VNC 简介

VNC 的全称是 Virtual Network Computing，是一种图形桌面系统共享协议。VNC 使用 RFB（Remote FrameBuffer）来控制远程计算机。它将键盘和鼠标的时间从一台计算机传输到另外一台计算机上，并更新相关的屏幕背景。

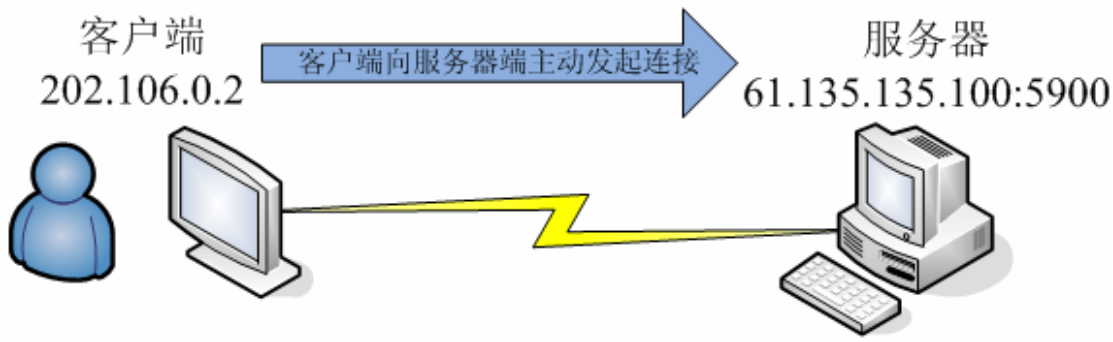
VNC 是平台独立的，一个 VNC 标准客户端可以连接到任何一个操作系统架构上的服务器端。除了标准的客户端外，VNC 还提供了 JAVA 客户端和 WEB 客户端。多个客户端可以同时连接到同一个服务器。VNC 最早由 AT&T 提出并开发，VNC 的代码按照 GNU 协议发行并已经有了多个不同的发行版本，比较著名的有 RealVNC 等。

VNC 的一大特点是基于物理控制台的遥控，即远程客户端操作的是服务器的物理终端，这点非常类似于 Symantec 出品的 PcAnyWhere。当远程客户端移动鼠标并使用键盘键入数据的时候，服务器端本地的物理终端会实时看到键盘鼠标的操作。这个特性使得 VNC 被广泛的用于各种操作演示场合。

