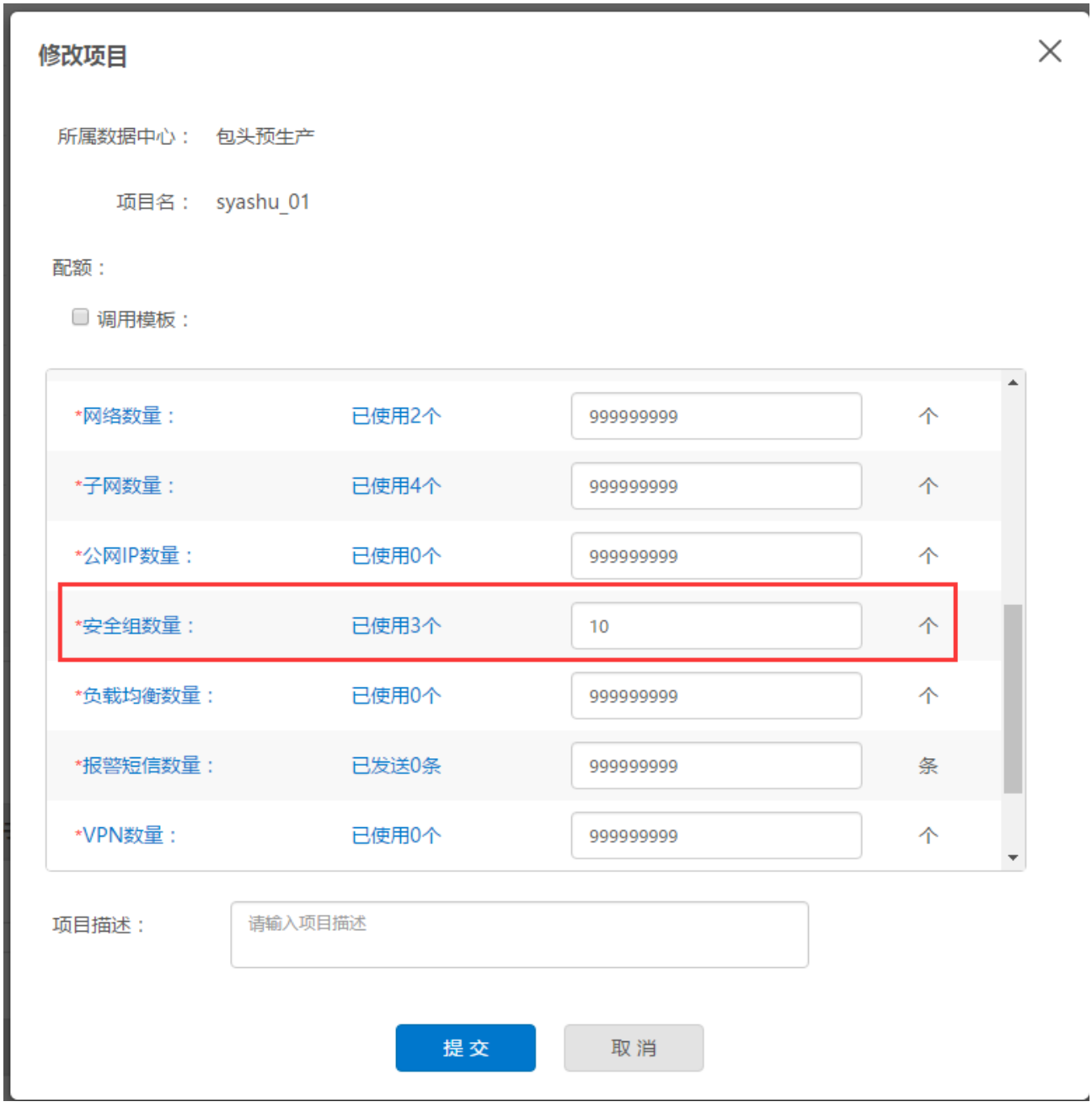
生产环境历史项目的默认安全组处理

由于在用户中心版本，简化了客户对云主机访问的安全组默认管理的工作，所以此版本中，客户在申请项目后，会默认生成3个默认的安全组，**default**、**Windows**安全组放通**3389**端口、**Linux**安全组放通**22**端口。但是在此版本之前项目下只有一个default的安全组，所以需要对在用户中心版本之前创建的项目初始化两个默认的安全组。处理方式如下：

一、项目下安全组的配额处理：

在为项目项目默认安全组之前，首先需要对项目的安全组配额做调整，确保默认的安全组能够创建成功，且不影响客户的安全组配额额度。对项目的安全组配额在原有基础上增加两个，即在ECMC平台上修改每个项目的安全组配额



