(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116582362 B
(45)授权公告日 2023.09.26

(21)申请号 202310841610.3
(22)申请日 2023.07.11
(65)同一申请的已公布的文献号
申请公布号 CN 116582362 A
(43)申请公布日 2023.08.11
(73)专利权人 建信金融科技有限责任公司
地址 200120 上海市浦东新区中国(上海)自由贸易试验区银城路99号12层、15层
(72)发明人 邱步云 康庄
(74)专利代理机构 中科专利商标代理有限责任公司 11021
专利代理师 樊晓
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 41/08(2022.01)

(56)对比文件
CN 111294365 A,2020.06.16
CN 101674606 A,2010.03.17
CN 102801659 A,2012.11.28
CN 104391882 A,2015.03.04
CN 105393497 A,2016.03.09
CN 107332813 A,2017.11.07
CN 107864126 A,2018.03.30
CN 109040037 A,2018.12.18
CN 109067585 A,2018.12.21
CN 109889546 A,2019.06.14
CN 114938288 A,2022.08.23
CN 115701019 A,2023.02.07
CN 115811434 A,2023.03.17
US 2015207813 A1,2015.07.23
US 2017181056 A1,2017.06.22
US 2017230373 A1,2017.08.10
US 2021120022 A1,2021.04.22
US 2021243605 A1,2021.08.05

审查员 谢思敏

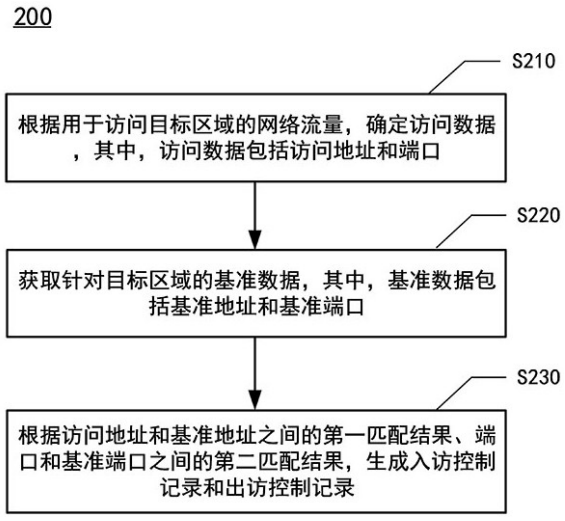
权利要求书3页 说明书17页 附图7页

(54)发明名称

网络访问的控制方法、装置、电子设备及存储介质

(57)摘要

本发明提供了一种网络访问的控制方法、装置、电子设备及存储介质，应用于云计算技术领域和信息安全技术领域。该方法包括：根据用于访问目标区域的网络流量，确定访问数据，访问数据包括访问地址和端口，网络流量包括多个网络访问请求；获取针对目标区域的基准数据，基准数据包括基准地址和基准端口；根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录。由于从基准地址和基本端口两个方面核对网络访问请求的安全性，并分别生成控制进入云服务器的入访控制记录、将网络访问请求输出至目标服务的出访控制记录，能够实现准确、高效地控制网络访问的技术效果。



CN 116582362 B

1.一种网络访问的控制方法,其特征在于,所述方法包括:

根据用于访问目标区域的网络流量,确定访问数据,其中,所述访问数据包括访问地址和端口,所述网络流量包括多个网络访问请求,所述目标区域属于云服务器;

获取针对所述目标区域的基准数据,其中,所述基准数据包括基准地址和基准端口;以及

根据所述访问地址和所述基准地址之间的第一匹配结果、所述端口和所述基准端口之间的第二匹配结果,生成入访控制记录和出访控制记录,其中,所述入访控制记录用于控制所述网络访问请求进入所述云服务器,所述出访控制记录用于将所述网络访问请求输出至所述云服务器中的目标服务;

所述云服务器包括外联网区、互联网区和开放区,所述目标区域为所述外联网区、所述互联网区和所述开放区其中之一;所述外联网区用于接收通过目标局域网进行访问的网络访问请求,所述互联网区用于接收通过互联网进行访问的网络访问请求;所述开放区用于接收通过所述外联网区或所述互联网区进行访问的网络访问请求;所述开放区的安全等级高于所述互联网区和所述外联网区;

所述访问地址包括源访问地址,所述端口包括源端口,所述基准地址包括多个入访基准地址,所述基准端口包括多个入访基准端口,所述第一匹配结果包括第一匹配子结果,所述第二匹配结果包括第二匹配子结果;所述入访控制记录包括第一入访记录或第二入访记录;

所述根据所述访问地址和所述基准地址之间的第一匹配结果、所述端口和所述基准端口之间的第二匹配结果,生成入访控制记录,包括:

在所述第一匹配子结果表征所述多个入访基准地址中存在与所述源访问地址相匹配的地址,且所述第二匹配子结果表征所述多个入访基准端口中存在与所述源端口相匹配的端口的情况下,基于所述第一匹配子结果,生成所述第一入访记录;

在所述第一匹配子结果表征所述多个入访基准地址中不存在与所述源访问地址相匹配的地址,且所述第二匹配子结果表征所述多个入访基准端口中存在与所述源端口相匹配的端口的情况下,基于所述目标区域,生成所述第二入访记录;

所述基于所述目标区域,生成所述第二入访记录包括:

在确定所述目标区域为所述外联网区的情况下,根据所述外联网区的标识、所述源端口和放行标识,生成所述第二入访记录;

在确定所述目标区域为所述互联网区的情况下,根据所述互联网区的标识、所述源端口和所述放行标识,生成所述第二入访记录;

在确定所述目标区域为所述开放区的情况下,根据所述源访问地址、所述源端口和所述放行标识,生成待确认入访记录;以及

根据对所述待确认入访记录的确认指令,生成所述第二入访记录。

2.根据权利要求1所述的方法,其特征在于,所述基于所述第一匹配子结果,生成所述第一入访记录,包括:

根据所述第一匹配子结果,获取与源访问地址相匹配的匹配访问地址;

确定所述匹配访问地址所属的网络区域;以及

根据所述网络区域和所述源端口,生成所述第一入访记录。

3.根据权利要求2所述的方法，其特征在于，所述根据所述网络区域和所述源端口，生成所述第一入访记录，包括：

在所述网络区域属于所述目标区域或云资源区的情况下，根据所述匹配访问地址、所述源端口和放行标识，生成所述第一入访记录；

在所述网络区域不属于所述目标区域且不属于所述云资源区的情况下，根据所述网络区域的标识、所述源端口和所述放行标识，生成所述第一入访记录。

4.根据权利要求1所述的方法，其特征在于，所述根据对所述待确认入访记录的确认指令，生成所述第二入访记录，包括：

将所述待确认入访记录存储至所述目标区域的待确认入访表；

响应于接收到针对所述待确认入访表中所述待确认入访记录的确认指令，将所述待确认入访记录作为第二入访记录。

5.根据权利要求1所述的方法，其特征在于，所述访问地址包括目标访问地址，所述端口包括目标端口，所述基准地址包括多个出访基准地址，所述基准端口包括多个出访基准端口，所述第一匹配结果包括第三匹配子结果，所述第二匹配结果包括第四匹配子结果；所述出访控制记录包括第一出访记录或第二出访记录；

所述根据所述访问地址和所述基准地址之间的第一匹配结果、所述端口和所述基准端口之间的第二匹配结果，生成出访控制记录，包括：

在所述第三匹配子结果表征所述多个出访基准地址中存在与所述目标访问地址相匹配的地址，且所述第四匹配子结果表征所述多个出访基准端口中存在与所述目标端口相匹配的端口的情况下，基于所述第三匹配子结果，生成第一出访记录；

在所述第三匹配子结果表征所述多个出访基准地址中不存在与所述目标访问地址相匹配的地址，且所述第四匹配子结果表征所述多个出访基准端口中存在与所述目标端口相匹配的端口的情况下，基于所述目标区域，生成所述第二出访记录。

6.根据权利要求1所述的方法，其特征在于，所述根据用于访问目标区域的网络流量，确定访问数据，包括：

获取所述网络流量的流量镜像，其中，所述流量镜像包括访问数据包；

解析所述访问数据包，得到解析数据；

对所述解析数据进行去重处理，得到所述访问数据，其中，所述访问数据存储于所述目标区域的数据库实时表。

7.根据权利要求1~6任一项所述的方法，其特征在于，在所述生成所述入访控制记录和所述出访控制记录之后，还包括：

将所述入访控制记录和所述出访控制记录存储至所述目标区域的安全组；

基于所述安全组，控制所述网络访问请求进入所述云服务器，并将所述网络访问请求输出至所述目标区域的目标服务；或者，基于所述安全组，控制所述网络访问请求进入所述云服务器，并将所述网络访问请求输出至其他区域的目标服务，所述其他区域包括所述云服务器中与所述目标区域不同的区域。

8.一种网络访问的控制装置，其特征在于，所述装置包括：

确定模块，用于根据用于访问目标区域的网络流量，确定访问数据，其中，所述访问数据包括访问地址和端口，所述网络流量包括多个网络访问请求，所述目标区域属于云服务

器；

获取模块，用于获取针对所述目标区域的基准数据，其中所述基准数据包括基准地址和基准端口；以及

生成模块，用于根据所述访问地址和所述基准地址之间的第一匹配结果、所述端口和所述基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录，其中，所述入访控制记录用于控制所述网络访问请求进入所述云服务器，所述出访控制记录用于将所述网络访问请求输出至所述云服务器中的目标服务；

所述云服务器包括外联网区、互联网区和开放区，所述目标区域为所述外联网区、所述互联网区和所述开放区其中之一；所述外联网区用于接收通过目标局域网进行访问的网络访问请求，所述互联网区用于接收通过互联网进行访问的网络访问请求；所述开放区用于接收通过所述外联网区或所述互联网区进行访问的网络访问请求；所述开放区的安全等级高于所述互联网区和所述外联网区；

所述访问地址包括源访问地址，所述端口包括源端口，所述基准地址包括多个入访基准地址，所述基准端口包括多个入访基准端口，所述第一匹配结果包括第一匹配子结果，所述第二匹配结果包括第二匹配子结果；所述入访控制记录包括第一入访记录或第二入访记录；

所述根据所述访问地址和所述基准地址之间的第一匹配结果、所述端口和所述基准端口之间的第二匹配结果，生成入访控制记录，包括：

在所述第一匹配子结果表征所述多个入访基准地址中存在与所述源访问地址相匹配的地址，且所述第二匹配子结果表征所述多个入访基准端口中存在与所述源端口相匹配的端口的情况下，基于所述第一匹配子结果，生成所述第一入访记录；

在所述第一匹配子结果表征所述多个入访基准地址中不存在与所述源访问地址相匹配的地址，且所述第二匹配子结果表征所述多个入访基准端口中存在与所述源端口相匹配的端口的情况下，基于所述目标区域，生成所述第二入访记录；

