

一种面向云主机全流量网络访问防护的方法及装置

技术领域

本发明涉及云计算以及信息安全技术领域，具体涉及一种面向云主机全流量网络访问防护的方法及装置。

背景技术

防火墙是一个由计算机硬件和软件组成的系统，部署于网络边界，是内部网络和外部网络之间的连接桥梁，同时对进出网络边界的数据进行保护，防止恶意入侵、恶意代码的传播等，保障内部网络数据的安全。防火墙技术是建立在网络技术和信息安全技术基础上的应用性安全技术，几乎所有的企业内部网络与外部网络（如因特网）相连接的边界设都会放置防火墙，防火墙能够起到安全过滤和安全隔离外网攻击、入侵等有害的网络安全信息和行为。但是面对云主机，传统网络防火墙技术已经不满足网络安全的要求。

云主机是云计算在基础设施应用上的重要组成部分，位于云计算产业链金字塔底层，产品源自云计算平台。该平台整合了互联网应用三大核心要素：计算、存储、网络，面向用户提供公用化的互联网基础设施服务。云主机是一种类似VPS主机的虚拟化技术，VPS是采用虚拟软件，VZ或VM在一台主机上虚拟出多个类似独立主机的部分，能够实现单机多用户，每个部分都可以做单独的操作系统，管理方法同主机一样。而云主机是在一组集群主机上虚拟出多个类似独立主机的部分，集群中每个主机上都有云主机的一个镜像，从而大大提高了虚拟主机的安全稳定性。随着云主机的应用与发展，网络安全的问题也不容忽视，尤其是多台云主机之间的网络安全问题。

目前，通过云主机所在宿主机配置防火墙防护策略，可以满足部分云主机微隔离的需求，但无法完成细化策略和叠加策略的需求。传统云主机的南北向防护通过本地防火墙完成，对于普通非专业技术领域的云租户存在较高的技术要求。而且，云主机东西向和南北向流量的防护策略易存在冲突，东西向防护、南北向防护如果在配置过程中，针对同一类型或网络段区域进行相同配置时，会存在实际网络通路上的冲突。例如，云主机防护配置了允许10.18.*.*网段对80端口的访问请求，而东西向流量中只允许了10.19.*.*网段对80端口的访问，则会发生均无法访问的问题。多台云主机间相关东西向和南北向流量防护的策略查询、新建、修改、排错的操作繁琐且缺乏协同性，对云租户存在较高的专业技术要求。

发明内容

为解决传统防火墙技术不能满足现云主机的安全防护，传统云主机的南北向防护通过本地防火墙的专业技术性要求较高，云主机东西向和南北向流量的防护方式容易存在防护策略配置的冲突，以及多台云主机间相关的东西向和南北向流量的防护策略配置缺乏协同性、操作步骤繁琐等问题，本发明开发了一种面向云主机全流量网络访问防护的方法及装置。

本发明请求保护以下技术方案：

利用云计算服务编排技术，通过“自助交互式”的方式实现云计算平台与云主机操作系统主机防火墙和云计算虚拟化平台的分布式防火墙的无缝交互，完成云主机间的微隔离，达到自动化网络防护策略配置，支持区域的自动划分、默认规则的自动配置、自定义添加规则及其类型等操作。

云主机操作系统的防火墙负责管理南北向流量管理；在传统数据中心级别的传统三层防护下，通过自助式云主机防火墙的策略下发和配置应用，实现在云主机资源在东西向流量有效管控的同时，叠加一层南北向流量的防护力度。明确各防火墙功能定位，同时也能有效的解决防护策略易存在冲突的问题。

相关策略的的查询、新建、修改统一交由云平台管理，云租户可通过既定的流程进行相关策略的自主查询、申请、自动下发等操作，大幅简化了云租户的操作步骤，并提供了直观的查询界面，便于多设备间的策略的协同配置。

具体的：

本发明提供了一种面向云主机全流量网络访问防护的方法，其特征在于，所述全流量网络访问防护是指全流量的网络安全防护，包括：云主机防火墙、传统数据中心防火墙的南北向流量访问防护以及云计算平台的分布式防火墙的东西向流量访问防护；

所述的南北向流量访问防护是指：通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置实施的南北向流量访问防护，所述分别配置是指对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等方式的南北向流量访问防护策略的配置、自动调度及下发；

所述的東西向流量访问防护是指：根据云资源层面的异构云基础环境的网络协议，通过在云计算平台上建立支撑分布式防火墙的增强适配模块，并实现在云计算平台上对多云异构环境下的云主机进行东西向流量访问防护策略的统一配

置,进而实现东西向流量访问的防护;

