

(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
2016 年 12 月 1 日 (01.12.2016)



(10) 国际公布号
WO 2016/188294 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/080311
- (22) 国际申请日: 2016 年 4 月 27 日 (27.04.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510284470.X 2015 年 5 月 28 日 (28.05.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼乔治城资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 张倩 (ZHANG, Qian) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。孙磊 (SUN, Lei) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.);

中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

(54) Title: NETWORK ATTACK PROCESSING METHOD AND DEVICE

(54) 发明名称: 一种网络攻击处理方法和装置

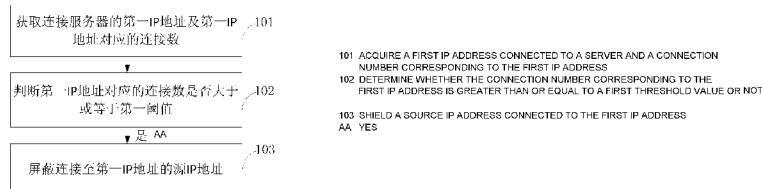


图 1

(57) Abstract: Embodiments of the present application provide a network attack processing method and device. The network attack processing method comprises: acquiring a first IP address connected to a server and a connection number corresponding to the first IP address; determining whether the connection number corresponding to the first IP address is greater than or equal to a first threshold value or not; and if so, shielding a source IP address connected to the first IP address. The embodiments of the present application not only ensure overall stability of a server and a network, but also reduce service influence on an attacked IP address by shielding a source IP address, thereby reducing the influence on website visiting.

(57) 摘要: 本申请实施例提供了一种网络攻击处理方法及装置。该网络攻击处理方法包括: 获取连接服务器的第一 IP 地址及所述第一 IP 地址对应的连接数; 判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值; 若是, 则屏蔽连接至所述第一 IP 地址的源 IP 地址。本申请实施例不仅保证了服务器和网络的整体稳定性, 而且, 通过屏蔽源 IP 地址减小了对受攻击 IP 地址的业务影响, 减小了对网站访问的影响。



WO 2016/188294 A1

一种网络攻击处理方法和装置

技术领域

本申请涉及通信技术领域，特别是涉及一种网络攻击处理方法和一种网络攻击处理装置。

5 背景技术

虚拟主机，也叫“网站空间”，是把一台运行在互联网上的服务器划分成多个具有一定大小的硬盘空间，每个空间都给予相应的 FTP（File Transfer Protocol，文件传输协议）权限和 Web 访问权限，以用于网站发布。

10 为了保护服务器整体的稳定和安全，服务器的防火墙会监测对各虚拟主机的网络攻击，防火墙一旦判断攻击规模达到一定的阈值后，会自动对被攻击的虚拟主机的 IP 地址做屏蔽处理。

然而，该对攻击目标 IP 地址的屏蔽虽然能够保证服务器和网络的整体稳定性，但对被攻击的 IP 地址屏蔽后，也会影响该 IP 地址所在的业务，影响网站访问。

15 因此，目前需要本领域技术人员迫切解决的一个技术问题就是：如何能减少网络攻击对被攻击 IP 地址的业务影响。

发明内容

本申请实施例所要解决的技术问题是提供一种网络攻击处理方法，能够减少网络攻击对被攻击 IP 地址的业务影响。

20 相应的，本申请实施例还提供了一种网络攻击装置，用以保证上述方法的实现及应用。

为了解决上述问题，本申请公开了一种网络攻击处理方法，包括：

获取连接服务器的第一 IP 地址及所述第一 IP 地址对应的连接数；

判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值；

25 若是，则屏蔽连接至所述第一 IP 地址的源 IP 地址。

进一步，所述屏蔽连接至所述第一 IP 地址的源 IP 地址，包括：

获取连接至所述第一 IP 地址的各源 IP 地址及所述各源 IP 地址对应的连接数;

判断所述各源 IP 地址中是否存在连接数大于或等于第二阈值的源 IP 地址;

5 若存在, 则屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

进一步, 所述方法还包括:

当所述各源 IP 地址中不存在连接数大于或等于所述第二阈值的源 IP 地址时, 屏蔽所述第一 IP 地址。

进一步, 所述屏蔽所述连接数大于或等于第二阈值的源 IP 地址, 包括:

10 判断所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和是否大于或等于所述第一阈值;

若是, 则屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

进一步, 所述方法还包括:

15 当所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和小于所述第一阈值时, 屏蔽所述第一 IP 地址。

进一步, 所述方法还包括:

当满足预置条件时, 停止对所述第一 IP 地址的屏蔽。

本申请实施例还公开了一种网络攻击处理装置, 包括:

20 获取单元, 被配置为获取连接服务器的第一 IP 地址及所述第一 IP 地址对应的连接数;

判断单元, 被配置为判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值;

处理单元, 被配置为当所述判断单元判定所述第一 IP 地址对应的连接数大于或等于第一阈值时, 屏蔽连接至所述第一 IP 地址的源 IP 地址。

25 进一步, 所述处理单元包括:

获取子单元, 被配置为获取连接至所述第一 IP 地址的各源 IP 地址及所述各源 IP 地址对应的连接数;

判断子单元, 被配置为判断所述各源 IP 地址中是否存在连接数大于或

等于第二阈值的源 IP 地址;

屏蔽子单元,被配置为当所述判断子单元判定所述各源 IP 地址中存在连接数大于或等于第二阈值的源 IP 地址时,屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

- 5 进一步,所述处理单元还被配置为当所述各源 IP 地址中不存在连接数大于或等于所述第二阈值的源 IP 地址时,屏蔽所述第一 IP 地址。

进一步,所述屏蔽子单元包括:

下层判断子单元,被配置为判断所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和是否大于或等于所述第一阈值;

- 10 下层屏蔽子单元,被配置为当所述下层判断子单元判定所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和大于或等于所述第一阈值时,屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

- 15 进一步,所述下层屏蔽子单元,还被配置为当所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和小于所述第一阈值时,屏蔽所述第一 IP 地址。

与现有技术相比,本申请实施例包括以下优点:

- 20 本申请实施例通过检测连接服务器的 IP 地址的连接数,并在连接数超过一定阈值时,确认该 IP 地址受到网络攻击,然后对连接该受攻击的 IP 地址的全部或部分源 IP 地址进行屏蔽,不仅保证了服务器和网络的整体稳定性,而且,通过屏蔽源 IP 地址减小了对受攻击 IP 地址的业务影响,减小了对网站访问的影响。并且,该方法通过监测连接数来确认受攻击的 IP 地址,相对于现有技术中硬件防火墙、黑洞等的监测手段,可以更加准确的确定出网络攻击的对象,也更适应于虚拟主机本身的网络攻击防护。

附图说明

- 25 图 1 是本申请的一种网络攻击处理方法实施例的步骤流程图;
图 2 是本申请的另一种网络攻击处理方法实施例的步骤流程图;
图 3 是本申请的一种网络攻击处理装置实施例的结构框图;
图 4 是本申请实施例中一种处理单元的结构框图;

图 5 是本申请实施例中一种屏蔽子单元的结构框图。

具体实施方式

为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

5 参照图 1，示出了本申请的一种网络攻击处理方法实施例的步骤流程图，具体可以包括如下步骤：

步骤 101，获取连接服务器的第一 IP 地址及第一 IP 地址对应的连接数。

本申请实施例中，服务器上可以划分出多个虚拟主机，服务器可以通过公开的端口如 80 端口与各虚拟主机连接。

10 网络攻击处理装置可以是服务器本身，也可以是设置在服务器中的一装置，或者独立于服务器但可以与服务器进行通信的装置。

该装置不同于服务器的防火墙通过带宽等指标来检测各虚拟主机受到的网络攻击。本步骤中，该装置要获取连接在服务器上的各虚拟主机的 IP 地址，及各 IP 地址对应的连接数。其中，第一 IP 地址为其中任一连接在服
15 务器上的虚拟主机的 IP 地址，“第一”仅为了表述方便，并非特指某一 IP 地址。第一 IP 地址对应的连接数是指所有源 IP 地址连接该第一 IP 地址的连接次数。