所述基于所述目标区域，生成所述第二入访记录包括：

在确定所述目标区域为所述外联网区的情况下，根据所述外联网区的标识、所述源端口和放行标识，生成所述第二入访记录；

在确定所述目标区域为所述互联网区的情况下，根据所述互联网区的标识、所述源端口和所述放行标识，生成所述第二入访记录；

在确定所述目标区域为所述开放区的情况下，根据所述源访问地址、所述源端口和所述放行标识，生成待确认入访记录；以及

根据对所述待确认入访记录的确认指令，生成所述第二入访记录。

9.一种电子设备，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，

其中，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器执行根据权利要求1~7中任一项所述的方法。

10.一种计算机可读存储介质，其上存储有可执行指令，该指令被处理器执行时使处理器执行根据权利要求1~7中任一项所述的方法。

网络访问的控制方法、装置、电子设备及存储介质

技术领域

[0001] 本发明涉及云计算技术领域和信息安全技术领域，更具体地涉及一种网络访问的控制方法、装置、电子设备及存储介质。

背景技术

[0002] 随着云计算技术的发展，企业能够通过云服务器向用户提供多种服务。由于云服务器面向的服务提供方和用户众多，使得云服务器容易遭受网络攻击。

[0003] 相关技术中，一般基于“按需开通”的原则，由开发人员手动配置网络请求的访问权限，以保证云服务器的安全性。

[0004] 在实现上述发明构思的过程中，发明人发现相关技术存在如下技术问题：由开发人员手动配置网络请求的访问权限，存在安全访问控制效率低的问题。并且，手动配置访问权限还会导致遗漏网络访问关系，从而影响安全访问的控制准确性。

发明内容

[0005] 鉴于上述问题，本发明提供了一种网络访问的控制方法、装置、电子设备及存储介质。

[0006] 根据本发明的第一个方面，提供了一种网络访问的控制方法，包括：

[0007] 根据用于访问目标区域的网络流量，确定访问数据，其中，访问数据包括访问地址和端口，网络流量包括多个网络访问请求，目标区域属于云服务器；

[0008] 获取针对目标区域的基准数据，其中，基准数据包括基准地址和基准端口；以及

[0009] 根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录，其中，入访控制记录用于控制网络访问请求进入云服务器，出访控制记录用于将网络访问请求输出至云服务器中的目标服务。

[0010] 根据本发明的实施例，访问地址包括源访问地址，端口包括源端口，基准地址包括多个入访基准地址，基准端口包括多个入访基准端口，第一匹配结果包括第一匹配子结果，第二匹配结果包括第二匹配子结果；入访控制记录包括第一入访记录或第二入访记录；

[0011] 根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录，包括：

[0012] 在第一匹配子结果表征多个入访基准地址中存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，基于第一匹配子结果，生成第一入访记录；

[0013] 在第一匹配子结果表征多个入访基准地址中不存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，基于目标区域，生成第二入访记录。

[0014] 根据本发明的实施例，基于第一匹配子结果，生成第一入访记录，包括：

[0015] 根据第一匹配子结果，获取与源访问地址相匹配的匹配访问地址；

[0016] 确定匹配访问地址所属的网络区域;以及

[0017] 根据网络区域和源端口,生成第一入访记录。

[0018] 根据本发明的实施例,根据网络区域和源端口,生成第一入访记录,包括:

[0019] 在网络区域属于目标区域或云资源区的情况下,根据匹配访问地址、源端口和放行标识,生成第一入访记录;

[0020] 在网络区域不属于目标区域且不属于云资源区的情况下,根据网络区域的标识、源端口和放行标识,生成第一入访记录。

[0021] 根据本发明的实施例,云服务器包括外联网区、互联网区和开放区,目标区域为外联网区、互联网区和开放区其中之一,外联网区用于接收通过目标局域网进行访问的网络访问请求,互联网区用于接收通过互联网进行访问的网络访问请求;开放区用于接收通过外联网区或互联网区进行访问的网络访问请求。

[0022] 根据本发明的实施例,基于目标区域,生成第二入访记录,包括:

[0023] 在确定目标区域为外联网区的情况下,根据外联网区的标识、源端口和放行标识,生成第二入访记录;

[0024] 在确定目标区域为互联网区的情况下,根据互联网区的标识、源端口和放行标识,生成第二入访记录;

[0025] 在确定目标区域为开放区的情况下,根据源访问地址、源端口和放行标识,生成待确认入访记录;以及

[0026] 根据待确认入访记录,生成第二入访记录。

[0027] 根据本发明的实施例,根据待确认入访记录,生成第二入访记录,包括:

[0028] 将待确认入访记录存储至目标区域的待确认入访表;

[0029] 响应于接收到针对待确认入访表中待确认入访记录的确认指令,将待确认入访记录作为第二入访记录。

[0030] 根据本发明的实施例,访问地址包括目标访问地址,端口包括目标端口,基准地址包括多个出访基准地址,基准端口包括多个出访基准端口,第一匹配结果包括第三匹配子结果,第二匹配结果包括第四匹配子结果;出访控制记录包括第一出访记录或第二出访记录;

[0031] 根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果,生成出访控制记录,包括:

[0032] 在第三匹配子结果表征多个出访基准地址中存在与目标访问地址相匹配的地址,且第四匹配子结果表征多个出访基准端口中存在与目标端口相匹配的端口的情况下,基于第三匹配子结果,生成第一出访记录;

[0033] 在第三匹配子结果表征多个出访基准地址中不存在与目标访问地址相匹配的地址,且第四匹配子结果表征多个出访基准端口中存在与所述目标端口相匹配的端口的情况下,基于目标区域,生成第二出访记录。

[0034] 根据本发明的实施例,根据用于访问目标区域的网络流量,确定访问数据,包括:

[0035] 获取网络流量的流量镜像,其中,流量镜像包括访问数据包;

[0036] 解析访问数据包,得到解析数据;

[0037] 对解析数据进行去重处理,得到访问数据,其中,访问数据存储于目标区域的数据

库实时表。

[0038] 根据本发明的实施例，在生成入访控制记录和出访控制记录之后，还包括：

[0039] 将入访控制记录和出访控制记录存储至目标区域的安全组；

[0040] 基于安全组，控制网络访问请求进入云服务器，并将网络访问请求输出至目标区域的目标服务；或者，基于安全组，控制网络访问请求进入云服务器，并将网络访问请求输出至其他区域的目标服务，其他区域包括云服务器中与目标区域不同的区域。

[0041] 本发明的第二方面提供了一种网络访问的控制装置，包括：

[0042] 确定模块，用于根据用于访问目标区域的网络流量，确定访问数据，其中，访问数据包括访问地址和端口，网络流量包括多个网络访问请求，目标区域属于云服务器；

[0043] 获取模块，用于获取针对目标区域的基准数据，其中基准数据包括基准地址和基准端口；以及

[0044] 生成模块，用于根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录，其中，入访控制记录用于控制网络访问请求进入云服务器，出访控制记录用于控制网络访问输出云服务器。

[0045] 本发明的第三方面提供了一种电子设备，包括：一个或多个处理器；存储器，用于存储一个或多个程序，其中，当一个或多个程序被一个或多个处理器执行时，使得一个或多个处理器执行上述网络访问的控制方法。

[0046] 本发明的第四方面还提供了一种计算机可读存储介质，其上存储有可执行指令，该指令被处理器执行时使处理器执行上述网络访问的控制方法。

[0047] 本发明的第五方面还提供了一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现上述网络访问的控制方法。

[0048] 在本发明的实施例中，根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录，其中，入访控制记录用于控制网络访问请求进入云服务器，出访控制记录用于将网络访问请求输出至云服务器中的目标服务，能够实现准确、高效地控制网络访问的技术效果。在本发明的实施例中，由于从基准地址和基本端口两个方面核对网络访问请求的安全性，以及分别生成控制进入云服务器的入访控制记录、生成将网络访问请求输出至目标服务的出访控制记录，至少能够部分地解决由开发人员手动配置网络请求的访问权限导致的安全访问控制效率低和控制准确性低的技术问题，达到准确、高效地控制网络访问的技术效果。

附图说明

[0049] 通过以下参照附图对本发明实施例的描述，本发明的上述内容以及其他目的、特征和优点将更为清楚，在附图中：

[0050] 图1示出了根据本发明实施例的网络访问的控制方法的应用场景。

[0051] 图2示出了根据本发明实施例的网络访问的控制方法的流程图。

[0052] 图3示出了根据本发明实施例的入访控制记录生成方法的流程图。

[0053] 图4示出了根据本发明一具体实施例的第一入访记录生成方法的流程图。

[0054] 图5示出了根据本发明一具体实施例的第二入访记录生成方法的流程图。

[0055] 图6示出了根据本发明实施例的云服务器的系统架构图。

[0056] 图7示出了根据本发明实施例的网络访问的控制装置的结构框图。

[0057] 图8示出了根据本发明实施例的适于网络访问的控制方法的电子设备的方框图。

具体实施方式

[0058] 以下，将参照附图来描述本发明的实施例。但是应该理解，这些描述只是示例性的，而并非要限制本发明的范围。在下面的详细描述中，为便于解释，阐述了许多具体的细节以提供对本发明实施例的全面理解。然而，明显地，一个或多个实施例在没有这些具体细节的情况下也可以被实施。此外，在以下说明中，省略了对公知结构和技术的描述，以避免不必要地混淆本发明的概念。

[0059] 在此使用的术语仅仅是为了描述具体实施例，而并非意在限制本发明。在此使用的术语“包括”、“包含”等表明了所述特征、步骤、操作和/或部件的存在，但是并不排除存在或添加一个或多个其他特征、步骤、操作或部件。

[0060] 在此使用的所有术语(包括技术和科学术语)具有本领域技术人员通常所理解的含义，除非另外定义。应注意，这里使用的术语应解释为具有与本说明书的上下文相一致的含义，而不应以理想化或过于刻板的方式来解释。

[0061] 在使用类似于“A、B和C等中至少一个”这样的表述的情况下，一般来说应该按照本领域技术人员通常理解该表述的含义来予以解释(例如，“具有A、B和C中至少一个的系统”应包括但不限于单独具有A、单独具有B、单独具有C、具有A和B、具有A和C、具有B和C、和/或具有A、B、C的系统等)。

[0062] 在本发明的技术方案中，所涉及的数据(如包括但不仅限于用户个人信息)的收集、存储、使用、加工、传输、提供、发明和应用等处理，均符合相关法律法规的规定，且不违背公序良俗。

[0063] 在云计算领域中，服务提供方可以通过云服务器向用户提供多种服务，每个用户都可以看作云服务器的租户。在云服务器中，可以通过划分私有网络的方式，将租户可使用的云服务划分到该租户的私有网络中，实现租户之间隔离。云服务器可以将接收到的网络访问请求传输到私有网络或公有网络中，以便向用户提供多种服务。

