

(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
2023 年 4 月 6 日 (06.04.2023)



(10) 国际公布号
WO 2023/050070 A1

(51) 国际专利分类号:
H04L 9/00 (2022.01)

(21) 国际申请号: PCT/CN2021/121369

(22) 国际申请日: 2021 年 9 月 28 日 (28.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 中远海运科技股份有限公司 (COSCO SHIPPING TECHNOLOGY CO., LTD.)
[CN/CN]; 中国上海市浦东新区民生路 600 号, Shanghai 200135 (CN)。

(72) 发明人: 吴中岱 (WU, Zhongdai); 中国上海市浦东民生路 600 号, Shanghai 200135 (CN)。王骏翔 (WANG, Junxiang); 中国上海市浦东民生路 600 号, Shanghai 200135 (CN)。郭磊 (GUO, Lei); 中国上海市浦东民生路 600 号, Shanghai 200135 (CN)。胡蓉 (HU, Rong); 中国上海市浦东民生路 600 号, Shanghai 200135 (CN)。韩冰 (HAN, Bing); 中国上海市浦东民生路 600 号, Shanghai 200135 (CN)。刘晋 (LIU, Jin); 中国上海市浦东民生路 600 号, Shanghai 200135 (CN)。

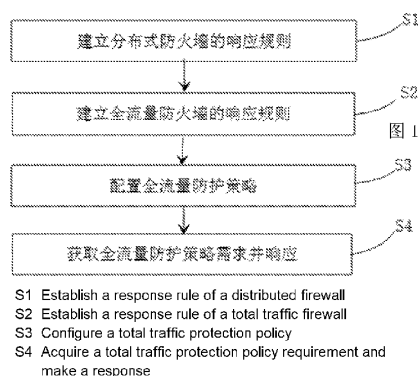
(74) 代理人: 北京海虹嘉诚知识产权代理有限公司 (HAIHONG JIACHENG INTELLECTUAL PROPERTY & PARTNERS); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 9 层, Beijing 100080 (CN)。

(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, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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,

(54) Title: METHOD AND DEVICE FOR CLOUD HOST TOTAL TRAFFIC NETWORK ACCESS PROTECTION

(54) 发明名称: 一种面向云主机全流量网络访问防护的方法及装置



(57) Abstract: The present invention relates to the technical field of cloud computing and information security, and in particular, to a method and device for cloud host total traffic network access protection. According to the present invention, under the conventional north-south traffic protection, the protection capability for cloud resources in an east-west level is realized by means of cloud computing service orchestration and automation technologies, and is complementary to the north-south traffic protection, so that total traffic network access protection is formed. Specifically, by establishing a response rule of a distributed firewall, establishing a response rule of a total traffic firewall, configuring a total traffic protection policy, acquiring a total traffic protection policy requirement, and making a response, total traffic network access protection is automatically realized. The present invention further provides a corresponding device, which solves the problems of high professional requirements of a conventional firewall technology, protection policy configuration conflict in protection mode, lack of collaboration in protection policy configuration among multiple cloud hosts, and tedious operation steps, etc.

[见续页]

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)。

根据细则4.17的声明:

— 发明人资格(细则4.17(iv))

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本发明涉及云计算及信息安全技术领域,具体涉及一种面向云主机全流量网络访问防护的方法及装置。本发明在传统南北向流量防护下,通过云计算服务编排及自动化技术实现了云资源东西向层面的一道防护能力,与南北向流量防护互补形成全流量网络访问防护。具体采用建立分布式防火墙的响应规则,建立全流量防火墙的响应规则,配置全流量防护策略以及获取全流量防护策略需求并响应,从而自动化实现全流量网络访问的防护。本发明还提供对应的装置,解决了传统防火墙技术的专业性要求较高,防护方式存在防护策略配置冲突,及多台云主机间的防护策略配置缺乏协同性、操作步骤繁琐等问题。