(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
2020 年 12 月 30 日 (30.12.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/258991 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2020/084226

(22) 国际申请日: 2020 年 4 月 10 日 (10.04.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910584234.8 2019年6月28日 (28.06.2019) CN

(71) 申请人: 深圳前海微众银行股份有限公司 (WEBANK CO., LTD) [CN/CN]; 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。

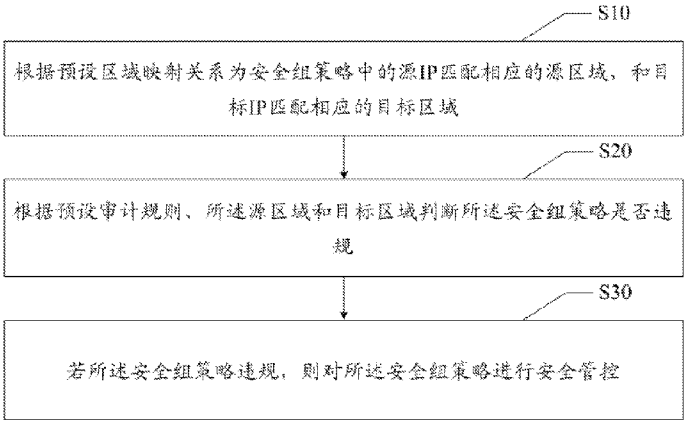
(72) 发明人: 蒋国梁 (JIANG, Guoliang); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 邹丽丽 (ZOU, Lili); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 邓丽铭 (DENG, Liming); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。 张英 (ZHANG, Ying); 中国广东省深圳市南山区沙河西路1819号深圳湾科技生态园7栋A座, Guangdong 518052 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区西丽街道松坪山社区松坪山路3号奥特迅电力大厦201, Guangdong 518052 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) **Title:** SECURITY GROUP POLICY MANAGEMENT METHOD, APPARATUS AND DEVICE, AND COMPUTER READABLE STORAGE MEDIUM

(54) **发明名称:** 安全组策略管理方法、装置、设备及计算机可读存储介质



S10 According to a preset region mapping relation, match a corresponding source region for a source IP in a security group policy, and match a corresponding target region for a target IP

S20 Determine whether the security group policy is illegitimate according to a preset audit rule, the source region, and the target region

S30 If the security group policy is illegitimate, perform security management and control on the security group policy

图 2

(57) **Abstract:** The present application relates to the field of Fintech, and disclosed are a security group policy management method, apparatus and device, and a computer readable storage medium. The method comprises the following steps: according to a preset region mapping relation, matching a corresponding source region for a source IP in a security group policy, and matching a corresponding target region for a target IP; determining whether the security group policy is illegitimate according to a preset audit rule, the source region, and the target region; and if the security group policy is illegitimate, performing security management and control on the security group policy. Whether the security group policy is illegitimate is automatically determined according to the regions to which the source IP and the target IP belong in the security group policy and the preset audit rule, so that when the security group policy is illegitimate, security management and control are automatically performed on the security group policy, thereby realizing automatic auditing of the security group policy, improving the auditing efficiency of the security group policy, and being capable of performing comprehensive auditing on a large number of security group policies.

WO 2020/258991 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))。

(57) 摘要：本申请公开了一种安全组策略管理方法、装置、设备及计算机可读存储介质，涉及金融科技领域，该方法包括以下步骤：根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；若所述安全组策略违规，则对所述安全组策略进行安全管控。实现了自动根据安全组策略中的源IP、目标IP所属的区域和预设审计规则判断安全组策略是否违规，从而在安全组策略违规时自动对该安全组策略提起安全管控，进而实现了对安全组策略的自动化审计，提升了安全组策略的审计效率，从而能够对海量的安全组策略进行全面的审计。

说明书

发明名称：安全组策略管理方法、装置、设备及计算机可读存储介质

[0001] 本申请要求于2019年6月28日提交中国专利局、申请号为201910584234.8、发明名称为“安全组策略管理方法、装置、设备及计算机可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

技术领域

[0002] 本申请涉及金融科技（Fintech）的网络安全领域，尤其涉及一种安全组策略管理方法、装置、设备及计算机可读存储介质。

背景技术

[0003] 随着计算机技术的发展，越来越多的技术应用在金融领域，传统金融业正在逐步向金融科技（Fintech）转变，但由于金融行业的安全性、实时性要求，也对技术提出了更高的要求

[0004] 云服务平台是一种新的企业信息化服务模式和管理方式，能够把海量的、高度虚拟化的企业资源和应用管理起来，组成一个集资源池、企业应用为一体的统一服务。

[0005] 银行等金融机构的云服务平台上的安全组是基于本地防火墙实现的，其使用与传统的网络层防火墙有本质的区别，且其中的策略与云主机的对应关系极其复杂，随着时间推移，伴随着越来越多的新系统上线，云上就会有越来越多的安全组策略。鉴于安全组策略能够直接影响企业公有云的网络安全，因此安全组策略的合格性就极其重要。现有的对安全组策略的合规性的审计是通过人工逐条审核的，面对海量的安全组策略，无法对安全组策略的合规性做出全面的、自动化的审计。显然面对与云主机具有复杂对应关系的安全组策略，现有的安全组策略审计方案无法做到对越来越多的安全组策略的自动化审计，这种情况不符合银行等金融机构的业务需求，影响银行等金融机构对各种业务平台（如开发贷款业务平台、存款业务平台等）的安全组策略管理。

