(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110677383 B
(45)授权公告日 2023.02.24

(21)申请号 201910780197.8

(22)申请日 2019.08.22

(65)同一申请的已公布的文献号
申请公布号 CN 110677383 A

(43)申请公布日 2020.01.10

(73)专利权人 平安科技(深圳)有限公司
地址 518000 广东省深圳市福田街道福安社区益田路5033号平安金融中心23楼

(72)发明人 池红露

(74)专利代理机构 北京中强智尚知识产权代理有限公司 11448
专利代理师 黄耀威 李月

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 104580078 A,2015.04.29
CN 104580078 A,2015.04.29
CN 109688093 A,2019.04.26
CN 103561002 A,2014.02.05

审查员 周萍

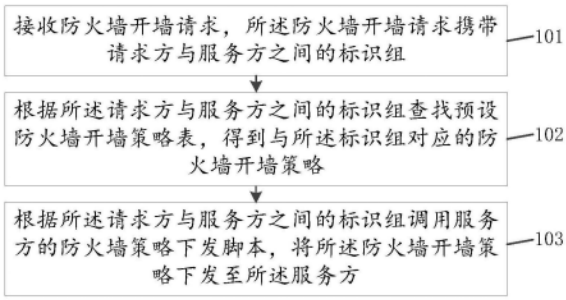
权利要求书2页 说明书7页 附图3页

(54)发明名称

防火墙开墙方法、装置、存储介质及计算机设备

(57)摘要

本发明公开了一种防火墙开墙方法、装置、存储介质及计算机设备，主要在于能够缩短不同服务间的架构变更周期，提高架构变更效率，节省大量人力和时间。所述方法包括：接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略，所述预设防火墙开墙策略表中存储有请求方与服务方之间的标识组及其对应的防火开墙策略；根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方。本发明适用于防火墙策略的下发。



CN 110677383 B

1.一种防火墙开墙方法,其特征在于,包括:

接收防火墙开墙请求,所述防火墙开墙请求携带请求方与服务方之间的标识组;

根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略;

根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方;

其中,开墙发起人员向防火墙管理平台发起开墙请求之前,所述开墙发起人员会在所述防火墙管理平台上预先填写所述请求方和所述服务方之间的开墙信息,评审人员会对所述开墙信息进行架构评审,评审通过后,所述请求方与所述服务方之间的所述开墙信息会自动录入至所述防火墙管理平台,将所述开墙信息确定为所述请求方与所述服务方之间的所述防火墙开墙策略。

2.根据权利要求1所述的方法,其特征在于,所述根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方包括:

根据所述请求方与服务方之间的标识组,利用SSH远程协议调用服务方的防火墙策略下发脚本,将所述防火墙策略下发至所述服务方。

3.根据权利要求2所述的方法,所述根据所述请求方与服务方之间的标识组,利用SSH远程协议调用服务方的防火墙策略下发脚本,将所述防火墙策略下发至所述服务方包括:

根据所述请求方与服务方之间的标识组,利用SSH远程协议将所述防火墙策略中的开墙参数传递至所述服务方的防火墙策略下发脚本,生成防火墙策略下发指令;

调用所述防火墙策略下发指令,将所述防火墙策略下发至所述服务方。

4.根据权利要求3所述的方法,其特征在于,在所述根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方之后,所述方法还包括:

根据所述请求方与服务方之间的标识组调用请求方的防火墙验墙脚本,验证所述请求方与所述服务方之间是否开墙成功。

5.根据权利要求4所述的方法,其特征在于,所述根据所述请求方与服务方之间的标识组调用请求方的防火墙验墙脚本,验证所述请求方与所述服务方之间是否开墙成功包括:

根据所述请求方与服务方之间的标识组,利用SSH远程协议调用请求方的防火墙验墙脚本,验证所述请求方与所述服务方之间是否开墙成功。

6.根据权利要求5所述的方法,其特征在于,所述根据所述请求方与服务方之间的标识组,利用SSH远程协议调用请求方的防火墙脚本,验证所述请求方与所述服务方之间是否开墙成功包括:

接收所述服务方发送的防火墙策略下发完成信息,所述防火墙策略下发完成信息包括所述开墙参数;

根据所述请求方与服务方之间的标识组,利用SSH远程协议将所述开墙参数传递至所述请求方的防火墙验墙脚本,生成防火墙验墙指令;

调用所述防火墙验墙指令,验证所述请求方与所述服务方之间是否开墙成功。

7.根据权利要求4-6任一项所述的方法,其特征在于,在所述根据所述请求方与服务方之间的标识组调用请求方的防火墙验墙脚本,验证所述请求方与所述服务方之间是否开墙

成功之后，所述方法还包括：

接收所述请求方反馈的防火墙验墙状态，并将所述防火墙验墙状态发送至防火墙开墙发起方。

8.一种防火墙开墙装置，其特征在于，包括：

接收单元，用于接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；

查找单元，用于根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略，所述预设防火墙开墙策略表中存储有请求方与服务方之间的标识组及其对应的防火开墙策略；

调用单元，用于根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方；

其中，开墙发起人员向防火墙管理平台发起开墙请求之前，所述开墙发起人员会在所述防火墙管理平台上预先填写所述请求方和所述服务方之间的开墙信息，评审人员会对所述开墙信息进行架构评审，评审通过后，所述请求方与所述服务方之间的所述开墙信息会自动录入至所述防火墙管理平台，将所述开墙信息确定为所述请求方与所述服务方之间的所述防火墙开墙策略。

9.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

10.一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至7中任一项所述的方法的步骤。

防火墙开墙方法、装置、存储介质及计算机设备

技术领域

[0001] 本发明涉及信息技术领域，尤其是涉及一种防火墙开墙方法、装置、存储介质及计算机设备。

背景技术

[0002] 微服务作为一项在云中部署应用和服务的新技术已成为当下最热门的技术，微服务在实际的应用中关联的组件很多，相关的业务关联也越来越多，例如，微服务的授权，微服务的注册发现，微服务的监控，微服务的配置管理等都需要与外部服务进行相互联系，为了确保不同服务之间相互关联的安全性，需要在不同服务之间进行开墙、验墙等一系列操作。

[0003] 目前，不同服务之间进行相互关联时，都是通过人为来进行开墙和验墙等操作，例如，首先由开墙发起人员发起架构变更请求，之后由各个系统的关联方进行审核，审核通过后，开墙发起人员会发起开墙申请，接着由安全人员进行评审，评审通过后开墙人员进行防火墙策略下发，最终由运维人员验证是否通过，然而，通过人为的方式来进行开墙和验墙等操作，会耗费大量人力和时间，从而造成架构变更周期较长，导致架构变更效率低下。

发明内容

[0004] 本发明提供了一种防火墙开墙方法、装置、存储介质及计算机设备，主要在于能够缩短不同服务间的架构变更周期，提高架构变更效率，节省大量人力和时间。

[0005] 根据本发明的第一个方面，提供一种防火墙开墙方法，包括：

[0006] 接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；

[0007] 根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略；

[0008] 根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方。

[0009] 根据本发明的第二个方面，提供一种防火墙开墙装置，包括：

[0010] 接收单元，用于接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；

[0011] 查找单元，用于根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略；

[0012] 调用单元，用于根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方。

[0013] 根据本发明的第三个方面，提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现以下步骤：

[0014] 接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；

[0015] 根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述

标识组对应的防火墙开墙策略；

[0016] 根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方。

[0017] 根据本发明的第四个方面，提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现以下步骤：

[0018] 接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；

[0019] 根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略；

[0020] 根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方。

[0021] 本发明提供的一种防火墙开墙方法、装置、存储介质及计算机设备，与目前通过人为的方式来进行防火墙的开墙和验墙相比，本发明能够接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；并根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略；与此同时，根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方，从而能够缩短不同服务间的架构变更周期，提高不同服务间的架构变更效率，实现了防火墙策略的自动下发和自动验墙，节省大量人力和时间。