通过在云计算平台上对所述东西向和所述南北向流量访问防护的入口的统一配置,结合云计算平台中云租户、云主机业务分组和预置的规则策略,实现所述的南北向流量访问防护和所述的東西向流量访问防护的无缝交互,进一步对全流量网络访问防护策略进行自动化配置,从而实现对单个或多云资源的全流量的网络访问的防护。

进一步的,包括以下步骤:

S1 建立分布式防火墙的响应规则,根据云资源层面的异构云基础环境的网络协议,在云计算平台的云主机上建立分布式防火墙的响应规则,通过获取的东西向流量访问防护策略的配置、自动调度及下发的命令后,自动实现对所述东西向流量访问防护;其中,所述分布式防火墙是预先在云计算平台上云资源层面,根据异构云基础环境的网络协议,通过增强适配模块来部署的支持异种网络的分布式防火墙;

S2 建立全流量防火墙的响应规则,通过云服务编排及自动化技术对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等的配置,建立所述南北向流量访问的响应规则;并同时通过对所述东西向和所述南北向防护的入口的统一配置,结合在云计算平台中云租户、云主机业务分组和预置的规则策略,实现所述东西向流量访问防护与所述南北向流量访问防护的双向流量防护策略的融合优化、自动划分、自动配置,进而建立所述全流量防火墙的响应规则;

S3 配置全流量防护策略,云租户根据需求在终端显示界面分别配置相关所述南北向流量访问防护策略或所述东西向流量访问防护策略,配置完成后,自动生成全流量网络访问防护策略需求订单;

S4 获取全流量防护策略需求并响应,基于云租户在云计算平台提交的所述全流量网络访问防护策略需求订单,云主机自动读取所述全流量网络访问防护策略,并根据读取的策略自动响应步骤 S1、S2 中的规则,通过不断获取步骤 S3 中的配置全流量防护策略,进行自适应配置、自动调度及下发命令,实现实时自动执行所述的全流量网络访问防护。

进一步的,在所述步骤 S4 获取全流量防护策略需求并响应中,所述自动执行,包括在未开启防火墙时,则自动开启。

进一步的,在所述步骤 S4 获取全流量防护策略需求并响应中,根据获取的

所述云租户统一在云平台进行的申请、审核，最终通过云服务编排和自动化技术，自动响应所述全流量网络访问防护策略的下发和生效，起到自动的防护能力；上述所有操作均有日志记录和查阅回溯，提供日后运维排错的定位用途。

本发明还提供了一种面向云主机的实现南北向流量访问防护的方法，其特征在于，通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的云主机防火墙进行配置实施的南北向流量访问防护，所述配置是指对云主机防火墙的入站出站策略的配置，进而实现南北向流量访问防护策略的配置、自动调度及下发；所述云主机防火墙的入站出站策略的配置对象包括：端口级别、协议级别、源 IP 及目标 IP 级别。

本发明还提供了另一种面向云主机的实现南北向流量访问防护的方法，其特征在于，通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置实施的南北向流量访问防护，所述分别配置是指对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的入站出站策略的配置，进而实现南北向流量访问防护策略的配置、自动调度及下发；所述云主机防火墙的入站出站策略的配置对象包括：端口级别、协议级别、源 IP 及目标 IP 级别。

本发明还提供了一种面向云主机的实现东西向流量访问防护的方法，其特征在于，所述的東西向流量访问防护是指：根据云资源层面的异构云基础环境的网络协议，通过在云计算平台上建立支撑分布式防火墙的增强适配模块，并实现在云计算平台上对多云异构环境下的云主机进行东西向流量访问防护策略的统一配置，进而实现东西向流量访问的防护。

进一步的，所述的防护的方法中，所述防护策略都支持云租户自定义。

进一步的，所述防护策略都支持云租户自定义包括，云租户根据需求在终端显示界面分别配置相关所述的访问防护策略，配置完成后，自动生成对应的所述的访问防护策略需求订单；由云计算平台获取所述防护策略订单，并自适应配置所述防护策略，以便进行实施对应的所述防护策略。

本发明还提供了一种面向云主机的全流量网络访问防护的装置，其特征在于，包括：

分布式防火墙的响应规则模块，用于根据云资源层面的异构云基础环境的网络协议，在云计算平台的云主机上建立分布式防火墙的响应规则，通过获取的东西向流量访问防护策略的配置、自动调度及下发的命令后，自动实现对所述东西