发明概述

技术问题

问题的解决方案

技术解决方案

[0006] 本申请的主要目的在于提供一种安全组策略管理方法、装置、设备及可读存储介质，旨在解决现有技术无法对安全组策略的合规性做出全面的自动化审计的技术问题。

[0007] 为实现上述目的，本申请提供一种安全组策略管理方法，所述安全组策略管理方法包括以下步骤：

[0008] 根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

[0009] 根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

[0010] 若所述安全组策略违规，则对所述安全组策略进行安全管控。

[0011] 可选地，所述根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域的步骤之前，还包括：

[0012] 判断所述安全组策略是否在白名单中；

[0013] 若所述安全组策略不在白名单中，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域。

[0014] 可选地，所述根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域的步骤之前，还包括：

[0015] 根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；

[0016] 若所述安全组策略中不包括下线IP，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域；

[0017] 若所述安全组策略中包括下线IP，则将所述安全组策略下线。

[0018] 可选地，所述根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规的步骤包括：

[0019] 若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区

域不包括所述目标区域，则判定所述安全组策略不违规；

[0020] 若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[0021] 可选地，所述若所述安全组策略违规，则对所述安全组策略进行安全管控的步骤包括：

[0022] 若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

[0023] 对所述违规策略告警表中的安全组策略进行去重；

[0024] 对去重后的违规策略告警表中的安全组策略进行安全管控。

[0025] 可选地，所述对去重后的违规策略告警表中的安全组策略进行安全管控的步骤包括：

[0026] 将所述去重后的违规策略告警表发送给预设管控终端；

[0027] 在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起IT服务管理ITSM工单。

[0028] 可选地，所述根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作的步骤之后，还包括：

[0029] 按照预设统计频率对违规策略告警表中的安全组策略的安全管控情况进行统计，得到管控完成率和管控及时率，所述违规策略告警表中已进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控完成率，所述违规策略告警表中在预设时长内进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控及时率；

[0030] 将所述管控完成率和管控及时率发送至预设检阅终端，以供检阅。

[0031] 进一步地，为实现上述目的，本申请还提供一种安全组策略管理装置，所述安全组策略管理装置包括：

[0032] 匹配模块，用于根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

[0033] 判断模块，用于根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

[0034] 管控模块，用于若所述安全组策略违规，则对所述安全组策略进行安全管控。

[0035] 进一步地，为实现上述目的，本申请还提供一种安全组策略管理设备，所述安全组策略管理设备包括存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的安全组策略管理程序，所述安全组策略管理程序被所述处理器执行时实现如上述所述的安全组策略管理方法的步骤。

[0036] 进一步地，为实现上述目的，本申请还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有安全组策略管理程序，所述安全组策略管理程序被处理器执行时实现如上所述的安全组策略管理方法的步骤。

[0037] 本申请通过根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；若所述安全组策略违规，则对所述安全组策略进行安全管控。实现了自动根据安全组策略中的源IP、目标IP所属的区域和预设审计规则判断安全组策略是否违规，从而在安全组策略违规时自动对该安全组策略提起安全管控，进而实现了对安全组策略的自动化审计，提升了安全组策略的审计效率，从而能够对海量的安全组策略进行全面的审计。

发明的有益效果

对附图的简要说明

附图说明

[0038] 图1为本申请安全组策略管理设备实施例方案涉及的设备硬件运行环境的结构示意图；

[0039] 图2为本申请安全组策略管理方法第一实施例的流程示意图；

[0040] 图3为本申请安全组策略管理装置的功能模块示意图。

[0041] 本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

发明实施例

本发明的实施方式

[0042] 应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。

[0043] 需要说明的是，银行等金融机构的云服务平台上的安全组是基于本地防火墙实现的，其使用与传统的网络层防火墙有本质的区别，且其中的策略与云主机的对应关系极其复杂，随着时间推移，伴随着越来越多的新系统上线，云上就会有越来越多的安全组策略。鉴于安全组策略能够直接影响企业公有云的网络安全，因此安全组策略的合格性就极其重要。现有的对安全组策略的合规性的审计是通过人工逐条审核的，面对海量的安全组策略，无法对安全组策略的合规性做出全面的、自动化的审计。显然面对与云主机具有复杂对应关系的安全组策略，现有的安全组策略审计方案无法做到对越来越多的安全组策略的自动化审计，这种情况不符合银行等金融机构的业务需求，影响银行等金融机构对各种业务平台（如开发贷款业务平台、存款业务平台等）的安全组策略管理。

[0044] 基于上述缺陷，本申请提供一种安全组策略管理设备，参照图1，图1为本申请安全组策略管理设备实施例方案涉及的设备硬件运行环境的结构示意图。

[0045] 如图1所示，该安全组策略管理设备可以包括：处理器1001，例如CPU，通信总线1002、用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏（Display）、输入单元比如键盘（Keyboard），可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口（如WI-FI接口）。存储器1005可以是高速RAM存储器，也可以是稳定的存储器（non-volatile memory），例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储设备。

[0046] 本领域技术人员可以理解，图1中示出的安全组策略管理设备的硬件结构并不构成对安全组策略管理设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0047] 如图1所示，作为一种计算机可读存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及安全组策略管理程序。其中，操作系统是管理和控制安全组策略管理设备与软件资源的程序，支持网络通信模块、用户

接口模块、安全组策略管理程序以及其他程序或软件的运行；网络通信模块用于管理和控制网络接口1004；用户接口模块用于管理和控制用户接口1003。

[0048] 在图1所示的安全组策略管理设备硬件结构中，网络接口1004主要用于连接后台服务器，与后台服务器进行数据通信；用户接口1003主要用于连接客户端（用户端），与客户端进行数据通信；处理器1001可以调用存储器1005中中存储的安全组策略管理程序，并执行以下操作：