该装置可以定时获取该第一 IP 地址及其连接数，也可以实时监测获取该第一 IP 地址及其连接数。

20 步骤 102，判断第一 IP 地址对应的连接数是否大于或等于第一阈值。

该装置在获得第一 IP 地址及其对应的连接数后，判断该连接数是否大于或等于预先设定的第一阈值。该第一阈值可以根据服务器的规模、虚拟主机的应用场景，及连接数经验值等设置，此处不做限定。

若该第一 IP 地址对应的连接数大于或等于第一阈值，则说明该第一 IP
25 地址受到网络攻击，进而执行步骤 103；若小于该第一阈值，则说明该第一 IP 地址未受到网络攻击，处于安全状态。

步骤 103，屏蔽连接至第一 IP 地址的源 IP 地址。

当第一 IP 地址对应的连接数大于或等于第一阈值时，在本实施例中不

是直接对该第一 IP 地址进行屏蔽，而是对连接至该第一 IP 地址的部分或全部源 IP 地址进行屏蔽。具体的，该装置可以根据连接至该第一 IP 地址的源 IP 地址的连接数来确定需要屏蔽的源 IP 地址。

5 该装置可以按照上述方法对所有连接在服务器上的虚拟主机的 IP 地址进行检测和处理。

本申请实施例通过检测连接服务器的 IP 地址的连接数，并在连接数超过一定阈值时，确认该 IP 地址受到网络攻击，然后对连接该受攻击的 IP 地址的全部或部分源 IP 地址进行屏蔽，不仅保证了服务器和网络的整体稳定性，而且，通过屏蔽源 IP 地址减小了对受攻击 IP 地址的业务影响，减小了对网站访问的影响。并且，该方法通过监测连接数来确认受攻击的 IP 地址，10 相对于现有技术中硬件防火墙、黑洞等的监测手段，可以更加准确的确定出网络攻击的对象，也更适应于虚拟主机本身的网络攻击防护。

参照图 2，示出了本申请的另一种网络攻击处理方法实施例的步骤流程图，具体可以包括如下步骤：

15 步骤 201，获取连接服务器的第一 IP 地址及第一 IP 地址对应的连接数。

步骤 202，判断第一 IP 地址对应的连接数是否大于或等于第一阈值。

步骤 201~202 与前述实施例中的步骤 101~102 类似，此处不再赘述。

在本实施例中，当第一 IP 地址对应的连接数小于第一阈值时，该网络攻击处理装置确认该第一 IP 地址未受到网络攻击。

20 当第一 IP 地址对应的连接数大于或等于第一阈值时，该网络攻击处理装置需要屏蔽连接至第一 IP 地址的源 IP 地址，该过程具体可以包括以下步骤：

步骤 203，获取连接至第一 IP 地址的各源 IP 地址及各源 IP 地址对应的连接数。

25 该装置进一步获取连接至该第一 IP 地址的各源 IP 地址及其对应的连接数，如源 IP 地址 1，连接数为 10；源 IP 地址 2，连接数为 100；源 IP 地址 3，连接数为 1000；... ..

步骤 204，判断各源 IP 地址中是否存在连接数大于或等于第二阈值的源

IP 地址。

该装置从上步骤获取的结果中，查看是否存在连接数大于或等于第二阈值的源 IP 地址，该第二阈值的设置方法与第一阈值类似。该第二阈值可以小于第一阈值。

- 5 若结果为不存在连接数大于或等于第二阈值的源 IP 地址，则该装置可以认为该第一 IP 地址遭到多个源 IP 地址的大规模攻击，无法判断来源。该情况下根据具体情况，可以直接屏蔽所有的源 IP 地址，也可以执行步骤 205。