[0064] 相关技术中，开发人员一般基于“按需开通”的原则，手动针对多个租户开放不同的权限，以便将网络访问请求输入到对应的私有网络或共有网络中。

[0065] 然而，由于云服务器面向的租户众多、云服务器内多个服务之间的调用关系复杂，由人工梳理网络访问关系并配置网络访问请求的控制权限，不仅存在配置效率低的问题，还会因遗漏网络访问关系造成正确的网络访问请求无法被放行的现象，导致影响安全访问的控制准确性。

[0066] 本发明的实施例提供了一种网络访问的控制方法，包括：根据用于访问目标区域的网络流量，确定访问数据，其中，访问数据包括访问地址和端口，网络流量包括多个网络访问请求，目标区域属于云服务器；获取针对目标区域的基准数据，其中，基准数据包括基准地址和基准端口；以及根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录。

[0067] 需要说明的是，本发明网络访问的控制方法和装置可用于金融领域在云计算的应用，也可用于除金融领域之外的任意领域，如信息安全技术领域，本发明对网络访问的控制

方法和装置的应用领域不做限定。

[0068] 图1示出了根据本发明实施例的网络访问的控制方法的应用场景。

[0069] 如图1所示，根据该实施例的应用场景100可以包括第一终端设备101、第二终端设备102、第三终端设备103、网络104和服务器105。网络104用以在第一终端设备101、第二终端设备102、第三终端设备103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。

[0070] 用户可以使用第一终端设备101、第二终端设备102、第三终端设备103中的至少一个通过网络104与服务器105交互，以接收或发送消息等。第一终端设备101、第二终端设备102、第三终端设备103上可以安装有各种通讯客户端应用，例如购物类应用、网页浏览器应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等(仅为示例)。

[0071] 第一终端设备101、第二终端设备102、第三终端设备103可以是具有显示屏并且支持网页浏览的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。

[0072] 服务器105可以是提供各种服务的服务器，例如，可以是云服务器(Cloud Virtual Machine，CVM)。云服务器可以在云中提供可扩展的计算服务。例如，对用户利用第一终端设备101、第二终端设备102、第三终端设备103所请求的金融交易等服务提供支持的后台管理服务器(仅为示例)。后台管理服务器可以对接收到的用户请求等数据进行分析等处理，并将处理结果(例如根据用户请求获取或生成的网页、信息、或数据等)反馈给终端设备。

[0073] 需要说明的是，本发明实施例所提供的网络访问的控制方法一般可以由服务器105执行。相应地，本发明实施例所提供的网络访问的控制装置一般可以设置于服务器105中。本发明实施例所提供的网络访问的控制方法也可以由不同于服务器105且能够与第一终端设备101、第二终端设备102、第三终端设备103和/或服务器105通信的服务器或服务器集群执行。相应地，本发明实施例所提供的网络访问的控制装置也可以设置于不同于服务器105且能够与第一终端设备101、第二终端设备102、第三终端设备103和/或服务器105通信的服务器或服务器集群中。

[0074] 应该理解，图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要，可以具有任意数目的终端设备、网络和服务器。

[0075] 以下将基于图1描述的场景，通过图2~图6对发明实施例的网络访问的控制方法进行详细描述。

[0076] 图2示出了根据本发明实施例的网络访问的控制方法的流程图。

[0077] 如图2所示，该方法200包括操作S210~S230。

[0078] 在操作S210，根据用于访问目标区域的网络流量，确定访问数据，其中，访问数据包括访问地址和端口。

[0079] 根据本发明的实施例，根据云服务器的物理架构，可以将云服务器的网络框架划分为多个网络区域。目标区域可以理解为上述多个网络区域中的一个区域。用户可以访问云服务器中目标区域的服务。

[0080] 根据本发明的实施例，网络流量(traffic)可以理解为用户对云服务器的访问量。每个用户可以通过多个网络访问请求，向云服务器请求访问多个服务。由此，网络流量可以包括多个网络访问请求。

[0081] 根据本发明的实施例，访问数据包括访问地址和端口。访问地址包括互联网协议地址(Internet Protocol Address，IP地址)，端口(port)可以理解为终端设备与外界通讯交流的出口。

[0082] 根据本发明的实施例，用户可以通过终端设备发起网络访问请求，网络访问请求包括用户所使用的终端设备的IP地址和端口，要访问的云服务器中服务器的IP地址和端口。

[0083] 在操作S220，获取针对目标区域的基准数据，其中，基准数据包括基准地址和基准端口。

[0084] 根据本发明的实施例，云服务器能够对用户授予使用不同服务的权限，之后，用户才能获取并使用云服务中的服务。由此，基准地址包括用户的访问地址，也可以理解为用户使用的终端设备的访问地址；基准端口包括用户的端口，也可以理解为用户使用的终端设备的端口。

[0085] 根据本发明的实施例，云服务器可以根据基准地址和基准端口，确定用户是否为已授权用户。

[0086] 例如，用户的IP地址为“2.1.01”和端口“10”，基准地址中包括“2.1.01”，基准端口包括“10”，由此，允许IP地址为“2.1.01”和端口“10”的用户访问云服务器。

[0087] 根据本发明的实施例，云服务器可以提供多个服务，多个服务可以部署在多个服务器上，每个服务器对应有IP地址和至少一个端口。基准地址包括云服务器中存在的访问地址，基准端口包括云服务器中存在的端口。

[0088] 根据本发明的实施例，根据基准地址和基准端口，云服务器能够确定用户是否能够访问云服务器中的某个服务。

[0089] 例如，访问数据中包括用户要访问的IP地址“1.1.11”，端口“80”。由于“推荐服务”设置于云服务器中IP地址为“1.1.11”、端口为“80”的服务器上。由此，云服务器能够控制网络请求访问IP地址为“1.1.11”，端口为“80”的服务器，以便请求“推荐服务”。如果用户要访问的服务器的IP地址为“1.2.11”，端口为“20”，由于服务器中不存在该服务器，因此，不允许用户访问云服务器，用户无法利用“推荐服务”。

[0090] 在操作S230，根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录。

[0091] 根据本发明的实施例，入访控制记录用于控制网络访问请求进入云服务器，出访控制记录用于将网络访问请求输出至云服务器中的目标服务。

[0092] 根据本发明的实施例，通过入访控制记录可以允许网络请求进入云服务器。但是，由于云服务器中的多个服务是由服务提供方提供的，由此，在控制网络访问请求进入云服务器之后，还可以通过出访控制记录，将网络访问请求输出至云服务器中的目标服务。

[0093] 根据本发明的实施例，目标服务包括由多个服务提供方提供的、多个种类的服务。例如，目标服务包括金融交易服务、推荐服务、查询服务、抢购服务等多种服务。

[0094] 根据本发明的实施例，用户向云服务器发起网络访问请求之后，云服务器生成入访控制记录，以确定是否允许某个用户发起的网络访问请求进入云服务器。云服务还可以生成出访控制记录，在网络访问请求进入云服务器之后，通过出访控制记录确定是否将该网络访问请求传输至云服务器中的目标服务中。

[0095] 在本发明的实施例中，根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录，其中，入访控制记录用于控制网络访问请求进入云服务器，出访控制记录用于将网络访问请求输出至云服务器中的目标服务，能够实现准确、高效地控制网络访问的技术效果。在本发明的实施例中，由于从基准地址和基本端口两个方面核对网络访问请求的安全性，以及分别生成控制进入云服务器的入访控制记录、生成将网络访问请求输出至目标服务的出访控制记录，至少能够部分地解决由开发人员手动配置网络请求的访问权限导致的安全访问控制效率低和控制准确性低的技术问题，达到准确、高效地控制针对云服务器的网络访问的技术效果。

[0096] 根据本发明的实施例，访问地址包括源访问地址，端口包括源端口，基准地址包括多个入访基准地址，基准端口包括多个入访基准端口。

[0097] 根据本发明的实施例，源访问地址表征发起网络访问请求的用户的访问地址，源端口表征发起网络访问请求的用户的端口。入访基准地址可以表征与云服务器中的服务已经建立关系的IP地址，入访基准端口表征与云服务器中的服务已经建立关系的多个端口。其中，根据入访基准地址和入访基准端口可以确定源访问地址和源端口的用户是否为已授权用户。

[0098] 根据本发明的实施例，第一匹配结果包括第一匹配子结果，第二匹配结果包括第二匹配子结果。入访控制记录包括第一入访记录和第二入访记录。

[0099] 根据本发明的实施例，根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成访问控制记录，包括以下步骤：

[0100] 在第一匹配子结果表征多个入访基准地址中存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，基于第一匹配子结果，生成第一入访记录。

[0101] 在第一匹配子结果表征多个入访基准地址中不存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，基于目标区域，生成第二入访记录。

[0102] 根据本发明的实施例，第一匹配子结果包括表征源访问地址与入访基准地址是否匹配的判断结果，如“是”或“否”；在源访问地址与入访基准地址相匹配的情况下，第一匹配子结果还包括多个入访基准地址中与源访问地址相匹配的匹配访问地址，如匹配访问地址“1.1.20”。第二匹配子结果包括表征源端口与入访基准端口是否匹配的判断结果，如“是”或“否”；在源端口与入访基准端口相匹配的情况下，第二匹配子结果还包括多个入访基准端口中与源端口相匹配的匹配端口，如匹配端口“80”。

[0103] 根据本发明的实施例，多个入访基准地址中存在与源访问地址相匹配的地址、且多个入访基准端口中存在与源端口相匹配的地址，表征发起该网络请求的用户已经与云服务器建立了关系，该用户为授权用户，可以允许该网络访问请求进入云服务器。

[0104] 根据本发明的实施例，由于用户可能使用多个路由器或其他局域网设备发起网络访问请求，导致用户的源访问地址发生改变。因此，在多个入访基准地址中不存在与源访问地址相匹配的地址、且多个入访基准端口中存在与源端口相匹配的地址，也认为发起该网络请求的用户已经与云服务器建立了关系，该用户为授权用户，可以允许该网络访问请求进入云服务器。

[0105] 根据本发明的实施例，在满足第一预定条件的情况下，确定网络访问请求存在风险，不生成入访控制记录，以便拒绝该网络访问请求进入云服务器。其中，第一预定条件包括：多个入访基准地址中不存在与源访问地址相匹配的地址、且多个入访基准端口中不存在与源端口相匹配的地址；或者，多个入访基准地址中不存在与源访问地址相匹配的地址、且多个入访基准端口中存在与源端口相匹配的地址。

[0106] 根据本发明的实施例，源访问地址匹配到入访基准地址但源端口没有匹配到入访基准地址的情况下，可能是用户使用了已经授权用户的访问地址，但是，由于用户的源端口没有匹配到入访基准端口，为了保证网络访问的安全性，将该用户作为未授权用户，不生成入访控制记录。