向流量访问防护；其中，所述分布式防火墙是预先在云计算平台上云资源层面，根据异构云基础环境的网络协议，通过增强适配模块来部署的支持异种网络的分布式防火墙；

全流量防火墙的响应规则模块，用于通过云服务编排及自动化技术对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等的配置，建立所述南北向流量访问的响应规则；并同时通过对所述东西向和所述南北向防护的入口的统一配置，结合在云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述东西向流量访问防护与所述南北向流量访问防护的双向流量防护策略的融合优化、自动划分、自动配置，进而建立所述全流量防火墙的响应规则；

配置全流量防护策略模块，用于云租户按需在终端显示界面分别配置相关所述南北向流量访问防护策略或所述东西向流量访问防护策略，并自动生成全流量网络访问防护策略需求订单；

获取全流量防护策略需求并响应模块，用于基于云租户在云计算平台提交的所述全流量网络访问防护策略需求订单，云主机自动读取所述全流量网络访问防护策略，并根据读取的策略所述通过分布式防火墙的响应规则模块与所述全流量防火墙的响应规则模块实现自动响应，通过不断获取所述配置全流量防护策略模块中的配置全流量防护策略，进行自动调度及下发命令，实现实时自动执行所述的全流量网络访问防护。

进一步的，所述配置全流量防护策略模块还包括：

显示子模块，用于在用户终端界面显示平台的交互式订单流程；

自助配置子模块，用于支持用户自定义配置，包括通过所述平台的交互式订单流程进行配置，实现自动下发、自主查询、历史记录查询等配置和操作。

本发明还提供了一种电子装置，其特征在于，该装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行所述的装置的配置程序系统，所述配置程序被所述处理器执行时可以实现所述防护的方法。

本发明还提供了一种计算机可读存储介质，其特征在于，所述计算机可读的存储介质上存储有所述装置的配置程序，所述配置程序可以被一个或多个处理器执行，以实现所述防护的方法。

与现有技术相比，本发明的优点在于：

由云平台统一纳管，实现交互式网络防护策略配置，支持区域自动划分、默认规则自动配置、自定义添加规则及其类型等操作。

通过操作系统防火墙，用户可进行更精确和更有针对性的南北向流量限制。

通过分布式防火墙提供东西向流量的网络通讯效率，管理更为高效，实现快速的网络安全策略配置和下发。

云租户可通过平台的交互式订单流程，实现配置自动下发、自主查询、历史记录查询等操作。优化对于云租户的操作体验，无需云租户进行复杂的操作也能进行防护策略的配置。

附图说明

图 1. 本发明提供的一种面向云主机全流量网络访问防护的方法步骤。

图 2. 本发明提供的一种面向云主机全流量网络访问防护的装置的配置程序模块图。

图 3. 本发明提供的另一种面向云主机全流量网络访问防护装置中的配置全流量防护策略的配置程序子模块图。

图 4. 本发明提供的另一种面向云主机全流量网络访问防护的具体流程图。

图 5. 本发明提供的第一种面向云主机的实现南北向流量访问防护的装置的配置程序图。

图 6. 本发明提供的第二种面向云主机的实现南北向流量访问防护的装置的配置程序图。

图 7. 本发明提供的一种面向云主机的实现东西向流量访问防护的装置的配置程序图。

具体实施方式

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应

该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统，产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

首先，在对本申请实施例进行描述的过程中出现的部分名词或术语适用于如下解释：

云服务编排技术是在云环境中部署服务的过程的端到端自动化。更具体地讲，它是复杂计算机系统、中间件和服务的自动化的安排、协调和管理——所有这些都有助于加速 IT 服务的交付，同时减少成本。它用于管理云基础架构，后者向客户提供和分配需要的云资源，比如创建虚拟机、分配存储容量、管理网络资源，以及授予云软件访问权。通过使用合适的编排机制，用户可在服务器上或任何云平台上部署和开始使用服务。

传统云主机的南北向防护通过本地防火墙完成，对于普通非专业技术领域的云租户存在较高的技术要求。而且，云主机东西向和南北向流量的防护策略易存在冲突，东西向防护、南北向防护如果在配置过程中，针对同一类型或网络段区域进行相同配置时，会存在实际网络通路上的冲突。例如，云主机防护配置了允许10.18.*.* 网段对80端口的访问请求，而东西向流量中只允许了10.19.*.* 网段对80端口的访问，则会发生均无法访问的问题。本发明通过云计算服务编排技术和自动化技术实现了全流量的网络访问的防护，有效的避免了上述问题。

为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明做详细说明。

本发明提供了一种面向云主机全流量网络访问防护的方法，其中，所述全流量网络访问防护是指全流量的网络安全防护，包括：云主机防火墙、传统数据中心防火墙的南北向流量访问防护以及云计算平台的分布式防火墙的东西向流量访问防护。

