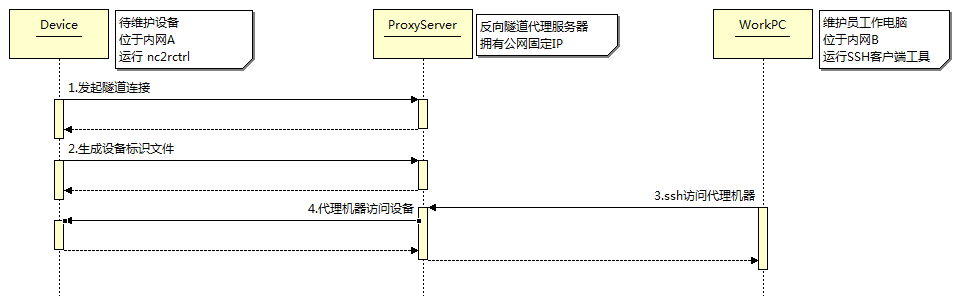
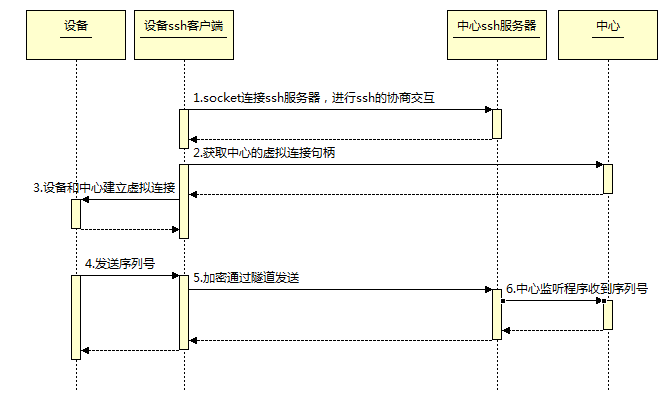
需求流程图：



SSH远程端口转发流程图：



1. 发起转发的起始人：

肯定是内网的发起，才能利用NAT连接通信。

1. 本地转发和远程转发的区别：

都能实现一样的效果，区别在于谁是ssh服务器，ssh服务器能够指定22端口监听。中心不能主动连接设备，因此要设备主动连接中心，设备是ssh客户端。

由内网发起ssh转发，数据流从内网往外，是远程转发；数据流由外往内，是本地转发。

本机验证：

1．命令行



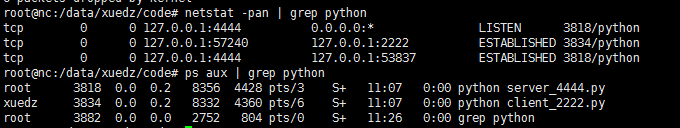
|  |  |
| --- | --- |
| Remote\_host | 内网代理的host |
| Remote\_port | 内网代理的监听端口 |
| Local\_port | 外网代理的转发端口 |
| Hostname | ssh服务器地址 |

2．实验

|  |  |
| --- | --- |
| Remote\_host | localhost |
| Remote\_port | 4444 设备监听端口 |
| Local\_port | 2222 中心转发端口 |
| Hostname | localhost |

执行命令： ssh -p 8022 -R 2222:localhost:4444 localhost

1. 执行4444端口监听的服务器；
2. 执行命令ssh -p 8022 -R 2222:localhost:4444 localhost
3. 执行连接2222端口，接收数据。
4. 结果，成功接通。



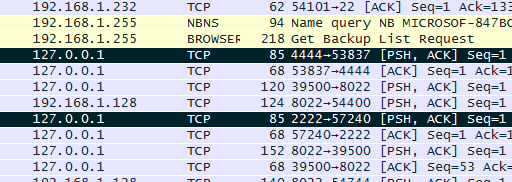
由上图：

* 图中 server是设备，client是中心

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 设备 | 监听 | 4444 |
| 设备 | Ssh代理 | 53837 |
| 中心 | 接收转发 | 57240 |

由上图可知，服务器除了程序运行时指定的4444端口去监听外，还多了一个连接到本机53837端口的连接。而客户端用57240端口连接上了2222端口，接收到信息。

以下是抓包



真实搭建环境实验：

|  |  |  |
| --- | --- | --- |
| 内网服务器（虚拟机） | 代理（不能访问内网服务器） | 开发人员远程操作（PC） |
| 192.168.183.128 | 192.168.1.232 | 192.168.1.128 |

1.在内网服务器执行命令：

Ssh –Nf –l xuedz –p 8022 –R 2222:localhost:22 192.168.1.232

ssh -p 2222 localhost -l xdz