[0107] 根据本发明的实施例，入访控制记录可以理解为通行标识，在生成入访控制记录之后，云服务器可以根据入访控制记录，控制具有该源访问地址和源端口的用户的网络访问请求进入云服务器。

[0108] 根据本发明的实施例，在没有生成入访控制记录的情况下，云服务器无法根据入访控制记录放行用户，由此，能够实现拒绝当前网络访问请求进入云服务器。

[0109] 例如，入访基准地址包括XXA和XXB，入访基准端口包括XXC和XXD。

[0110] 在源访问地址为YYA，源端口为YYC的情况下，源访问地址YYA与XXA、XXB均不匹配，源端口YYC与XXC、XXD均不匹配，由此，不生成入访控制记录。

[0111] 在源访问地址为YYA，源端口为XXC的情况下，源访问地址YYA与XXA、XXB均不匹配，源端口XXC与入访基准端口中的XXC匹配。一般情况下，源访问地址不匹配、端口匹配的情况可以视为错误信息，由此，不生成入访控制记录。

[0112] 在源访问地址为XXA，源端口为YYC的情况下，源访问地址XXA与入访基准地址中的XXA匹配，源端口YYC与XXC、XXD均不匹配，由此，生成第二访问记录。

[0113] 在源访问地址为XXA，源端口为XXC的情况下，源访问地址XXA与入访基准地址中的XXA匹配，源端口XXC与入访基准端口中的XXC匹配，由此，生成第一访问记录。

[0114] 图3示出了根据本发明实施例的入访控制记录生成方法的流程图。

[0115] 如图3所示，入访控制记录生成方法300展示了根据访问数据和基准数据生成入访控制记录的过程。

[0116] 根据本发明的实施例，访问数据包括源访问地址301和源端口303，基准数据包括多个入访基准地址302和多个入访基准端口304。

[0117] 比较源访问地址301和多个入访基准地址302是否相同，可以得到第一匹配子结果305；比较源端口303和多个入访基准端口304是否相同，可以得到第二匹配子结果306。其中，云服务器能够以基准表的形式包括多个入访基准地址和多个入访基准端口，通过比较基准表中是否存在与源访问地址或源端口，得到第一匹配子结果或第二匹配子结果。

[0118] 在第一匹配子结果305表征多个入访基准地址302中存在与源访问地址301相匹配的地址，且第二匹配子结果306表征多个入访基准端口304中存在与源端口303相匹配的端口的情况下，生成第一入访记录307。在第一匹配子结果305表征多个入访基准地址302中不存在与源访问地址301相匹配的地址，且第二匹配子结果306表征多个入访基准端口304中存在与源端口303相匹配的端口的情况下，生成第二入访记录308。

[0119] 根据本发明的实施例，基于第一匹配子结果，生成第一入访记录，包括：根据第一

匹配子结果，获取与源访问地址相匹配的匹配访问地址；确定匹配访问地址所属的网络区域；根据网络区域和源端口，生成第一入访记录。

[0120] 根据本发明的实施例，在源访问地址与入访基准地址相匹配的情况下，第一匹配子结果还包括多个入访基准地址中与源访问地址相匹配的匹配访问地址，由此，可以根据第一匹配子结果直接获取入访基准地址中与源访问地址相匹配的匹配访问地址。

[0121] 根据本发明的实施例，云服务器包括多个网络区域，多个网络区域的授权范围不同。

[0122] 根据本发明的实施例，按照云服务器的物理架构，可以将云服务器划分为多个网络区域，目标区域为外联网区、互联网区和开放区其中之一，外联网区用于接收通过目标局域网进行访问的网络访问请求，互联网区用于接收通过互联网进行访问的网络访问请求；开放区用于接收通过外联网区或互联网区进行访问的网络访问请求。其中，目标区域可以属于外联网区、互联网区和开放区其中之一。

[0123] 根据本发明的实施例，云服务器还包括云资源区，用于存储多种云上负载均衡、云存储、云数据库等多种数据。

[0124] 根据本发明的实施例，匹配访问地址中包括表征该匹配访问地址所属网络区域的区域标识，根据该区域标识，可以确定匹配网络区域所属的网络区域。

[0125] 例如，匹配访问地址为“1.2.10”，其中，两个点中间的数字为区域标识。2为外联网区的区域标识，由此，根据“1.2.10”中的“2”可以确定匹配访问地址所属的网络区域为外联网区。

[0126] 根据本发明的实施例，在确定匹配访问地址之后，可以根据匹配访问地址所属的网络区域，调用不同的生成规则；基于生成规则，根据网络区域和源端口生成第一访问记录。

[0127] 本发明的实施在源访问地址和源端口均能匹配到入访基准地址和入访基准端口的情况下，进一步确定匹配访问地址的网络区域，并根据网络区域，能够生成不同控制权限的第一入访记录。本发明的实施例利用基于入访基准地址和网络区域的双层处理，能够针对不同的网络访问请求生成不同控制权限的第一入访记录，从而提高网络访问请求的控制准确性。

[0128] 图4示出了根据本发明一具体实施例的第一入访记录生成方法的流程图。

[0129] 根据本发明的实施例，第一入访记录生成方法400示意性使出了根据第一匹配子结果生成第一入访记录的过程。

[0130] 例如，在第一匹配子结果401表征多个入访基准地址中存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，从第一匹配子结果401中获取匹配访问地址402。

[0131] 进一步地，确定匹配访问地址402所属的网络区域403，之后，基于网络区域403和源端口404，生成第一入访记录405。

[0132] 根据本发明的实施例，根据网络区域和源端口，生成第一入访记录，包括：在网络区域属于目标区域或云资源区的情况下，根据匹配访问地址、源端口和放行标识，生成第一入访记录；在网络区域不属于目标区域且不属于云资源区的情况下，根据网络区域的标识、源端口和放行标识，生成第一入访记录。

[0133] 根据本发明的实施例，网络区域属于目标区域或云资源区，表征该用户调用目标区域中的服务，或者调用云资源区中的服务。在匹配访问地址属于目标区域或云资源区的情况下，该用户发起的网络访问请求可以进入目标区域或通过目标区域进入云资源区，由此，可以直接根据匹配访问地址、源端口和放行标识，生成第一入访记录，以便在目标区域或云资源区控制网络访问请求的通行。

[0134] 根据本发明的实施例，在网络区域不属于目标区域且不属于云资源区时，表征该用户调用的服务不属于目标区域和云资源区。此时，由于该网络访问请求是由目标区域进入的，因此，该用户发起的网络访问请求需要通过目标区域进入用户调用服务所属的网络区域，需要向用户开放进入用户调用服务所属网络区域的权限。由此，可以直接根据匹配访问地址所属的网络区域的标识、源端口和放行标识，生成第一入访记录，以便控制网络访问请求的进入匹配访问地址所属的网络区域。

[0135] 根据本发明的实施例，在网络区域为目标区域或云资源区时，生成的第一入访记录为“IP地址+源端口+允许通行”。在网络区域不属于目标区域且不属于云资源区时，生成的第一入访记录为“网络区域的ID+源端口+允许通行”。

[0136] 例如，源访问地址为“1.1.11”也就是IP地址为“1.1.11”，源端口为“80”。在网络区域为目标区域或云资源区时，第一入访记录为“1.1.11+80+允许通行”。在网络区域为区域A，且区域A不属于目标区域和云资源区的情况下，区域A的ID为“1.2.00”，第一入访记录为“1.2.00+80+允许通行”。

[0137] 根据本发明的实施例，基于目标区域，生成第二入访记录，包括：在确定目标区域为外联网区的情况下，根据外联网区的标识、源端口和放行标识，生成第二入访记录；在确定目标区域为互联网区的情况下，根据互联网区的标识、源端口和放行标识，生成第二入访记录；在确定目标区域为开放区的情况下，根据源访问地址、源端口和放行标识，生成待确认入访记录；以及根据待确认入访记录，生成第二入访记录。

[0138] 根据本发明的实施例，云服务器中多个网络区域的安全等级不同，为了保证每个网络区域的安全性，针对每个网络区域释放的安全控制权限也不同。

[0139] 例如，互联网区对外提供互联网访问入口；外联网区对外提供专线访问入口，也就是局域网专线访问入口；开放区不对外暴露，仅对内提供服务调用及实现。由此，开放区的安全等级要高于互联网区和外联网区。

[0140] 根据本发明的实施例，针对互联网区和外联网区，在源访问地址未匹配到入访基准地址、源端口匹配到入访基准端口时，认为用户可能使用未授权的IP地址，可以开放互联网区和外联网区的控制权限，使得来自源端口的网络访问请求能够进入互联网区和外联网区。

[0141] 根据本发明的实施例，针对开放区，在源访问地址未匹配到入访基准地址、源端口匹配到入访基准端口时，由于开放区的安全控制权限高于互联网区和外联网区，因此，根据源访问地址和源端口生成待确认入访记录，并基于待确认入访记录生成第二入访记录，以便控制来自源访问地址和源端口的网络访问请求进入开放区。

[0142] 例如，在目标区域为互联网区或外联网区时，生成的第二入访记录为“互联网区的ID+源端口+允许通行”或“外联网区的ID+源端口+允许通行”。在目标区域为开放区时，生成的待确认入访记录为“IP地址+源端口+允许通行”。

[0143] 在本发明的实施例中，针对不同的目标区域，通过不同方式生成第二访问记录，不仅能够针对不同安全等级的网络区域设置不同的控制权限，还能在保证访问安全的基础上，提高网络访问控制的灵活性和适用性。

[0144] 需要说明的是，采用上述实施例，保证因更换局域网等操作导致IP地址发生变化的用户也能顺利调用云服务器中的服务，能够提高用户体验。由于针对不同目标区域开放不同的控制权限，既能够保证用户下次更换IP地址时也能顺利调用部分安全等级较低的服务，至少部分地提高了用户体验；又能减少安全等级较高的服务的暴露程度，降低安全风险。

[0145] 图5示出了根据本发明一具体实施例的第二入访记录生成方法的流程图。

[0146] 如图5所示，第二入访记录生成方法500包括操作S501~S505。

[0147] 在操作S501，确定目标区域的类型。具体地，在确定目标区域属于外联网区时，进入操作S502；在确定目标区域属于互联网区时，进入操作S503；在确定目标区域属于开放区时，进入操作S504。

[0148] 在操作S502，根据外联网区的标识、源端口和放行标识，生成第二入访记录。

[0149] 在操作S503，根据互联网区的标识、源端口和放行标识，生成第二入访记录。

[0150] 在操作S504，根据源访问地址、源端口和放行标识，生成待确认入访记录。在执行操作S504之后，进入操作S505。

[0151] 在操作S505，根据待确认入访记录，生成第二入访记录。

[0152] 根据本发明的实施例，根据待确认入访记录，生成第二入访记录，包括：将待确认入访记录存储至目标区域的待确认入访表；响应于接收到针对待确认入访表中待确认入访记录的确认指令，将待确认入访记录作为第二入访记录。