在本实施例中，这里的云主机防火墙是指现有技术中云主机操作系统防火墙。云主机操作系统的防火墙负责管理南北向流量管理；在传统数据中心级别的传统三层防护下，通过自助式云主机防火墙的策略下发和配置应用，实现在云主机资源在东西向流量有效管控的同时，叠加一层南北向流量的防护力度。明确各防火

墙功能定位，同时也能有效的解决防护策略易存在冲突的问题。

所述的南北向流量访问防护是指：通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置实施的南北向流量访问防护，所述分别配置是指对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等方式的南北向流量访问防护策略的配置、自动调度及下发，并支持云租户自定义。

在本实施例中，所述共同配置也是指对传统数据中心防火墙入站出站策略的配置、自动调度及下发，并支持云租户自定义；这里指的云租户不限于企业、个人用户，这里的自定义是指云租户根据自身需求设置有所系统提供的终端显示界面上的自定义的配置。

所述的東西向流量访问防护是指：根据云资源层面的异构云基础环境的网络协议，通过在云计算平台上建立支撑分布式防火墙的增强适配模块，并实现在云计算平台上对多云异构环境下的云主机进行东西向流量访问防护策略的统一配置，进而实现东西向流量访问的防护；

在本实施例中，东西向流量访问防护策略的配置包括：对云计算平台上的多云异构环境下的云主机，进行统一的東西向流量的防护策略配置；且通过与云计算平台中云租户、云主机业务分组等深度融合，实现基于云资源开设交付、业务组变更、资源回收消亡等全生命周期下的策略自动配置和下发生效。

通过在云计算平台上对所述东西向和所述南北向流量访问防护的入口的统一配置，结合云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述的南北向流量访问防护和所述的東西向流量访问防护的无缝交互，进一步对全流量网络访问防护策略进行自动化配置，从而实现对单个或多云资源的全流量的网络访问的防护。

在本实施例中，东西向流量主要负责云主机业务系统层的对外策略配置、南北向流量主要负责云主机单体对外的策略防护。

图 1 是本发明提供的一种面向云主机全流量网络访问防护的方法步骤。

如图 1 所示，本实施例展示的一种面向云主机的全流量网络访问防护的方法，其中包括以下步骤：

S1 建立分布式防火墙的响应规则，根据云资源层面的异构云基础环境的网络协议，在云计算平台的云主机上建立分布式防火墙的响应规则，通过获取的东

西向流量访问防护策略的配置、自动调度及下发的命令后，自动实现对所述东西向流量访问防护；其中，所述分布式防火墙是预先在云计算平台上云资源层面，根据异构云基础环境的网络协议，通过增强适配模块来部署的支持异种网络的分布式防火墙。

S2 建立全流量防火墙的响应规则，通过云服务编排及自动化技术对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等的配置，建立所述南北向流量访问的响应规则；并同时通过对所述东西向和所述南北向防护的入口的统一配置，结合在云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述东西向流量访问防护与所述南北向流量访问防护的双向流量防护策略的融合优化、自动划分、自动配置，进而建立所述全流量防火墙的响应规则。

S3 配置全流量防护策略，云租户根据需求在终端显示界面分别配置相关所述南北向流量访问防护策略或所述东西向流量访问防护策略，配置完成后，自动生成全流量网络访问防护策略需求订单。

在本实施例中，具体包括将云主机对应的预设防护策略生成表单显示与云租户终端界面，以供云租户按需填写相关南北向流量访问防护策略；将云主机对应的工作空间中预设防护策略生成相应的条目，以供云租户按需填写相关东西向流量访问防护策略；并自动生成全流量网络访问防护策略需求订单。

S4 获取全流量防护策略需求并响应，基于云租户在云计算平台提交的所述全流量网络访问防护策略需求订单，云主机自动读取所述全流量网络访问防护策略，并根据读取的策略自动响应步骤 S1、S2 中的规则，通过不断获取步骤 S3 中的配置全流量防护策略，进行自适应配置、自动调度及下发命令，实现实时自动执行所述的全流量网络访问防护。

在本实施例中，在所述步骤 S4 获取全流量防护策略需求并响应中，所述自动执行，包括在未开启防火墙时，则自动开启。

在本实施例中，在所述步骤 S4 获取全流量防护策略需求并响应中，根据获取的所述云租户统一在云平台进行的申请、审核，最终通过云服务编排和自动化技术，自动响应所述全流量网络访问防护策略的下发和生效，起到自动的防护能力；所有操作均有日志记录和查阅回溯，提供日后运维排错的定位用途。