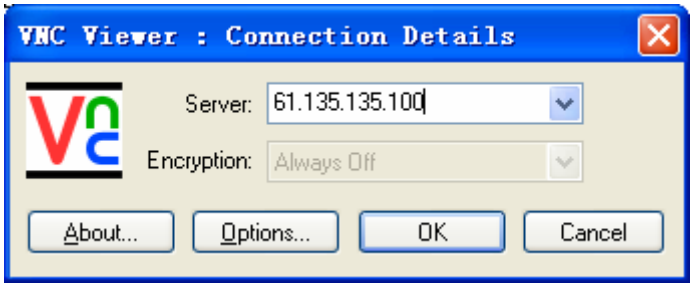
VNC 的四种模式

VNC 分成服务器端、客户端，当客户端和服务器端分别使用公网 IP、内网 IP 的时候，可能有如下组合方式：

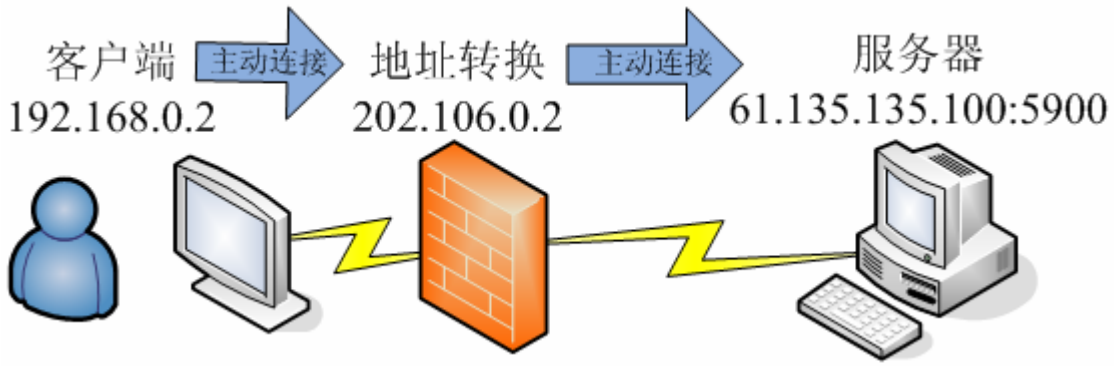
1. 客户机使用公网 IP，服务器也使用公网 IP。



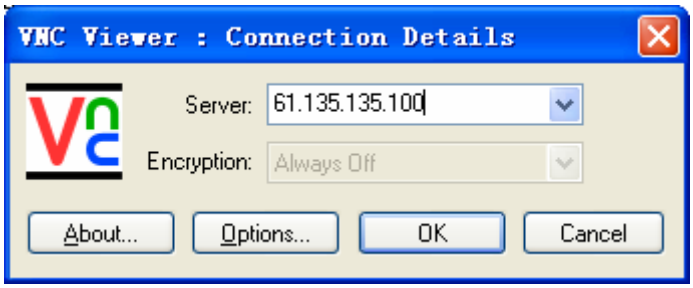
在这种情况下，在服务器端安装 VNC Server，并打开 5900 端口的监听，客户端使用 VNC Client 直接连接到服务器端，只要在客户端程序中输入服务器的 IP 即可，不需要经过额外的配置。



2. 客户机使用内网 IP+防火墙 NAT 地址映射，服务器使用公网 IP。

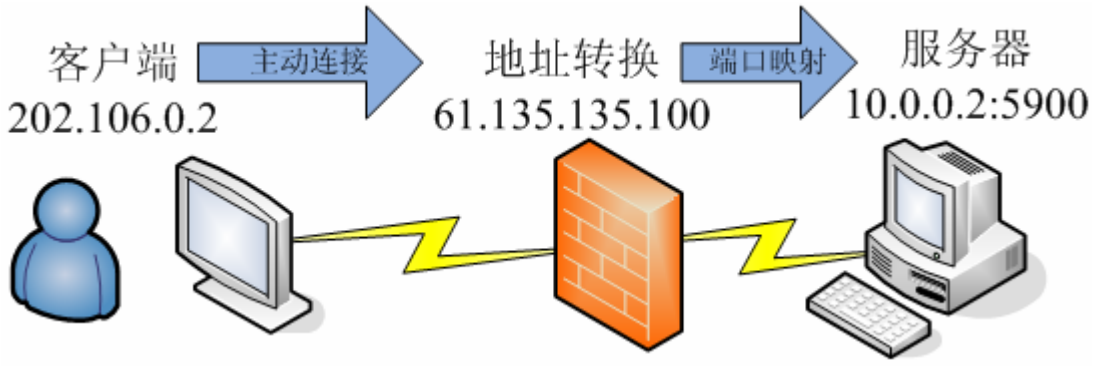


这种场景是非常典型的企业应用场景。服务器位于 IDC 机房内，使用公网 IP，并安装服务器端软件，监听于 5900 端口。客户端程序使用内网 IP，并通过 NAT 路由器连接到互联网。连接建立时，由 192.168.0.2 的客户端发起连接，并穿过防火墙，到达服务器。此情景下，也只要在客户端程序中输入服务器的 IP 即可，不需要经过额外的配置。