[0153] 根据本发明的实施例，待确认入访表可以包括多个待确认入访记录，以便审核人员根据待确认入访表确定一个或多个待确认入访记录。

[0154] 根据本发明的实施例，在将待确认入访记录存储至目标区域的待确认入访表之后，可以向审核人员的终端设备发送一条提示，以便审核人员确认该待确认指令。

[0155] 根据本发明的实施例，还可以定时将待确认入访表发送至审核人员的终端设备，以便审核人员批量确认。

[0156] 根据本发明的实施例，审核人员确认待确认入访表中的待确认入访记录之后，由审核人员的终端设备向云服务器发送有关该待确认入访记录的确认指令。云服务器响应于接收到上述待确认指令，可以将待确认入访记录作为第二入访记录。

[0157] 在本发明的实施例中，在源访问地址未匹配到入访基准地址、且源端口匹配到入访基准端口的情况下，该网络访问请求可能存在风险，为了保证开放区的安全，增加了确认指令的操作，通过人工确认后生成第二访问记录，能够进一步提高开放区的安全性。

[0158] 根据本发明的实施例，访问地址包括目标访问地址，端口包括目标端口，基准地址包括多个出访基准地址，基准端口包括多个出访基准端口。

[0159] 根据本发明的实施例，目标访问地址表征网络访问请求要访问的服务的地址，目标端口表征网络访问请求要访问的服务的端口。出访基准地址可以表征云服务器中服务的IP地址，出访基准端口表征云服务器中服务的端口。其中，根据出访基准地址和出访基准端口可以确定网络访问请求是否能调用云服务器中的某个服务。

[0160] 例如，出访基准地址包括XXE和XXF，出访基准端口包括XXG和XXH，其中服务A的地址为XXE、端口为XXG。在访问数据中的目标访问地址为XXE，目标端口为XXG的情况下，由于目标访问地址和目标端口均能匹配到出访基准地址和出访基准端口，因此，用户能够使用服务A。由此，云服务器可以通过出访控制记录将网络访问请求输出至服务A。

[0161] 第一匹配结果包括第三匹配子结果，第二匹配结果包括第四匹配子结果；出访控制记录包括第一出访记录和第二出访记录。

[0162] 根据本发明的实施例，根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成访问控制记录，包括：

[0163] 在第三匹配子结果表征多个出访基准地址中存在与目标访问地址相匹配的地址，且第四匹配子结果表征多个出访基准端口中存在与目标端口相匹配的端口的情况下，基于第三匹配子结果，生成第一出访记录；

[0164] 在第三匹配子结果表征多个出访基准地址中不存在与目标访问地址相匹配的地址，且第四匹配子结果表征多个出访基准端口中存在与目标端口相匹配的端口的情况下，基于目标区域，生成第二出访记录。

[0165] 根据本发明的实施例，在满足第二预定条件的情况下，确定网络访问请求存在风险，不生成出访控制记录，以便拒绝该网络访问请求调用云服务器中的目标服务。其中，第二预定条件包括：多个出访基准地址中不存在与目标访问地址相匹配的地址、且多个出访基准端口中不存在与目标端口相匹配的地址；或者，多个出访基准地址中不存在与目标访问地址相匹配的地址、且多个出访基准端口中存在与目标端口相匹配的地址。

[0166] 根据本发明的实施例，生成第一出访记录的操作与生成第一入访记录的操作相同或相似，生成第二出访记录的操作与生成第一入访记录的操作相同或相似，在此不再赘述。

[0167] 根据本发明的实施例，根据用于访问目标区域的网络流量，确定访问数据，包括：获取网络流量的流量镜像，其中，流量镜像包括访问数据包；解析访问数据包，得到解析数据；对解析数据进行去重处理，得到访问数据，其中，访问数据存储于目标区域的数据库实时表。

[0168] 根据本发明的实施例，流量镜像(Mirroring/traffic-shadow)，也称为作影子流量，是指通过一定的配置将线上的真实网络流量复制到镜像服务中。本发明的实施例通过流量镜像转发获取访问数据包，能够在不影响线上云服务的情况下对流量或网络访问请求的内容进行分析。

[0169] 根据本公开的实施例，可以按照预定周期，定时采集多个流量镜像。

[0170] 根据本发明的实施例，解析访问数据包的过程包括：对访问数据包进行解析，得到多个二进制比特流；之后，对二进制比特流中的多个字段进行提取和解析，得到解析数据。解析数据包括入访流量和出访流量的时间戳、源访问地址、源端口、目标访问地址、目标端口等结构化数据信息。

[0171] 根据本发明的实施例，去重处理用于删除解析数据中源访问地址、源端口、目标访问地址、目标端口相同的网络访问请求。

[0172] 根据本发明的实施例，在生成入访控制记录和出访控制记录之后，还包括：将入访控制记录和出访控制记录存储至目标区域的安全组；基于安全组，控制网络访问请求进入云服务器，并将网络访问请求输出至目标区域的目标服务；或者，基于安全组，控制网络访

问请求进入云服务器，并将网络访问请求输出至其他区域的目标服务，其他区域包括云服务器中与目标区域不同的区域。

[0173] 根据本发明的实施例，安全组是一种有状态的虚拟防火墙，用于管理云服务器中一个或多个服务器的网络访问控制权限。将入访控制记录和出访控制记录存储至目标区域的安全组之后，目标区域的安全组可以确定网络访问请求是否进入云服务器，并确定是否将网络访问请求输出至目标区域的目标服务。

[0174] 根据本发明的实施例，由于网络访问请求也可能访问云服务器中不属于目标区域的服务，由此，目标区域的安全组也可以控制网络访问请求进入云服务器，并将网络访问请求输出至其他区域的安全组，以便其他区域的安全组控制网络访问请求输出至目标服务。

[0175] 图6示出了根据本发明实施例的云服务器的系统架构图。

[0176] 如图6所示，云服务器的系统架构600包括互联网区、外联网区、开放区。

[0177] 互联网区通过互联入口接收通过互联网进行访问的网络访问请求，并由互联网安全组控制多个网络访问请求的进入、输出至目标服务。

[0178] 外联网区通过外联入口接收通过目标局域网进行访问的网络访问请求，并由外联网安全组控制多个网络访问请求的进入、输出至目标服务。

[0179] 其中，目标服务可以设置于互联网区和外联网区内部，可以设置于云资源处，还可以设置于开放区。

[0180] 互联网区安全组和外联网区安全组通过将网络访问请求输出至外部访问入口，由开放区安全组将网络访问请求输出至开放区中的服务中。

[0181] 根据本发明的实施例，互联网安全组、外联网区安全组和开放区安全组也可以通过交互获取入访控制记录和出访控制记录。本发明实施例中的安全组可以为互联网安全组、外联网区安全组和开放区安全组其中之一。

[0182] 图7示出了根据本发明实施例的网络访问的控制装置的结构框图。

[0183] 如图7所示，该实施例的网络访问的控制装置700包括确定模块710、获取模块720和生成模块730。

[0184] 确定模块710，用于根据用于访问目标区域的网络流量，确定访问数据，其中，访问数据包括访问地址和端口，网络流量包括多个网络访问请求，目标区域属于云服务器。在一实施例中，确定模块710，可以用于执行前文描述的操作S210，在此不再赘述。

[0185] 获取模块720，用于获取针对目标区域的基准数据，其中，基准数据包括基准地址和基准端口。在一实施例中，获取模块720可以用于执行前文描述的操作S220，在此不再赘述。

[0186] 生成模块730，用于根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录，其中，入访控制记录用于控制网络访问请求进入云服务器，出访控制记录用于将网络访问请求输出至云服务器中的目标服务。在一实施例中，生成模块730可以用于执行前文描述的操作S230，在此不再赘述。

[0187] 根据本发明的实施例，访问地址包括源访问地址，端口包括源端口，基准地址包括多个入访基准地址，基准端口包括多个入访基准端口，第一匹配结果包括第一匹配子结果，第二匹配结果包括第二匹配子结果；入访控制记录包括第一入访记录或第二入访记录。

[0188] 生成模块730包括第一生成子模块和第二生成子模块。

[0189] 第一生成子模块用于在第一匹配子结果表征多个入访基准地址中存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，基于第一匹配子结果，生成第一入访记录。

[0190] 第二生成子模块用于在第一匹配子结果表征多个入访基准地址中不存在与源访问地址相匹配的地址，且第二匹配子结果表征多个入访基准端口中存在与源端口相匹配的端口的情况下，基于目标区域，生成第二入访记录。

[0191] 根据本发明的实施例，第一生成子模块包括获取单元、确定单元和第一生成单元。

[0192] 获取单元用于根据第一匹配子结果，获取与源访问地址相匹配的匹配访问地址。

[0193] 确定单元用于确定匹配访问地址所属的网络区域。

[0194] 第一生成单元用于根据网络区域和源端口，生成第一入访记录。

[0195] 根据本发明的实施例，第一生成单元包括第一生成子单元和第二生成子单元。

[0196] 第一生成子单元用于在网络区域属于目标区域或云资源区的情况下，根据匹配访问地址、源端口和放行标识，生成第一入访记录。

[0197] 第二生成子单元用于在网络区域不属于目标区域且不属于云资源区的情况下，根据网络区域的标识、源端口和放行标识，生成第一入访记录。

[0198] 根据本发明的实施例，云服务器包括外联网区、互联网区和开放区，目标区域为外联网区、互联网区和开放区其中之一，外联网区用于接收通过目标局域网进行访问的网络访问请求，互联网区用于接收通过互联网进行访问的网络访问请求；开放区用于接收通过外联网区或互联网区进行访问的网络访问请求。

[0199] 根据本发明的实施例，第二生成子模块包括第二生成单元、第三生成单元、第四生成单元和第五生成单元。

[0200] 第二生成单元用于在确定目标区域为外联网区的情况下，根据外联网区的标识、源端口和放行标识，生成第二入访记录。

[0201] 第三生成单元用于在确定目标区域为互联网区的情况下，根据互联网区的标识、源端口和放行标识，生成第二入访记录。

[0202] 第四生成单元用于在确定目标区域为开放区的情况下，根据源访问地址、源端口和放行标识，生成待确认入访记录。

[0203] 第五生成单元用于根据待确认入访记录，生成第二入访记录。

[0204] 根据本发明的实施例，第五生成单元包括存储子单元和确认子单元。

[0205] 存储子单元用于将待确认入访记录存储至目标区域的待确认入访表。

[0206] 确认子单元用于响应于接收到针对待确认入访表中待确认入访记录的确认指令，将待确认入访记录作为第二入访记录。

[0207] 根据本发明的实施例，访问地址包括目标访问地址，端口包括目标端口，基准地址包括多个出访基准地址，基准端口包括多个出访基准端口，第一匹配结果包括第三匹配子结果，第二匹配结果包括第四匹配子结果；出访控制记录包括第一出访记录或第二出访记录。