在本实施例中，所述全流量网络访问防护均采用规则访问控制，不仅局限于访问的防护，实际上还包括，在策略配置中可以与云计算平台的威胁情报库做了

互动，将恶意的一些黑名单ip作为拦截策略防护。

图2 本发明提供的第一种面向云主机全流量网络访问防护的装置的配置程序模块图。

如图2所示，一种面向云主机的全流量网络访问防护的装置，其中，包括：

分布式防火墙的响应规则模块101，用于用于根据云资源层面的异构云基础环境的网络协议，在云计算平台的云主机上建立分布式防火墙的响应规则，通过获取的东西向流量访问防护策略的配置、自动调度及下发的命令后，自动实现对所述东西向流量访问防护；其中，所述分布式防火墙是预先在云计算平台上云资源层面，根据异构云基础环境的网络协议，通过增强适配模块来部署的支持异种网络的分布式防火墙。

全流量防火墙的响应规则模块102，用于通过云服务编排及自动化技术对传统数据中心防火墙所开放的api接口以及对云主机防火墙的端口级别、协议级别、源IP及目标IP级别等的配置，建立所述南北向流量访问的响应规则；并同时通过对所述东西向和所述南北向防护的入口的统一配置，结合在云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述东西向流量访问防护与所述南北向流量访问防护的双向流量防护策略的融合优化、自动划分、自动配置，进而建立所述全流量防火墙的响应规则。

配置全流量防护策略模块103，用于云租户按需在终端显示界面分别配置相关所述南北向流量访问防护策略或所述东西向流量访问防护策略，并自动生成全流量网络访问防护策略需求订单。

获取全流量防护策略需求并响应模块104，用于基于云租户在云计算平台提交的所述全流量网络访问防护策略需求订单，云主机自动读取所述全流量网络访问防护策略，并根据读取的策略所述通过分布式防火墙的响应规则模块与所述全流量防火墙的响应规则模块实现自动响应，通过不断获取所述配置全流量防护策略模块中的配置全流量防护策略，进行自动调度及下发命令，实现实时自动执行所述的全流量网络访问防护。

图3 是本发明提供的另一种面向云主机全流量网络访问防护装置中的配置全流量防护策略的配置程序子模块图。

进一步的，如图3所示，本发明提供的另一种面向云主机全流量网络访问防护装置中，所述配置全流量防护策略模块103还包括：

显示子模块1031，用于在用户终端界面显示平台的交互式订单流程；

自助配置子模块 1032，用于支持用户自定义配置，包括平台的交互式订单流程；所述云租户可通过平台的交互式订单流程，实现配置自动下发、自主查询、历史记录查询等操作；所述云租户确定云主机南北向流量访问防护后，再确定目标云主机，并按照预设表单填写相关策略；或/和，所述云租户确定云主机东西向流量访问防护后，再确定目标工作空间，并按照预设表单填写相关策略。

在本实施例中，所述云租户确定云主机南北向流量访问防护后，再确定目标云主机，并按照预设表单填写相关策略；或/和，所述云租户确定云主机东西向流量访问防护后，再确定目标工作空间，并按照预设表单填写相关策略。

具体的，云主机对应的预设防护策略生成表单显示与云租户终端界面，以供云租户按需填写相关南北向流量访问防护策略；将云主机对应的工作空间中预设防护策略生成相应的条目，以供云租户按需填写相关东西向流量访问防护策略；并自动生成全流量网络访问防护策略需求订单。

进一步的，所述自助配置子模块 1032 还支持所有操作均有日志记录和查阅回溯，提供日后运维排错的定位用途；查询入口设置在所述交互式订单流程中。

图 4 是本发明提供的另一种面向云主机全流量网络访问防护的具体流程图。

如图 4 所示，全流量的防护由以下流程步骤实现：通过配置全流量防护策略模块 103，云租户可以在客户端发起申请，在显示界面自主选择并确定云主机的全流量访问防护订单需求，具体包括：在确定云主机南北向流量防护时，云租户选择目标云主机，按照预设表单填写相关策略；在确定云主机东西向流量防护时，云租户选择目标工作空间，按照预设条目填写相关策略需求。

在确定云主机的全流量访问防护订单需求之后，直接提交云租户订单需求至云计算平台，云计算平台会根据用户提交的订单自动进行全流量需求适配。

进一步的，在全流量需求适配过程中，系统会首先确认全流量需求中的流量防护类型，如果是南北向流量防护则继续调用云主机防火墙或/和传统数据中心防火墙，并基于云租户需求，由云计算平台获取所述防护策略，并自适应配置相应安全防护策略；如果是东西向流量防护，则调用已配置的分布式防火墙，并基于云租户需求，由云计算平台获取所述防护策略，并自适应配置相应安全防护策略；之后，自适应配置后的双向流量防护（东西向以及南北向）策略进行经过建立分布式防火墙的响应规则模块 101 与建立全流量防火墙的响应规则模块 102 实现自动响应，获取全流量防护策略需求并响应模块 104 下发策略并执行，进而实现对云主机的全流量网络访问的防护。

