(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106878302 A
(43)申请公布日 2017.06.20

(21)申请号 201710078467.1

(22)申请日 2017.02.14

(71)申请人 武汉烽火信息服务有限公司
地址 430074 湖北省武汉市洪山区邮科院路88号

(72)发明人 张傲

(74)专利代理机构 北京捷诚信通专利事务所（普通合伙）11221
代理人 王卫东

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

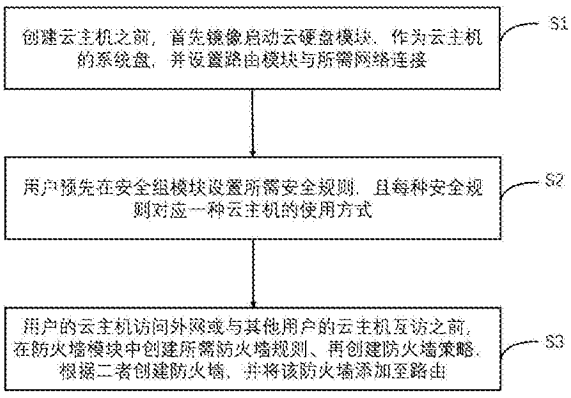
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种云平台系统及设置方法

(57)摘要

一种云平台系统及设置方法，涉及云计算领域，包括云硬盘模块、路由模块、防火墙模块和安全组模块；用户创建云主机之前，首先镜像启动云硬盘模块，作为云主机的系统盘，并设置路由模块与所需网络连接；用户预先在安全组模块设置所需安全规则，且每种安全规则对应一种云主机的使用方式；用户的云主机访问外网或与其他用户的云主机互访之前，在防火墙模块中创建所需防火墙规则、再创建防火墙策略，根据二者创建防火墙，并将该防火墙添加至路由。本发明提高用户使用的安全性，防护外界病毒骚扰，避免信息泄露。



CN 106878302 A

1.一种云平台系统,其特征在于,包括:

云硬盘模块,用于存储云资源;

路由模块,用于连接用户私有网络以及公网;

防火墙模块,用于对云硬盘模块中存储的云资源提供安全防护;

安全组模块,用于用户设置安全组规则,且不同安全组规则对应云主机的不同使用方式。

2.如权利要求1所述的云平台系统,其特征在于:所述安全组模块的安全组规则包括ICMP协议,用于用户云主机之间ping通。

3.如权利要求1所述的云平台系统,其特征在于:所述安全组模块的安全组规则包括TCP协议,用于户远程访问自己的云主机。

4.如权利要求1所述的云平台系统,其特征在于:所述防火墙模块根据防火墙规则和防火墙策略创建防火墙,防火墙策略包含防火墙规则。

5.如权利要求1所述的云平台系统,其特征在于:所述云硬盘模块挂载于用户的云主机,且为所挂云主机的系统盘。

6.一种基于权利要求1所述云平台系统的设置方法,其特征在于,包括:

用户创建云主机之前,首先镜像启动云硬盘模块,作为云主机的系统盘,并设置路由模块与所需网络连接;

用户预先在安全组模块设置所需安全规则,且每种安全规则对应一种云主机的使用方式;

用户的云主机访问外网或与其他用户的云主机互访之前,在防火墙模块中创建所需防火墙规则、再创建防火墙策略,根据二者创建防火墙,并将该防火墙添加至路由。

7.如权利要求6所述云平台系统的设置方法,其特征在于:用户将防火墙添加至路由后,防火墙状态为正常,没添加至路由的防火墙状态为异常。

8.如权利要求6所述云平台系统的设置方法,其特征在于:防火墙使用防火墙策略或防火墙规则时,先删除防火墙,再删除防火墙策略或防火墙规则。

9.如权利要求6所述云平台系统的设置方法,其特征在于:所述安全规则包括云主机的入口和所需出口协议。

10.如权利要求9所述云平台系统的设置方法,其特征在于:若用户云主机之间需要ping通,通过安全组模块内部添加ICMP协议进行;若用户远程访问自己的云主机,通过安全组模块内部添加TCP协议进行。

一种云平台系统及设置方法

技术领域

[0001] 本发明涉及云计算领域，具体来讲涉及一种云平台系统及设置方法。

背景技术

[0002] 云计算是一种基于互联网的计算方式，通过这种方式，共享的软硬件资源和信息可以通过网络对外提供。

[0003] 而云平台是云计算领域中重要部分，允许用户使用“云”里提供的服务。由于云平台要向多个用户提供服务，业务数据安全和网络通信保护成为云平台建设的关键问题。由于现有云平台的用户较多，云平台的安全防护不够，用户在使用云平台的同时面临信息泄露的隐患、同时还会面临外界病毒的骚扰，用户使用中安全性较低。

