

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2025 年 1 月 30 日 (30.01.2025)



(10) 国际公布号
WO 2025/020439 A1

- (51) 国际专利分类号:
H04L 9/40 (2022.01)
- (21) 国际申请号: PCT/CN2023/140249
- (22) 国际申请日: 2023 年 12 月 20 日 (20.12.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202310906721.8 2023年7月24日 (24.07.2023) CN
- (71) 申请人: 中国电信股份有限公司(CHINA TELECOM CORPORATION LIMITED) [CN/CN]; 中国北京市西城区金融大街31号, Beijing 100033 (CN)。
- (72) 发明人: 邓博仁 (DENG, Boren); 中国北京市西城区金融大街 31 号, Beijing 100033 (CN)。 汪

来富 (WANG, Laifu); 中国北京市西城区金融大街 31 号, Beijing 100033 (CN)。 刘东鑫 (LIU, Dongxin); 中国北京市西城区金融大街 31 号, Beijing 100033 (CN)。 谢泳 (XIE, Yong); 中国北京市西城区金融大街 31 号, Beijing 100033 (CN)。 吴波 (WU, Bo); 中国北京市西城区金融大街31号, Beijing 100033 (CN)。

(74) 代理人: 华进联合专利商标代理有限公司 (ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区珠江东路 6 号 4501 房 (部位: 自编 01-03 和 08-12 单元) (仅限办公用途), Guangdong 510623 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) Title: SECURITY RULE BASE MANAGEMENT METHOD AND APPARATUS, COMPUTER DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 安全规则库管理方法、装置、计算机设备和存储介质

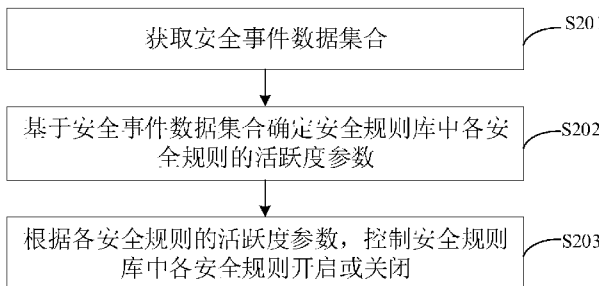


图 2

- S201 Acquire a security event data set
- S202 On the basis of the security event data set, determine activeness parameters of security rules in a security rule base
- S203 On the basis of the activeness parameters of the security rules, control the security rules in the security rule base to be enabled or disabled

(57) Abstract: The present application relates to a security rule base management method and apparatus, a computer device, and a storage medium. The method comprises: acquiring a security event data set, wherein the security event data set comprises event data of a plurality of security events detected by a network security system on the basis of a security rule base within a preset historical time period; on the basis of the security event data set, determining activeness parameters of security rules in the security rule base; and on the basis of the activeness parameters of the security rules, controlling the security rules in the security rule base to be enabled or disabled. By employing the present method, the detection efficiency of the network security system can be improved.

(57) 摘要: 本申请涉及一种安全规则库管理方法、装置、计算机设备和存储介质。所述方法包括: 获取安全事件数据集; 其中, 所述安全事件数据集包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据; 基于所述安全事件数据集确定所述安全规则库中各安全规则的活跃度参数; 根据各所述安全规则的活跃度参数, 控制所述安全规则库中各所述安全规则开启或关闭。采用本方法能够提升网络安全系统的检测效率。

CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ,
IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ,
LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN,
MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA,
PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,
SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

- (84) 指定国(除另有指明，要求每一种可提供的地区
保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚
(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,
HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,
PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN,
TD, TG)。

本国际公布:

- 包括国际检索报告(条约第21条(3))。

安全规则库管理方法、装置、计算机设备和存储介质

相关申请

本申请要求 2023 年 7 月 24 日申请的，申请号为 202310906721.8，名称为“安全规则库管理方法、装置、计算机设备和存储介质”的中国专利申请的优先权，在此将其全文引入作为参考。

技术领域

本申请涉及网络安全技术领域，特别是涉及一种安全规则库管理方法、装置、计算机设备和存储介质。

背景技术

用于检测或防护恶意攻击行为的网络安全系统，如 IDS（Intrusion Detection Systems，入侵检测系统）、WAF（Web Application Firewall，网站应用级入侵防御系统）、安全网关等主要依赖特征检测技术实现对攻击行为的检测，而基于特征检测的攻击检测依赖规则库。

为维持对攻击行为的检测能力，网络安全系统必须维护一个广泛且全面的规则库。随着漏洞的层出不穷、规则库规模的不断扩大，检测效率逐渐降低。

发明内容

本申请实施例提供一种安全规则库管理方法、装置、计算机设备和存储介质，能够提升网络安全系统的检测效率。

第一方面，本申请实施例提供了一种安全规则库管理方法，该方法包括：

获取安全事件数据集合，其中安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据；

基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数；

根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭。

在其中一个实施例中，上述基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数，包括：

基于安全事件数据集合确定本地活跃度集合和全局最大活跃度集合；本地活跃度集合包括各安全规则的本地活跃度，全局最大活跃度集合包括各安全规则的全局最大活跃度；

根据预先获取的历史活跃度集合、本地活跃度集合和全局最大活跃度集合，确定各安全规则的活跃度参数。

在其中一个实施例中，上述基于安全事件数据集合确定本地活跃度集合，包括：

基于安全事件数据集合和预设的时间窗口大小，确定规则组集合；规则组集合包括多个规则组，各规则组包括多个安全规则；

根据各安全规则所属的目标规则组的事件总量，确定各安全规则的本地活跃度，并由多个安全规则的本地活跃度组成本地活跃度集合。

在其中一个实施例中，事件数据包括事件时间、源地址和规则标识，上述基于安全事件数据集合和预设的时间窗口大小，确定规则组集合，包括：

根据安全事件数据集合中各安全事件的事件时间与时间窗口大小，确定多个时间窗口；

对于各时间窗口，从安全事件数据集合中提取出时间窗口内的安全事件，并根据源地址和规则标识对提取出的安全事件进行划分得到初始事件组集合，其中初始事件组集合包括多个初始事件组，各初始事件组包括多个源地址相同和规则标识相同的安全事件；

对初始事件组集合进行过滤处理，得到时间窗口对应的目标事件组集合，其中目标事件组集合包括多个目标事件组，各目标事件组包括按照源地址划分的多个规则组；

根据源地址对多个时间窗口对应的目标事件组集合进行合并处理，得到规则组集合。

在其中一个实施例中，上述对初始事件组进行过滤处理，得到时间窗口对应的目标事件组集合，包括：

根据事件数量对各初始事件组进行归一化处理，得到各初始事件组的事件组参数；

根据各初始事件组的事件组参数和预设事件阈值对初始事件组集合进行过滤处理，得到目标事件组集合。

在其中一个实施例中，上述根据事件数量对各初始事件组进行归一化处理，得到各初始事件组的事件组参数，包括：

根据初始事件组的事件数量和预设常量进行归一化处理，得到归一化后的事件数量；

根据初始事件组中的事件数量和请求成功事件的事件数量进行归一化处理，得到归一化后的成功事件数量；

根据归一化后的事件数量和归一化后的成功事件数量，确定初始事件组的事件组参数。

在其中一个实施例中，上述根据各初始事件组的事件组参数和预设事件阈值对初始事件组集合进行过滤处理，得到目标事件组集合，包括：

对于初始事件组集合中的各初始事件组，若初始事件组的事件组参数小于预设事件阈值，则过滤该初始事件组；

根据初始事件组集合中未被过滤掉的初始事件组，得到目标事件组集合。

在其中一个实施例中，上述根据安全事件数据集合中各安全事件的事件时间与时间窗口大小，确定多个时间窗口，包括：

根据安全事件数据集合中各安全事件的事件时间，确定首个时间窗口的起始时间；

根据首个时间窗口的起始时间和时间窗口大小，确定多个时间窗口。

在其中一个实施例中，确定全局最大活跃度集合的步骤包括：

将本地活跃度集合发送至预设服务器，以供预设服务器根据多个本地活跃度集合确定各安全规则的全局最大活跃度，并由多个安全规则的全局最大活跃度组成全局最大活跃度集合；

接收预设服务器反馈的全局活跃度集合。

在其中一个实施例中，上述根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭，包括：

根据活跃度参数和网络安全系统的运行负载数据，确定各安全规则的开启概率；

根据各安全规则的开启概率，控制安全规则库中各安全规则开启或关闭。

在其中一个实施例中，上述根据活跃度参数和网络安全系统的运行负载数据，确定各安全规则的开启概率，包括：

从预设的多个负载区间中，确定出运行负载数据所在的目标负载区间；

对于安全规则库中的各安全规则，根据活跃度参数确定安全规则的规则类别；

根据运行负载数据、安全规则的规则类别对应的类别参数、和目标负载区间对应的预设关系式，确定各安全规则的开启概率。

在其中一个实施例中，上述根据各安全规则的开启概率，控制安全规则库中各安全规则开启或关闭，包括：

获取各安全规则对应的随机数；

根据随机数和各安全规则的开启概率，控制各安全规则开启或关闭。

第二方面，本申请实施例提供了一种安全规则库管理装置，该装置包括：

数据获取模块，用于获取安全事件数据集合；其中，安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据；

活跃度确定模块，用于基于安全事件数据集合确定安全规则库中各安全规则的活跃度

参数；

规则库管理模块，用于根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭。

第三方面，本申请实施例提供了一种计算机设备，包括存储器和处理器，存储器存储有计算机程序，处理器执行计算机程序时实现如第一方面所述方法的步骤。

第四方面，本申请实施例提供了一种计算机可读存储介质，其上存储有计算机程序，计算机程序被处理器执行时如第一方面所述方法的步骤。

第五方面，本申请实施例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如第一方面所述方法的步骤。

上述安全规则库管理方法、装置、计算机设备和存储介质，获取安全事件数据集合；基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数；根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭。通过本申请实施例，可以将安全规则库中命中次数较低的安全规则关闭，这样，网络安全系统在进行安全检测时，无需遍历安全规则库中的所有安全规则，因此，可以提升网络安全系统的检测效率。