- 若结果为存在连接数大于或等于第二阈值的源 IP 地址，则该装置可以直接屏蔽这些连接数大于或等于第二阈值的源 IP 地址，也可以首先记录下
10 这些连接数大于或等于第二阈值的源 IP 地址及其对应的连接数，如 IP N1 连接数 Y1；IP N2 连接数 Y2；IP N3 连接数 Y3，然后执行步骤 206。

 步骤 205，屏蔽第一 IP 地址。

- 在屏蔽第一 IP 地址后，可以进一步通知用户该第一 IP 地址被攻击，等待攻击结束。当检测到攻击结束后，或者满足预置条件时，可以自动停止对
15 第一 IP 地址的屏蔽。

 步骤 206，判断连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和是否大于或等于第一阈值。

 该装置计算连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和，例如 $Y1+Y2+Y3$ ，然后判断该和是否大于或等于第一阈值。

- 20 若连接数的和大于或等于第一阈值，则说明该第一 IP 地址受到的网络攻击为少数源 IP 地址发起的网络攻击，此时可以执行步骤 207。

 若连接数的和小于该第一阈值，则说明该第一 IP 地址遭到多个源 IP 地址的大规模攻击，无法判断来源。该情况下根据具体情况，可以直接屏蔽所有的源 IP 地址，也可以执行步骤 205。

- 25 步骤 207，屏蔽连接数大于或等于第二阈值的源 IP 地址。

 在屏蔽了源 IP 地址后，可以通知用户攻击防护成功，用户可以继续访问该第一 IP 地址。

 本实施例通过对网络连接数进行监控，根据连接数的情况确定网络攻击

的规模与来源，并根据不同的网络攻击情况，分别对发起攻击的源 IP 地址或被攻击的 IP 地址做屏蔽操作，如对于少量 IP 发起的大规模攻击，可以通过采取屏蔽这部分 IP 的方式予以防御；对于不能判断是由少量 IP 发起的攻击则对被攻击 IP 进行屏蔽，保护服务器和整体网络，从而达到保护服务器整体稳定和安全的目的。该方法对被攻击的 IP 地址不是单纯的从虚拟主机的防火墙端屏蔽，而是根据攻击来源定量的进行分析处理，该方法可以更加准确的确定出网络攻击的对象并进行对应的防护处理。

需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为依据本申请实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请实施例所必须的。

参照图 3，示出了本申请一种网络攻击处理装置实施例的结构框图，具体可以包括如下单元：

获取单元 301，被配置为获取连接服务器的第一 IP 地址及所述第一 IP 地址对应的连接数。

判断单元 302，被配置为判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值。

处理单元 303，被配置为当所述判断单元 302 判定所述第一 IP 地址对应的连接数大于或等于第一阈值时，屏蔽连接至所述第一 IP 地址的源 IP 地址。

该装置通过上述单元检测连接服务器的 IP 地址的连接数，并在连接数超过一定阈值时，确认该 IP 地址受到网络攻击，然后对连接该受攻击的 IP 地址的全部或部分源 IP 地址进行屏蔽，不仅保证了服务器和网络的整体稳定性，而且，通过屏蔽源 IP 地址减小了对受攻击 IP 地址的业务影响，减小了对网站访问的影响。并且，该装置通过监测连接数来确认受攻击的 IP 地址，相对于现有技术中硬件防火墙、黑洞等的监测手段，可以更加准确的确定出网络攻击的对象，也更适应于虚拟主机本身的网络攻击防护。

在另一实施例中，如图 4 所示，处理单元 303 可以进一步包括：

获取子单元 401, 被配置为获取连接至所述第一 IP 地址的各源 IP 地址及所述各源 IP 地址对应的连接数;

判断子单元 402, 被配置为判断所述各源 IP 地址中是否存在连接数大于或等于第二阈值的源 IP 地址;

5 屏蔽子单元 403, 被配置为当所述判断子单元 402 判定所述各源 IP 地址中存在连接数大于或等于第二阈值的源 IP 地址时, 屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