[0208] 根据本发明的实施例，生成模块730包括第三生成子模块和第四生成子模块。

[0209] 第三生成子模块用于在第三匹配子结果表征多个出访基准地址中存在与目标访问地址相匹配的地址，且第四匹配子结果表征多个出访基准端口中存在与目标端口相匹配

的端口的情况下,基于第三匹配子结果,生成第一出访记录。

[0210] 第四生成子模块用于在第三匹配子结果表征多个出访基准地址中不存在与目标访问地址相匹配的地址,且第四匹配子结果表征多个出访基准端口中存在与目标端口相匹配的端口的情况下,基于目标区域,生成第二出访记录。

[0211] 根据本发明的实施例,确定模块710包括镜像获取子模块、解析子模块和去重子模块。

[0212] 镜像获取子模块用于获取网络流量的流量镜像,其中,流量镜像包括访问数据包。

[0213] 解析子模块用于解析访问数据包,得到解析数据。

[0214] 去重子模块用于对解析数据进行去重处理,得到访问数据,其中,访问数据存储于目标区域的数据库实时表。

[0215] 根据本发明的实施例,网络访问的控制装置700还包括存储模块和控制模块。

[0216] 存储模块用于将入访控制记录和出访控制记录存储至目标区域的安全组。

[0217] 控制模块用于基于安全组,控制网络访问请求进入云服务器,并将网络访问请求输出至目标区域的目标服务;或者,基于安全组,控制网络访问请求进入云服务器,并将网络访问请求输出至其他区域的目标服务,其他区域包括云服务器中与目标区域不同的区域。

[0218] 根据本发明的实施例,确定模块710、获取模块720和生成模块730中的任意多个模块可以合并在一个模块中实现,或者其中的任意一个模块可以被拆分成多个模块。或者,这些模块中的一个或多个模块的至少部分功能可以与其他模块的至少部分功能相结合,并在一个模块中实现。

[0219] 根据本发明的实施例,确定模块710、获取模块720和生成模块730中的至少一个可以至少被部分地实现为硬件电路,例如现场可编程门阵列(FPGA)、可编程逻辑阵列(PLA)、片上系统、基板上的系统、封装上的系统、专用集成电路(ASIC),或可以通过对电路进行集成或封装的任何其他的合理方式等硬件或固件来实现,或以软件、硬件以及固件三种实现方式中任意一种或以其中任意几种的适当组合来实现。或者,确定模块710、获取模块720和生成模块730中的至少一个可以至少被部分地实现为计算机程序模块,当该计算机程序模块被运行时,可以执行相应的功能。

[0220] 图8示出了根据本发明实施例的适于网络访问的控制方法的电子设备的方框图。

[0221] 如图8所示,根据本发明实施例的电子设备800包括处理器801,其可以根据存储在只读存储器(ROM)802中的程序或者从存储部分808加载到随机访问存储器(RAM)803中的程序而执行各种适当的动作和处理。处理器801例如可以包括通用微处理器(例如CPU)、指令集处理器和/或相关芯片组和/或专用微处理器(例如,专用集成电路(ASIC))等等。处理器801还可以包括用于缓存用途的板载存储器。处理器801可以包括用于执行根据本发明实施例的方法流程的不同动作的单一处理单元或者是多个处理单元。

[0222] 在RAM803中,存储有电子设备800操作所需的各种程序和数据。处理器801、ROM802以及RAM803通过总线804彼此相连。处理器801通过执行ROM802和/或RAM803中的程序来执行根据本发明实施例的方法流程的各种操作。需要注意,所述程序也可以存储在除ROM802和RAM803以外的一个或多个存储器中。处理器801也可以通过执行存储在所述一个或多个存储器中的程序来执行根据本发明实施例的方法流程的各种操作。

[0223] 根据本发明的实施例，电子设备800还可以包括输入/输出(I/O)接口805，输入/输出(I/O)接口805也连接至总线804。电子设备800还可以包括连接至输入/输出I/O接口805的以下部件中的一项或多项：包括键盘、鼠标等的输入部分806；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分807；包括硬盘等的存储部分808；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分809。通信部分809经由诸如因特网的网络执行通信处理。驱动器810也根据需要连接至I/O接口805。可拆卸介质811，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器810上，以便于从其上读出的计算机程序根据需要被安装入存储部分808。

[0224] 本发明还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中描述的设备/装置/系统中所包含的；也可以是单独存在，而未装配入该设备/装置/系统中。上述计算机可读存储介质承载有一个或者多个程序，当上述一个或者多个程序被执行时，实现根据本发明实施例的方法。

[0225] 根据本发明的实施例，计算机可读存储介质可以是非易失性的计算机可读存储介质，例如可以包括但不限于：便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本发明中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。例如，根据本发明的实施例，计算机可读存储介质可以包括上文描述的ROM802和/或RAM803和/或ROM802和RAM803以外的一个或多个存储器。

[0226] 本发明的实施例还包括一种计算机程序产品，其包括计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。当计算机程序产品在计算机系统中运行时，该程序代码用于使计算机系统实现本发明实施例所提供上述方法。

[0227] 在该计算机程序被处理器801执行时执行本发明实施例的系统/装置中限定的上述功能。根据本发明的实施例，上文描述的系统、装置、模块、单元等可以通过计算机程序模块来实现。

[0228] 在一种实施例中，该计算机程序可以依托于光存储器件、磁存储器件等有形存储介质。在另一种实施例中，该计算机程序也可以在网络介质上以信号的形式进行传输、分发，并通过通信部分809被下载和安装，和/或从可拆卸介质811被安装。该计算机程序包含的程序代码可以用任何适当的网络介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

[0229] 在这样的实施例中，该计算机程序可以通过通信部分809从网络上被下载和安装，和/或从可拆卸介质811被安装。在该计算机程序被处理器801执行时，执行本发明实施例的系统中限定的上述功能。根据本发明的实施例，上文描述的系统、设备、装置、模块、单元等可以通过计算机程序模块来实现。

[0230] 根据本发明的实施例，可以以一种或多种程序设计语言的任意组合来编写用于执行本发明实施例提供的计算机程序的程序代码，具体地，可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。程序设计语言包括但不限于诸如Java，C++，python，“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、部分在远程计算设备上执行、或者完全在远程计算设备

或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网(LAN)或广域网(WAN)，连接到用户计算设备，或者，可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0231] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0232] 本领域技术人员可以理解，本发明的各个实施例和/或权利要求中记载的特征可以进行多种组合或/或结合，即使这样的组合或结合没有明确记载于本发明中。特别地，在不脱离本发明精神和教导的情况下，本发明的各个实施例和/或权利要求中记载的特征可以进行多种组合和/或结合。所有这些组合和/或结合均落入本发明的范围。