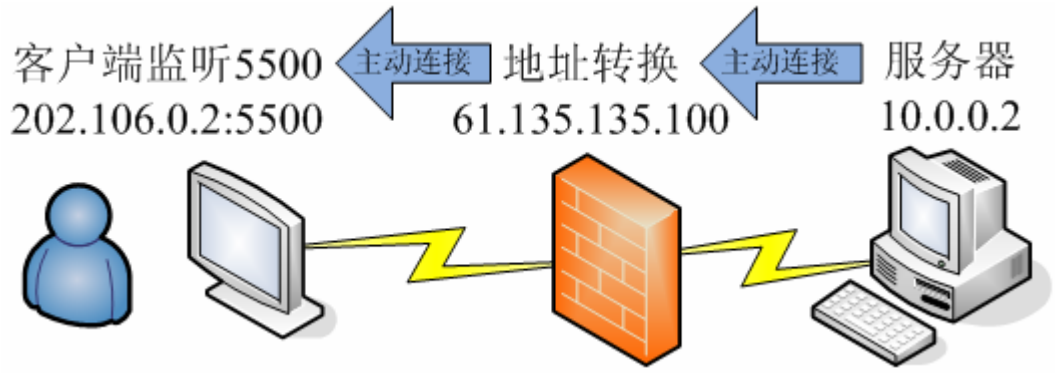
3. 客户机使用公网 IP，服务器使用内网 IP+防火墙 NAT 地址映射。

第三种可能的情况是服务器位于防火墙后，使用内网 IP，而客户端使用公网 IP。此时，服务器端监听的地址是 10.0.0.2:5900，客户端是无法穿透防火墙连接到服务器上的。所以，必须在防火墙上添加相应的地址映射规则，例如把公网地址 61.135.135.100:5900 端口映射到内网的 10.0.0.2:5900 地址上。然后在客户端连接地址框中输入相应的公网 IP，即可建立链接。

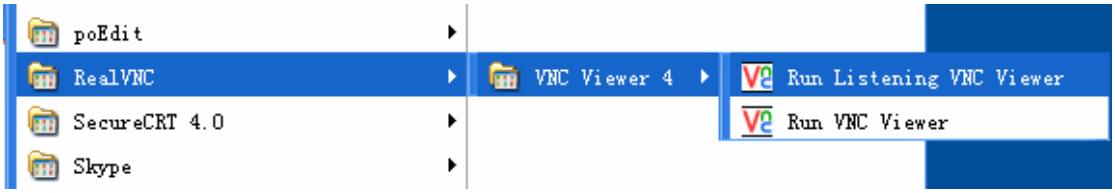


这种使用模式有一个主要的问题，即必须在服务器前端的防火墙或者路由器上，设置端口映射规则。但是，受到条件所限，并非所有的防火墙都能设置端口映射；同时，由于安全策略所限，并非所有的技术操作员都具有调整公司整体防火墙的安全权限。所以，这种模式能否使用，取决于是否能设置端口映射规则。

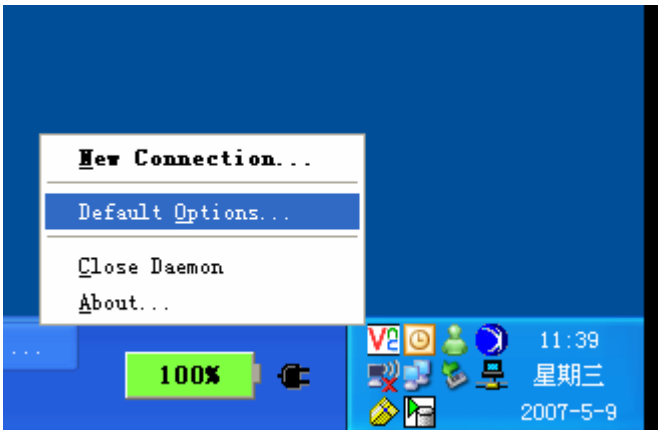
如何避开端口映射规则呢？从 VNC 的连接过程中可以看到，是客户端发起请求，寻找服务器端监听的端口，然后双方建立连接。**反之，可以由客户端监听在某端口，位于防火墙后的服务器端主控发起连接，寻找客户端，并建立连接。**



这种反向建立连接的过程，是由 RealVNC 的“Listening VNC Viewer”来实现的。它启动后，驻留在客户端的 5500 端口，此时需要服务器端使用“Add Client”功能建立连接。在客户端上，首先运行开始菜单中的“Listening VNC Viewer” 。