附图说明

[0022] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0023] 图1示出了本发明实施例提供的一种防火墙开墙方法流程图；

[0024] 图2示出了本发明实施例提供的另一种防火墙开墙方法流程图；

[0025] 图3示出了本发明实施例提供的一种防火墙开墙装置的结构示意图；

[0026] 图4示出了本发明实施例提供的另一种防火墙开墙装置的结构示意图；

[0027] 图5示出了本发明实施例提供的一种计算机设备的实体结构示意图。

具体实施方式

[0028] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0029] 如背景技术，目前，不同服务之间进行相互关联时，都是通过人为来进行开墙和验墙等操作，例如，首先由开墙发起人员发起架构变更请求，之后由各个系统的关联方进行审核，审核通过后，开墙发起人员会发起开墙申请，接着由安全人员进行评审，评审通过后开墙人员进行防火墙策略下发，最终由运维人员验证是否通过，然而，通过人为的方式来进行开墙和验墙等操作，会耗费大量人力和时间，从而造成架构变更周期较长，导致架构变更效率低下。

[0030] 为了解决上述问题，本发明实施例提供了一种防火墙开墙方法，如图1所示，所述方法包括：

[0031] 101、接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识

组。

[0032] 其中，请求方与服务方之间的标识组为请求方标识和服务方标识的组合，请求方与服务方为进行开墙操作的双方，请求方标识和服务方标识可以为请求方的IP地址和服务方的IP地址，此外，本发明实施例主要应用于防火墙管理平台，对于本发明实施例，开墙发起人员向防火墙管理平台发起开墙请求之前，开墙发起人员会在防火墙管理平台上预先填写请求方和服务方之间的开墙信息，例如，请求方的计算机A要访问服务方的计算机B的端口21，端口22和端口23，开墙发起人员将该开墙信息填写至防火墙管理平台，开墙信息具体包括请求方计算机A的IP地址，服务方计算机B的IP地址，计算机A要访问计算机B的端口21，端口22，端口23的端口信息，以及请求方计算机A的IP和服务方计算机B的IP分别属于哪个逻辑实体等，例如，计算机A的IP属于A系统，计算机B的IP属于B系统，之后评审人员会对开墙信息进行架构评审，即评审计算机A访问计算机B的端口21，端口22和端口23是否安全，评审通过后，请求方与服务方之间的开墙信息会自动录入至防火墙管理平台，即防火墙管理平台存储计算机A与计算机B之间的开墙信息。

[0033] 进一步地，架构评审通过后，评审人员会向防火墙管理平台发送防火墙开墙申请，该防火墙开墙申请携带请求方与服务方之间的标识组，例如，请求方的计算机A要访问服务方的计算机B的端口21，该请求方与服务方之间的标识组为计算机A的IP地址-计算机B的IP地址，根据该请求方与服务方之间的标识组可以进一步查找预设防火墙开墙策略表。

[0034] 102、根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略。

[0035] 其中，所述预设防火墙开墙策略表中存储有请求方与服务方之间的标识组及其对应的防火开墙策略，对于本发明实施例，在评审通过后，请求方与服务方之间的开墙信息会自动录入至防火墙管理平台，例如，请求方的计算机A要访问服务方的计算机B的端口21，端口22和端口23，开墙信息具体包括请求方计算机A的IP地址，服务方计算机B的IP地址，计算机A要访问计算机B的端口21，端口22，端口23的端口信息，将该开墙信息确定为请求方与服务方之间的防火墙开墙策略，并将请求方与服务方之间的标识组与防火墙开墙策略对应存储至预设防火墙开墙策略表，通过请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与该请求方与服务方之间的标识组对应的防火墙开墙策略。