[0049] 根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

[0050] 根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

[0051] 若所述安全组策略违规，则对所述安全组策略进行安全管控。

[0052] 进一步地，所述根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域的步骤之前，处理器1001还用于调用存储器1005中存储的安全组策略管理程序，并执行以下操作：

[0053] 判断所述安全组策略是否在白名单中；

[0054] 若所述安全组策略不在白名单中，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域。

[0055] 进一步地，所述根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域的步骤之前，处理器1001还用于调用存储器1005中存储的安全组策略管理程序，并执行以下操作：

[0056] 根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；

[0057] 若所述安全组策略中不包括下线IP，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域；

[0058] 若所述安全组策略中包括下线IP，则将所述安全组策略下线。

[0059] 进一步地，所述根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规的步骤包括：

[0060] 若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区

域不包括所述目标区域，则判定所述安全组策略不违规；

[0061] 若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[0062] 进一步地，所述若所述安全组策略违规，则对所述安全组策略进行安全管控的步骤包括：

[0063] 若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

[0064] 对所述违规策略告警表中的安全组策略进行去重；

[0065] 对去重后的违规策略告警表中的安全组策略进行安全管控。

[0066] 进一步地，所述对去重后的违规策略告警表中的安全组策略进行安全管控的步骤包括：

[0067] 将所述去重后的违规策略告警表发送给预设管控终端；

[0068] 在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起IT服务管理ITSM工单。

[0069] 进一步地，所述根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作的步骤之后，处理器1001还用于调用存储器1005中存储的安全组策略管理程序，并执行以下操作：

[0070] 按照预设统计频率对违规策略告警表中的安全组策略的安全管控情况进行统计，得到管控完成率和管控及时率，所述违规策略告警表中已进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控完成率，所述违规策略告警表中在预设时长内进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控及时率；

[0071] 将所述管控完成率和管控及时率发送至预设检阅终端，以供检阅。

[0072] 本申请安全组策略管理设备的具体实施方式与下述安全组策略管理方法各实施例基本相同，在此不再赘述。

[0073] 本申请还提供一种安全组策略管理方法。

[0074] 本申请实施例提供了安全组策略管理方法的实施例，需要说明的是，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0075] 在安全组策略管理方法的各个实施例中，为了便于描述，省略执行主体进行阐述各个实施例。参照图2，图2为本申请安全组策略管理方法第一实施例的流程示意图，所述安全组策略管理方法包括：

[0076] 步骤S10，根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

[0077] 银行等金融机构的云服务平台上的安全组是基于本地防火墙实现的，其使用与传统的网络层防火墙有本质的区别，且其中的策略与云主机的对应关系极其复杂，随着时间推移，伴随着越来越多的新系统上线，云上就会有越来越多的安全组策略。鉴于安全组策略能够直接影响企业公有云的网络安全，因此安全组策略的合格性就极其重要。现有的对安全组策略的合规性的审计是通过人工逐条审核的，面对海量的安全组策略，无法对安全组策略的合规性做出全面的自动化审计。显然面对与云主机具有复杂对应关系的安全组策略，现有的安全组策略审计方案无法做到对越来越多的安全组策略的自动化审计，这种情况不符合银行等金融机构的业务需求，影响银行等金融机构对各种业务平台（如开发贷款业务平台、存款业务平台等）的安全组策略管理。基于此，提出本申请的技术方案。

[0078] 在本申请实施例中，要对安全组策略进行全面的自动化管理，安全组策略管理装置首先需要根据预设区域映射关系为所有的安全组策略中的源IP和目标IP匹配其所对应的区域，将源IP所对应的区域定义为源区域，将目标IP所对应的区域定义为目标区域。其中，预设区域映射关系指的是管理人员根据需要（例如企业内部的网络划分）为IP地址划分的预设区域（例如生产区域、管理区域、开发区域等），每个区域为一系列IP地址的集合，每个IP都有唯一对应的区域。

[0079] 进一步地，为了提高安全组策略管理的灵活性，减轻安全组策略管理装置的运算压力，本实施例中，在步骤S10之前还可以包括对安全组策略进行白名单过滤

的步骤，即：判断所述安全组策略是否在白名单中，所述白名单中存储有预设开通策略名单；若所述安全组策略不在白名单中，则执行步骤S10。即，安全组策略管理装置在获取所有安全组策略后，可先判断安全组策略是否命中白名单中的预设开通策略名单，该预设开通策略名单是管理人员根据需要自定义的必须开通的安全组策略名单，若安全组策略命中白名单中的预设开通策略名单，即安全组策略在白名单中，则不对该策略进行后续的安全组策略管理操作；若安全组策略未命中白名单中的预设开通策略名单，即安全组策略不在白名单中，则对该策略进行区域匹配操作。

[0080] 进一步地，为了提高安全组策略管理的灵活性，减轻安全组策略管理装置的运算压力，本实施例中，在步骤S10之前还可以包括对安全组策略进行下线IP过滤的步骤，即：根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；若所述安全组策略中不包括下线IP，则执行步骤S10；若所述安全组策略中包括下线IP，则将所述安全组策略下线。其中，下线IP为已停止使用的IP。需要说明的是，对安全组策略进行下线IP过滤的步骤可以在对安全组策略进行白名单过滤的步骤之前或之后，本实施例不做具体限定。

[0081] 安全组策略，指的是对源IP和目标IP的入和/或出流量控制。

[0082] 在本实施例中，以上安全组策略管理装置对安全组策略进行白名单过滤和下线IP过滤的方案可以择其一实施，也可以组合在一起实施，本实施例不做限制。

[0083] 步骤S20，根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

[0084] 在本实施例中，在安全组策略管理装置为所有的安全组策略中的源IP和目标IP匹配对应的源区域和目标区域后，根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规，具体地：若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不违规；若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区