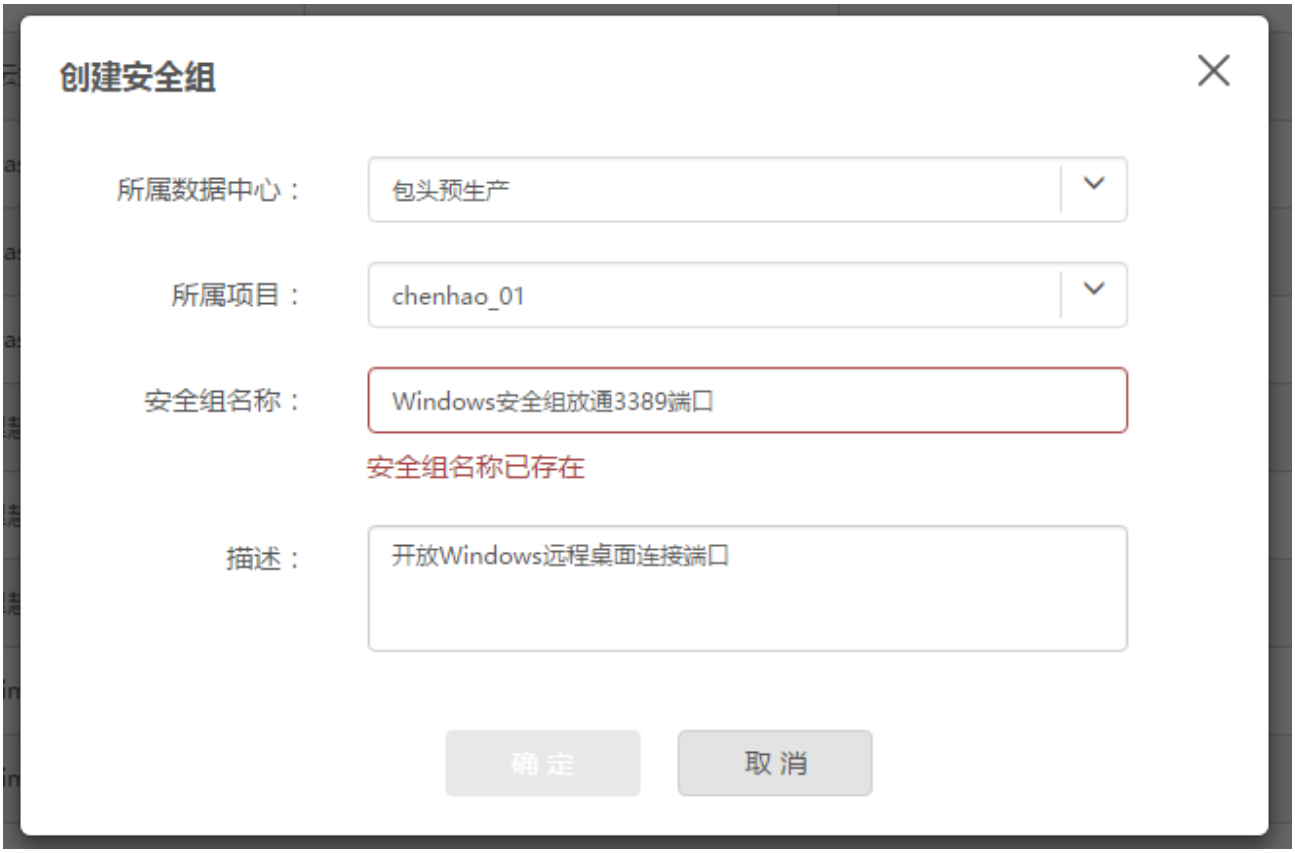
新的安全组数量 = 原有的安全组数量 + 2

二、新增默认安全组

在ECMC平台上位每个项目创建两个安全组名称分别为：**Windows**安全组放通**3389**端口、**Linux**安全组放通**22**端口，并为创建的安全组关联规则