附图说明

为了更清楚地说明本申请实施例或相关技术中的技术方案，下面将对实施例或相关技术描述中所需要使用的附图作简单地介绍。显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图1为本申请一实施例中安全规则库管理方法的应用环境图。

图2为本申请一实施例中安全规则库管理方法的流程示意图。

图3为本申请一实施例中确定各安全规则的活跃度参数步骤的流程示意图。

图4为本申请一实施例中确定本地活跃度集合步骤的流程示意图。

图5为本申请一实施例中确定规则组集合步骤的流程示意图。

图6为本申请一实施例中确定目标事件组集合步骤的流程示意图。

图7为本申请一实施例中控制安全规则库中各安全规则步骤的流程示意图。

图8为本申请一实施例中确定各安全规则的开启概率步骤的流程示意图。

图9为本申请一实施例中开启概率曲线的示意图。

图10为本申请一实施例中安全规则库管理装置的结构框图。

图11为本申请一实施例中计算机设备的内部结构图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

图1为本申请实施例提供的一种安全规则库管理的应用场景示意图。如图1所示，该应用场景包括管理服务器101和多个设置在不同网络中的网络服务器102。管理服务器101上设置有网络安全管理系统；网络服务器102上设置有网络安全系统，网络安全系统可以对其所在的网络进行安全检测，从而检测出入侵、攻击等行为。管理服务器101通过网络与网络服务器102通信，比如，网络服务器102将确定出的本地活跃度集合发送至管理服务器101，管理服务器101根据多个本地活跃度集合确定全局活跃度集合；之后，管理服务器101再将全局活跃度集合返回至网络服务器102。数据存储系统可以存储网络服务器102需要处理的数据，比如，数据存储系统存储安全事件数据集合和安全规则库。数据存储系统可以集成在网络服务器102上，也可以放在云上或其他网络服务器上。管理服务器

101 和网络服务器 102 分别可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

传统技术中，网络安全系统根据安全规则库进行安全检测，需要遍历安全规则库中的每个安全规则。为维持对入侵、攻击等行为的检测能力，网络安全系统必须维护一个广泛且全面的安全规则库。而随着漏洞的层出不穷、安全规则库规模的不断扩大，需要遍历的安全规则越来越多，导致检测效率逐渐降低。

基于上述传统技术，本申请实施例提供了一种安全规则库的管理方案，该方案先获取安全事件数据集合；然后，基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数；再根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭。通过本申请实施例，可以将安全规则库中命中次数较低的安全规则关闭，即对安全规则库进行自适应调整。这样，网络安全系统在进行安全检测时，无需遍历安全规则库中的所有安全规则，因此，可以提升检测效率。

需要说明的是，本申请实施例所带来的有益效果或者所解决的技术问题并不限于这一个，还可以是其它隐含或者关联的问题，具体可以参见下述实施例的描述。

下面以具体地实施例对本申请的技术方案以及本申请的技术方案如何解决上述技术问题进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例中不再赘述。下面将结合附图，对本申请的实施例进行描述。

在一个实施例中，如图 2 所示，提供了一种安全规则库管理方法，以该方法应用于图 1 中的网络服务器为例进行说明，可以包括如下步骤：

步骤 S201，获取安全事件数据集合。

其中，安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据。事件数据包括事件时间、安全事件的源地址、安全事件命中的安全规则的规则标识、以及网络安全系统对安全事件响应的响应码等，参照表 1 所示。

表 1

事件	事件时间	源地址	规则标识	响应码
event1	2023-01-01 01:01	ip1	id1	404
event2	2023-01-01 01:02	ip1	id2	404
event3	2023-01-01 01:02	ip2	id2	200
.....				

网络安全系统基于安全规则库进行安全检测，得到安全事件的事件数据；之后，存储安全事件的事件数据。在需要对安全规则库进行管理时，从存储的事件数据中获取到预设历史时段内的事件数据以得到安全事件数据集合。

对安全规则库进行管理，可以是按照预设时间，也可以按照预设周期。例如，预设时间为 X 年 X 月 X 日，则在该预设时间对安全规则库进行管理；或者，预设周期为每月，则每月对安全规则库进行管理。需要说明的是，对安全规则库进行管理的触发条件不限于上述描述。

步骤 S202，基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数。

其中，活跃度参数表征安全规则的命中情况。可选地，活跃度参数越大，表明安全规则被命中的次数越多；活跃度参数越小，表明安全规则被命中的次数越少。

在获取到安全事件数据集合后，可以根据安全事件数据集合确定安全规则库中各安全规则的命中情况，得到活跃度参数。

例如，根据事件时间、源地址、规则标识和响应码等事件数据，确定安全规则库中的安全规则 1 在预设历史时段内被频繁命中，而安全规则 2 在预设历史时段内未被命中.....。然后，根据上述事件数据计算出表征安全规则 1 被频繁命中的参数，得到安全规则 1 的活跃度参数。以此类推，计算出其他各安全规则的活跃度参数。

步骤 S203，根据各安全规则的活跃度参数，控制安全规则库中各安全规则的开启或关

闭。

对于安全规则库中的各安全规则，如果活跃度参数表征该安全规则在预设历史时段内被频繁命中，则控制该安全规则开启；如果活跃度参数表征该安全规则在预设历史时段内被命中的次数较低，则控制该安全规则关闭。

例如，安全规则 1 对应的活跃度参数为 a ，大于预设参数阈值 x ，则控制安全规则 1 开启；而安全规则 2 对应的活跃度参数为 b ，小于预设参数阈值 x ，则控制安全规则 2 关闭。

上述实施例中，先获取安全事件数据集合；然后，基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数；再根据各安全规则的活跃度参数，控制安全规则库中各安全规则的开启或关闭。通过本申请实施例，可以将安全规则库中命中次数较低的安全规则关闭，这样，网络安全系统在进行安全检测时，无需遍历安全规则库中的所有安全规则，因此，可以提升网络安全系统的检测效率。

在一个实施例中，如图 3 所示，涉及上述步骤 S202 中基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数的过程，本申请实施例可以包括如下步骤：

步骤 S301，基于安全事件数据集合确定本地活跃度集合和全局最大活跃度集合。

其中，本地活跃度集合包括各安全规则的本地活跃度，本地活跃度表征安全规则在单个网络中的命中情况。全局最大活跃度集合包括各安全规则的全局最大活跃度，全局最大活跃度表征安全规则在所有网络中命中情况的最大值。

在获取到安全事件数据集合后，可以根据安全事件数据集合确定各安全规则在网络中的命中情况，得到各安全规则的本地活跃度，并由多个安全规则的本地活跃度组成本地活跃度集合。

在确定各安全规则的本地活跃度后，可以从其他网络获取各安全规则在其他网络的本地活跃度；然后，对于各安全规则，确定其在所有网络中本地活跃度的最大值，得到安全规则的全局最大活跃度；最后，由多个安全规则的全局最大活跃度组成全局活跃度集合。

步骤 S302，根据预先获取的历史活跃度集合、本地活跃度集合和全局最大活跃度集合，确定各安全规则的活跃度参数。

其中，历史活跃度集合包括多个安全规则的历史活跃度，该历史活跃度为按照历史时间确定出的本地活跃度。

根据历史活跃度集合、本地活跃度集合和全局最大活跃度集合，确定各安全规则的历史活跃度、本地活跃度和全局最大活跃度；然后，对历史活跃度、本地活跃度和全局最大活跃度进行加权计算，得到安全规则的活跃度参数。

确定安全规则的活跃度参数可以参照公式 (1) 确定：

$$w_i = \begin{cases} w_i + \sigma \times \text{history\_}w_i, & \text{当 } w_i > 0 \text{ 时} \\ w_i + \delta \times \max\_w + \sigma \times \text{history\_}w_i, & \text{当 } w_i = 0 \text{ 时} \end{cases} \quad \text{-----}; (1)$$