除了上述实现全流量网络访问防护的方法之外，本发明同样的通过利用云计算自动化技术或利用云计算服务编排技术，还提供了另外两种实现南北向流量访问防护的方法；其中，

第一种是：一种面向云主机的实现南北向流量访问防护的方法，其中，通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的云主机防火墙进行配置实施的南北向流量访问防护，所述配置是指对云主机防火墙的入站出站策略的配置，进而实现南北向流量访问防护策略的配置、自动调度及下发；所述云主机防火墙的入站出站策略的配置对象包括：端口级别、协议级别、源 IP 及目标 IP 级别。

如图 5 所示，是本发明提供的第一种面向云主机的实现南北向流量访问防护的装置的配置程序图。其中：

云主机防火墙的配置模块 201：用于通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的云主机防火墙的入站出站策略进行配置；

自适配响应模块 202：用于在云计算平台建立云主机防火墙的自适配响应规则，实现所述南北向流量访问防护策略自动适配、自动调度与下发；

配置防护策略模块 203：用于云租户根据需求在终端显示界面配置相关所述南北向流量访问防护策略，配置完成后，自动生成所述南北向防护策略需求订单；

获取防护策略并响应模块 204：用于基于云租户在云计算平台提交的所述访问防护策略需求订单，云主机自动读取所述访问防护策略，并根据读取的策略自动响应自适配规则，通过不断获取配置防护策略模块中的策略，进行自适应配置、自动调度及下发命令，实现实时自动执行所述南北向流量访问防护。

第二种是：另一种面向云主机的实现南北向流量访问防护的方法，其中，通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置实施的南北向流量访问防护，所述分别配置是指对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的入站出站策略的配置，进而实现南北向流量访问防护策略的配置、自动调度及下发；所述云主机防火墙的入站出站策略的配置对象包括：端口级别、协议级别、源 IP 及目标 IP 级别。

如图 6 所示，是本发明提供的第二种面向云主机的实现南北向流量访问防护的装置的配置程序图。其中：

防火墙的配置模块 301：用于通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置；

自适应响应模块 302：用于在云计算平台建立云主机防火墙的自适应响应规则，实现所述南北向流量访问防护策略自动适配、自动调度与下发；

配置防护策略模块 303：用于云租户根据需求在终端显示界面配置相关所述南北向流量访问防护策略，配置完成后，自动生成所述南北向访问防护策略需求订单；

获取防护策略并响应模块 304：用于基于云租户在云计算平台提交的所述访问防护策略需求订单，云主机自动读取所述访问防护策略，并根据读取的策略自动响应自适应规则，通过不断获取配置防护策略模块中的策略，进行自适应配置、自动调度及下发命令，实现实时自动执行所述南北向流量访问防护。

除了上述实现全流量网络访问防护的方法之外，本发明同样的通过利用云计算自动化技术或利用云计算服务编排技术，还提供了一种面向云主机的实现东西向流量访问防护的方法，其中，所述的东西向流量访问防护是指：根据云资源层面的异构云基础环境的网络协议，通过在云计算平台上建立支撑分布式防火墙的增强适配模块，并实现在云计算平台上对多云异构环境下的云主机进行东西向流量访问防护策略的统一配置，进而实现东西向流量访问的防护。

如图 7 所示是本发明提供的一种面向云主机的实现东西向流量访问防护的装置的配置程序图。其中：

分布式防火墙的响应规则模块 401：用于根据云资源层面的异构云基础环境的网络协议，在云计算平台的云主机上建立分布式防火墙的响应规则，通过获取的东西向流量访问防护策略的配置、自动调度及下发的命令后，自动实现对所述东西向流量访问防护；其中，所述分布式防火墙是预先在云计算平台上云资源层面，根据异构云基础环境的网络协议，通过增强适配模块来部署的支持异种网络的分布式防火墙；

自适应响应模块 402：用于在云计算平台建立云主机防火墙的自适应响应规则，实现所述东西向流量访问防护策略自动适配、自动调度与下发；

配置防护策略模块 403：用于云租户根据需求在终端显示界面配置相关所述东西向流量访问防护策略，配置完成后，自动生成所述东西向访问防护策略需求订单；

获取防护策略并响应模块 404：用于基于云租户在云计算平台提交的所述访问防护策略需求订单，云主机自动读取所述访问防护策略，并根据读取的策略自动响应自适应规则，通过不断获取配置防护策略模块中的策略，进行自适应配置、自动调度及下发命令，实现实时自动执行所述东西向流量访问防护。