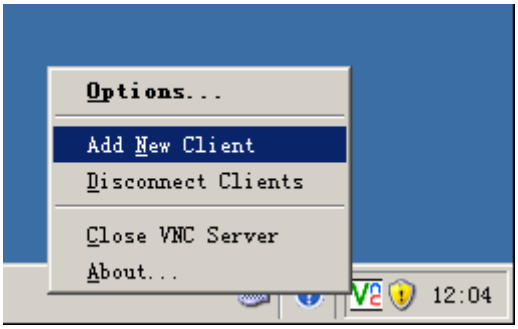
运行之后，会在客户端的任务栏上看到一个 VNC 的图标。



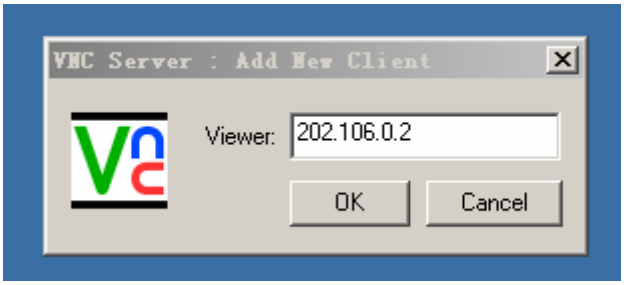
能看到这个图标，就表示“Listening VNC Viewer”启动成功。现在运行 cmd，并执行 netstat -an 命令，可以发现它正在监听 5500 端口。请在防火墙上打开这个端口。

```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:990            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1000           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5500           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1442         127.0.0.1:1443         ESTABLISHED
```