[0036] 103、根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方。

[0037] 对于本发明实施例，根据请求方与服务方之间的标识组，确定服务方标识，根据该服务方标识，使用SSH协议远程调用相应服务方的防火墙策略下发脚本，例如，查找的请求方与服务方之间的防火墙开墙策略为允许计算机A访问计算机B的端口21，端口22和端口23，防火墙管理平台通过SSH协议远程调用服务方计算机B的防火墙策略下发脚本，例如，远程命令为sshnick@192.168.171.147<test.sh，其中，test.sh为计算机B的脚本文件，在使用远程指令调用服务方的防火墙策略下发脚本的同时，将请求方的IP地址和请求方要访问服务方的哪些端口参数传递给服务方的脚本，之后服务方的防火墙策略下发脚本调用iptable指令，并将请求方的IP地址和将要访问服务方的端口信息传递给iptable指令，由此生成防火墙开墙指令，例如，允许请求方的计算机A访问服务方的计算机B的22号端口，计算机A的IP地址为172.16.0.0/16，计算机B的IP地址为172.16.100.1，生成的防火墙开墙指

令为iptables-t filter-A INPUT-s 172.16.0.0/16-d 172.16.100.1-p tcp-dport 22-j,进一步地,只要去调用该指令,就会下发相关的开墙配置,即把相关的信息存储到linux系统的防火墙配置文件里,就实现了请求方与服务方之间的开墙操作。

[0038] 本发明实施例提供的一种防火墙开墙方法,与目前通过人为的方式来进行防火墙的开墙和验墙相比,本发明能够接收防火墙开墙请求,所述防火墙开墙请求携带请求方与服务方之间的标识组;并根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略;与此同时,根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方,从而能够缩短不同服务间的架构变更周期,提高不同服务间的架构变更效率,实现了防火墙策略的自动下发和自动验墙,节省大量人力和时间。

[0039] 进一步的,为了更好的说明上述防火墙策略的下发过程,作为对上述实施例的细化和扩展,本发明实施例提供了另一种防火墙开墙方法,如图2所示,所述方法包括:

[0040] 201、接收防火墙开墙请求,所述防火墙开墙请求携带请求方与服务方之间的标识组。

[0041] 对于本发明实施例,防火墙管理平台接收防火墙开墙请求的过程与步骤101相同,在此不再赘述。

[0042] 202、根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略。

[0043] 其中,所述预设防火墙开墙策略表中存储有请求方与服务方之间的标识组及其对应的防火开墙策略,对于本发明实施例,开墙发起人员会预先在防火墙管理平台上填写请求方与服务方之间的开墙信息,评审通过后,该开墙信息会自动录入至防火墙管理平台,从该开墙信息中获取请求方IP地址和服务方IP地址,根据该请求方IP地址和服务方IP地址,确定请求方与服务方之间的标识组,同时将该开墙信息确定为请求方与服务方之间的防火墙开墙策略,并将请求方与服务方之间的标识组和防火墙开墙策略对应存储至防火墙管理平台中的预设防火墙开墙策略表。进一步地,根据防火墙开墙请求中携带的请求方与服务方之间的标识组,查找预设防火墙开墙策略表,得到与该请求方与服务方之间的标识组对应的防火墙开墙策略,进一步地,将该防火墙开墙策略下发至服务方,实现请求方与服务方之间的自动开墙操作。

[0044] 203、根据所述请求方与服务方之间的标识组,利用SSH远程协议调用服务方的防火墙策略下发脚本,将所述防火墙策略下发至所述服务方。

[0045] 对于本发明实施例,为了将查找的防火墙开墙策略下发至服务方,步骤203具体包括:根据所述请求方与服务方之间的标识组,利用SSH远程协议将所述防火墙策略中的开墙参数传递至所述服务方的防火墙策略下发脚本,生成防火墙策略下发指令;调用所述防火墙策略下发指令,将所述防火墙策略下发至所述服务方。例如,请求方与服务方之间的防火墙开墙策略为允许计算机A访问计算机B的端口21,端口22和端口23,根据请求方与服务方之间的标识组,利用SSH远程协议调用服务方计算机B的防火墙策略下发脚本,并将防火墙开墙策略中的开墙参数传递至服务方计算机B的防火墙策略下发脚本,该开墙参数包括请求方的IP地址和服务方的端口信息,之后服务方计算机B的防火墙策略下发脚本调用iptable指令,并将开墙参数传递给iptable指令,生成防火墙开墙指令,进一步地,调用该