在另一实施例中, 该处理单元 303 还被配置为当所述各源 IP 地址中不存在连接数大于或等于所述第二阈值的源 IP 地址时, 屏蔽所述第一 IP 地址。

10 在另一实施例中, 如图 5 所示, 该屏蔽子单元 403 可以进一步包括:

下层判断子单元 501, 被配置为判断所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和是否大于或等于所述第一阈值;

15 下层屏蔽子单元 502, 被配置为当所述下层判断子单元 501 判定所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和大于或等于所述第一阈值时, 屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

该下层屏蔽子单元 502, 还可以被配置为当所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和小于所述第一阈值时, 屏蔽所述第一 IP 地址。

20 该装置通过对网络连接数进行监控, 根据连接数的情况确定网络攻击的规模与来源, 并根据不同的网络攻击情况, 分别对发起攻击的源 IP 地址或被攻击的 IP 地址做屏蔽操作, 如对于少量 IP 发起的大规模攻击, 可以通过采取屏蔽这部分 IP 的方式予以防御; 对于不能判断是由少量 IP 发起的攻击则对被攻击 IP 进行屏蔽, 保护服务器和整体网络, 从而达到保护服务器整体稳定和安全的目的。该装置对被攻击的 IP 地址不是单纯的从虚拟主机的
25 防火墙端屏蔽, 而是根据攻击来源定量的进行分析处理, 该装置可以更加准确的确定出网络攻击的对象并进行对应的防护处理。

本申请实施例还公开了一种服务器, 包括存储器和处理器。

处理器与存储器通过总线相互连接; 总线可以是 ISA 总线、PCI 总线或

EISA 总线等。所述总线可以分为地址总线、数据总线、控制总线等。

其中，存储器用于存储一段程序，具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可能包含高速 RAM 存储器，也可能还包括非易失性存储器 (non-volatile memory)，例如至少一个磁盘存储器。

5 处理器用于读取存储器中的程序代码，执行以下步骤：

获取连接服务器的第一 IP 地址及所述第一 IP 地址对应的连接数；

判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值；

若是，则屏蔽连接至所述第一 IP 地址的源 IP 地址。

对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较
10 简单，相关之处参见方法实施例的部分说明即可。

本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

15 本领域内的技术人员应明白，本申请实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。
20

在一个典型的配置中，所述计算机设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM) 和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的
25 示例。计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存

取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带, 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的
5 界定, 计算机可读介质不包括非持续性的电脑可读媒体(transitory media), 如调制的数据信号和载波。

本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令
10 实现流程图和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处理器以产生一个机器, 使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或
15 多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中, 使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品, 该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

20 这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上, 使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理, 从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

25 尽管已描述了本申请实施例的优选实施例, 但本领域内的技术人员一旦得知了基本创造性概念, 则可对这些实施例做出另外的变更和修改。所以, 所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得

5 包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

10

以上对本申请所提供的一种网络攻击处理方法和一种网络攻击处理装置，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本

15 申请的限制。

权利要求书

1、一种网络攻击处理方法，其特征在于，包括：

获取连接服务器的第一 IP 地址及所述第一 IP 地址对应的连接数；

判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值；

5 若是，则屏蔽连接至所述第一 IP 地址的源 IP 地址。

2、根据权利要求 1 所述的方法，其特征在于，所述屏蔽连接至所述第一 IP 地址的源 IP 地址，包括：

获取连接至所述第一 IP 地址的各源 IP 地址及所述各源 IP 地址对应的连接数；

10 判断所述各源 IP 地址中是否存在连接数大于或等于第二阈值的源 IP 地址；

若存在，则屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

3、根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

15 当所述各源 IP 地址中不存在连接数大于或等于所述第二阈值的源 IP 地址时，屏蔽所述第一 IP 地址。

4、根据权利要求 2 所述的方法，其特征在于，所述屏蔽所述连接数大于或等于第二阈值的源 IP 地址，包括：

判断所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和是否大于或等于所述第一阈值；

20 若是，则屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

5、根据权利要求 4 所述的方法，其特征在于，所述方法还包括：

当所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和小于所述第一阈值时，屏蔽所述第一 IP 地址。

6、根据权利要求 3 或 5 所述的方法，其特征在于，所述方法还包括：

25 当满足预置条件时，停止对所述第一 IP 地址的屏蔽。

7、一种网络攻击处理装置，其特征在于，包括：

获取单元，被配置为获取连接服务器的第一 IP 地址及所述第一 IP 地址

对应的连接数;

