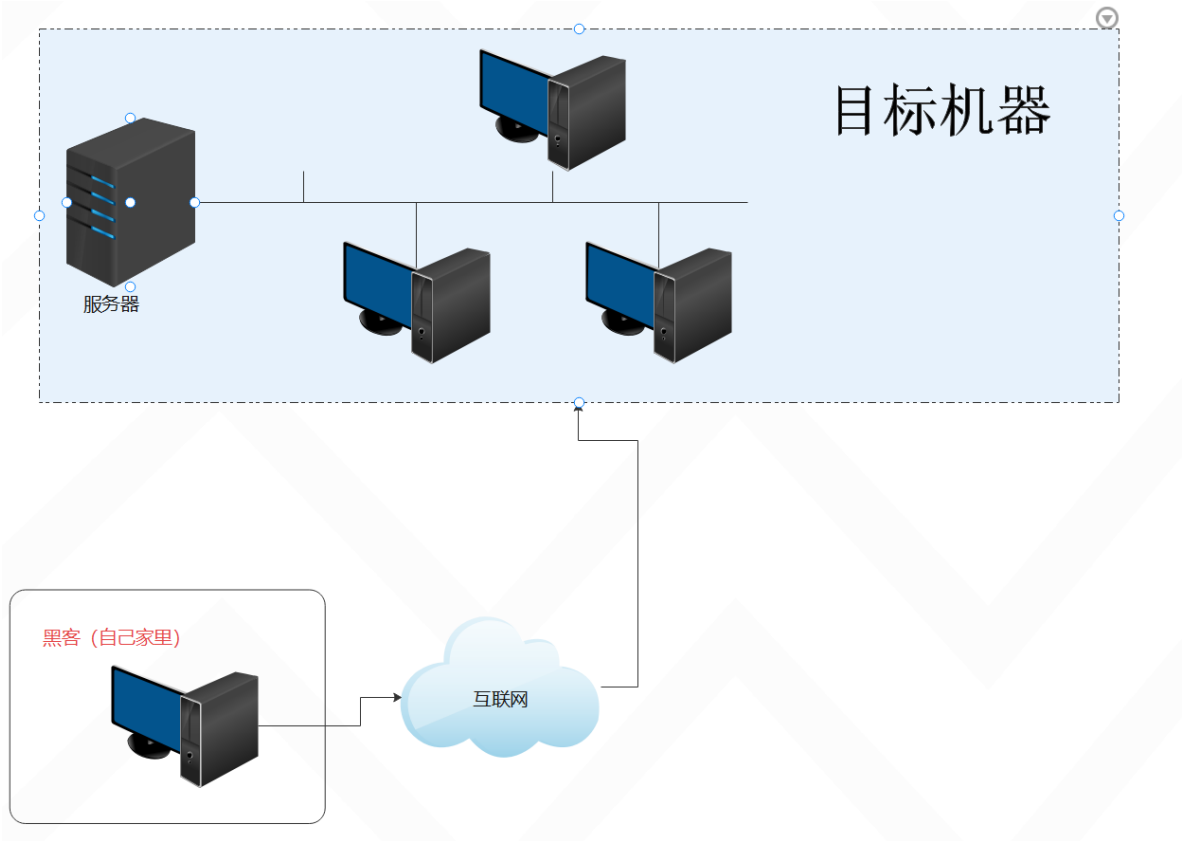
5、还有自定义的一些协议和加密规则（强烈谴责，正经人谁用这些，都是目的不纯）这个技术我们不讨论