域，则判定所述安全组策略违规。

[0085] 步骤S30，若所述安全组策略违规，则对所述安全组策略进行安全管控。

[0086] 在本实施例中，在安全组策略管理装置判定所述安全组策略违规后，对所述安全组策略进行安全管控，具体地：若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；对所述违规策略告警表中的安全组策略进行去重；将去重后的违规策略告警表发送给预设管控终端；在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括但不限于将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起ITSM工单中的一种。

[0087] 本实施例通过根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；若所述安全组策略违规，则对所述安全组策略进行安全管控。实现了自动根据安全组策略中的源IP、目标IP所属的区域和预设审计规则判断安全组策略是否违规，从而在安全组策略违规时自动对该安全组策略提起安全管控，进而实现了对安全组策略的自动化审计，提升了安全组策略的审计效率，从而能够对海量的安全组策略进行全面的审计。

[0088] 进一步地，提出本申请安全组策略管理方法第二实施例，上述步骤S10之前还包括：

[0089] 步骤S11，判断所述安全组策略是否在白名单中；

[0090] 若所述安全组策略不在白名单中，则执行步骤S10。

[0091] 为了提高安全组策略管理的灵活性，减轻安全组策略管理装置的运算压力。在本实施例中，在步骤S11之前还包括对白名单的设置步骤，运维人员为因为特殊原因必须开通，无需进行安全审计的安全组策略而创建的策略名单，即为白名单，具体原因本实施例不做限定。在对安全组策略进行违规审计之前，先判断该策略是否在白名单中，若该策略不在白名单中，则对该策略进行违规审计，即执行步骤S10；若该策略在白名单中，则可为该条策略添加白名单标记位，对此类添加有白名单标记位的安全组策略不进行违规审计，以此减轻安全组策略管理装置的运算压力。

[0092] 进一步地，上述步骤S10之前还包括：

[0093] 步骤S12，根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；

[0094] 步骤S13，若所述安全组策略中包括下线IP，则将所述安全组策略下线；

[0095] 若所述安全组策略中不包括下线IP，则执行步骤S10。

[0096] 为了提高安全组策略管理的灵活性，减轻安全组策略管理装置的运算压力。在本实施例中，在步骤S12之前还包括对下线IP库的设置和更新步骤，下线IP库中存储有已停止使用的IP地址，该下线IP库按照预设频率或者在更新的IP地址数量大于预设阈值时更新，本实施例不做具体限制。在本实施例中，先判断该安全组策略中的源IP和目标IP是否在下线IP库中，若该策略不在下线IP库中，说明该策略中的IP都为有效IP，则可对该策略进行违规审计，即执行步骤S10；若该策略中的源IP和目标IP中的一个或者两个在下线IP库中，说明说明该策略中的IP包括已停止使用的IP地址，则将该策略下线。

[0097] 需要说明的是，对安全组策略进行下线IP过滤的步骤可以在对安全组策略进行白名单过滤的步骤之前或之后，本实施例不做具体限定。

[0098] 进一步地，上述步骤S20包括：

[0099] 步骤S21，若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不违规；

[0100] 在本实施例中，在步骤S21之前还包括对预设审计规则的设置步骤，运维人员根据企业内部制度、网络安全规范等内容设置预设审计规则。预设审计规则是对预设区域映射关系中的预设区域之间互相访问的权限的设置，是以预设区域为核心的，预设审计规则中包括源区域和与之对应的、该源区域不能访问的预设目标区域。

[0101] 在安全组策略管理装置为所有的安全组策略中的源IP和目标IP匹配对应的源区域和目标区域后，根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规，即，判断所述预设审计规则中是否包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述

目标区域。若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，所述预设审计规则中包括所述源区域和所述目标区域，但在所述预设审计规则中与所述源区域相对应的该源区域不能访问的预设目标区域中不包括所述目标区域，则判定所述安全组策略不违规。

[0102] 步骤S22，若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[0103] 在本实施例中，若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的该源区域不能访问的预设目标区域中包括所述目标区域，则判定所述安全组策略违规。

[0104] 进一步地，为了增加判断安全组策略是否违规的方法的灵活性，上述步骤S20还可以包括：若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略违规；若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略不违规。这种情况下，预设审计规则中包括源区域和与之对应的、该源区域能访问的预设目标区域。

[0105] 本实施例通过白名单过滤和下线IP过滤能够过滤掉不需要进行违规审计的安全组策略，减少需要进行违规审计的安全组策略数量，从而减轻安全组策略管理装置的运算压力，进而提升违规审计的效率；根据安全组策略的源区域、目标区域以及预设审计规则自动确定安全组策略是否违规，实现了对安全组策略的自动化审计，提升了安全组策略的审计效率。

[0106] 进一步地，提出本申请安全组策略管理方法第三实施例，上述步骤S30包括：

[0107] 步骤S31，若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

[0108] 在本实施例中，若判定该安全组策略违规，则将该安全组策略加入违规策略告警表中，该违规策略告警表中存储有本次违规审计中被判定违规的安全组策略

，以及历史违规审计中被判定违规，且尚未进行安全管控的安全组策略。

[0109] 步骤S32，对所述违规策略告警表中的安全组策略进行去重；

[0110] 对于海量的安全组策略，其中或多或少会有重复的安全组策略，违规的安全组策略也难免重复，若对所有违规的安全组策略都进行安全管控，重复的安全管控会造成不必要的资源浪费，也会增大安全组策略管理装置的运算压力。基于此，提出本实施例的技术方案。