其中， w_i 为活跃度参数， w_i 为本地活跃度， $\text{history\_}w_i$ 为历史活跃度， $\max\_w$ 为全局最大活跃度， σ 为历史活跃度对应的权重， δ 为全局最大活跃度对应的权重。

由公式 (1) 可以看出，在安全规则的本地活跃度为 0 时，使用全局最大活跃度确定活跃度参数；而在安全规则的本地规则大于 0 时，并不使用全局最大活跃度确定活跃度参数。可选地，在安全规则的本地活跃度为 0 时，全局最大活跃度对应的权重 δ 为 0.5，在安全规则的本地规则大于 0 时，全局最大活跃度对应的权重 δ 为 0。可选地，历史活跃度对应的权重 σ 为 0.5。

上述实施例中，基于安全事件数据集合确定本地活跃度集合和全局最大活跃度集合；基于安全事件数据集合确定本地活跃度集合和全局最大活跃度集合。通过本申请实施例，综合考虑不同网络的环境差异性，融合本地活跃度、全局最大活跃度和历史活跃度确定活

跃度参数，可以提升活跃度参数的有效性与全面性。

在一个实施例中，如图 4 所示，涉及上述步骤 S301 中基于安全事件数据集合确定本地活跃度集合的过程，本申请实施例可以包括如下步骤 S401-S402：

步骤 S401，基于安全事件数据集合和预设的时间窗口大小，确定规则组集合。

其中，规则组集合包括多个规则组，各规则组包括多个安全规则，参照表 2，id 为安全规则的规则标识。

表 2

规则组集合rule_group_set	规则组	事件总量
rule_group1	{id1.id2.id3.id5.id6...}	C1
rule_group2	{id3.id4.id5.id7.id8...}	C2
rule_group3	{id3.id7.id8.id9...}	C3

根据预设的时间窗口大小确定多个时间窗口，基于安全事件数据集合确定各时间窗口的事件数据；对每个时间窗口的事件数据进行处理，得到每个时间窗口对应的多个规则组以及各规则组对应的事件总量；然后，对多个时间窗口分别对应的规则组和事件总量进行处理，得到规则组集合。

步骤 S402，根据各安全规则所属的目标规则组的事件总量，确定各安全规则的本地活跃度，并由多个安全规则的本地活跃度组成本地活跃度集合。

对于各安全规则，确定安全规则所属的至少一个目标规则组，对至少一个目标规则组的事件总量进行求和处理，得到安全规则的本地活跃度。如公式（2）所示：

$$wi = \sum_{idi \in rule\_groupj} Cj \text{ -----}; (2)$$

其中，wi 为本地活跃度，i 为安全规则的序号，j 为规则组的序号。

参照表 2，id3 所属的目标规则组包括 rule_group1、rule_group2、rule_group3；rule_group1 的事件总量为 C1，rule_group2 的事件总量为 C2，rule_group3 的事件总量为 C3，则 id3 的本地活跃度 w3=C1+C2+C3。

上述实施例中，基于安全事件数据集合和预设的时间窗口大小，确定规则组集合；根据各安全规则所属的目标规则组的事件总量，确定各安全规则的本地活跃度，并由多个安全规则的本地活跃度组成本地活跃度集合。通过本申请实施例，以规则组的视角进行分析，可以有效地评估安全规则的命中情况，为管理安全规则库提供了依据。

在一个实施例中，上述事件数据包括事件时间、源地址和规则标识，如图 5 所示，涉及上述步骤 S401 中基于安全事件数据集合和预设的时间窗口大小，确定规则组集合的过程，本申请实施例可以包括如下步骤 S501-S504：

步骤 S501，根据安全事件数据集合中各安全事件的事件时间与时间窗口大小，确定多个时间窗口。

根据安全事件数据集合中各安全事件的事件时间，确定首个时间窗口的起始时间；根据首个时间窗口的起始时间和时间窗口大小，确定多个时间窗口。

例如，将所有安全事件的事件时间按照时间先后顺序排列，然后将时间最靠前的事件时间确定为首个时间窗口的起始时间 time1，根据首个时间窗口的起始时间 time1 和时间窗口大小 time_window 确定首个时间窗口的结束时间 time2=time1+time_window，则首个时间窗口表示为(time1, time2)。将首个时间窗口的结束时间作为第二个时间窗口的起始时间，根据第二时间窗口的起始时间和时间窗口大小可以确定第二个时间窗口的结束时间。以此类推，可以确定多个时间窗口。

步骤 S502，对于各时间窗口，从安全事件数据集合中提取出时间窗口内的安全事件，

并根据源地址和规则标识对提取出的安全事件进行划分得到初始事件组集合。

其中，初始事件组集合包括多个初始事件组，各初始事件组包括多个源地址相同和规则标识相同的安全事件。

对于每个时间窗口，先根据事件时间从安全事件数据集合中提取出时间窗口内的安全事件；然后，根据源地址和规则标识对提取出的安全事件进行划分，得到多个初始事件组；再由多个初始事件组组成初始事件组集合。参照表 3，示出了首个时间窗口的初始事件组集合。

表 3

序号	时间窗口	源IP	规则ID	响应码
event_group1	(time1,time2)	ip1	id1	200, 400, 404.....
event_group2	(time1,time2)	ip1	id2	200, 200, 404.....
event_group3	(time1,time2)	ip2	id2	404, 404, 404.....
.....				

步骤 S503，对初始事件组集合进行过滤处理，得到时间窗口对应的目标事件组集合。

其中，目标事件组集合包括多个目标事件组，各目标事件组包括按照源地址划分的多个规则组。

网络安全系统在进行安全检测时，可能会出现误报的情况，因此，在确定初始事件组集合后，可以根据响应码确定是否存在误报的情况，然后根据误报的情况对初始事件组集合进行过滤处理，并根据过滤后的初始事件组集合确定目标事件组集合。

参照表 4，示出了首个时间窗口的目标事件组集合 event_group {event_group1, event_group2, event_group3.....}。滑动时间窗口，参照上述方式可以确定其他时间窗口的目标事件组集合。

表 4

序号	时间窗口	源IP	规则ID	事件总量
event_group1	(time1,time2)	ip1	id1	cnt1
event_group2	(time1,time2)	ip1	id2	cnt2
event_group3	(time1,time2)	ip2	id2	cnt3
.....				

步骤 S504，根据源地址对多个时间窗口对应的目标事件组集合进行合并处理，得到规则组集合。

在确定每个时间窗口对应的目标事件组集合后，对多个时间窗口对应的目标事件组集合进行合并处理，得到规则组集合。

例如，如果时间窗口 1 中的一个源地址 ip 在时间窗口 2 中存在，则将时间窗口 1 的目标事件组集合与时间窗口 2 的目标事件组集合进行合并得到一个规则组；并且，合并后事件总量为两个目标事件组集合的事件总量之和。如果时间窗口 1 中的一个源地址在时间窗口 2 中不存在，则将时间窗口 1 的目标事件组集合直接作为一个规则组。依次类推，得到多个规则组，并由多个规则组组成规则组集合，如上述实施例中的表 2 所示。

上述实施例中，根据安全事件数据集合中各安全事件的事件时间与时间窗口大小，确定多个时间窗口；对于各时间窗口，从安全事件数据集合中提取出时间窗口内的安全事件，并根据源地址和规则标识对提取出的安全事件进行划分得到初始事件组集合；对初始事件组集合进行过滤处理，得到时间窗口对应的目标事件组集合；根据源地址对多个时间窗口对应的目标事件组集合进行合并处理，得到规则组集合。本申请实施例采用滑窗的方式对安全事件进行分组，每个时间窗口的运算量较小，并且多个时间窗口的运算可以并行进行，

因此，可以提高分组速度和分组效率，从而提升了安全规则库的自适应调整效率。

在一个实施例中，如图 6 所示，涉及上述步骤 S503 中对初始事件组进行过滤处理，得到时间窗口对应的目标事件组集合的过程，本申请实施例可以包括如下步骤 S601-S602：

步骤 S601，根据事件数量对各初始事件组进行归一化处理，得到各初始事件组的事件组参数。

其中，事件组参数表征初始事件组中请求成功事件的占比。可以理解地，事件组参数越大，表明初始事件组中请求成功事件的占比越高，误报事件越少；事件组参数越小，表明初始事件组中请求成功事件的占比越低，误报事件越多。

在对初始事件组进行过滤处理时，可以先确定初始事件组中请求成功事件的事件数量，再根据请求成功事件的事件数量与初始事件组的事件数量进行归一化处理，得到初始事件组的事件组参数。

可选地，步骤 S601 中归一化处理过程可以包括如下步骤 S6011-S6013：

步骤 S6011，根据初始事件组的事件数量和预设常量进行归一化处理，得到归一化后的事件数量，如公式（3）所示：

$$\text{cnt\_n} = \frac{\min(\text{cnt}, \text{MAX\_cnt})}{\text{MAX\_cnt}} \text{-----}; (3)$$