每种代理应用的场景不同，在不同的场景需要选择不同的代理，接下来我们看一下需要代理的场景

代理场景介绍

一、公网资产扫描

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，我们需要挂代理



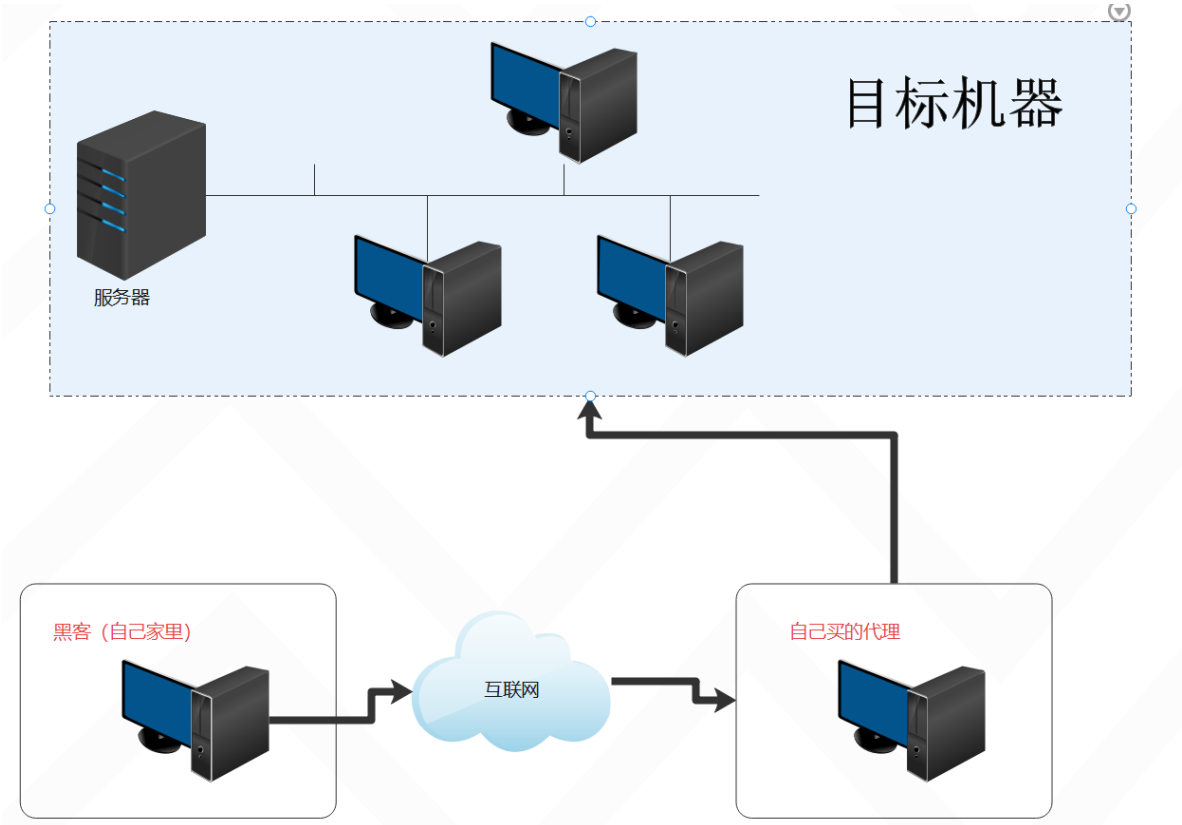
在这种情况我我们需要哪些东西走代理呢?

