内网穿透方法调研

由于目前的NAT技术和IP地址的分配策略，大部分机器都只能在局域网内被访问到。例如在家中搭建的NAS服务器，只能获取到一个私有ip地址，一旦离开家中的路由器，就无法访问到该NAS提供的云存储服务。

这时候如果想在外部网络中访问到内部网络中的机器，就需要进行内网穿透。

目前一些NAS厂商会直接提供内网穿透服务，使用他们指定的域名即可在任意网络访问到该NAS，这种方式的本质是NAS建立长链接到NAS厂商专门的代理服务器，

内网穿透有两种方法：

1. 使用一台拥有公网ip的**代理服务器**
2. 使用第三方服务直接穿透

通过代理服务器

以下拥有公网ip，可以从任何位置访问到的服务器称为**代理机**，IP假设为1.1.1.1

没有公网IP，位于路由器内部的机器称为**内网机**，IP假设为192.168.1.2

假设现在想从外部网络访问**内网机**的SSH服务，所以我们的目标是将**代理机**的10022收到的流量全部转发到**内网机**的22端口

SSH反向代理

原理

通过SSH建立**代理机**到**内网机**的隧道

操作

1. 建立反向代理

因为**内网机**可以通过SSH访问到**代理机**，所以执行如下命令

```
ssh -fCNR 20022:localhost:22 root@1.1.1.1
```

然后输入代理机的密码即可

当完成这一步后，就已经可以通过代理机做跳板来访问内网机了

我们在代理机上执行命令，访问自己的20022端口，就等同于访问内网机的22端口了

```
ssh root@localhost -p 20022
```

2. 建立正向代理

当完成第一步后，代理机相当于一个客户端，从20022端口向外发送流量

所以需要再开启代理机的10022端口用于接收流量，并将所有流量转发至自身的20022端口

```
ssh -fCNL 10022:localhost:20022 root@localhost
```

当完成这一步以后，内网穿透就已经完成了，在任意一个网络，可以通过如下命令直接SSH到内网机

```
ssh root@1.1.1.1 -p 10022
```

同样的方法也可以将任何一个端口穿透出去，即使非SSH服务也可以。

备注：在使用云服务厂商提供的服务器时，要注意使用的端口是否被安全组策略限制而无法访问。

3. 解决SSH超时的问题

因为SSH连接会超时关闭，所以需要通过autossh建立一个稳定的隧道。 在此之前需要先确保服务器之间的无密码访问是有效的 然后安装autossh工具，`yum install autossh` 用下一条命令替换第一步中执行的命令

```
autossh -M 11111 -fCNR 20022:localhost:22 root@1.1.1.1
```

这里的11111端口是用来监视ssh状态的，如果ssh断开将会自动重连 **备注**：实测在群晖的DSM系统上无法便捷的安装autossh，需要安装ipkg包管理系统，而在基于AR架构的DSM系统上安装ipkg则是一个更加麻烦的事情。所以如果内网机无法安装autossh命令，甚至没ssh功能的情况下，可以考虑再找一台能执行该命令的机器做中转，此时执行该命令就不能localhost，而是要写清该内网机的ip地址。

```
autossh -M 11111 -fCNR 20022:192.168.1.2:22 root@1.1.1.1
```

本此我用作中转的机器是一台旧手机安装了

相关参数解释

- -f 后台执行ssh指令
- -C 允许压缩数据
- -N 不执行远程指令
- -R 将远程主机(服务器)的某个端口转发到本地端指定机器的指定端口
- -L 将本地机(客户机)的某个端口转发到远端指定机器的指定端口
- -p 指定远程主机的端口

FRP

概述

frp 是一个专注于内网穿透的高性能的反向代理应用，支持 TCP、UDP、HTTP、HTTPS 等多种协议。

frp 由 **客户端(frpc)** 和 **服务端(frps)** 组成，相比于上面使用SSH进行内网穿透，FRP提供了更强大的内网穿透功能。

安装

在https://github.com/fatedier/frp/releases找到适合于自己版本的压缩包，直接解压即可使用。

部署

在**代理机**上修改配置文件`frps.ini`,修改如下

```
[common]
bind_port = 20000
```

然后执行`./frps -c frps.ini`来启动服务端，这时候服务端就会开始监听`20000`端口，等待客户端的连接。

在**内网机**上修改配置文件`frpc.ini`，修改如下

```
[common]
server_addr = 1.1.1.1
server_port = 20000

[ssh]
type = tcp
local_ip = 127.0.0.1
local_port = 22
remote_port = 10022
```

然后执行`./frpc -c frpc.ini`来启动客户端，`remote_port`就是希望服务端监听的端口，监听到的流量会通过`remote_port`转发到自己的`local_port`上。

这时在任意一台主机执行命令，即可访问到**内网机**的SSH服务

```
ssh root@1.1.1.1 -p 10022
```

其他

通过FRP可以实现除了简单端口转发以外更多的功能，例如通过域名访问内网机的web服务、提供文件访问服务、或者开启https等

具体配置细节可以查看文档https://gofrp.org/docs/

其他工具

Holer

项目地址：https://github.com/wisdom-projects/holer-client

简介：使用Java和Go编写编写的内网穿透工具，通过客户端软件和服务端实现内网穿透，也提供了一些公开的映射用来穿透。

rtcp

项目地址：https://github.com/knownsec/rtcp

简介：使用Python编写的socket端口转发，代码简单方便学习

Wireboy.Socket.P2PSocket

项目地址：https://github.com/hemaju/Wireboy.Socket.P2PSocket

简介：C#编写的内网穿透工具，可以让在不同内网的两台电脑之间互相远程控制。

nps

项目地址：https://github.com/ehang-io/nps

简介：用Go语言编写的提供web管理终端的内网穿透工具，功能比较强大

通过第三方服务

在没有公网IP的服务器时，可以考虑使用第三方提供的内网穿透服务

花生壳

软件：通过花生壳提供的客户端软件，可以将内网的主机映射到一个指定的域名上（或者使用花生壳提供的随机二级域名）。但需要购买专门的套餐，且带宽和流量受限。

例如花生壳SSH映射服务在带宽为**3M**的情况下，一年的费用为148年。

硬件：购买贝瑞科技旗下的花生棒或花生壳盒子，即硬件版的花生壳客户端。在使用此硬件的时候，可以免费享受80端口的映射，但有**1M**带宽的限制，且流量在1-2G。

NAT123

http://www.nat123.com/

使用方法与花生壳类似，也是需要根据所需要的服务搭配不同的套餐，拥有不同的带宽和流量。