其中，cnt_n 为归一化后的事件数量，cnt 为初始事件组的事件数量，MAX_cnt 为预设常量。可选地，预设常量 MAX_cnt 为 20。

根据上述公式（3），先从初始事件组的事件数量与预设常量中选取较小的值，再计算较小的值与预设常量的比值，得到归一化后的事件数量。

步骤 S6012，根据初始事件组中的事件数量和请求成功事件的事件数量进行归一化处理，得到归一化后的成功事件数量。

根据响应码确定初始事件组中请求成功事件的事件数量，然后计算请求成功事件的事件数量与初始事件组中的事件数量之间的比值，得到归一化后的成功事件数量。可选地，请求成功事件的响应码的第一位为 2，例如，响应码 201、202、203 等。

考虑到初始事件组的事件数量可能为 0 的情况，可以采用公式（4）确定归一化后的成功事件数量，如下：

$$\text{sreq\_n} = \frac{\text{sreq} + 1}{\text{cnt} + 1} \text{-----}; (4)$$

其中，sreq_n 为归一化后的成功事件数量，sreq 为请求成功事件的事件数量，cnt 为初始事件组的事件数量。

步骤 S6013，根据归一化后的事件数量和归一化后的成功事件数量，确定初始事件组的事件组参数。

计算归一化后的成功事件数量与归一化后的事件数量之间的比值，得到初始事件组的事件组参数，如公式（5）所示：

$$k = \frac{\text{cnt\_n}}{\text{sreq\_n}} \text{-----}; (5)$$

其中，k 为事件组参数，cnt_n 为归一化后的事件数量，sreq_n 为归一化后的成功事件数量。

步骤 S602，根据各初始事件组的事件组参数和预设事件阈值对初始事件组集合进行过

滤处理，得到目标事件组集合。

对于各初始事件组，将初始事件组的事件组参数与预设事件阈值进行比较，根据比较结果确定是否过滤该初始事件组；之后，由未被过滤掉的初始事件组组成目标事件组集合。

可选地，过滤处理的过程可以包括：对于初始事件组集合中的各初始事件组，若事件组参数小于预设事件阈值，则过滤该初始事件组；根据初始事件组集合中未被过滤掉的初始事件组，得到目标事件组集合。

例如，预设事件阈值为 3，如果初始事件组的事件参数小于 3，表明该初始事件组的请求成功事件较少、误报事件较多，因此，将该初始事件组被过滤掉。

上述实施例中，根据事件数量对各初始事件组进行归一化处理，得到各初始事件组的事件组参数；根据各初始事件组的事件组参数和预设事件阈值对初始事件组集合进行过滤处理，得到目标事件组集合。本申请实施例中，结合响应码对事件数量进行归一化处理得到事件组参数，可以有效过滤误报事件多的事件组，从而降低误报时间对活跃度参数造成的影响，提高活跃度参数的准确度。

在一个实施例中，上述全局最大活跃度集合的确定过程包括：将本地活跃度集合发送至预设服务器，以供预设服务器根据多个本地活跃度集合确定各安全规则的全局最大活跃度，并由多个安全规则的全局最大活跃度组成全局最大活跃度集合；接收预设服务器反馈的全局活跃度集合。

其中，预设服务器可以为图 1 中的管理服务器。

各网络的网络服务器在确定本地活跃度集合后，将本地活跃度集合发送到预设服务器。预设服务器获取到多个网络的本地活跃度集合后，确定每个安全规则在多个网络的本地活跃度，并选取出最大的本地活跃度作为全局最大活跃度。之后，由多个安全规则的全局最大活跃度组成全局最大活跃度。

管理服务器将全局活跃度集合分别反馈回各网络的网络服务器，以便网络服务器可以根据全局最大活跃度集合确定各安全规则的活跃度参数。

上述实施例中，将本地活跃度集合发送至预设服务器，以供预设服务器根据多个本地活跃度集合确定各安全规则的全局最大活跃度，并由多个安全规则的全局最大活跃度组成全局最大活跃度集合；接收预设服务器反馈的全局活跃度集合。本申请实施例获取全局最大活跃度集合，可以在安全规则本地未命中的情况下，考虑安全规则外地的命中情况，从而综合不同网络的环境差异性，提升安全规则的活跃度参数的有效性与全面性。

在一个实施例中，如图 7 所示，涉及上述步骤 S203 中根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭的过程，本申请实施例可以包括如下步骤 S701-S702：

步骤 S701，根据活跃度参数和网络安全系统的运行负载数据，确定各安全规则的开启概率。

其中，运行负载数据可以包括 CPU 利用率、内存利用率和丢包率中的至少一种。开启概率用于表征安全规则开启的概率。

运行负载数据影响网络安全系统的检测效率，在实际应用中，结合安全规则的活跃度参数以及网络安全系统的运行负载数据计算各安全规则的开启概率。可以理解地，运行负载数据越小，安全规则库中允许开启的安全规则就越多，计算出的开启概率就越大；运行负载数据越大，安全规则库中开启的安全规则越少，计算出的开启概率就越小。

步骤 S702，根据各安全规则的开启概率，控制安全规则库中各安全规则开启或关闭。

对于安全规则库中的各安全规则，如果安全规则的开启概率大于或等于预设概率阈值，则控制安全规则开启；如果安全规则的开启概率小于预设概率阈值，则控制安全规则关闭。

在其中一个实施例中，获取各安全规则的随机数；根据随机数和各安全规则的开启概率，控制各安全规则开启或关闭，如公式（6）所示：

$$v = \begin{cases} 0, & RAND(0,1) \geq y \\ 1, & RAND(0,1) < y \end{cases} \text{-----}; (6)$$

其中, v 为安全规则的状态, $v=0$ 表明控制安全规则关闭, $v=1$ 表明控制安全规则开启; $RAND(0, 1)$ 为 0 到 1 之间的随机数, y 为安全规则的开启概率。

上述实施例中, 根据活跃度参数和网络安全系统的运行负载数据, 确定各安全规则的开启概率; 根据各安全规则的开启概率, 控制安全规则库中各安全规则开启或关闭。本申请实施例结合网络安全系统的运行负载情况为各安全规则设置开启概率, 可以实现对安全规则库在不同允许负载情况下的自适应调整, 从而提升网络安全系统的检测效率。

在一个实施例中, 如图 8 所示, 涉及上述步骤 S701 中根据活跃度参数和网络安全系统的运行负载数据, 确定各安全规则的开启概率的过程, 本申请实施例可以包括如下步骤 S801-S803:

步骤 S801, 从预设的多个负载区间中, 确定出运行负载数据所在的目标负载区间。

预先设置多个负载区间, 根据运行负载数据确定出对应的目标负载区间。

例如, 设置运行负载阈值 ($0 < x_a < 1$) 与阈值 ($x_a < x_b < 1$), 根据运行负载阈值划分出 3 个负载区间: $[0, x_a]$ 、 $(x_a, x_b]$ 、 $(x_b, 1]$ 。可选地, $x_a=0.5$, $x_b=0.9$ 。将运行负载数据 x 所在的负载区间确定为目标负载区间。

其中, 运行负载数据可以按照预先设置的采集周期进行采集。可选地, 采集周期为 10 分钟, 即每 10 分钟采集一次运行负载数据。

步骤 S802, 对于安全规则库中的各安全规则, 根据活跃度参数确定安全规则的规则类别。

其中, 规则类别也可以表征安全规则的命中情况。在实际应用中, 规则类别按照命中次数从多到少排列, 可以包括活跃规则、沉默规则、睡眠规则、休眠规则。需要说明的是, 规则类别不限于上述描述, 还可以包括其他类别。

对于安全规则库中的各安全规则, 在确定安全规则的活跃度参数后, 可以根据预设的活跃阈值、睡眠阈值和活跃度参数确定安全规则的规则类别。

例如, 活跃阈值 t_1 , 睡眠阈值 t_2 , 其中 $t_1 > t_2$; 1) 当活跃度参数 $w_i > t_1$, 则确定安全规则的规则类别为活跃规则; 2) 当活跃度参数 $t_1 > w_i > t_2$, 则确定安全的规则类别为沉默规则; 3) 当活跃度参数 $t_2 > w_i > 0$, 则确定安全规则的规则类别为睡眠规则; 4) 当活跃度参数 $w_i = 0$, 则确定安全规则的规则类别为休眠规则。可选地, $t_1=100$, $t_2=10$ 。

步骤 S803, 根据运行负载数据、安全规则的规则类别对应的类别参数、和目标负载区间对应的预设关系式, 确定各安全规则的开启概率。

对于不同的负载区间, 确定安全规则的开启概率可以采用不同的预设关系式, 如公式 (7) 所示:

$$y = \begin{cases} 1, & x \in [0, x_a] \\ (x - x_a) \times \frac{f_1(w) - 1}{x_b - x_a} + 1, & x \in (x_a, x_b] \\ (x - x_b) \times \frac{f_2(w) - f_1(w)}{1 - x_b} + f_1(w), & x \in (x_b, 1] \end{cases} \text{-----}; (7)$$