[0111] 在本申请实施例中，为避免重复的安全管控，对违规策略告警表中的安全组策略进行哈希运算得到对应的哈希值，根据所述违规策略告警表中是否有与当前哈希值相同的值判断是否有重复的安全组策略；若有，则仅保留重复的安全组策略中的一条。其中，进行哈希运算的哈希函数包括但不限于安全散列算法SHA系列（例如SHA-1、SHA-256、SHA-384等）、消息摘要算法MD系列（例如MD2、MD3、MD4、MD5等）或者高级加密标准AES等哈希函数中的一种或多种，本实施例不做具体限制。

[0112] 步骤S33，对去重后的违规策略告警表中的安全组策略进行安全管控。

[0113] 在对违规策略告警表中的安全组策略去重之后，对去重后的违规策略告警表中的安全组策略进行安全管控。

[0114] 进一步地，上述步骤S33包括：

[0115] 步骤S331，将所述去重后的违规策略告警表发送给预设管控终端；

[0116] 步骤S332，在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起ITSM工单。

[0117] 在本实施例中，对违规策略告警表中的安全组策略去重后，将所述去重后的违规策略告警表发送给预设管控终端，以使预设管控终端的管理人员根据违规策略的具体类型确定具体地管控操作，并向安全组策略管理装置发送安全管控指令，该安全管控指令中包括具体地安全管控内容，安全组策略管理装置在接收到预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作。

[0118] 其中，所述安全管控内容包括将安全组策略加入白名单、将安全组策略挂起或者对安全组策略提起ITSM（IT服务管理）工单。具体地，若预设管控终端的管理人员确定当前违规安全组策略存在特殊原因必须开通，可将该违规安全组策略开通，并加入白名单；预设管控终端的管理人员将违规但短期无法解决的安全组策略挂起；安全组策略管理可与ITSM平台对接，预设管控终端的管理人员将违规且必须处理的安全组策略通过与ITSM平台对接接口提起ITSM工单。

[0119] 进一步地，上述步骤S332之后还包括：

[0120] 按照预设统计频率对违规策略告警表中的安全组策略的安全管控情况进行统计，得到管控完成率和管控及时率，所述违规策略告警表中已进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控完成率，所述违规策略告警表中在预设时长内进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控及时率；将所述管控完成率和管控及时率发送至预设检阅终端，以供检阅。

[0121] 本实施例通过对违规策略告警表中的安全组策略去重，再对去重后违规策略告警表中的安全组策略进行安全管控，能够避免不必要的资源浪费，也减轻了安全组策略管理装置的运算压力；对违规的安全组策略进行相应的安全管控，能够实现从违规安全组策略的审计到处理的运营闭环，进而实现更加完善的安全组策略管理流程。

[0122] 本申请还提供一种安全组策略管理装置。

[0123] 参照图3，图3为本申请安全组策略管理装置第一实施例的功能模块示意图，所述安全组策略管理装置包括：

[0124] 匹配模块10，用于根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

[0125] 判断模块20，用于根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

[0126] 管控模块30，用于若所述安全组策略违规，则对所述安全组策略进行安全管控。

[0127] 进一步地，所述安全组策略管理装置还包括：

[0128] 白名单判断模块，用于判断所述安全组策略是否在白名单中；

[0129] 所述匹配模块10还用于若所述安全组策略不在白名单中，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域。

[0130] 进一步地，所述安全组策略管理装置还包括：

[0131] IP判断模块，用于根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；

[0132] 所述匹配模块10还用于若所述安全组策略中不包括下线IP，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域；

[0133] 下线模块，用于若所述安全组策略中包括下线IP，则将所述安全组策略下线。

[0134] 进一步地，所述判断模块20还包括：

[0135] 合规判定单元，用于若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不违规；

[0136] 违规判定单元，用于若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[0137] 进一步地，所述管控模块30还包括：

[0138] 告警加入单元，用于若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

[0139] 去重单元，用于对所述违规策略告警表中的安全组策略进行去重；

[0140] 去重管控单元，用于对去重后的违规策略告警表中的安全组策略进行安全管控。

[0141] 进一步地，所述去重管控单元还包括：

[0142] 发送子单元，用于将所述去重后的违规策略告警表发送给预设管控终端；

[0143] 执行子单元，用于在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起IT服务管理ITSM工单。

[0144] 进一步地，所述安全组策略管理装置还包括：

[0145] 统计模块，用于按照预设统计频率对违规策略告警表中的安全组策略的安全管控情况进行统计，得到管控完成率和管控及时率，所述违规策略告警表中已进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控完成率，所述违规策略告警表中在预设时长内进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控及时率；

[0146] 检阅模块，用于将所述管控完成率和管控及时率发送至预设检阅终端，以供检阅。

[0147] 本申请安全组策略管理装置具体实施方式与上述安全组策略管理方法各实施例基本相同，在此不再赘述。

[0148] 此外，本申请实施例还提出一种计算机可读存储介质。

[0149] 计算机可读存储介质上存储有安全组策略管理程序，安全组策略管理程序被处理器执行时实现如上所述的安全组策略管理方法的步骤。

[0150] 本申请可读存储介质具体实施方式与上述安全组策略管理方法各实施例基本相同，在此不再赘述。

[0151] 上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，这些均属于本申请的保护之内。

权利要求书

[权利要求 1] 一种安全组策略管理方法，其中，所述安全组策略管理方法包括以下步骤：

根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

若所述安全组策略违规，则对所述安全组策略进行安全管控。

[权利要求 2] 如权利要求1所述的安全组策略管理方法，其中，所述根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域的步骤之前，还包括：

判断所述安全组策略是否在白名单中；

若所述安全组策略不在白名单中，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域。

[权利要求 3] 如权利要求1所述的安全组策略管理方法，其中，所述根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域的步骤之前，还包括：