判断单元,被配置为判断所述第一 IP 地址对应的连接数是否大于或等于第一阈值;

5 处理单元,被配置为当所述判断单元判定所述第一 IP 地址对应的连接数大于或等于第一阈值时,屏蔽连接至所述第一 IP 地址的源 IP 地址。

8、根据权利要求 7 所述的装置,其特征在于,所述处理单元包括:

获取子单元,被配置为获取连接至所述第一 IP 地址的各源 IP 地址及所述各源 IP 地址对应的连接数;

10 判断子单元,被配置为判断所述各源 IP 地址中是否存在连接数大于或等于第二阈值的源 IP 地址;

屏蔽子单元,被配置为当所述判断子单元判定所述各源 IP 地址中存在连接数大于或等于第二阈值的源 IP 地址时,屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

9、根据权利要求 8 所述的装置,其特征在于,

15 所述处理单元还被配置为当所述各源 IP 地址中不存在连接数大于或等于所述第二阈值的源 IP 地址时,屏蔽所述第一 IP 地址。

10、根据权利要求 8 所述的装置,其特征在于,所述屏蔽子单元包括:

下层判断子单元,被配置为判断所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和是否大于或等于所述第一阈值;

20 下层屏蔽子单元,被配置为当所述下层判断子单元判定所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和大于或等于所述第一阈值时,屏蔽所述连接数大于或等于第二阈值的源 IP 地址。