[0233] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

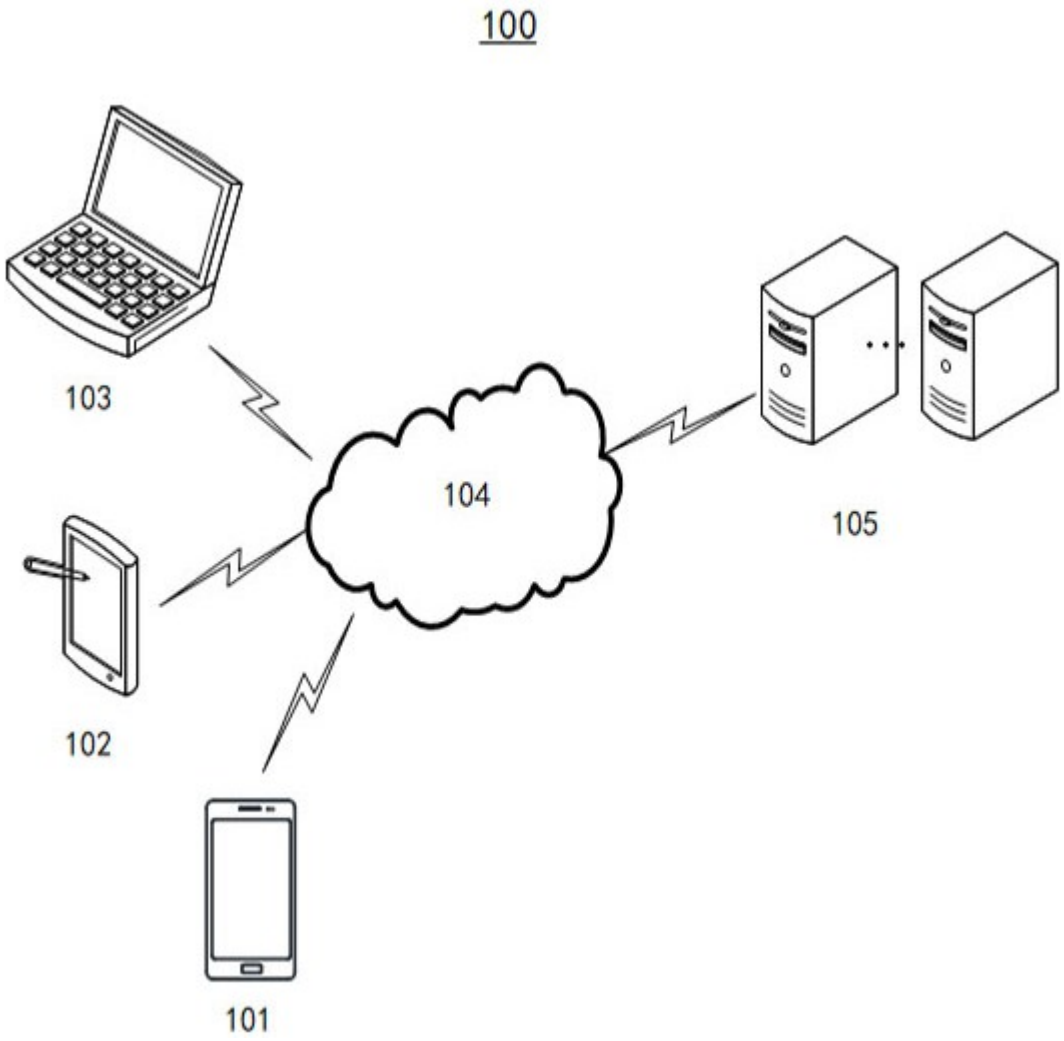


图 1

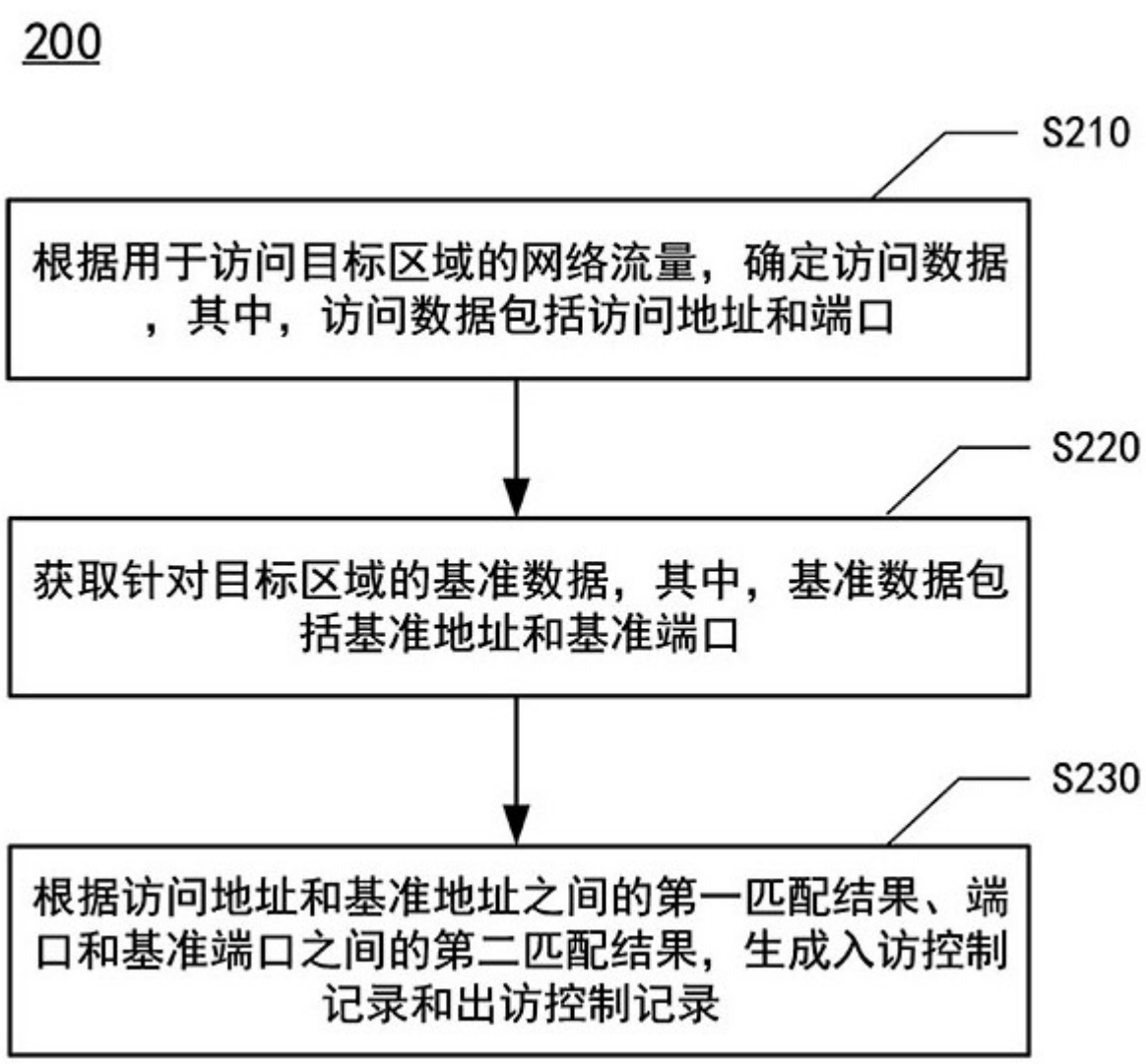

200
S210
根据用于访问目标区域的网络流量，确定访问数据，其中，访问数据包括访问地址和端口
S220
获取针对目标区域的基准数据，其中，基准数据包括基准地址和基准端口
S230
根据访问地址和基准地址之间的第一匹配结果、端口和基准端口之间的第二匹配结果，生成入访控制记录和出访控制记录

图 2

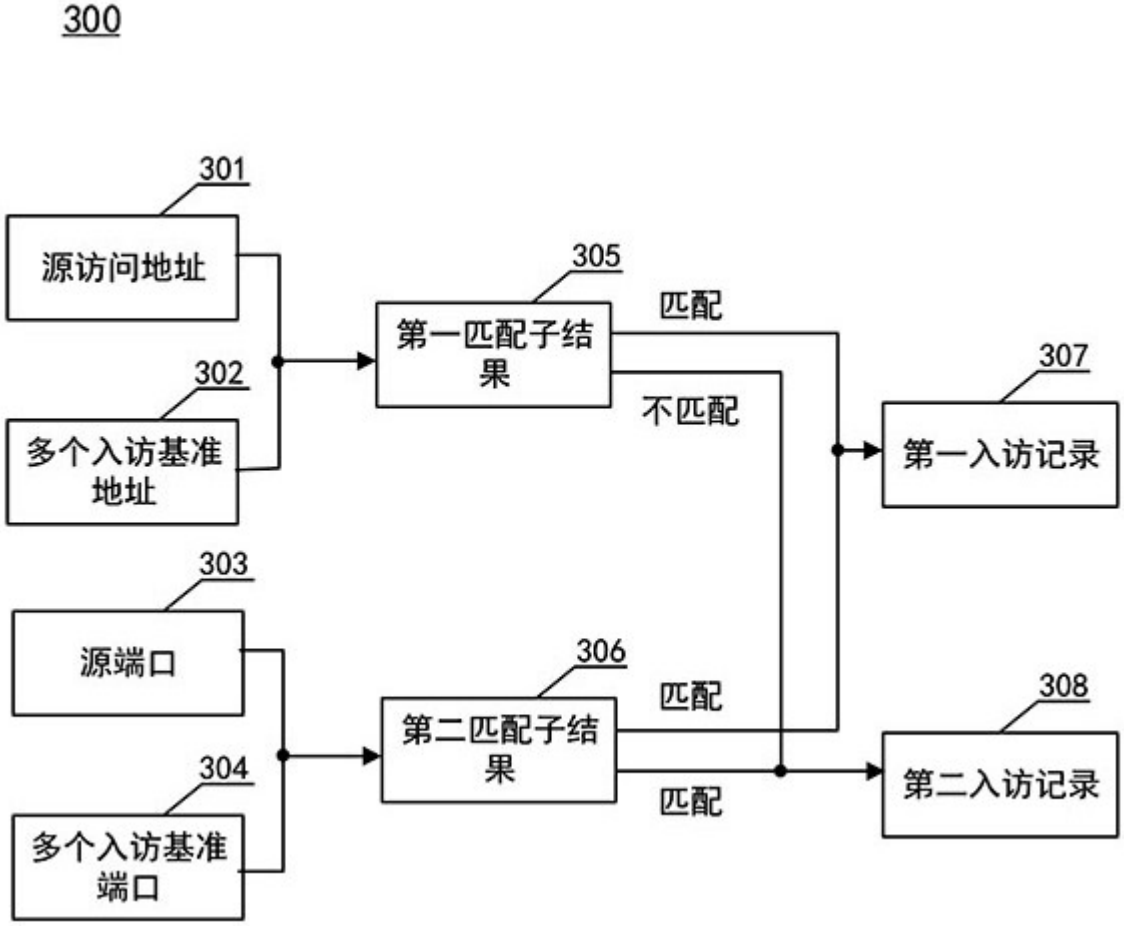

300
301
源访问地址
302
多个入访基准地址
303
源端口
304
多个入访基准端口
305
第一匹配子结果
306
第二匹配子结果
匹配
不匹配
匹配
匹配
307
第一入访记录
308
第二入访记录