其中, $f_1(w)$ 和 $f_2(w)$ 为安全规则的规则类别对应的类别参数。对于不同规则类别, $f_1(w)$ 和 $f_2(w)$ 的值不同。

例如, 对于活跃规则, 即当安全规则的活跃度参数 $w_i > t_1$ 时, $f_1(w) = 1$, $f_2(w) = 0.8$; 对于沉默规则, 即当安全规则的活跃度参数 $t_1 > w_i > t_2$ 时, $f_1(w) = 0.8$, $f_2(w) = 0.5$; 对

于睡眠规则，即当安全规则的活跃度参数 $t_2 > w_i > 0$ 时， $f_1(w) = 0.5$ ， $f_2(w) = 0$ ；对于休眠规则，即当安全规则的活跃度参数 $w_i = 0$ 时， $f_1(w) = 0$ ， $f_2(w) = 0$ 。

根据公式 7 可以得到如图 9 所示的开启概率曲线。

需要说明的是，在实际应用中，确定开启概率的预设关系式不限于上述公式 (7) 的线性关系式，还可以采用其他非线性关系式。

上述实施例中，从预设的多个负载区间中，确定出运行负载数据所在的目标负载区间；对于安全规则库中的各安全规则，根据活跃度参数确定安全规则的规则类别；根据运行负载数据、安全规则的规则类别对应的类别参数、和目标负载区间对应的预设关系式，确定各安全规则的开启概率。本申请实施例结合网络安全系统的运行负载情况为不同类别的安全规则设置不同的开启概率，差异性设置规则开启概率，可以实现对不同安全规则在不同运行负载情况下的自适应调整，从而提升安全规则的应用效率和网络安全系统的检测效率。

在一个实施例中，提供了一种安全规则库管理方法，以该方法应用于图 1 中的网络服务器为例进行说明，可以包括如下步骤：

步骤 1，获取安全事件数据集合。

其中，安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据。事件数据包括事件时间、源地址、规则标识和响应码中至少一种。

步骤 2，根据安全事件数据集合中各安全事件的事件时间，确定首个时间窗口的起始时间；根据首个时间窗口的起始时间和时间窗口大小，确定多个时间窗口。

步骤 3，对于各时间窗口，从安全事件数据集合中提取出时间窗口内的安全事件，并根据源地址和规则标识对提取出的安全事件进行划分得到初始事件组集合。

其中，初始事件组集合包括多个初始事件组，各初始事件组包括多个源地址相同和规则标识相同的安全事件。

步骤 4，根据初始事件组的事件数量和预设常量进行归一化处理，得到归一化后的事件数量；根据初始事件组中的事件数量和请求成功事件的事件数量进行归一化处理，得到归一化后的成功事件数量；根据归一化后的事件数量和归一化后的成功事件数量，确定初始事件组的事件组参数。

步骤 5，对于初始事件组集合中的各初始事件组，若事件组参数小于预设事件阈值，则过滤初始事件组；根据初始事件组集合中未被过滤掉的初始事件组，得到目标事件组集合。

步骤 6，根据源地址对多个时间窗口对应的目标事件组集合进行合并处理，得到规则组集合。

步骤 7，根据各安全规则所属的目标规则组的事件总量，确定各安全规则的本地活跃度，并由多个安全规则的本地活跃度组成本地活跃度集合。

步骤 8，将本地活跃度集合发送至预设服务器，以供预设服务器根据多个本地活跃度集合确定各安全规则的全局最大活跃度，并由多个安全规则的全局最大活跃度组成全局最大活跃度集合；接收预设服务器反馈的全局活跃度集合。

步骤 9，根据预先获取的历史活跃度集合、本地活跃度集合和全局最大活跃度集合，确定各安全规则的活跃度参数。

步骤 10，从预设的多个负载区间中，确定出运行负载数据所在的目标负载区间；对于安全规则库中的各安全规则，根据活跃度参数确定安全规则的规则类别；根据运行负载数据、安全规则的规则类别对应的类别参数和目标负载区间对应的预设关系式，确定各安全规则的开启概率。

步骤 11，获取各安全规则的随机数；根据随机数和各安全规则的开启概率，控制各安全规则开启或关闭。

应该理解的是，虽然上述流程图中的各个步骤按照箭头的指示依次显示，但是这些步

骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，上述流程图中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

在一个实施例中，如图 10 所示，提供了一种安全规则库管理装置，包括：

数据获取模块 901，用于获取安全事件数据集合；其中，安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据；

活跃度确定模块 902，用于基于安全事件数据集合确定安全规则库中各安全规则的活跃度参数；

规则库管理模块 903，用于根据各安全规则的活跃度参数，控制安全规则库中各安全规则开启或关闭。

在其中一个实施例中，活跃度确定模块 902，具体用于基于安全事件数据集合确定本地活跃度集合和全局最大活跃度集合；本地活跃度集合包括各安全规则的本地活跃度，全局最大活跃度集合包括各安全规则的全局最大活跃度；根据预先获取的历史活跃度集合、本地活跃度集合和全局最大活跃度集合，确定各安全规则的活跃度参数。

在其中一个实施例中，活跃度确定模块 902 具体用于基于安全事件数据集合和预设的时间窗口大小，确定规则组集合；规则组集合包括多个规则组，各规则组包括多个安全规则；根据各安全规则所属的目标规则组的事件总量，确定各安全规则的本地活跃度，并由多个安全规则的本地活跃度组成本地活跃度集合。

在其中一个实施例中，事件数据包括事件时间、源地址和规则标识；活跃度确定模块 902 具体用于根据安全事件数据集合中各安全事件的事件时间与时间窗口大小，确定多个时间窗口；对于各时间窗口，从安全事件数据集合中提取出时间窗口内的安全事件，并根据源地址和规则标识对提取出的安全事件进行划分得到初始事件组集合；初始事件组集合包括多个初始事件组，各初始事件组包括多个源地址相同和规则标识相同的安全事件；对初始事件组集合进行过滤处理，得到时间窗口对应的目标事件组集合；目标事件组集合包括多个目标事件组，各目标事件组包括按照源地址划分的多个规则组；根据源地址对多个时间窗口对应的目标事件组集合进行合并处理，得到规则组集合。

在其中一个实施例中，活跃度确定模块 902 具体用于根据事件数量对各初始事件组进行归一化处理，得到各初始事件组的事件组参数；根据各初始事件组的事件组参数和预设事件阈值对初始事件组集合进行过滤处理，得到目标事件组集合。

在其中一个实施例中，活跃度确定模块 902 具体用于根据初始事件组的事件数量和预设常量进行归一化处理，得到归一化后的事件数量；根据初始事件组中的事件数量和请求成功事件的事件数量进行归一化处理，得到归一化后的成功事件数量；根据归一化后的事件数量和归一化后的成功事件数量，确定初始事件组的事件组参数。

在其中一个实施例中，活跃度确定模块 902 具体用于对于初始事件组集合中的各初始事件组，若事件组参数小于预设事件阈值，则过滤初始事件组；根据初始事件组集合中未被过滤的初始事件组，得到目标事件组集合。

在其中一个实施例中，活跃度确定模块 902 具体用于根据安全事件数据集合中各安全事件的事件时间，确定首个时间窗口的起始时间；根据首个时间窗口的起始时间和时间窗口大小，确定多个时间窗口。

在其中一个实施例中，活跃度确定模块 902 具体用于将本地活跃度集合发送至预设服务器，以供预设服务器根据多个本地活跃度集合确定各安全规则的全局最大活跃度，并由多个安全规则的全局最大活跃度组成全局最大活跃度集合；接收预设服务器反馈的全局活跃度集合。

在其中一个实施例中，规则库管理模块 903 具体用于根据活跃度参数和网络安全系统

的运行负载数据，确定各安全规则的开启概率；根据各安全规则的开启概率，控制安全规则库中各安全规则开启或关闭。

在其中一个实施例中，规则库管理模块 903 具体用于从预设的多个负载区间中，确定出运行负载数据所在的目标负载区间；对于安全规则库中的各安全规则，根据活跃度参数确定安全规则的规则类别；根据运行负载数据、安全规则的规则类别对应的类别参数、和目标负载区间对应的预设关系式，确定各安全规则的开启概率。

在其中一个实施例中，规则库管理模块 903 具体用于获取各安全规则对应的随机数；根据随机数和各安全规则的开启概率，控制各安全规则开启或关闭。

关于安全规则库管理装置的具体限定可以参见上文中对于安全规则库管理方法的限定，在此不再赘述。上述安全规则库管理装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图 11 所示。该计算机设备包括处理器、存储器、输入/输出接口(Input/Output，简称 I/O)和通信接口。其中，处理器、存储器和输入/输出接口通过系统总线连接，通信接口通过输入/输出接口连接到系统总线。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质和内存存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储安全规则库管理数据。该计算机设备的输入/输出接口用于处理器与外部设备之间交换信息。该计算机设备的通信接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种安全规则库管理方法。

在一个实施例中，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，计算机程序可由服务器的处理器执行以完成上述方法。存储介质可以是非临时性计算机可读存储介质，例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