防火墙开墙指令，下发相关的开墙配置，就实现了请求方与服务方之间的开墙操作。

[0046] 204、根据所述请求方与服务方之间的标识组调用请求方的防火墙验墙脚本，验证所述请求方与所述服务方之间是否开墙成功。

[0047] 对于本发明实施例，为了验证请求方与服务方之间是否开墙成功，需要进一步进行验墙操作，步骤204具体包括：根据所述请求方与服务方之间的标识组，利用SSH远程协议调用请求方的防火墙验墙脚本，验证所述请求方与所述服务方之间是否开墙成功。进一步地，所述根据所述请求方与服务方之间的标识组，利用SSH远程协议调用请求方的防火墙脚本，验证所述请求方与所述服务方之间是否开墙成功包括：接收所述服务方发送的防火墙策略下发完成信息，所述防火墙策略下发完成信息包括所述开墙参数；根据所述请求方与服务方之间的标识组，利用SSH远程协议将所述开墙参数传递至所述请求方的防火墙验墙脚本，生成防火墙验墙指令；调用所述防火墙验墙指令，验证所述请求方与所述服务方之间是否开墙成功。具体地，服务方进行相应的开墙配置操作之后，如果防火墙策略下发成功，则服务方会向防火墙管理平台发送防火墙策略下发完成信息，并将请求方IP地址、服务方IP地址以及服务方的端口信息等开墙参数返回至防火墙管理平台，根据请求方的IP地址，防火墙管理平台通过SSH协议远程调用请求方的防火墙验墙脚本，并将服务方IP和服务方的端口信息参数传输给请求方的防火墙验证脚本，之后防火墙的验墙脚本调用telnet指令，并将服务方IP地址和服务方的端口信息参数传输给telnet指令，例如，验证请求方计算机A是否可以访问服务方计算机B的端口22，调用telnet ip port指令，其中，ip为服务方的IP地址，port为请求方将要访问的服务方的端口，由此通过telnet指令验证请求方是否可以访问服务方的端口。

[0048] 205、接收所述请求方反馈的防火墙验墙状态，并将所述防火墙验墙状态发送至防火墙开墙发起方。

[0049] 对于本发明实施例，在完成请求方与服务方之间的验墙操作之后，请求方会向防火墙管理平台反馈防火墙验墙状态，防火墙管理平台收到防火墙验墙状态后，会将防火墙验墙状态发送给开墙发起人员，开墙发起人员便知道请求方是否可以访问相应的服务方，例如，防火墙管理平台接收到请求方反馈的防火墙验墙状态，开墙发起人员便知道请求方计算机A是否可以访问服务方计算机B的端口22。

[0050] 本发明实施例提供的另一种防火墙开墙方法，与目前通过人为的方式来进行防火墙的开墙和验墙相比，本发明能够接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组；并根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略；与此同时，根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方，从而能够缩短不同服务间的架构变更周期，提高不同服务间的架构变更效率，实现了防火墙策略的自动下发和自动验墙，节省大量人力和时间。

[0051] 进一步地，作为图1的具体实现，本发明实施例提供了一种防火墙开墙装置，如图3所示，所述装置包括：接收单元31、查找单元32、调用单元33。

[0052] 所述接收单元31，可以用于接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组。所述接收单元31是本装置中接收防火墙开墙请求的主要功能模块。

[0053] 所述查找单元32,可以用于根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略。所述查找32是本装置中根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略的主要功能模块,也是核心模块。

[0054] 所述调用单元33,可以用于根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方。所述调用单元33是本装置中根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方的主要功能模块,也是核心模块。