1. 创建Windows安全组

名称为：**Windows**安全组放通**3389**端口
描述：开放**Windows**远程桌面连接端口
如下图：

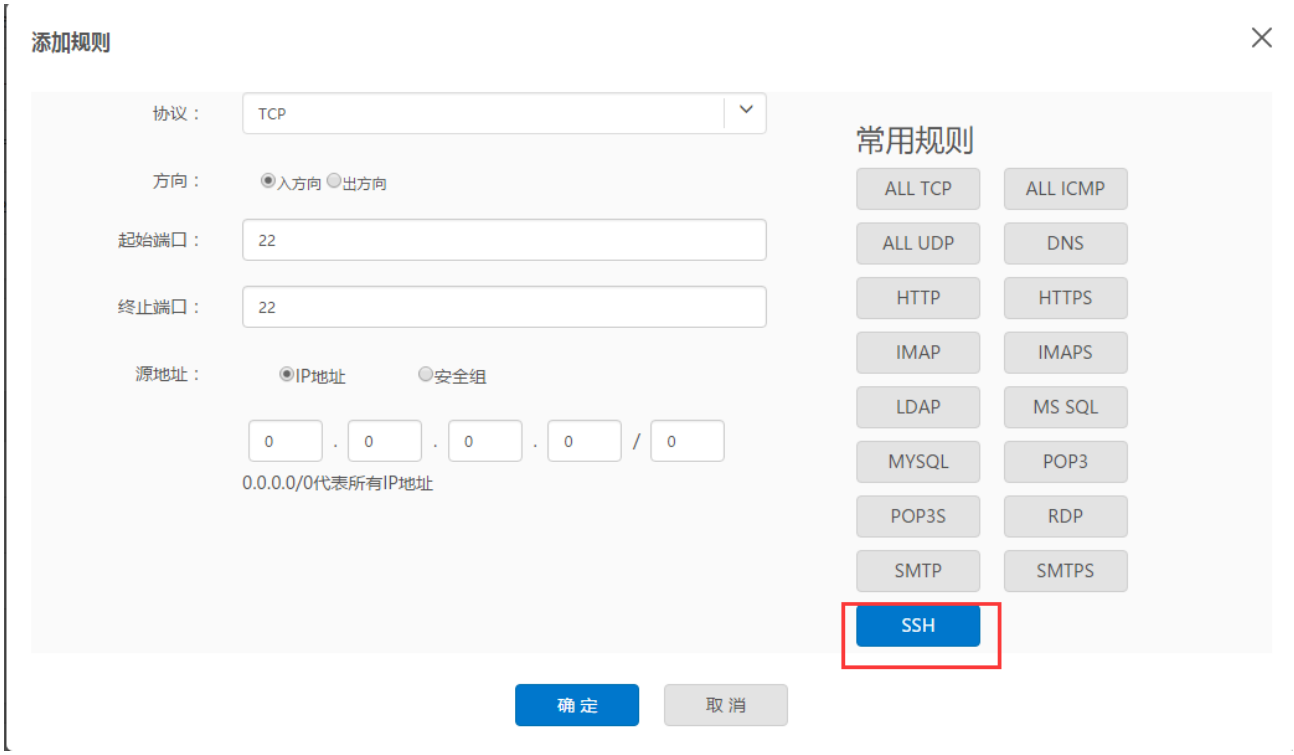


并为**Windows**安全组放通**3389**端口 创建一个安全组规则，如下图：

2. 创建Linux安全组

名称为：**Linux**安全组放通**22**端口
描述：开放**SSH**远程连接端口
如下图：

并为 **Linux**安全组放通**22**端口 创建一个安全组如下图：



3. 放通与当前安全组关联云主机的所有流量

然后还需要在dashboard上为手动创建的两个安全组（**Windows**安全组放通**3389**端口、**Linux**安全组放通**22**端口） 放通与当前安全组关联云主机的所有流量，
Windows安全组放通**3389**端口 需要关联的规则如下：

Linux安全组放通**22**端口 需要关联的规则如下：

4. 将安全组修改为默认为安全组

为所有的项目做完以上的操作后，需要 同步数据中心 ，将在dashboard上添加的规则同步到上层，然后修改eayuncloud数据库中新创建的默认安全组：
SQL如下：

```
update  cloud_securitygroup  set    default_group  =  'defaultGroup'
where  sg_name  in  ('Windows安全组放通3389端口','Linux安全组放通22端口');
```

三、验证

将上述所有的操作完成后，需要在ECMC验证上述操作是否完成，

- 查看 安全组列表 下根据名称分别查询 **Windows**安全组放通**3389**端口、**Linux**安全组放通**22**端口 是否等于项目的个数
- 在云主机的购买页面，查看默认安全组是否为：**default**、**Windows**安全组放通**3389**端口、**Linux**安全组放通**22**端口
- 分别使用 **Windows**安全组放通**3389**端口、**Linux**安全组放通**22**端口 创建云主机，查

看云主机的默认安全组是否为所选安全组，绑定安全组后，测试云主机是够能够远程登录。