在一个实施例中，还提供了一种计算机程序产品，该计算机程序被处理器执行时，可以实现上述方法。该计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行这些计算机指令时，可以全部或部分地按照本公开实施例所述的流程或功能实现上述方法中的部分或者全部。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所述的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器(Read-Only Memory, ROM)、磁带、软盘、闪存或光存储器等。易失性存储器可包括随机存取存储器(Random Access Memory, RAM)或外部高速缓冲存储器。作为说明而非局限，RAM 可以是多种形式，比如静态随机存取存储器(Static Random Access Memory, SRAM)或动态随机存取存储器(Dynamic Random Access Memory, DRAM)等。

以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范

围。因此，本申请专利的保护范围应以所附权利要求为准。

权利要求

1. 一种安全规则库管理方法，包括：

获取安全事件数据集合，其中所述安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据；

基于所述安全事件数据集合确定所述安全规则库中各安全规则的活跃度参数；

根据各所述安全规则的活跃度参数，控制所述安全规则库中各所述安全规则开启或关闭。

2. 根据权利要求1所述的方法，其中所述基于所述安全事件数据集合确定所述安全规则库中各安全规则的活跃度参数，包括：

基于所述安全事件数据集合确定本地活跃度集合和全局最大活跃度集合，所述本地活跃度集合包括各所述安全规则的本地活跃度，所述全局最大活跃度集合包括各所述安全规则的全局最大活跃度；

根据预先获取的历史活跃度集合、所述本地活跃度集合和所述全局最大活跃度集合，确定各所述安全规则的活跃度参数。

3. 根据权利要求2所述的方法，其中所述基于所述安全事件数据集合确定本地活跃度集合，包括：

基于所述安全事件数据集合和预设的时间窗口大小，确定规则组集合，所述规则组集合包括多个规则组，各所述规则组包括多个安全规则；

根据各所述安全规则所属的目标规则组的事件总量，确定各所述安全规则的本地活跃度，并由多个所述安全规则的本地活跃度组成所述本地活跃度集合。

4. 根据权利要求3所述的方法，其中所述事件数据包括事件时间、源地址和规则标识，所述基于所述安全事件数据集合和预设的时间窗口大小，确定规则组集合包括：

根据所述安全事件数据集合中各安全事件的事件时间与所述时间窗口大小，确定多个时间窗口；

对于各所述时间窗口，从所述安全事件数据集合中提取出所述各时间窗口内的安全事件，并根据所述源地址和所述规则标识对提取出的安全事件进行划分得到初始事件组集合，其中所述初始事件组集合包括多个初始事件组，各所述初始事件组包括多个源地址相同和规则标识相同的安全事件；

对所述初始事件组集合进行过滤处理，得到所述时间窗口对应的目标事件组集合，其中所述目标事件组集合包括多个目标事件组，各所述目标事件组包括按照源地址划分的多个规则组；

根据所述源地址对多个所述时间窗口对应的目标事件组集合进行合并处理，得到所述规则组集合。

5. 根据权利要求4所述的方法，其中所述对所述初始事件组进行过滤处理，得到所述时间窗口对应的目标事件组集合，包括：

根据事件数量对各所述初始事件组进行归一化处理，得到各所述初始事件组的事件组参数；

根据各所述初始事件组的事件组参数和预设事件阈值对所述初始事件组集合进行过滤处理，得到所述目标事件组集合。

6. 根据权利要求5所述的方法，其中所述根据事件数量对各所述初始事件组进行归一化处理，得到各所述初始事件组的事件组参数，包括：

根据所述初始事件组的事件数量和预设常量进行归一化处理，得到归一化后的事件数量；

根据所述初始事件组中的事件数量和请求成功事件的事件数量进行归一化处理，得到归一化后的成功事件数量；

根据所述归一化后的事件数量和所述归一化后的成功事件数量，确定所述初始事件组的事件组参数。

7. 根据权利要求 5 所述的方法，其中所述根据各所述初始事件组的事件组参数和预设事件阈值对所述初始事件组集合进行过滤处理，得到所述目标事件组集合，包括：

对于所述初始事件组集合中的各所述初始事件组，若初始事件组的事件组参数小于所述预设事件阈值，则过滤所述初始事件组；

根据所述初始事件组集合中未被过滤掉的初始事件组，得到所述目标事件组集合。

8. 根据权利要求 6 所述的方法，其中所述根据所述安全事件数据集合中各安全事件的事件时间与所述时间窗口大小，确定多个时间窗口，包括：

根据所述安全事件数据集合中各安全事件的事件时间，确定首个时间窗口的起始时间；

根据所述首个时间窗口的起始时间和所述时间窗口大小，确定所述多个时间窗口。

9. 根据权利要求 2 所述的方法，其中所述确定全局最大活跃度集合的步骤包括：

将所述本地活跃度集合发送至预设服务器，以供所述预设服务器根据多个所述本地活跃度集合确定各所述安全规则的全局最大活跃度，并由多个所述安全规则的全局最大活跃度组成所述全局最大活跃度集合；

接收所述预设服务器反馈的所述全局活跃度集合。

10. 根据权利要求 1-9 任一项所述的方法，其中所述根据各所述安全规则的活跃度参数，控制所述安全规则库中各所述安全规则开启或关闭，包括：

根据所述活跃度参数和所述网络安全系统的运行负载数据，确定各所述安全规则的开启概率；

根据各所述安全规则的开启概率，控制所述安全规则库中各所述安全规则开启或关闭。

11. 根据权利要求 10 所述的方法，其中所述根据所述活跃度参数和所述网络安全系统的运行负载数据，确定各所述安全规则的开启概率，包括：

从预设的多个负载区间中，确定出所述运行负载数据所在的目标负载区间；

对于所述安全规则库中的各安全规则，根据所述活跃度参数确定所述安全规则的规则类别；

根据所述运行负载数据、所述安全规则的规则类别对应的类别参数、和所述目标负载区间对应的预设关系式，确定各所述安全规则的开启概率。

12. 根据权利要求 11 所述的方法，其中所述根据各所述安全规则的开启概率，控制所述安全规则库中各所述安全规则开启或关闭，包括：

获取各所述安全规则对应的随机数；

根据所述随机数和各所述安全规则的开启概率，控制各所述安全规则开启或关闭。

13. 一种安全规则库管理装置，包括：

数据获取模块，用于获取安全事件数据集合，其中所述安全事件数据集合包括预设历史时段内网络安全系统基于安全规则库检测到的多个安全事件的事件数据；

活跃度确定模块，用于基于所述安全事件数据集合确定所述安全规则库中各安全规则的活跃度参数；

规则库管理模块，用于根据各所述安全规则的活跃度参数，控制所述安全规则库中各所述安全规则开启或关闭。

14. 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，其中所述处理器执行所述计算机程序时实现权利要求 1 至 12 中任一项所述的方法的步骤。