[0055] 对于本发明实施例,为了将防火墙策略下发至服务方,所述调用单元33,具体可以用于根据所述请求方与服务方之间的标识组,利用SSH远程协议调用服务方的防火墙策略下发脚本,将所述防火墙策略下发至所述服务方。

[0056] 进一步地,为了生成防火墙下发指令,所述调用单元33包括:生成模块331和调用模块332,如图4所示。

[0057] 所述生成模块331,可以用于根据所述请求方与服务方之间的标识组,利用SSH远程协议将所述防火墙策略中的开墙参数传递至所述服务方的防火墙策略下发脚本,生成防火墙策略下发指令。

[0058] 所述调用模块332,可以用于调用所述防火墙策略下发指令,将所述防火墙策略下发至所述服务方。

[0059] 此外,为了验证请求方与服务方之间是否开墙成功,所述调用单元33,还可以用于根据所述请求方与服务方之间的标识组调用请求方的防火墙验墙脚本,验证所述请求方与所述服务方之间是否开墙成功。

[0060] 进一步地,所述调用单元33,具体还可以用于根据所述请求方与服务方之间的标识组,利用SSH远程协议调用请求方的防火墙验墙脚本,验证所述请求方与所述服务方之间是否开墙成功。

[0061] 在具体应用场景中,为了生成防火墙验墙指令,所述调用单元33,还包括接收模块333。

[0062] 所述接收模块333,可以用于接收所述服务方发送的防火墙策略下发完成信息,所述防火墙策略下发完成信息包括所述开墙参数。

[0063] 所述生成模块331,还可以用于根据所述请求方与服务方之间的标识组,利用SSH远程协议将所述开墙参数传递至所述请求方的防火墙验墙脚本,生成防火墙验墙指令。

[0064] 所述调用模块332,还可以用于调用所述防火墙验墙指令,验证所述请求方与所述服务方之间是否开墙成功。

[0065] 进一步地,为了让防火墙开墙发起方了解防火墙开墙策略是否下发成功,所述接收单元31,还可以用于接收所述请求方反馈的防火墙验墙状态,并将所述防火墙验墙状态发送至防火墙开墙发起方。

[0066] 需要说明的是,本发明实施例提供的一种防火墙开墙装置所涉及各功能模块的其他相应描述,可以参考图1所示方法的对应描述,在此不再赘述。

[0067] 基于上述如图1所示方法,相应的,本发明实施例还提供了一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现以下步骤:接收防火墙开墙请求,

所述防火墙开墙请求携带请求方与服务方之间的标识组;根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略;根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方

[0068] 基于上述如图1所示方法和如图3所示装置的实施例,本发明实施例还提供了一种计算机设备的实体结构图,如图5所示,该计算机设备包括:处理器41、存储器42、及存储在存储器42上并可在处理器上运行的计算机程序,其中存储器42和处理器41均设置在总线43上所述处理器41执行所述程序时实现以下步骤:接收防火墙开墙请求,所述防火墙开墙请求携带请求方与服务方之间的标识组;根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略;根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方。

[0069] 通过本发明的技术方案,能够接收防火墙开墙请求,所述防火墙开墙请求携带请求方与服务方之间的标识组;并根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表,得到与所述标识组对应的防火墙开墙策略;与此同时,根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本,将所述防火墙开墙策略下发至所述服务方,从而能够缩短不同服务间的架构变更周期,提高不同服务间的架构变更效率,实现了防火墙策略的自动下发和自动验墙,节省大量人力和时间。

[0070] 显然,本领域的技术人员应该明白,上述的本发明的各模块或各步骤可以用通用的计算装置来实现,它们可以集中在单个的计算装置上,或者分布在多个计算装置所组成的网络上,可选地,它们可以用计算装置可执行的程序代码来实现,从而,可以将它们存储在存储装置中由计算装置来执行,并且在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤,或者将它们分别制作成各个集成电路模块,或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样,本发明不限制于任何特定的硬件和软件结合。

