安全组配置指南

交大JCloud平台从属于教育平台，教育网相关安全人员会实时扫描器JCloud平台上机器的安全漏洞，并通知学校安全部门。目前，已有一些同学由于弱密码等相关漏洞收到了相关管理人员的提醒，因此，特此对大家配置安全组提出建议，以提高大家机器的安全性。请各位同学遵循以下步骤与原则，对安全组策略进行修正

安全组配置简介

相较于防火墙或更加复杂的Iptables等安全配置方式，JCloud安全组提供了更为简单的配置接口：即对来自特定地址的特定协议的入站/出站流量进行允许/禁止操作。安全组的配置入口在JCloud->安全->安全组下，通常直接针对default安全组添加规则即可。

对安全组添加规则的操作如上图，其中：

- 协议：该安全组所使用的协议种类（TCP、UDP、ICMP、以及高层级的HTTP等协议）
- 方向：安全组所应用的方向：入口（其他机器访问安全组所管理的机器）、出口（安全组所管理的机器访问其他机器）
- 网络地址：安全组规则所适用的其他机器的地址

因此，本教程旨在帮助大家重新规划安全组的入站规则，以确保外部攻击者或安全检查人员的流量难以进入minik8s集群所包管理的JCloud云服务器中，从而达到提高安全性的效果。

删除非必要入站规则

默认安全组中存在有大量非必要入站规则（如RDP等），请先行删除

对于安全组的出站规则，由于目前无需限制安全组所管理的机器的对外操作，因此仍保留目前默认安全组的设置（允许IPV4/IPV6类型的任意地址任意协议的出口流量通过）即可

允许子网内机器互相访问

为了允许JCloud专有网络VPC下的不同机器间相互访问，需添加如下安全组规则，以允许内网机器间的任意流量均可互相访问。

其中，192.168.122.0/24为专有网络的网络地址，请大家根据自身专有网络的配置自行修改。

允许集群内机器通过浮动IP互相访问

由于每名同学的机器存在配额上限，因此，minik8s实验通常会涉及到需管理多名同学从属于不同专有网络VPC的机器集群。为此，需对集群中的每台机器绑定校园网内部浮动IP，并添加如下规则，允许来自集群内机器浮动IP的任意流量对安全组所管理机器进行访问。

其中，10.119.10.255即为浮动IP，请根据集群内机器浮动IP，自行添加足够数目的此类安全组规则

暴露必要外部接口

除上述两类规则外，安全组还需要对外暴露必要的接口（如80端口等），以方便集群外机器对集群内机器进行管理。为此，请添加形式如下的规则，允许来自任意地址对特定端口的访问。

其中，目的端口/端口范围即为需要对外暴露的端口。

注意，每当对外暴露端口时，需确保对该端口的访问是需要强密码进行认证的，否则，仍将会触发教育网相关安全漏洞检测机制！