11、根据权利要求 10 所述的装置,其特征在于,

25 所述下层屏蔽子单元,还被配置为当所述连接数大于或等于第二阈值的源 IP 地址所对应的连接数的和小于所述第一阈值时,屏蔽所述第一 IP 地址。

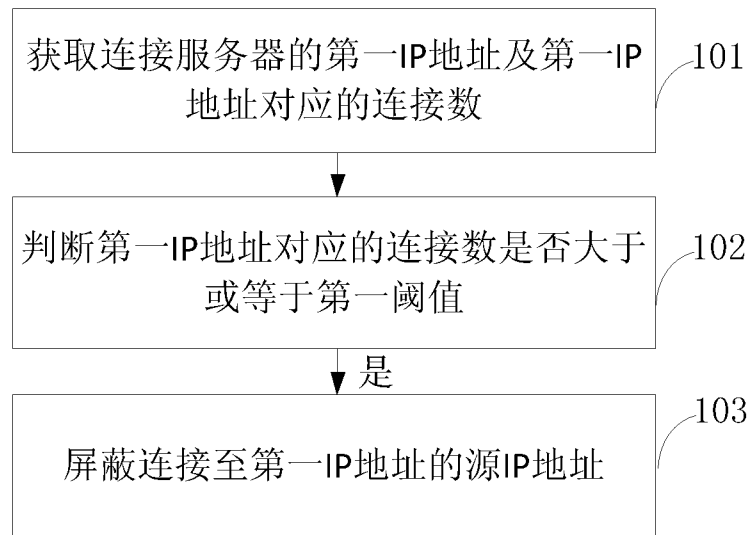


图 1

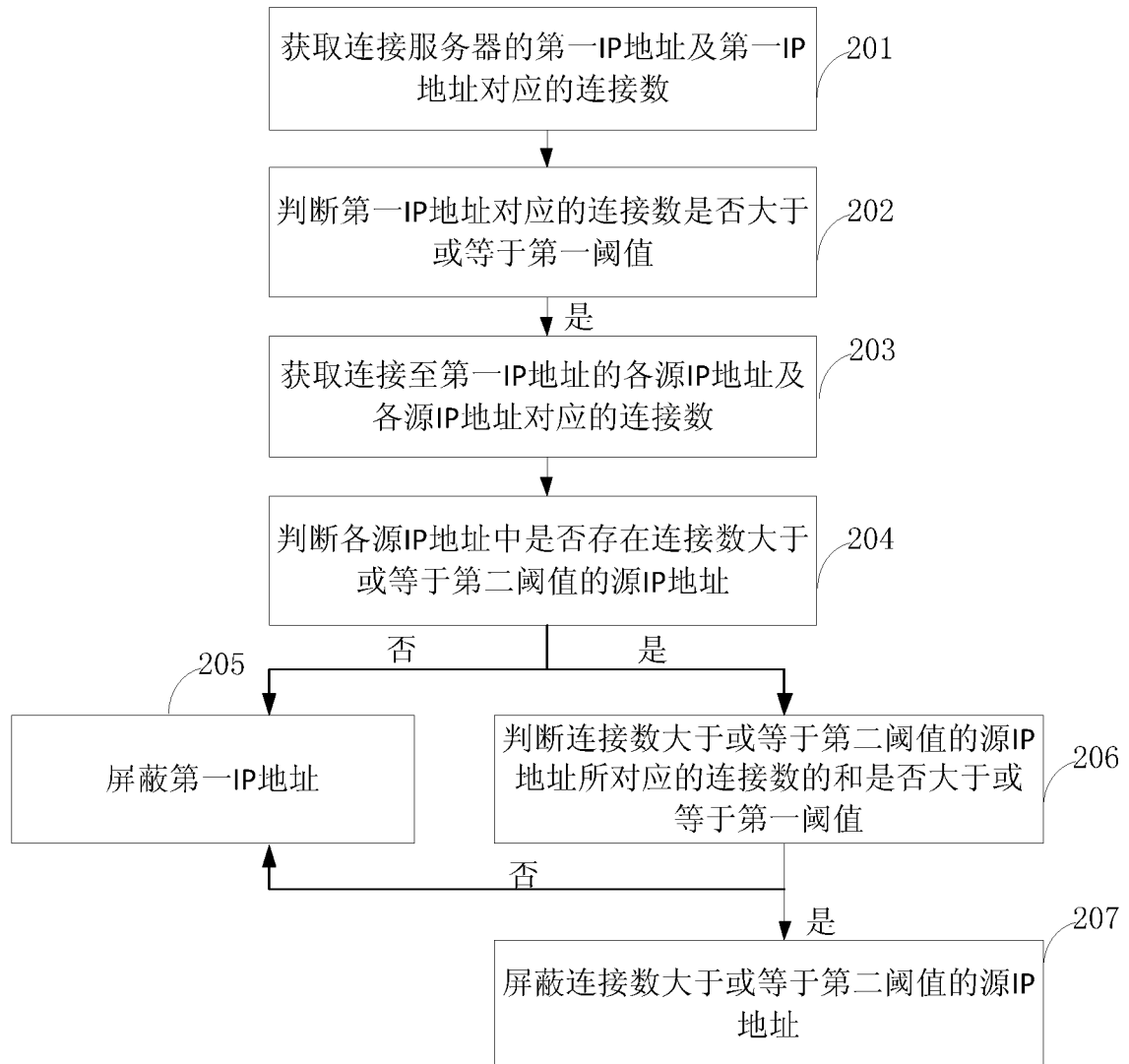


图 2

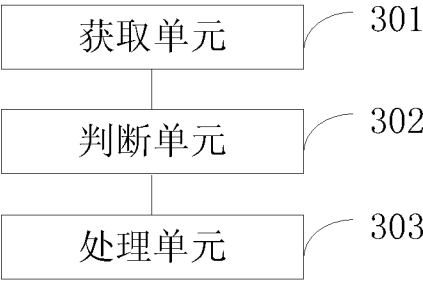


图 3

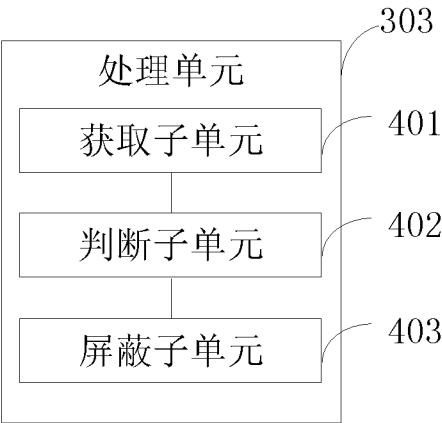


图 4

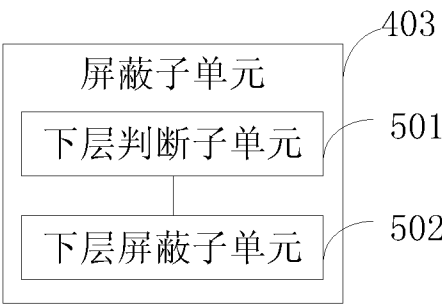


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/080311

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

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)

CNABS; CNTXT; CNKI; VEN; USTXT: intrusion detection system, connection, number, session, threshold, attack, DOS, IDS, source IP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102014116 A (JUNIPER NETWORKS INC.), 13 April 2011 (13.04.2011), claims 1-8, description, paragraphs [0030]-[0034] and figure 1	1-11
X	CN 103001972 A (SUZHOU HILLSTONE NETWORK CO., LTD.), 27 March 2013 (27.03.2013), description, paragraph [0003]	1-11
A	CN 104243223 A (TIANJIN SHUDU SCIENCE AND TECHNOLOGY CO., LTD.), 24 December 2014 (24.12.2014), the whole document	1-11
A	CN 103701795 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 02 April 2014 (02.04.2014), the whole document	1-11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 04 July 2016 (04.07.2016)	Date of mailing of the international search report 19 July 2016 (19.07.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer WANG, Rui Telephone No.: (86-10) 62089564

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/080311