[0071] 以上所述仅为本发明的优选实施例而已,并不用于限制本发明,对于本领域的技术人员来说,本发明可以有各种更改和变化。凡在本发明的精神和原则之内,所作的任何修改、等同替换、改进等,均应包括在本发明的保护范围之内。

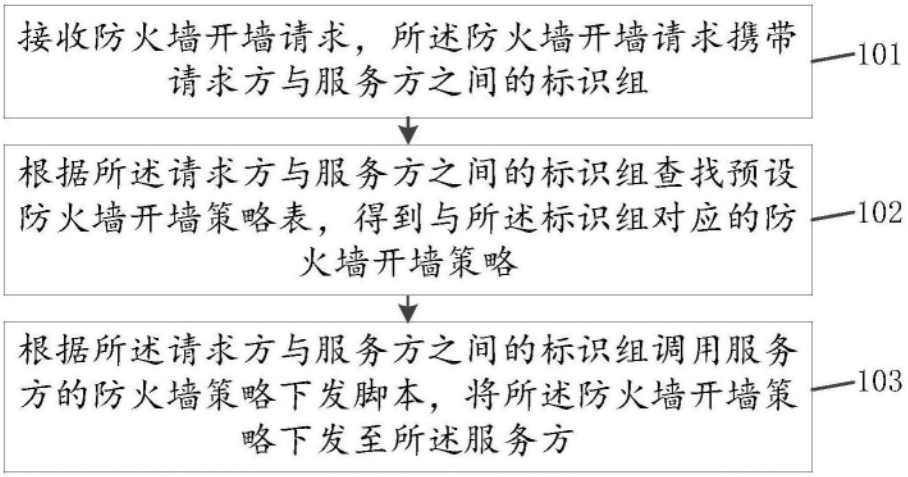

接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组
101
根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略
102
根据所述请求方与服务方之间的标识组调用服务方的防火墙策略下发脚本，将所述防火墙开墙策略下发至所述服务方
103