发明内容

[0004] 针对现有技术中存在的缺陷，本发明的目的在于提供一种云平台系统及设置方法，提高用户使用的安全性，防护外界病毒骚扰，避免信息泄露。

[0005] 为达到以上目的，本发明采取一种云平台系统，其特征在于，包括：

[0006] 云硬盘模块，用于存储云资源；

[0007] 路由模块，用于连接用户私有网络以及公网；

[0008] 防火墙模块，用于对云硬盘模块中存储的云资源提供安全防护；

[0009] 安全组模块，用于用户设置安全组规则，且不同安全组规则对应云主机的不同使用方式。

[0010] 在上述技术方案的基础上，所述安全组模块的安全组规则包括ICMP协议，用于用户云主机之间ping通。

[0011] 在上述技术方案的基础上，所述安全组模块的安全组规则包括TCP协议，用于户远程访问自己的云主机，

[0012] 在上述技术方案的基础上，所述防火墙模块根据防火墙规则和防火墙策略创建，防火墙策略包含防火墙规则。

[0013] 在上述技术方案的基础上，所述云硬盘模块挂载于用户的云主机，且为所挂云主机的系统盘。

[0014] 本发明还提供一种云平台系统的设置方法，包括：用户创建云主机之前，首先镜像启动云硬盘模块，作为云主机的系统盘，并设置路由模块与所需网络连接；用户预先在安全组模块设置所需安全规则，且每种安全规则对应一种云主机的使用方式；用户的云主机访问外网或与其他用户的云主机互访之前，在防火墙模块中创建所需防火墙规则、再创建防火墙策略，根据二者创建防火墙，并将该防火墙添加至路由。

[0015] 在上述技术方案的基础上，用户将防火墙添加至路由后，防火墙状态为正常，没添加至路由的防火墙状态为异常。

[0016] 在上述技术方案的基础上，防火墙使用防火墙策略或防火墙规则时，先删除防火

墙，再删除防火墙策略或防火墙规则。

[0017] 在上述技术方案的基础上，所述安全规则包括云主机的入口和所需出口协议。

[0018] 在上述技术方案的基础上，若用户云主机之间需要ping通，通过安全组模块内部添加ICMP协议进行；若用户远程访问自己的云主机，通过安全组模块内部添加TCP协议进行。

[0019] 本发明的有益效果在于：

[0020] 通过设置防火墙规则和策略，进而创建防火墙，为云主机访问外网或用户互访提供安全保障，提高用户使用的安全性，避免用户信息泄露，也对外界病毒和木马进行了隔离防护。另外，只有添加至路由的防火墙状态为正常，且在防火墙策略或防火墙规则使用中无法删除，用户在使用云平台的过程中，不会因为误删或者误操作而失去保护，更加提高了安全保障。

[0021] 用户可以通过安全组模块设置安全组规则，设置云主机入口和所需的出口协议，根据不同的云主机使用，选择对应的出口协议，确保云主机使用的安全性。

附图说明

[0022] 图1为本发明实施例云平台系统设置流程图。

具体实施方式

[0023] 以下结合附图及实施例对本发明作进一步详细说明。

[0024] 本发明所述云平台系统，包括云硬盘模块、路由模块、防火墙模块和安全组模块。

[0025] 所述云硬盘模块用于存储云资源，云硬盘模块以逻辑存储卷的形式设置，它是一种可弹性扩展的虚拟块存储设备。用户可以在线进行操作，使用方式与传统服务器硬盘完全一致。同时，云硬盘模块具有更高的数据可靠性，更高的I/O吞吐能力和更加简单易用等特点。所述云硬盘模块挂载于云主机，作为所挂云主机的系统盘，若云硬盘挂模块载在云主机时，是不能进行扩容的，需要先从云主机卸载，再进行扩容。

[0026] 所述路由模块用于连接用户私有网络及公网，用户可以通过向租户管理员申请创建路由器，创建后需要路由器与私有网络连接，若用户需要访问外网，需要路由器与公网连接。

[0027] 所述防火墙模块，用于对云硬盘模块中存储的云资源提供安全防护；防火墙模块根据防火墙规则和防火墙策略创建，防火墙策略包含防火墙规则，以便于用户的云主机需要访问外网或者与其他用户的云主机互访。