15. 一种计算机可读存储介质，其上存储有计算机程序，其中所述计算机程序被处理器执行时实现权利要求 1 至 12 中任一项所述的方法的步骤。

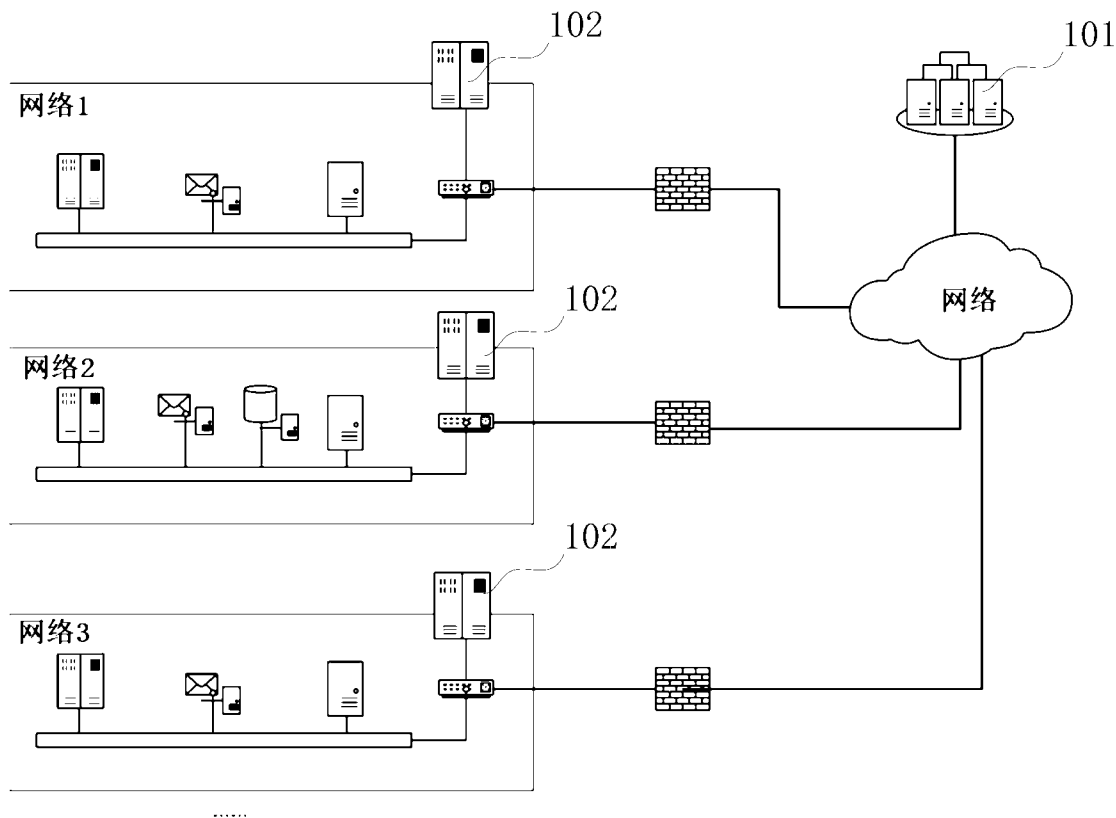


图 1

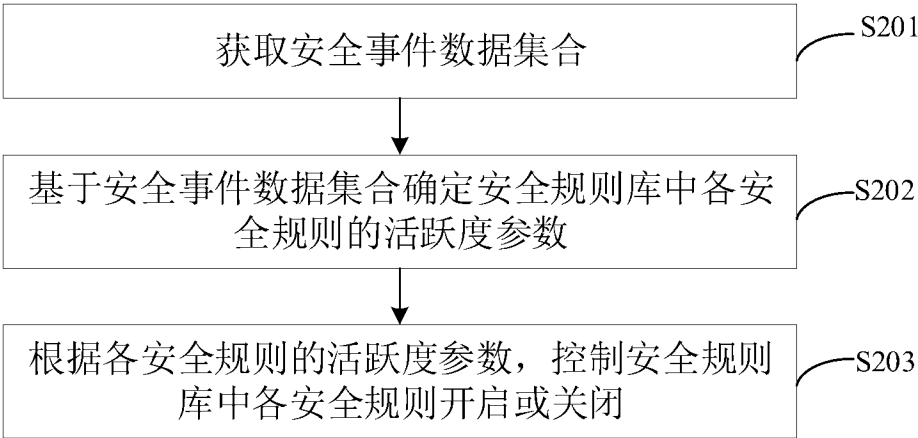


图 2

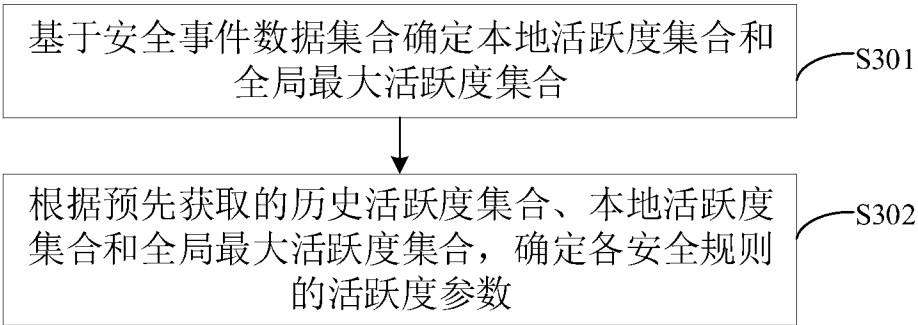


图 3

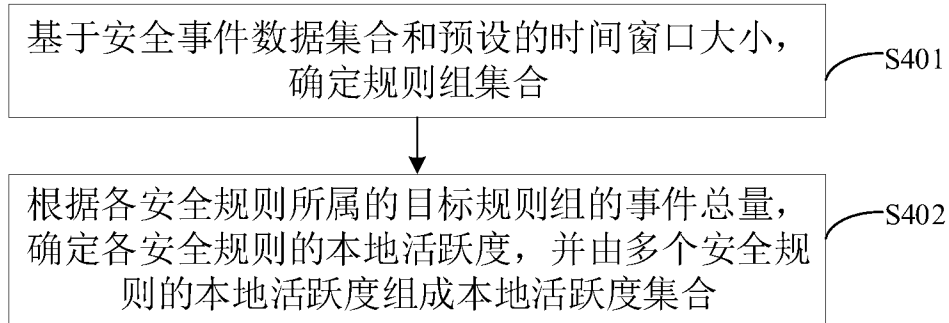


图 4

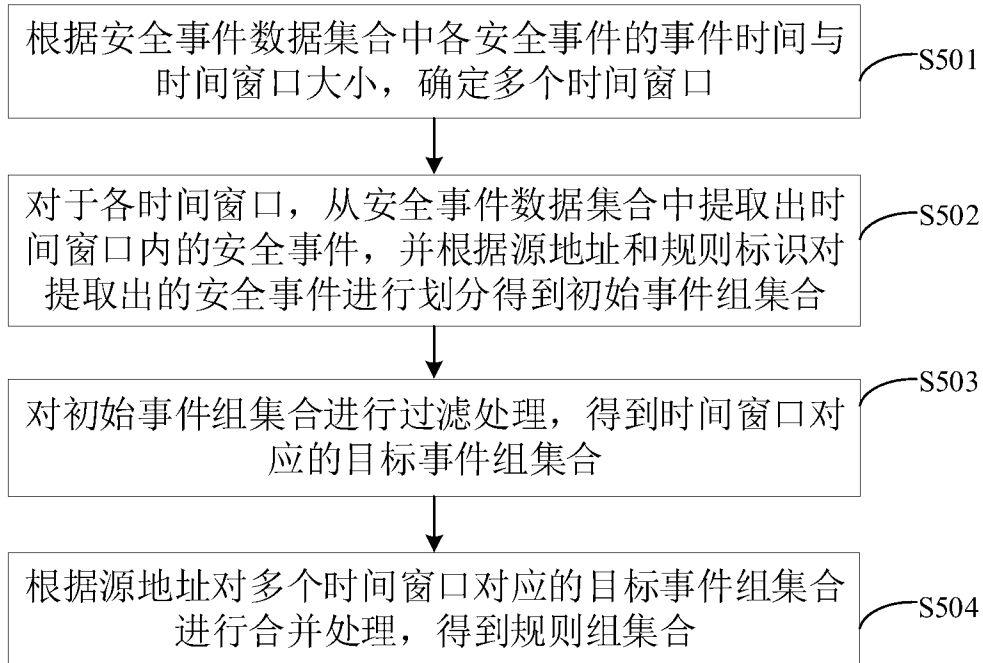


图 5

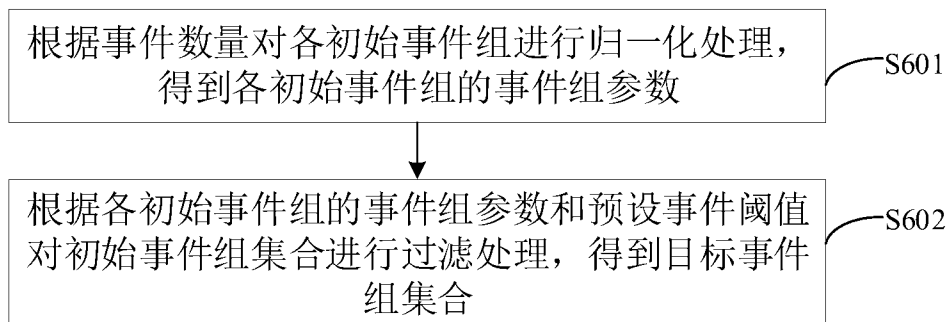


图 6

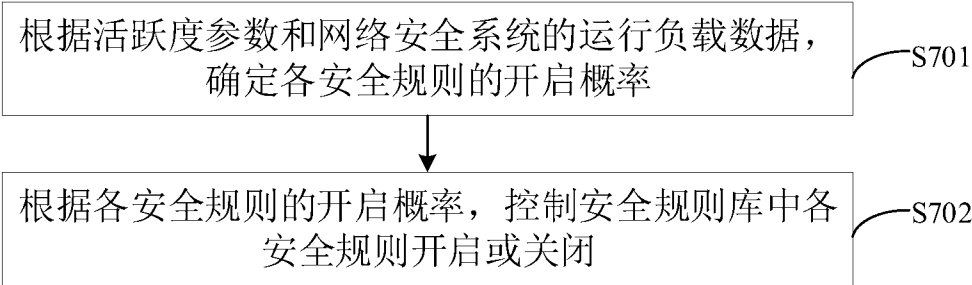


图 7

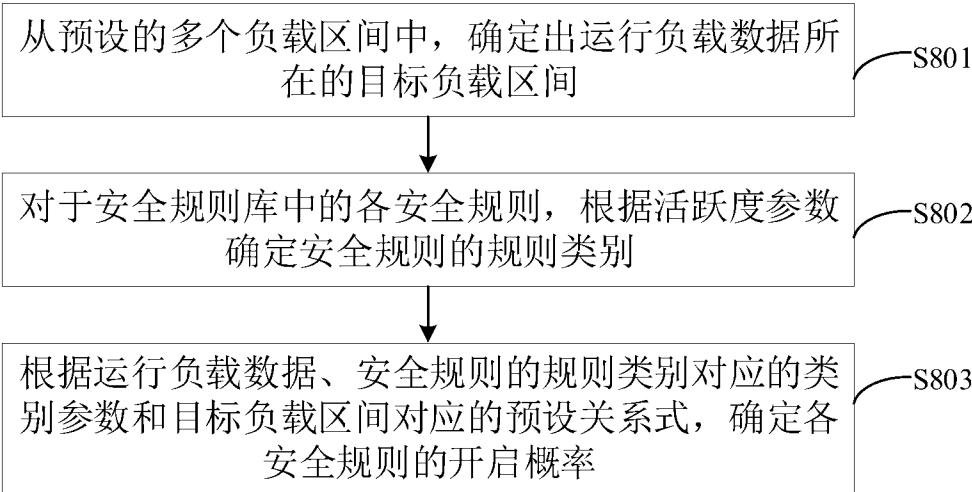


图 8

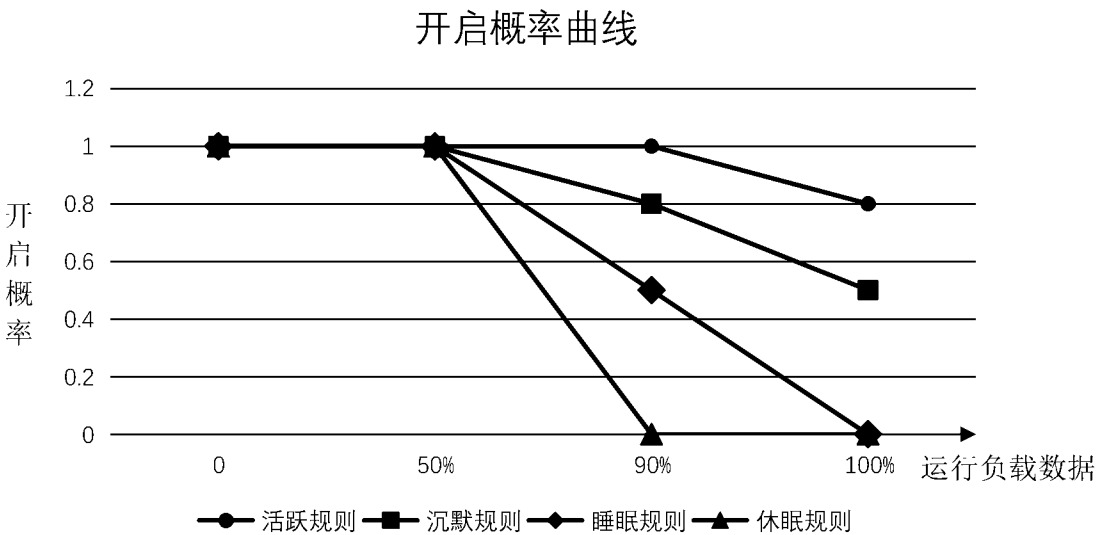


图 9

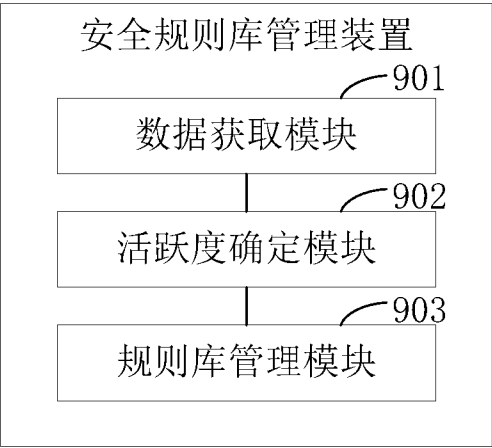


图 10

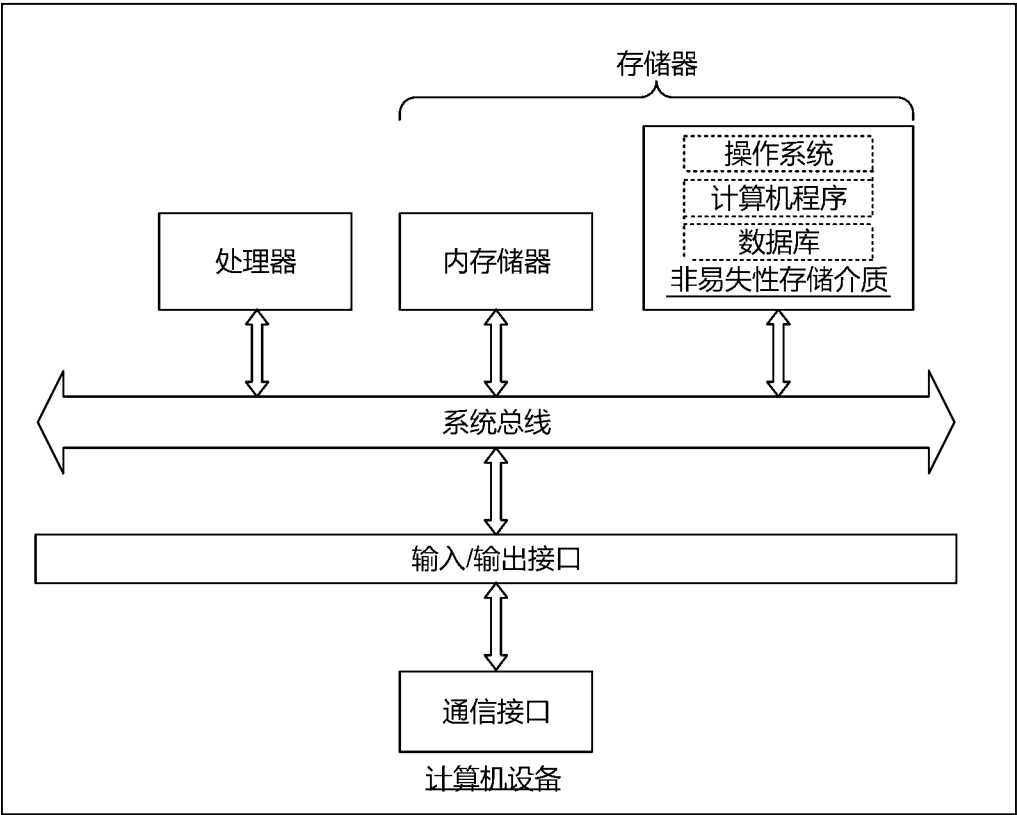


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/140249

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/40(2022.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; VEN; CNKI: 规则, 开启, 关闭, 活跃度, 命中, rule, turn on, close, activity, hit

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116633695 A (CHINA TELECOM CORP., LTD.) 22 August 2023 (2023-08-22) description, paragraphs [0004]-[0148], and figures 1-11	1-15
X	CN 112084036 A (NEW H3C INFORMATION SECURITY TECHNOLOGY CO., LTD.) 15 December 2020 (2020-12-15) description, paragraphs [0050]-[0151], and figures 1-6	1-15
A	CN 113722573 A (CHINA TELECOM CORP., LTD.) 30 November 2021 (2021-11-30) entire document	1-15
A	CN 105592061 A (HANGZHOU H3C TECHNOLOGIES CO., LTD.) 18 May 2016 (2016-05-18) entire document	1-15
A	CN 114598659 A (HUAWEI TECHNOLOGIES CO., LTD.) 07 June 2022 (2022-06-07) entire document	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“D” document cited by the applicant in the international application