1、扫描器工具

2、浏览器

3、burpsuite

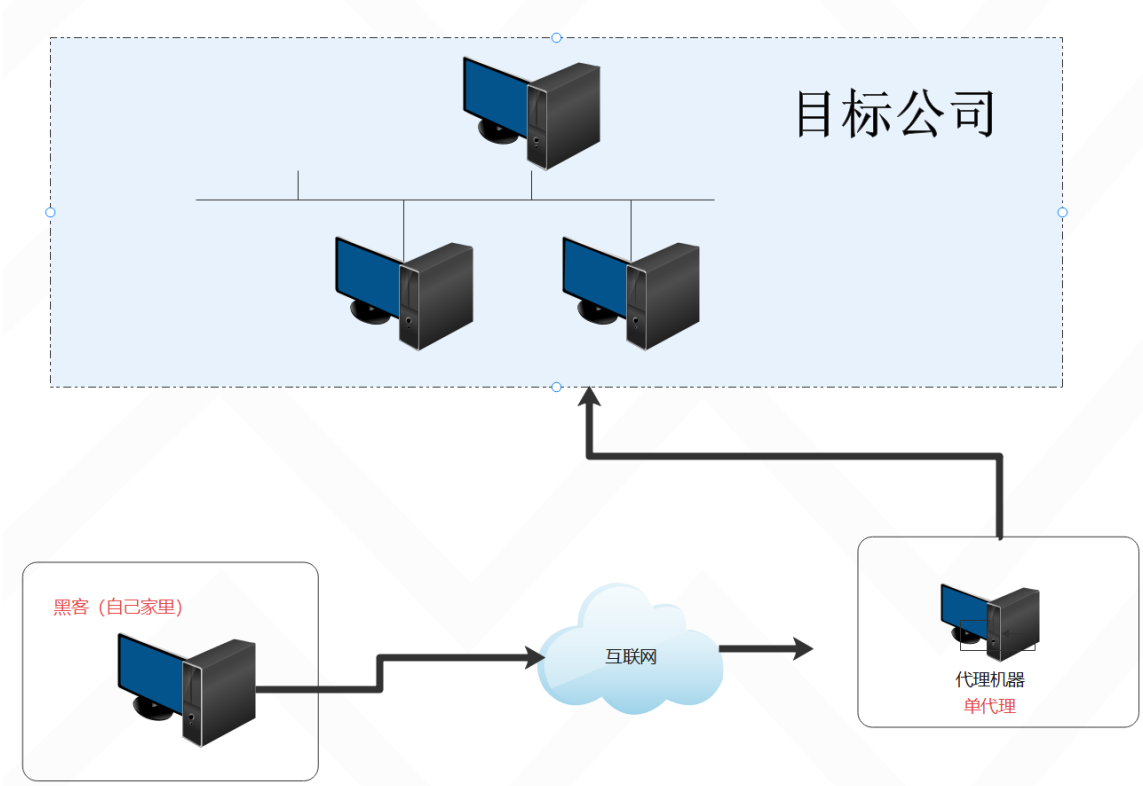
使用代理一般是用http代理或者socks代理代理后的拓扑如下



这里的代理分为两类

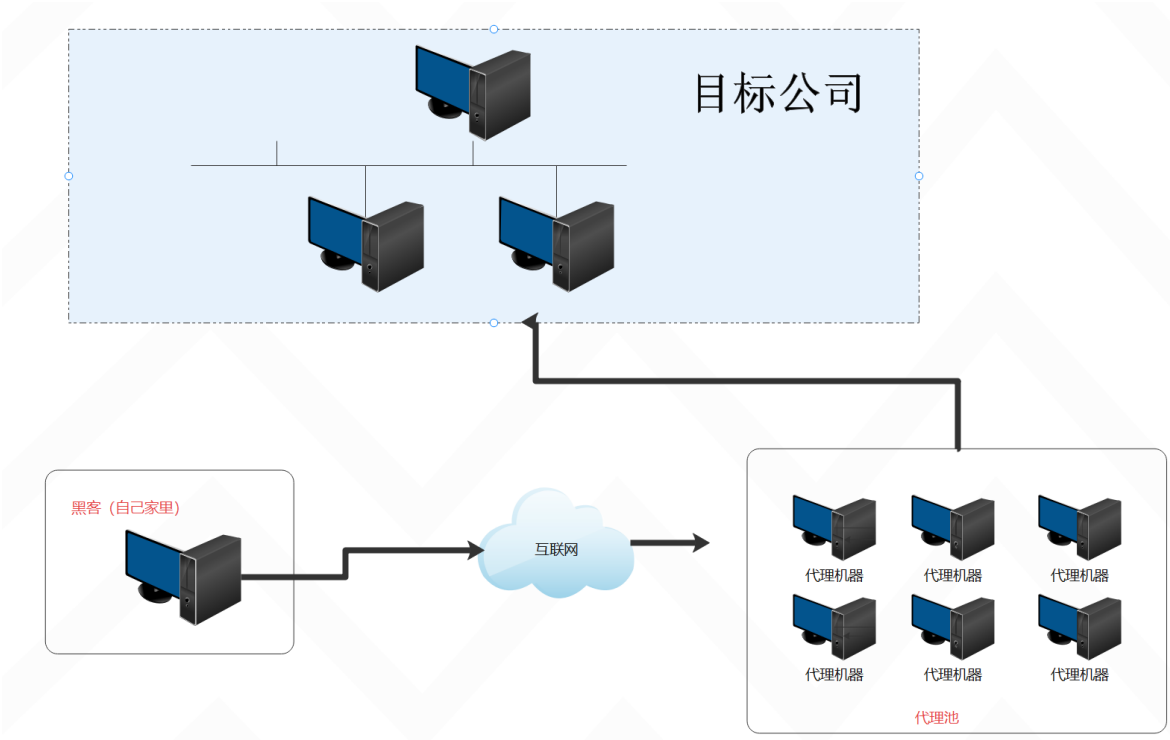
1、单个代理

单代理就是一个代理机器，只有一个IP，不会自动切换



2、代理池