进一步的，以上两种实现南北向流量访问防护的方法以及一种实现东西向流量访问防护的方法中，所述防护策略都支持云租户自定义，包括用户可以自定义配置所述防护策略后，由云计算平台获取所述防护策略，并自适应配置所述防护策略，以便进行实施对应的所述防护策略。

进一步的，所述自动执行，包括在未开启防火墙时，则自动开启。

进一步的，在获取策略需求并响应步骤中，根据获取的所述云租户统一在云平台进行的申请、审核，最终通过云服务编排和自动化技术，自动响应所述访问防护策略的下发和生效，起到自动的防护能力；上述所有操作均有日志记录和查阅回溯，提供日后运维排错的定位用途。

在本实施例中还包括一种电子装置，该装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行如本实施例提供的一种面向云主机全流量网络访问防护装置的配置程序系统，所述配置程序被所述处理器执行时可以实现如本实施例所述的一种面向云主机全流量网络访问防护方法。

在本实施例中还包括一种计算机可读存储介质，所述计算机可读的存储介质上存储有如本实施例提供的一种面向云主机全流量网络访问防护装置的配置程序，所述配置程序可以被一个或多个处理器执行，以实现如本实施例所述的一种面向云主机全流量网络访问防护方法。

以上所述仅是本发明的优选实施方式，应当指出，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，这些改进和润饰也应视为本发明的保护范围。

权利要求书

1、一种面向云主机全流量网络访问防护的方法，其特征在于，所述全流量网络访问防护是指全流量的网络安全防护，包括：云主机防火墙、传统数据中心防火墙的南北向流量访问防护以及云计算平台的分布式防火墙的东西向流量访问防护；

所述的南北向流量访问防护是指：通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置实施的南北向流量访问防护，所述分别配置是指对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等方式的南北向流量访问防护策略的配置、自动调度及下发；

所述的東西向流量访问防护是指：根据云资源层面的异构云基础环境的网络协议，通过在云计算平台上建立支撑分布式防火墙的增强适配模块，并实现在云计算平台上对多云异构环境下的云主机进行东西向流量访问防护策略的统一配置，进而实现东西向流量访问的防护；

通过在云计算平台上对所述东西向和所述南北向流量访问防护的入口的统一配置，结合云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述的南北向流量访问防护和所述的東西向流量访问防护的无缝交互，进一步对全流量网络访问防护策略进行自动化配置，从而实现对单个或多云资源的全流量的网络访问的防护。

2、根据权利要求 1 所述的全流量网络访问防护的方法，其特征还在于，包括以下步骤：

S1 建立分布式防火墙的响应规则，根据云资源层面的异构云基础环境的网络协议，在云计算平台的云主机上建立分布式防火墙的响应规则，通过获取的东西向流量访问防护策略的配置、自动调度及下发的命令后，自动实现对所述东西向流量访问防护；其中，所述分布式防火墙是预先在云计算平台上云资源层面，根据异构云基础环境的网络协议，通过增强适配模块来部署的支持异种网络的分布式防火墙；

S2 建立全流量防火墙的响应规则，通过云服务编排及自动化技术对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等的配置，建立所述南北向流量访问的响应规则；并同时通过对所述东西向和所述南北向防护的入口的统一配置，结合在云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述东西向流量访问防护与所述南北向流量访问防护的双向流量防护策略的融合优化、自动划分、自动配置，进而建立所述全流量防火墙的响应规则；

S3 配置全流量防护策略，云租户根据需求在终端显示界面分别配置相关所述南北向流量访问防护策略或所述东西向流量访问防护策略，配置完成后，自动生成全流量网络访问防护策略需求订单；

S4 获取全流量防护策略需求并响应，基于云租户在云计算平台提交的所述全流量网络访问防护策略需求订单，云主机自动读取所述全流量网络访问防护策略，并根据读取的策略自

动响应步骤 S1、S2 中的规则，通过不断获取步骤 S3 中的配置全流量防护策略，进行自适应配置、自动调度及下发命令，实现实时自动执行所述的全流量网络访问防护。

3、根据权利要求 1 或 2 所述的全流量网络访问防护的方法，其特征还在于，

在所述步骤 S4 获取全流量防护策略需求并响应中，所述自动执行，包括在未开启防火墙时，则自动开启。

4、根据权利要求 1 或 2 或 3 所述的全流量网络访问防护的方法，其特征还在于，在所述步骤 S4 获取全流量防护策略需求并响应中，根据获取的所述云租户统一在云平台进行的申请、审核，最终通过云服务编排和自动化技术，自动响应所述全流量网络访问防护策略的下发和生效，起到自动的防护能力；上述所有操作均有日志记录和查阅回溯，提供日后运维排错的定位用途。