[0028] 所述安全组模块，用于用户设置安全组规则，且不同安全组规则对应云主机的不同使用方式。所述安全组模块的安全组规则包括ICMP协议和TCP协议等，若用户云主机间需要ping通，需要添加安全组规则的ICMP协议；若用户需要远程访问(ssh)自己的云主机，需要添加安全组规则的TCP协议。默认情况下，任何安全组规则都只开通了出口，用户需要根据需要自己添加入口或需要的出口协议。

[0029] 如图1所示，为发明实施例一种云平台系统的设置方法流程，具体包括：

[0030] S1.用户创建云主机之前，首先镜像启动云硬盘模块，作为云主机的系统盘，并设置路由模块与所需网络连接。优选的，用户对租户管理员发起申请，租户管理员有权限新建

私有新建私有网络、添加子网、创建路由器，创建后，需要路由器与私有网络链接；若用户需要访问外网，需要路由器与公网链接。

[0031] S2.用户预先在安全组模块设置所需安全规则，且每种安全规则对应一种云主机的使用方式，安全规则包括ICMP协议和TCP协议等。优选的，若用户云主机之间需要ping通，通过安全组模块内部添加ICMP协议进行；若用户远程访问自己的云主机，通过安全组模块内部添加TCP协议进行。

[0032] S3.用户的云主机访问外网或与其他用户的云主机互访之前，在防火墙模块中创建所需防火墙规则、再创建防火墙策略，根据二者创建防火墙，并将该防火墙添加至路由。用户将防火墙添加至路由后，防火墙状态为正常，没添加至路由的防火墙状态为异常。防火墙策略或防火墙规则在防火墙使用过程中无法删除，必须先删除防火墙，再删除防火墙策略或防火墙规则。

[0033] 本发明不局限于上述实施方式，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也视为本发明的保护范围之内。本说明书中未作详细描述的内容属于本领域专业技术人员公知的现有技术。

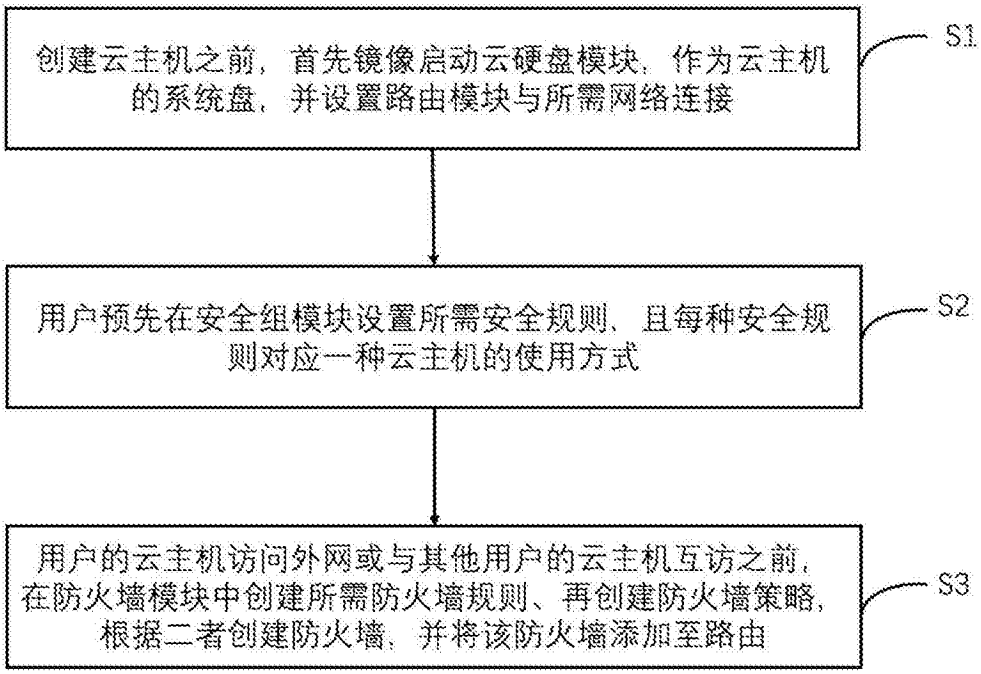

创建云主机之前，首先镜像启动云硬盘模块，作为云主机的系统盘，并设置路由模块与所需网络连接
S1
用户预先在安全组模块设置所需安全规则，且每种安全规则对应一种云主机的使用方式
S2
用户的云主机访问外网或与其他用户的云主机互访之前，在防火墙模块中创建所需防火墙规则、再创建防火墙策略，根据二者创建防火墙，并将该防火墙添加至路由
S3

图1