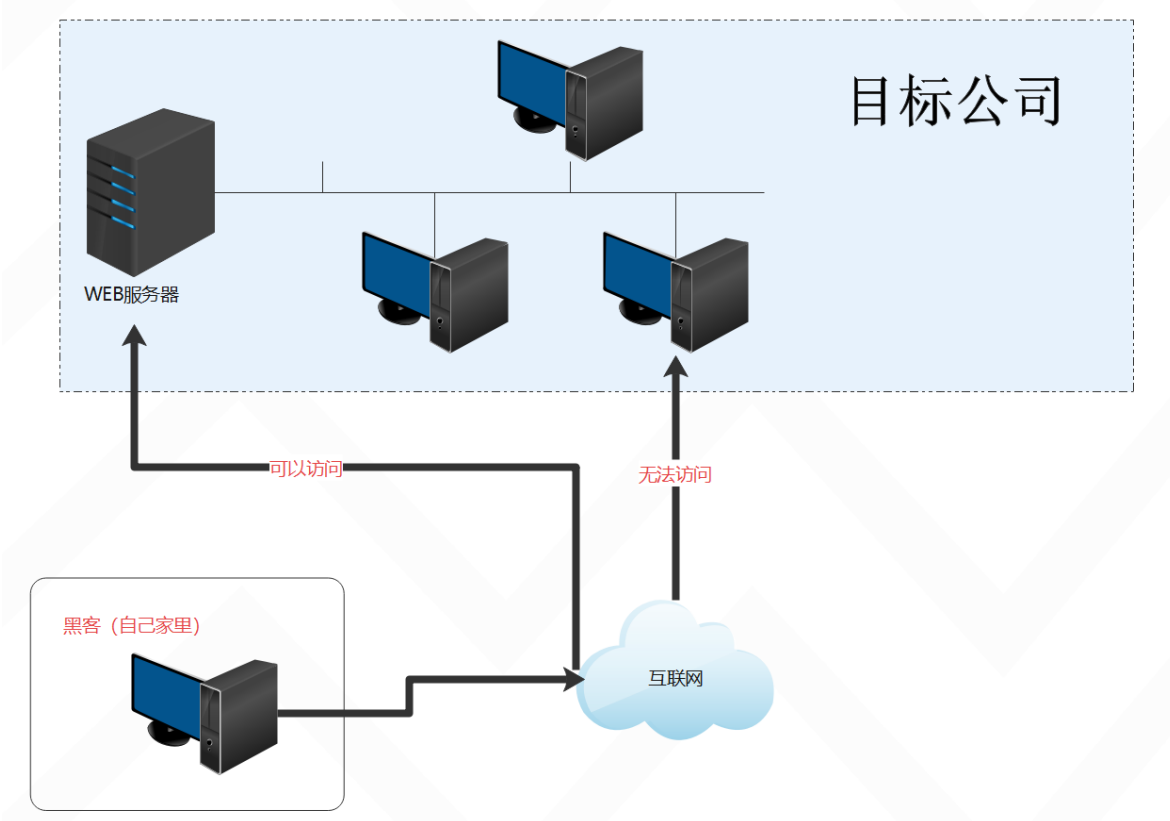
代理池就是一推IP地址，可以实现自动变化，每次请求都变化



注意：有些工具支持可以将单个代理IP写到文本中，从而实现代理池的功能

二、内网资产扫描

内网资产扫描这种场景一般是进行内网渗透才需要的代理技术，如果你不打内网一般是不需要这种技术的，内网代理技术一般也是采用http或者socks代理



针对以上的情况我们需要如何对内网进行扫描呢?