根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；

若所述安全组策略中不包括下线IP，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域；

若所述安全组策略中包括下线IP，则将所述安全组策略下线。

[权利要求 4] 如权利要求1所述的安全组策略管理方法，其中，所述根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规的步骤包括：

若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不

违规；

若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[权利要求 5] 如权利要求1所述的安全组策略管理方法，其中，所述若所述安全组策略违规，则对所述安全组策略进行安全管控的步骤包括：

若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

对所述违规策略告警表中的安全组策略进行去重；

对去重后的违规策略告警表中的安全组策略进行安全管控。

[权利要求 6] 如权利要求5所述的安全组策略管理方法，其中，所述对去重后的违规策略告警表中的安全组策略进行安全管控的步骤包括：

将所述去重后的违规策略告警表发送给预设管控终端；

在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起IT服务管理ITSM工单。

[权利要求 7] 如权利要求6所述的安全组策略管理方法，其中，所述根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作的步骤之后，还包括：

按照预设统计频率对违规策略告警表中的安全组策略的安全管控情况进行统计，得到管控完成率和管控及时率，所述违规策略告警表中已进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控完成率，所述违规策略告警表中在预设时长内进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控及时率；

将所述管控完成率和管控及时率发送至预设检阅终端，以供检阅。

[权利要求 8] 一种安全组策略管理装置，其中，所述安全组策略管理装置包括：

匹配模块，用于根据预设区域映射关系为安全组策略中的源IP匹配相

应的源区域，和目标IP匹配相应的目标区域；

判断模块，用于根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

管控模块，用于若所述安全组策略违规，则对所述安全组策略进行安全管控。

[权利要求 9] 如权利要求8所述的安全组策略管理装置，其中，所述安全组策略管理装置还包括：

白名单判断模块，用于判断所述安全组策略是否在白名单中；

所述匹配模块还用于若所述安全组策略不在白名单中，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域。

[权利要求 10] 如权利要求8所述的安全组策略管理装置，其中，所述安全组策略管理装置还包括：

IP判断模块，用于根据所述安全组策略中的源IP和目标IP是否存在于下线IP库中判断所述安全组策略中是否包括下线IP；

所述匹配模块还用于若所述安全组策略中不包括下线IP，则执行步骤：根据预设区域映射关系为安全组策略中的源IP和目标IP匹配相应的所属区域；

下线模块，用于若所述安全组策略中包括下线IP，则将所述安全组策略下线。

[权利要求 11] 如权利要求8所述的安全组策略管理装置，其中，所述判断模块还包括：

合规判定单元，用于若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不违规；

违规判定单元，用于若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区

域包括所述目标区域，则判定所述安全组策略违规。

[权利要求 12] 如权利要求8所述的安全组策略管理装置，其中，所述管控模块还包括：

告警加入单元，用于若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

去重单元，用于对所述违规策略告警表中的安全组策略进行去重；

去重管控单元，用于对去重后的违规策略告警表中的安全组策略进行安全管控。

[权利要求 13] 如权利要求12所述的安全组策略管理装置，其中，所述去重管控单元还包括：

发送子单元，用于将所述去重后的违规策略告警表发送给预设管控终端；

执行子单元，用于在接收到所述预设管控终端发送的安全管控指令时，根据所述安全管控指令携带的安全管控内容执行相应的安全管控操作，所述安全管控内容包括将所述安全组策略加入白名单、将所述安全组策略挂起或者对所述安全组策略提起IT服务管理ITSM工单。

[权利要求 14] 如权利要求13所述的安全组策略管理装置，其中，所述安全组策略管理装置还包括：

统计模块，用于按照预设统计频率对违规策略告警表中的安全组策略的安全管控情况进行统计，得到管控完成率和管控及时率，所述违规策略告警表中已进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控完成率，所述违规策略告警表中在预设时长内进行安全管控的安全组策略的数量除以所述违规策略告警表中的安全组策略的总数为所述管控及时率；

检阅模块，用于将所述管控完成率和管控及时率发送至预设检阅终端，以供检阅。

[权利要求 15] 一种安全组策略管理设备，其中，所述安全组策略管理设备包括存储器、处理器以及存储在所述存储器上并可在所述处理器上运行的安全

组策略管理程序，所述安全组策略管理程序被所述处理器执行时实现如下步骤：

根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

若所述安全组策略违规，则对所述安全组策略进行安全管控。

[权利要求 16] 如权利要求15所述的安全组策略管理设备，其中，所述安全组策略管理设备程序被所述处理器执行时还实现如下步骤：

若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不违规；

若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[权利要求 17] 如权利要求15所述的安全组策略管理设备，其中，所述安全组策略管理设备程序被所述处理器执行时还实现如下步骤：

若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

对所述违规策略告警表中的安全组策略进行去重；

对去重后的违规策略告警表中的安全组策略进行安全管控。

[权利要求 18] 一种计算机可读存储介质，其中，所述可读存储介质上存储有安全组策略管理程序，所述安全组策略管理程序被处理器执行时实现如下步骤：

根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域，和目标IP匹配相应的目标区域；

根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规；

若所述安全组策略违规，则对所述安全组策略进行安全管控。

[权利要求 19] 如权利要求18所述的安全组策略管理设备，其中，所述安全组策略管理设备程序被所述处理器执行时还实现如下步骤：

若所述预设审计规则中不包括所述源区域，或者所述预设审计规则中不包括所述目标区域，或者，在所述预设审计规则中与所述源区域相对应的预设目标区域不包括所述目标区域，则判定所述安全组策略不违规；