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

24 January 2024

Date of mailing of the international search report

08 February 2024

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
China No. 6, Xitucheng Road, Jimenqiao, Haidian District,
Beijing 100088

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/140249

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	116633695	A	22 August 2023	None	
CN	112084036	A	15 December 2020	None	
CN	113722573	A	30 November 2021	None	
CN	105592061	A	18 May 2016	None	
CN	114598659	A	07 June 2022	None	

A. 主题的分类

H04L9/40(2022.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNTEXT;VEN;CNKI: 规则, 开启, 关闭, 活跃度, 命中, rule, turn on, close, activity, hit

C. 相关文件

类型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 116633695 A (中国电信股份有限公司) 2023年8月22日 (2023 - 08 - 22) 说明书第[0004]-[0148]段, 附图1-11	1-15
X	CN 112084036 A (新华三信息安全技术有限公司) 2020年12月15日 (2020 - 12 - 15) 说明书第[0050]-[0151]段, 附图1-6	1-15
A	CN 113722573 A (中国电信股份有限公司) 2021年11月30日 (2021 - 11 - 30) 全文	1-15
A	CN 105592061 A (杭州华三通信技术有限公司) 2016年5月18日 (2016 - 05 - 18) 全文	1-15
A	CN 114598659 A (华为技术有限公司) 2022年6月7日 (2022 - 06 - 07) 全文	1-15

☐ 其余文件在C栏的续页中列出。

☒ 见同族专利附件。

★ 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2024年1月24日

国际检索报告邮寄日期

2024年2月8日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

赵静

电话号码 (+86) 0512-88996135

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/140249

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	116633695	A	2023年8月22日	无	
CN	112084036	A	2020年12月15日	无	
CN	113722573	A	2021年11月30日	无	
CN	105592061	A	2016年5月18日	无	
CN	114598659	A	2022年6月7日	无	