1、直接使用web服务进行扫描（这种方式请看内网渗透）

2、做代理让web服务成为代理机器

针对于内网的机器要考虑是用代理隧道还是使用端口转发

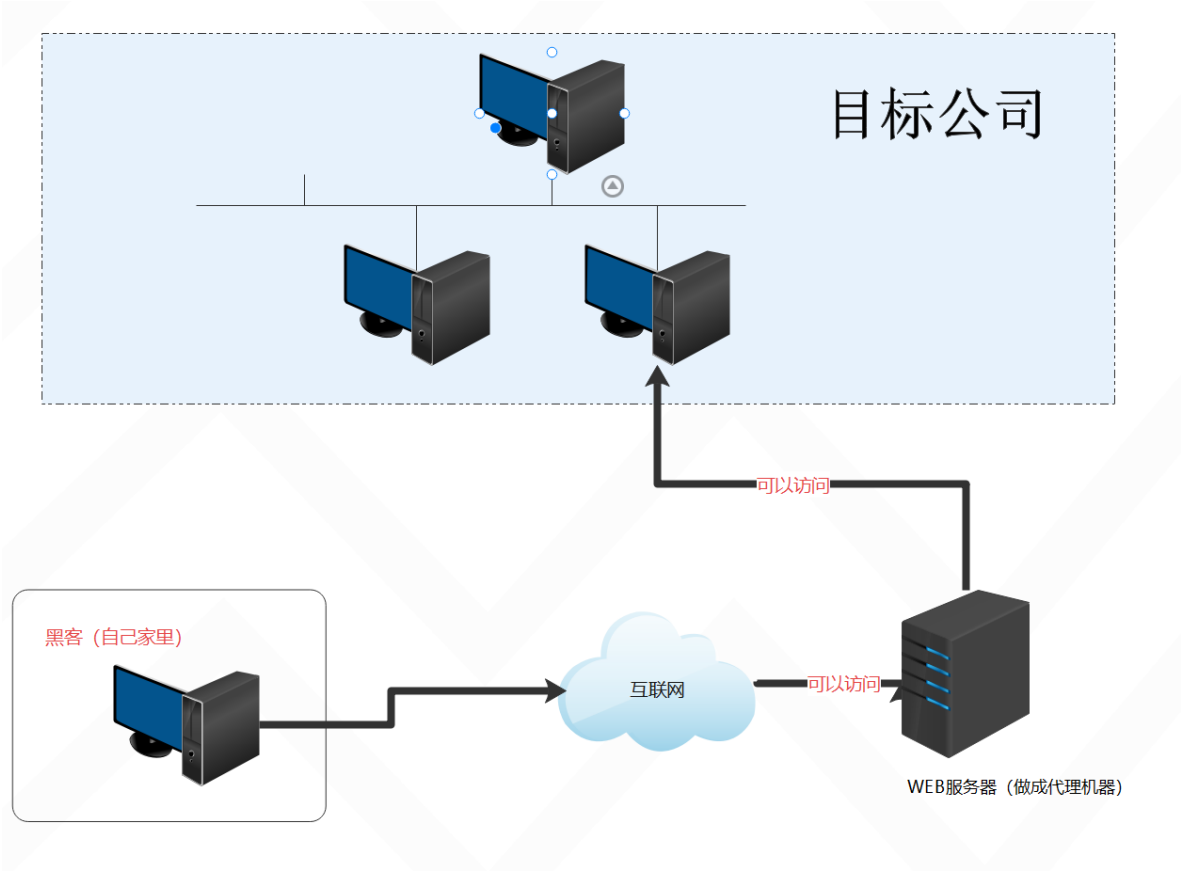
在这种情况需要用什么工具走代理呢?

1、扫描工具

2、浏览器

3、burp

使用代理一般是用http代理或者socks代理代理后的拓扑如下



总体就是这样的情况第一种一般是买代理，第二种一般是做代理，

注意：买代理可以，不要买到国外哦