图1

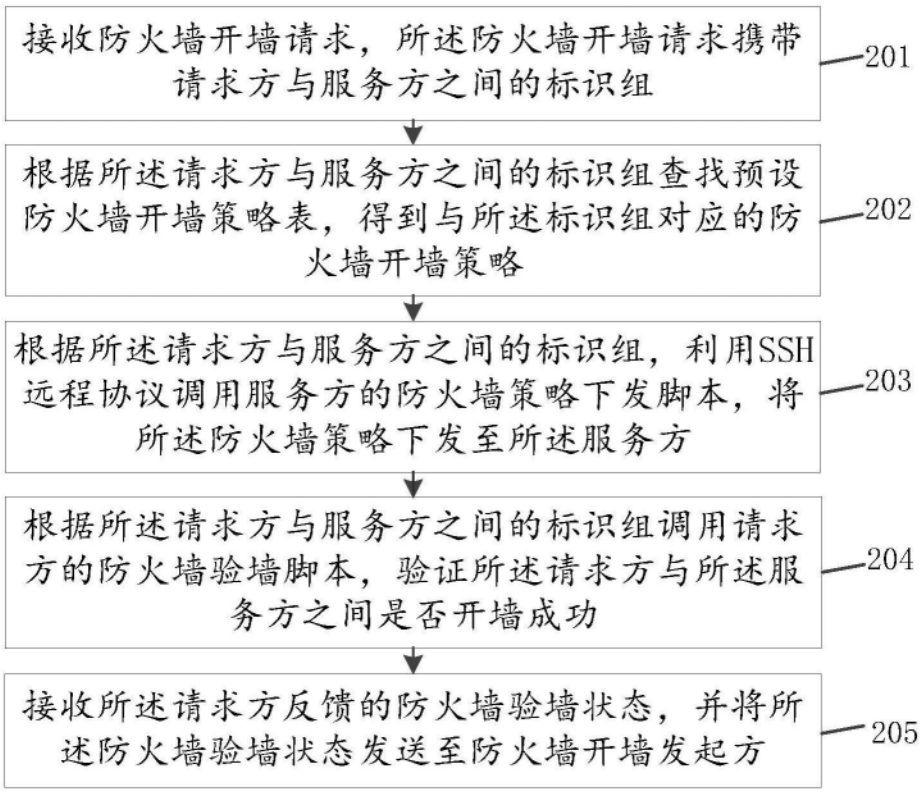

接收防火墙开墙请求，所述防火墙开墙请求携带请求方与服务方之间的标识组
201
根据所述请求方与服务方之间的标识组查找预设防火墙开墙策略表，得到与所述标识组对应的防火墙开墙策略
202
根据所述请求方与服务方之间的标识组，利用SSH远程协议调用服务方的防火墙策略下发脚本，将所述防火墙策略下发至所述服务方
203
根据所述请求方与服务方之间的标识组调用请求方的防火墙验墙脚本，验证所述请求方与所述服务方之间是否开墙成功
204
接收所述请求方反馈的防火墙验墙状态，并将所述防火墙验墙状态发送至防火墙开墙发起方
205

图2

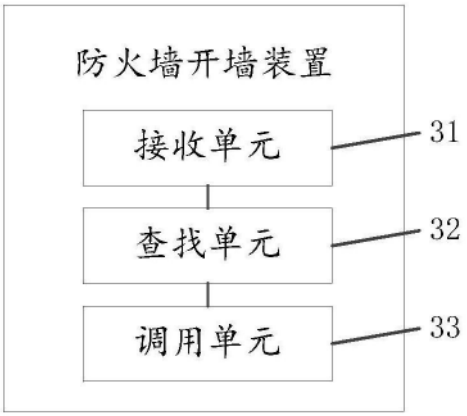

防火墙开墙装置
接收单元
31
查找单元
32
调用单元
33

图3

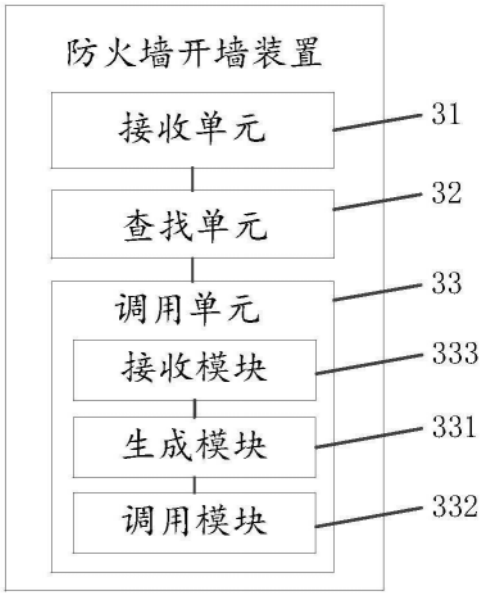

防火墙开墙装置
接收单元
31
查找单元
32
调用单元
33
接收模块
333
生成模块
331
调用模块
332

图4

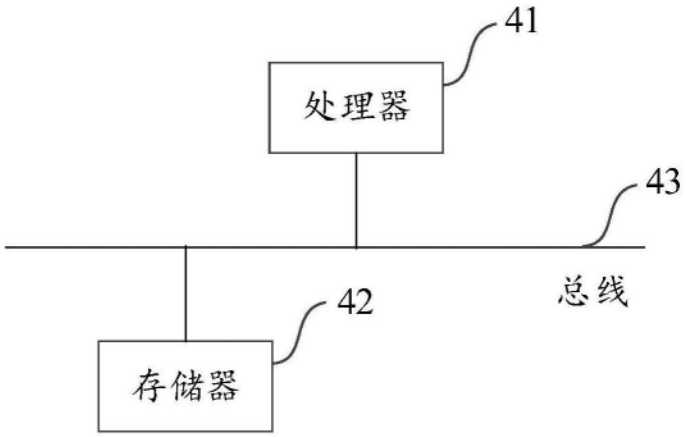


图5