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102014116 A	13 April 2011	US 2011055921 A1	03 March 2011
		EP 2293513 A1	09 March 2011
		CN 102014116 B	21 January 2015
		EP 2293513 B1	03 September 2014
		US 8789173 B2	22 July 2014
CN 103001972 A	27 March 2013	CN 103001972 B	25 November 2015
CN 104243223 A	24 December 2014	None	
CN 103701795 A	02 April 2014	None	

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 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)) CNABS; CNTXT; CNKI; VEN; USTXT; 连接, 数, 会话, 阈值, 攻击, DOS, 入侵检测系统, 源 IP, connection, number, session, threshold, attack, DOS, IDS, source IP		
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
X	CN 102014116 A (丛林网络公司) 2011年 4月 13日 (2011 - 04 - 13) 权利要求1-8, 说明书第[0030]-[0034]段及图1	1-11
X	CN 103001972 A (苏州山石网络有限公司) 2013年 3月 27日 (2013 - 03 - 27) 说明书第[0003]段	1-11
A	CN 104243223 A (天津蜀都科技有限公司) 2014年 12月 24日 (2014 - 12 - 24) 全文	1-11
A	CN 103701795 A (北京奇虎科技有限公司等) 2014年 4月 2日 (2014 - 04 - 02) 全文	1-11
☐ 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 2016年 7月 4日		国际检索报告邮寄日期 2016年 7月 19日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		授权官员 王瑞 电话号码 (86-10) 62089564

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/080311

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	102014116	A	2011年 4月 13日	US	2011055921	A1	2011年 3月 3日
				EP	2293513	A1	2011年 3月 9日
				CN	102014116	B	2015年 1月 21日
				EP	2293513	B1	2014年 9月 3日
				US	8789173	B2	2014年 7月 22日
CN	103001972	A	2013年 3月 27日	CN	103001972	B	2015年 11月 25日
CN	104243223	A	2014年 12月 24日	无			
CN	103701795	A	2014年 4月 2日	无			