现在到服务器端，找到任务栏上驻留的 VNC Server，使用鼠标右键点击，然后选择“Add New Client” 。

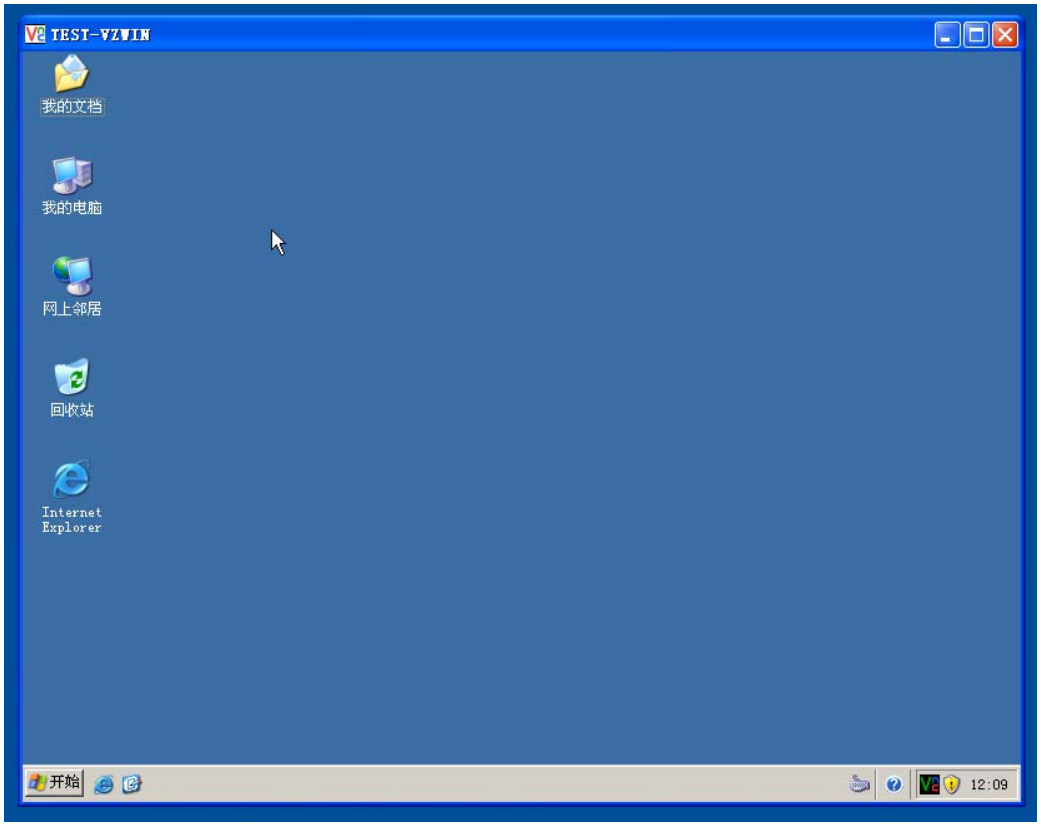


输入客户端的 IP，例如 202.106.0.2:5500。注意，默认 Listener 是 5500 端口，不输入端口号码也可以。

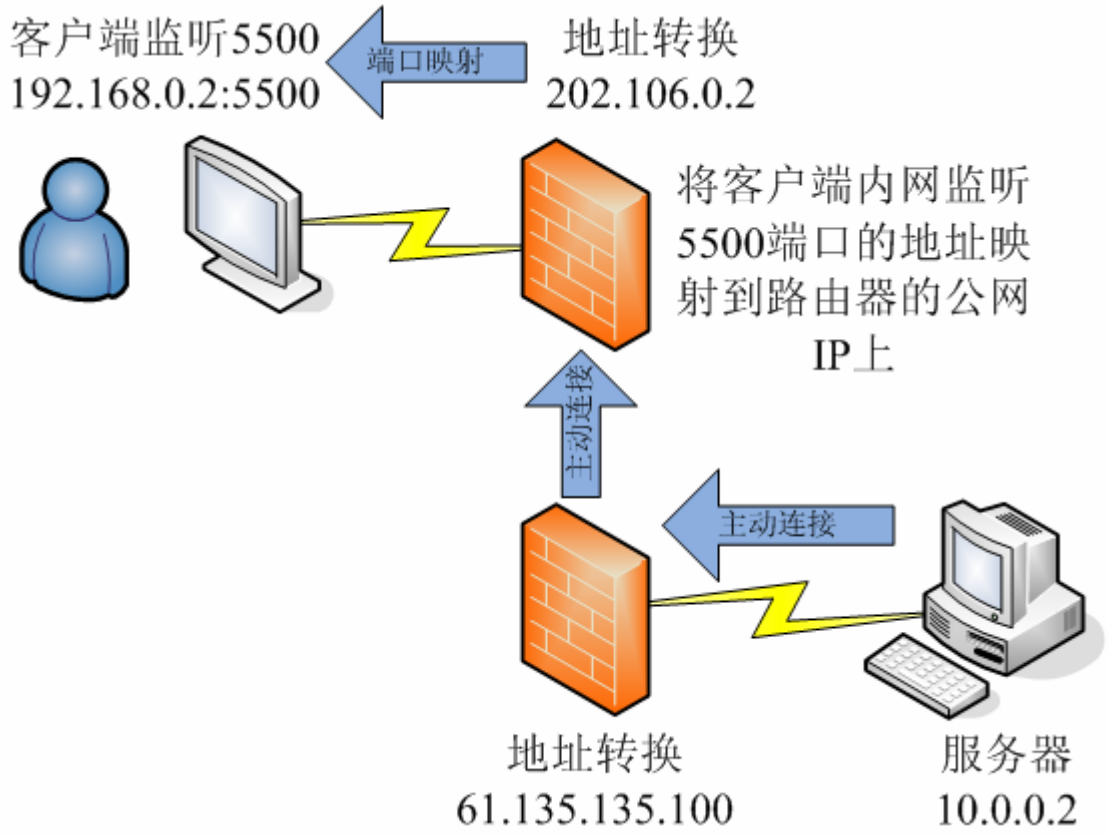


点击 OK 后，连接成功。现在到客户端界面上，就可以看到 VNC 窗口弹出，成功建立连接。此时就可以在客户端上操作位于内网的 10.0.0.2 这台服务器了。

使用 VNC 反向连接功能，可以在一定程度上穿透防火墙内网保护，实现对防火墙后的服务器的维护、演示等需求。



4. 客户端和服务器都在防火墙后



这种情况是对第三种情况的一个扩展。在第三种应用场景下，客户端使用公网 IP 地址，监听 5500 端口，这是处于内网的服务器可以连接到的保证。那么加入客户端也处于防火墙保护下的内网中，应该如何操作？

考虑到在服务器端添加相应的端口映射规则可能非常不便，所以这里采用在客户端添加端口映射规则的方法。也就是说，在双方都有防火墙做地址转换的情况下，通过过如下的方式可以建立连接：

1) 客户端启动 VNC Listener 监听 5500 端口
2) 客户端增加防火墙端口映射，将 5500 端口映射到公网 IP 上
3) 服务器端主控执行添加客户端的操作，输入客户端公网 IP，建立连接

再满足上述三个条件的情况下，即可远程操作位于内网服务器的，实现安装、维护、演示、培训等用途。