5、一种面向云主机的实现南北向流量访问防护的方法，其特征在于，通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的云主机防火墙进行配置实施的南北向流量访问防护，所述配置是指对云主机防火墙的入站出站策略的配置，进而实现南北向流量访问防护策略的配置、自动调度及下发；所述云主机防火墙的入站出站策略的配置对象包括：端口级别、协议级别、源 IP 及目标 IP 级别。

6、另一种面向云主机的实现南北向流量访问防护的方法，其特征在于，通过利用云计算自动化技术对单个或利用云计算服务编排技术对一组业务系统的云资源的传统数据中心防火墙及云主机防火墙进行分别配置实施的南北向流量访问防护，所述分别配置是指对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的入站出站策略的配置，进而实现南北向流量访问防护策略的配置、自动调度及下发；所述云主机防火墙的入站出站策略的配置对象包括：端口级别、协议级别、源 IP 及目标 IP 级别。

7、一种面向云主机的实现东西向流量访问防护的方法，其特征在于，所述的東西向流量访问防护是指：根据云资源层面的异构云基础环境的网络协议，通过在云计算平台上建立支撑分布式防火墙的增强适配模块，并实现在云计算平台上对多云异构环境下的云主机进行东西向流量访问防护策略的统一配置，进而实现东西向流量访问的防护。

8、根据权利要求 1-7 任一项所述的防护的方法，其特征还在于，所述防护策略都支持云租户自定义。

9、根据权利要求 8 所述的防护的方法，其特征还在于，所述防护策略都支持云租户自定义包括，云租户根据需求在终端显示界面分别配置相关所述的访问防护策略，配置完成后，自动生成对应的所述的访问防护策略需求订单；由云计算平台获取所述防护策略订单，并自适应配置所述防护策略，以便进行实施对应的所述防护策略。

10、一种面向云主机的全流量网络访问防护的装置，其特征在于，包括：

分布式防火墙的响应规则模块，用于根据云资源层面的异构云基础环境的网络协议，在云计算平台的云主机上建立分布式防火墙的响应规则，通过获取的东西向流量访问防护策略的配置、自动调度及下发的命令后，自动实现对所述东西向流量访问防护；其中，所述分布式防火墙是预先在云计算平台上云资源层面，根据异构云基础环境的网络协议，通过增强适配模块来部署的支持异种网络的分布式防火墙；

全流量防火墙的响应规则模块，用于通过云服务编排及自动化技术对传统数据中心防火墙所开放的 api 接口以及对云主机防火墙的端口级别、协议级别、源 IP 及目标 IP 级别等的配置，建立所述南北向流量访问的响应规则；并同时通过对所述东西向和所述南北向防护的入口的统一配置，结合在云计算平台中云租户、云主机业务分组和预置的规则策略，实现所述东西向流量访问防护与所述南北向流量访问防护的双向流量防护策略的融合优化、自动划分、自动配置，进而建立所述全流量防火墙的响应规则；

配置全流量防护策略模块，用于云租户按需在终端显示界面分别配置相关所述南北向流量访问防护策略或所述东西向流量访问防护策略，并自动生成全流量网络访问防护策略需求订单；

获取全流量防护策略需求并响应模块，用于基于云租户在云计算平台提交的所述全流量网络访问防护策略需求订单，云主机自动读取所述全流量网络访问防护策略，并根据读取的策略所述通过分布式防火墙的响应规则模块与所述全流量防火墙的响应规则模块实现自动响应，通过不断获取所述配置全流量防护策略模块中的配置全流量防护策略，进行自动调度及下发命令，实现实时自动执行所述的全流量网络访问防护。

11、根据权利要求 10 所述的全流量网络访问防护的装置，其特征在于，

所述配置全流量防护策略模块还包括：

显示子模块，用于在用户终端界面显示平台的交互式订单流程；

自助配置子模块，用于支持用户自定义配置，包括通过所述平台的交互式订单流程进行配置，实现自动下发、自主查询、历史记录查询等配置和操作。

12、一种电子装置，其特征在于，该装置包括存储器、处理器，所述存储器上存储有可在所述处理器上运行如权利要求10-11所述的装置的配置程序系统，所述配置程序被所述处理器执行时可以实现如权利要求1-9所述防护的方法。

13、一种计算机可读存储介质，其特征在于，所述计算机可读的存储介质上存储有如权利要求10-11所述装置的配置程序，所述配置程序可以被一个或多个处理器执行，以实现如权利要求1-9所述防护的方法。