图 3

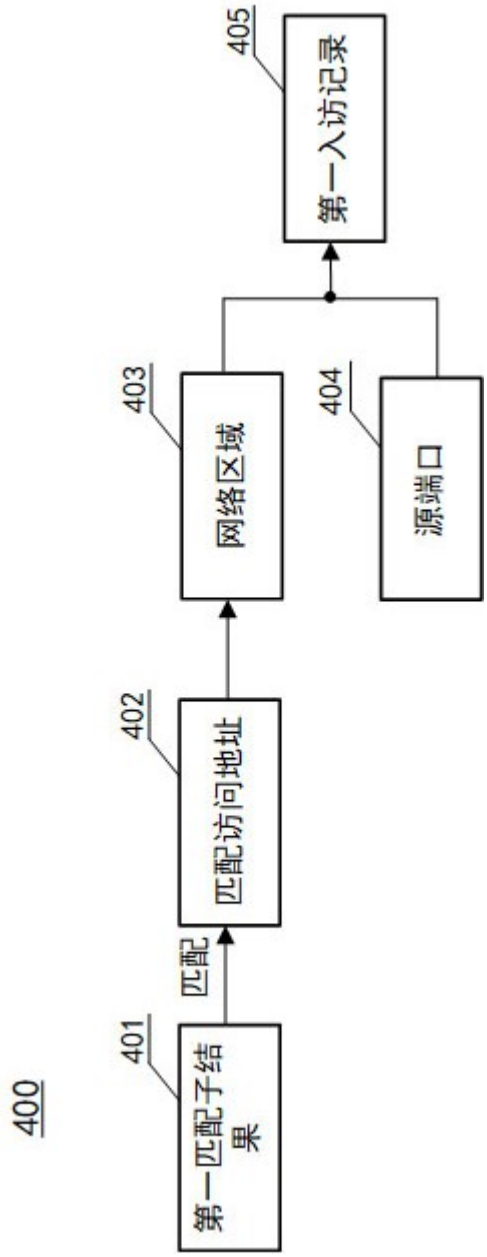


图 4

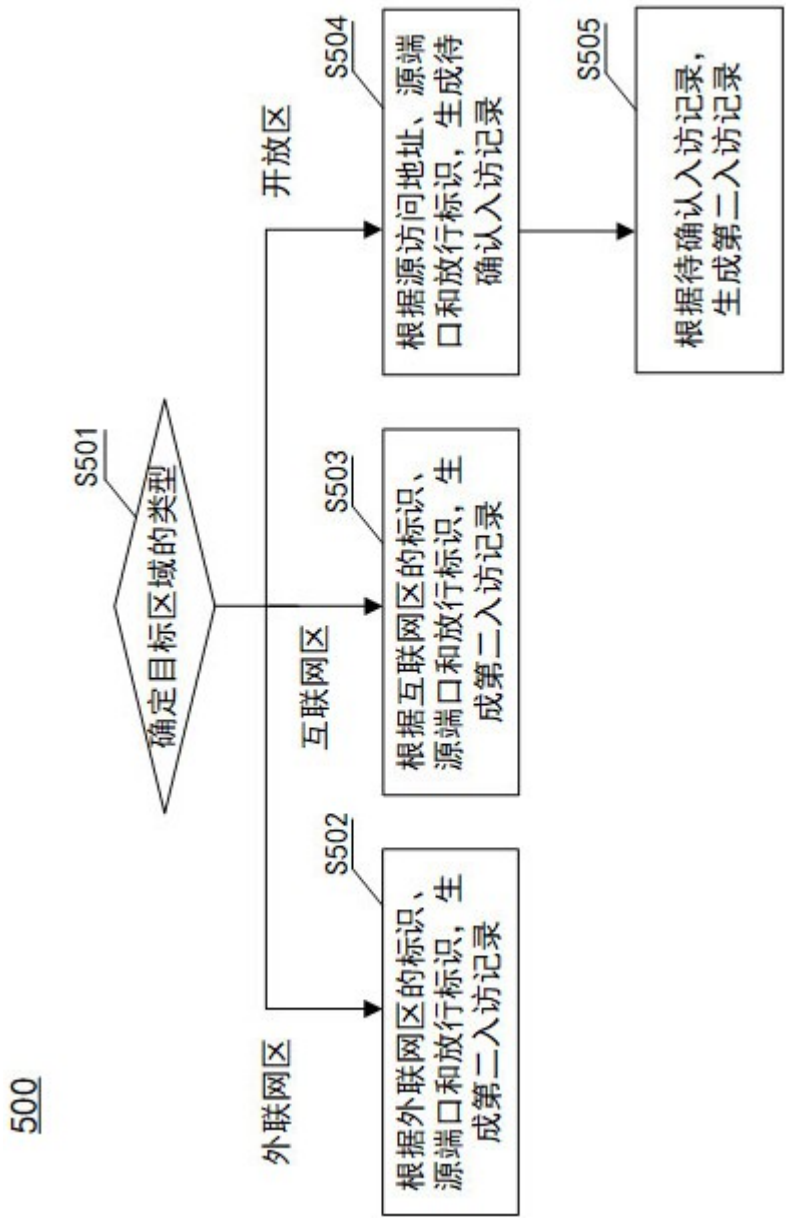

500
确定目标区域的类型
S501
外联网区
S502
根据外联网区的标识、源端口和放行标识，生成第二入访记录
互联网区
S503
根据互联网区的标识、源端口和放行标识，生成第二入访记录
开放区
S504
根据源访问地址、源端口和放行标识，生成待确认入访记录
S505
根据待确认入访记录，生成第二入访记录

图 5

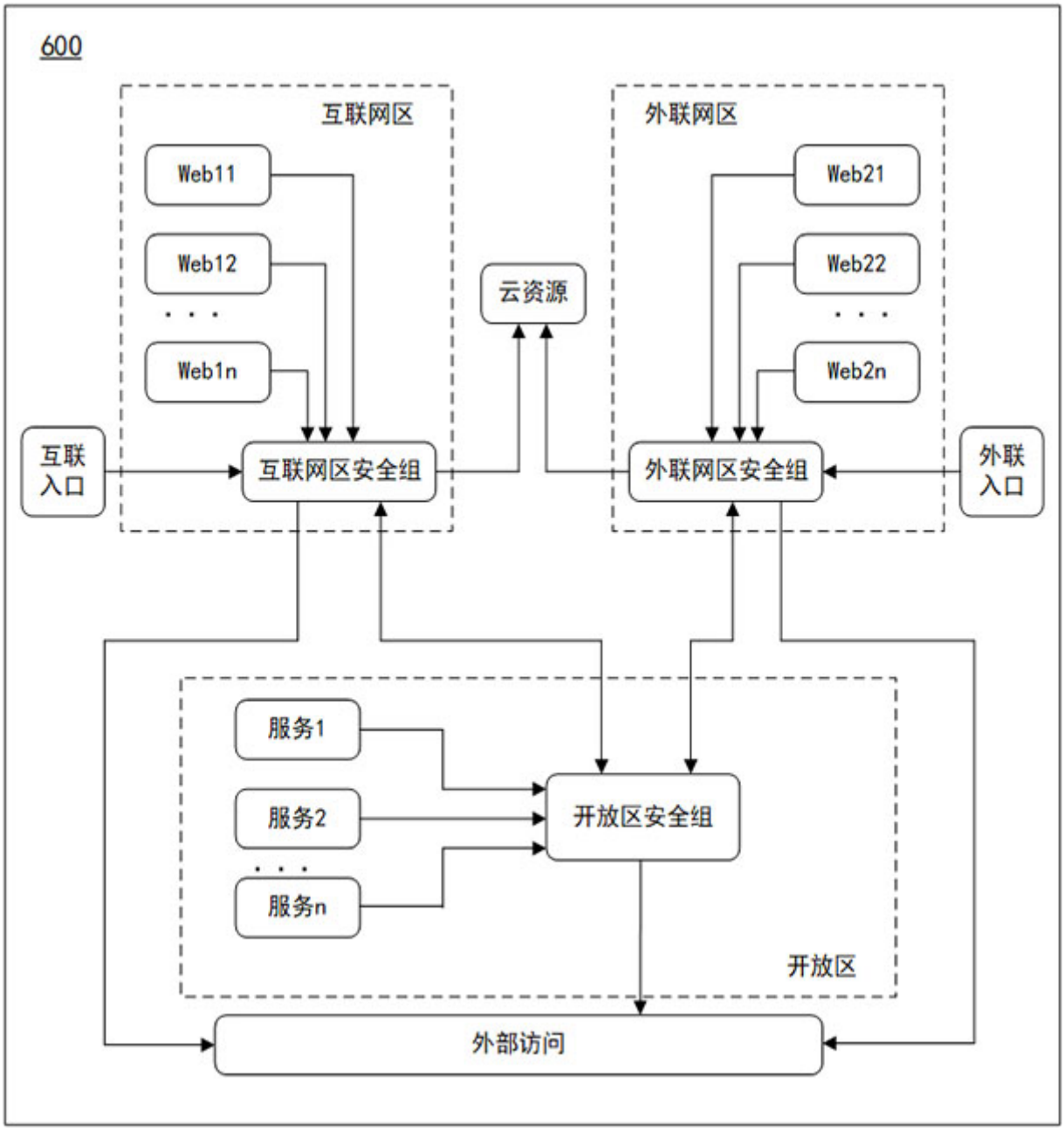

600
互联网区
外联网区
Web11
Web12
Web1n
Web21
Web22
Web2n
云资源
互联入口
互联网区安全组
外联网区安全组
外联入口
服务1
服务2
服务n
开放区安全组
开放区
外部访问

图 6

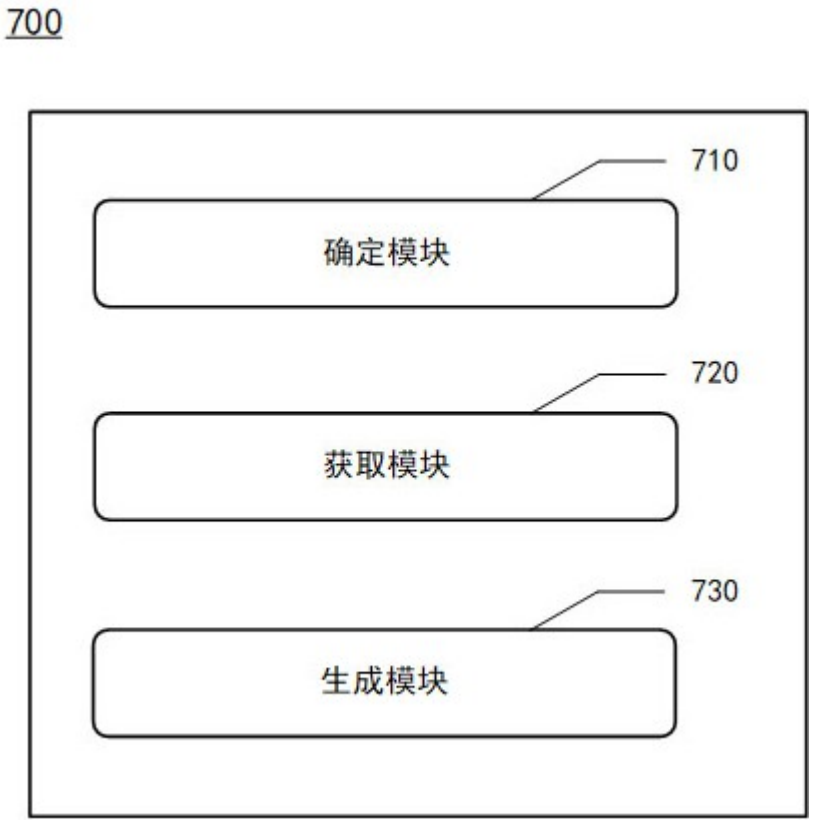

700
710
确定模块
720
获取模块
730
生成模块

图 7

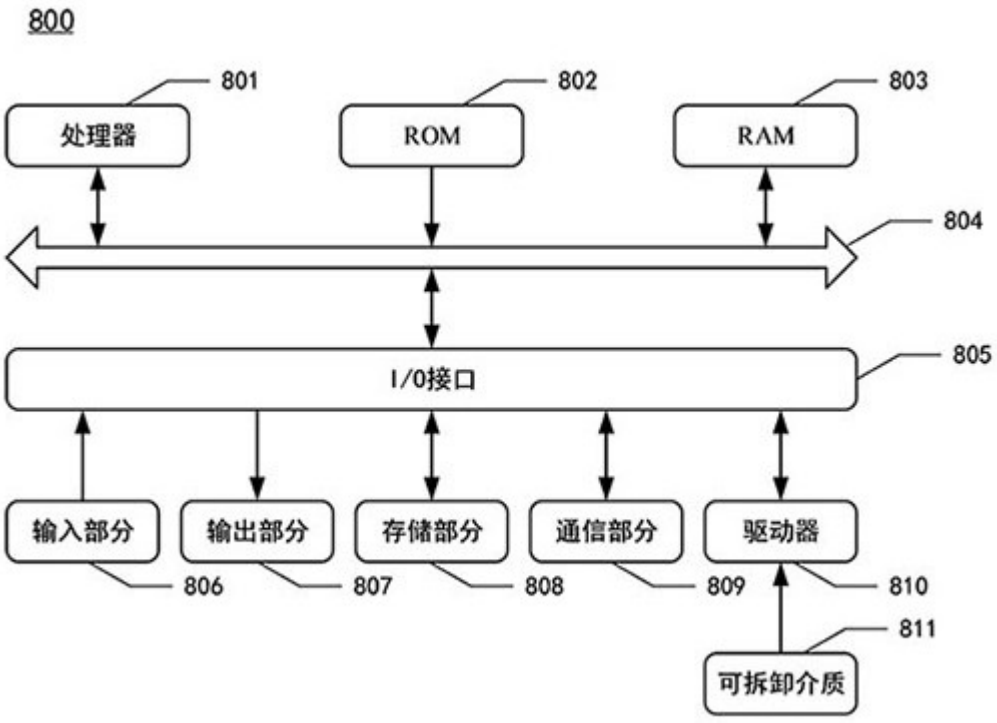

800
801
处理器
802
ROM
803
RAM
804
805
I/O接口
输入部分
输出部分
存储部分
通信部分
驱动器
806
807
808
809
810
811
可拆卸介质

图 8