若所述预设审计规则中包括所述源区域和所述目标区域，且在所述预设审计规则中与所述源区域相对应的预设目标区域包括所述目标区域，则判定所述安全组策略违规。

[权利要求 20] 如权利要求18所述的安全组策略管理设备，其中，所述安全组策略管理设备程序被所述处理器执行时还实现如下步骤：

若所述安全组策略违规，则将所述安全组策略加入违规策略告警表；

对所述违规策略告警表中的安全组策略进行去重；

对去重后的违规策略告警表中的安全组策略进行安全管控。

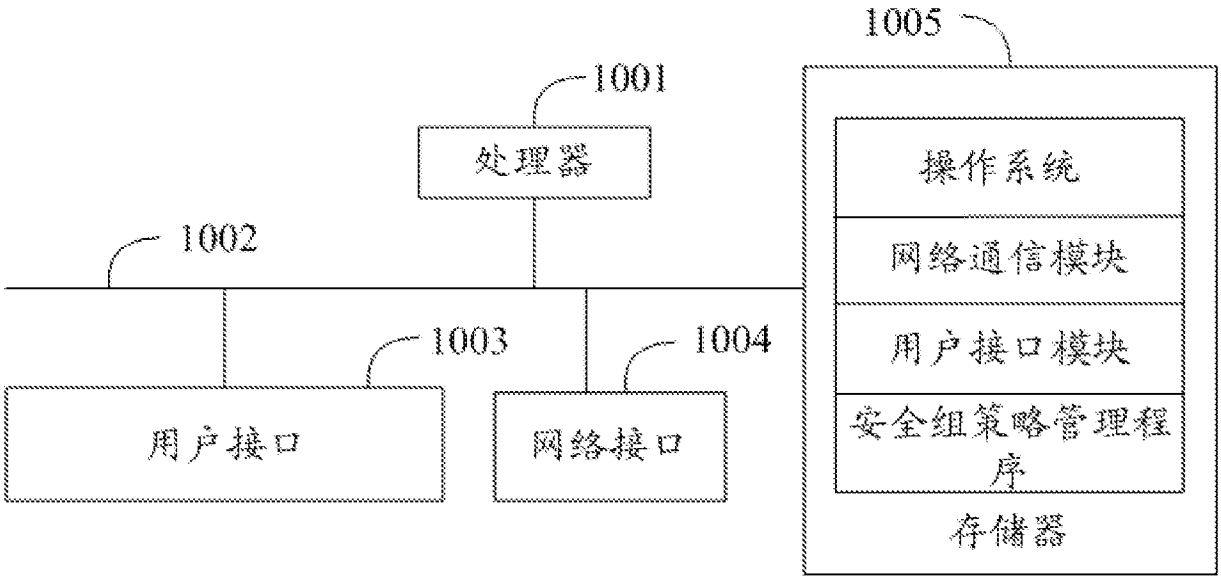

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
安全组策略管理程序
用户接口
网络接口
存储器

图 1

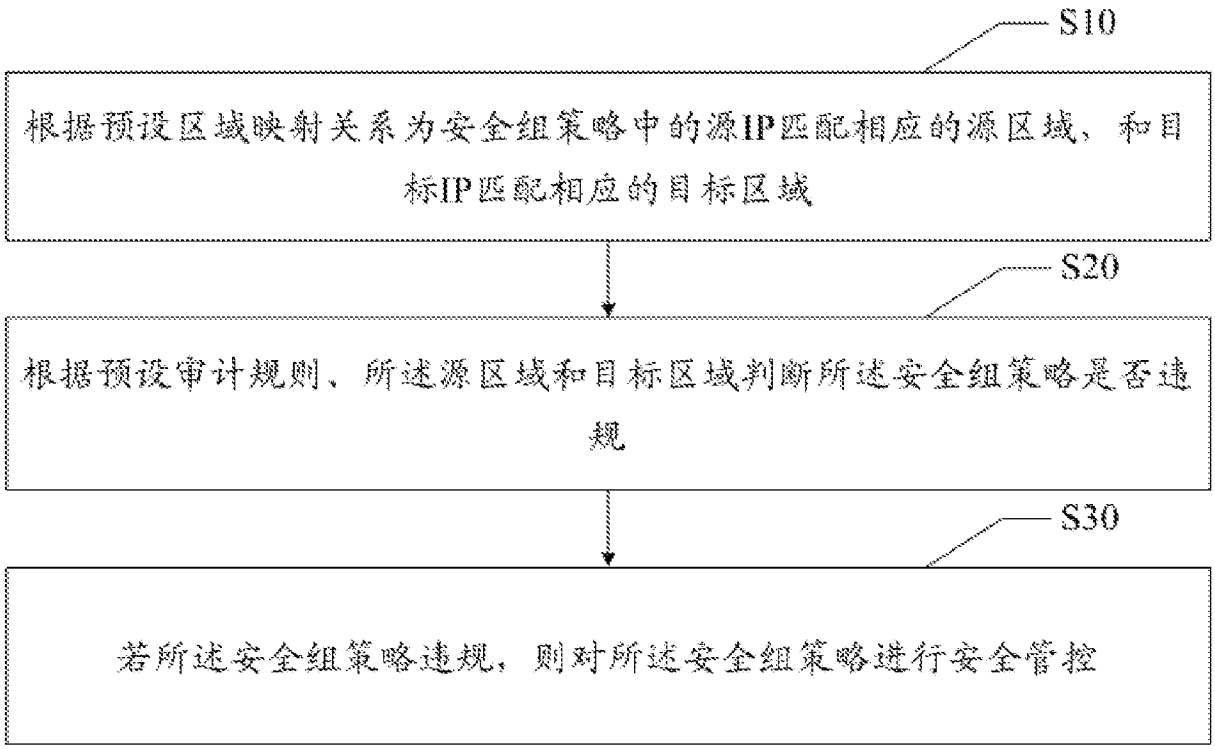

S10
根据预设区域映射关系为安全组策略中的源IP匹配相应的源区域、和目标IP匹配相应的目标区域
S20
根据预设审计规则、所述源区域和目标区域判断所述安全组策略是否违规
S30
若所述安全组策略违规，则对所述安全组策略进行安全管控

图 2

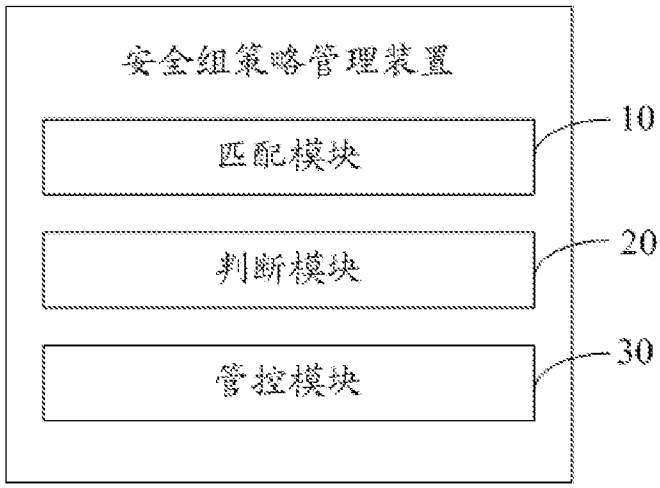


图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/084226

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)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)

H04L G06F

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)

WPI, EPODOC, CNPAT, CNKI: IP, 地址, 警报, 报警, 告警, 警告, 原, 源, 目标, 目的, 地区, 区域, 地域, 对应, 相应, 违规, 犯规, 安全, 白名单, address, alert, alarm, source, destination, target, area, region, zone, correspond, violate, safe, white, list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110324334 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 11 October 2019 (2019-10-11) description, paragraphs [0005]-[0056]	1-20
X	CN 106034131 A (BEIJING VENUS INFORMATION SECURITY TECHNOLOGY CO., LTD. et al.) 19 October 2016 (2016-10-19) description paragraphs [0004]-[0079], [0127]	1, 3-5, 8, 10-12, 15-20
Y	CN 106034131 A (BEIJING VENUS INFORMATION SECURITY TECHNOLOGY CO., LTD. et al.) 19 October 2016 (2016-10-19) description paragraphs [0004]-[0079], [0127]	2, 6-7, 9, 13-14
Y	CN 107135187 A (ALIBABA GROUP HOLDING LIMITED) 05 September 2017 (2017-09-05) description, paragraph [0077]	2, 6-7, 9, 13-14
A	CN 108449444 A (JIANGSU FUTURE NETWORKS INNOVATION INSTITUTE) 24 August 2018 (2018-08-24) entire document	1-20
A	US 7516492 B1 (RSA SECURITY INC.) 07 April 2009 (2009-04-07) entire document	1-20

☐ 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
"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	Date of mailing of the international search report
19 June 2020	**29 June 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/084226

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110324334	A	11 October 2019	None			
CN	106034131	A	19 October 2016	None			
CN	107135187	A	05 September 2017	TW	201738796	A	01 November 2017
				WO	2017148263	A1	08 September 2017
				US	2018367566	A1	20 December 2018
CN	108449444	A	24 August 2018	None			
US	7516492	B1	07 April 2009	US	7954151	B1	31 May 2011

国际检索报告

国际申请号
PCT/CN2020/084226

A. 主题的分类

H04L 29/06(2006.01)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)

H04L G06F

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））

WPI, EPODOC, CNPAT, CNKI: IP, 地址, 警报, 报警, 告警, 警告, 原, 源, 目标, 目的, 地区, 区域, 地域, 对应, 相应, 违规, 犯规, 安全, 白名单, address, alert, alarm, source, destination, target, area, region, zone, correspond, violate, safe, white, list

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 110324334 A (深圳前海微众银行股份有限公司) 2019年 10月 11日 (2019-10-11) 说明书第[0005]-[0056]段	1-20
X	CN 106034131 A (北京启明星辰信息安全技术有限公司等) 2016年 10月 19日 (2016-10-19) 说明书第[0004]-[0079]、[0127]段	1, 3-5, 8, 10-12, 15-20
Y	CN 106034131 A (北京启明星辰信息安全技术有限公司等) 2016年 10月 19日 (2016-10-19) 说明书第[0004]-[0079]、[0127]段	2, 6-7, 9, 13-14
Y	CN 107135187 A (阿里巴巴集团控股有限公司) 2017年 9月 5日 (2017-09-05) 说明书第[0077]段	2, 6-7, 9, 13-14
A	CN 108449444 A (江苏省未来网络创新研究院) 2018年 8月 24日 (2018-08-24) 全文	1-20
A	US 7516492 B1 (RSA SECURITY INC.) 2009年 4月 7日 (2009-04-07) 全文	1-20

☐ 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

“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	国际检索报告邮寄日期
2020年 6月 19日	2020年 6月 29日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王欣
传真号 (86-10)62019451	电话号码 86-(10)-53961617

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/084226

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	110324334	A	2019年 10月 11日	无			
CN	106034131	A	2016年 10月 19日	无			
CN	107135187	A	2017年 9月 5日	TW	201738796	A	2017年 11月 1日
				WO	2017148263	A1	2017年 9月 8日
				US	2018367566	A1	2018年 12月 20日
CN	108449444	A	2018年 8月 24日	无			
US	7516492	B1	2009年 4月 7日	US	7954151	B1	2011年 5月 31日