



(12) 发明专利申请

(10) 申请公布号 CN 104917779 A

(43) 申请公布日 2015.09.16

(21) 申请号 201510364395.8

(22) 申请日 2015.06.26

(71) 申请人 北京奇虎科技有限公司

地址 100088 北京市西城区新街口外大街
28号D座112室(德胜园区)

(72) 发明人 李亮 姚熙

(74) 专利代理机构 北京鼎佳达知识产权代理事
务所(普通合伙) 11348

代理人 王伟锋 刘铁生

(51) Int. Cl.

H04L 29/06(2006.01)

H04L 29/08(2006.01)

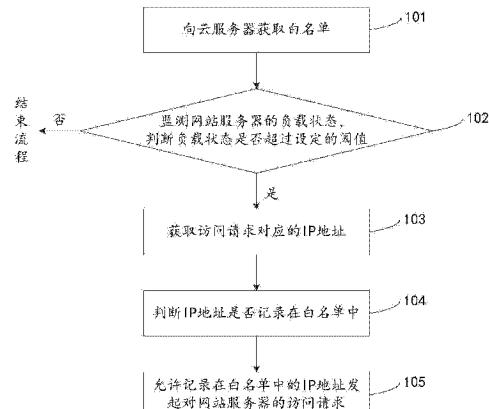
权利要求书2页 说明书9页 附图2页

(54) 发明名称

一种基于云的CC攻击的防护方法、装置及系
统

(57) 摘要

本发明公开了一种基于云的CC攻击的防护方法、装置及系统，涉及网络安全领域，解决了对CC攻击进行防护时占用处理资源的问题。本发明的方法包括：向云服务器获取白名单，白名单用于记录发起正常访问请求的网间协议IP地址；监测网站服务器的负载状态，判断负载状态是否超过设定的阈值；若当前的负载状态超过阈值，则获取访问请求对应的IP地址；判断IP地址是否记录在白名单中；允许记录在白名单中的IP地址发起对网站服务器的访问请求。本发明主要用于对CC攻击进行防护的过程中。



1. 一种基于云的 CC 攻击的防护方法, 其特征在于, 所述方法包括 :

向云服务器获取白名单, 所述白名单用于记录发起正常访问请求的网间协议 IP 地址 ;

监测网站服务器的负载状态, 判断所述负载状态是否超过设定的阈值 ;

若当前的负载状态超过所述阈值, 则获取访问请求对应的 IP 地址 ;

判断所述 IP 地址是否记录在所述白名单中 ;

允许记录在所述白名单中的 IP 地址发起对所述网站服务器的访问请求。

2. 根据权利要求 1 所述的方法, 其特征在于, 所述监测网站服务器的负载状态, 判断所述负载状态是否超过设定的阈值, 包括 :

监测当前的请求并发数 ;

判断所述请求并发数是否超过设定的访问请求上限。

3. 根据权利要求 1 所述的方法, 其特征在于, 所述监测网站服务器的负载状态, 判断所述负载状态是否超过设定的阈值, 包括 :

监测所述网站服务器的中央处理器 CPU 占用率 ;

判断所述网站服务器的 CPU 占用率是否超过设定的 CPU 占用上限。

4. 根据权利要求 1 所述的方法, 其特征在于, 若所述 IP 地址未记录在所述白名单中, 则所述方法还包括 :

将未记录在所述白名单中的 IP 地址记录在黑名单中 ;

禁止记录在所述黑名单中的 IP 地址发起对所述网站服务器的访问请求。

5. 根据权利要求 1 所述的方法, 其特征在于, 在所述允许记录在所述白名单中的 IP 地址发起对所述网站服务器的访问请求之后, 所述方法还包括 :

当监测到所述网站服务器的负载状态未超过设定的阈值时, 允许所有 IP 地址发起对所述网站服务器的访问请求。

6. 根据权利要求 1 至 5 中任一项所述的方法, 其特征在于, 所述方法还包括 : 通过所述云服务器更新白名单。

7. 一种基于云的 CC 攻击的防护装置, 其特征在于, 所述装置包括 :

获取单元, 用于向云服务器获取白名单, 所述白名单用于记录发起正常访问请求的网间协议 IP 地址 ;

判断单元, 用于监测网站服务器的负载状态, 判断所述负载状态是否超过设定的阈值 ;

所述获取单元还用于当所述判断单元判断当前的负载状态超过所述阈值时, 获取访问请求对应的 IP 地址 ;

所述判断单元还用于判断所述 IP 地址是否记录在所述白名单中 ;

访问单元, 用于允许记录在所述白名单中的 IP 地址发起对所述网站服务器的访问请求。

8. 根据权利要求 7 所述的装置, 其特征在于, 所述判断单元包括 :

监测模块, 用于监测当前的请求并发数 ;

判断模块, 用于判断所述请求并发数是否超过设定的访问请求上限。

9. 根据权利要求 7 所述的装置, 其特征在于, 所述判断单元包括 :

监测模块, 用于监测所述网站服务器的中央处理器 CPU 占用率 ;

判断模块，用于判断所述网站服务器的 CPU 占用率是否超过设定的 CPU 占用上限。

10. 一种基于云的 CC 攻击的防护系统，其特征在于，所述系统包括：

云服务器和网关；其中，所述云服务器用于对白名单进行更新；所述网关包含如权利要求 7 至权利要求 9 中任一项所述的装置。

一种基于云的 CC 攻击的防护方法、装置及系统

技术领域

[0001] 本发明涉及网络安全领域，特别是涉及一种基于云的 CC 攻击的防护方法、装置及系统。

背景技术

[0002] CC(Challenge Collapsar) 攻击是一种针对应用层 WEB 服务的攻击方法，它与分布式拒绝服务 (Distributed Denial of Service, 简称DDOS) 攻击在本质上是一样的，都是以耗尽服务器资源造成拒绝服务为目的。CC 攻击通常以网站中性能不佳的数据查询、不良的程序执行结构以及比较消耗资源的功能为攻击目标。例如，论坛的搜索功能，需要消耗大量的数据库查询时间和系统资源。攻击者通过频繁调用搜索功能，使查询请求积累不能立即完成，资源无法释放，导致数据库请求连接过多，数据库阻塞，网站无法正常打开。

[0003] 在通过现有的方法对 CC 攻击进行防护的过程中，发明人发现：目前对 CC 攻击的防护大多是通过监测 IP 的请求频率实现，当 IP 的请求频率达到设定阈值时，判定为攻击，则阻止该 IP 的访问请求。然而，对每一次 IP 请求都进行攻击判定的方式无疑会浪费网站服务器大量的处理资源，甚至会影响到用户的正常访问请求，给网站的运维造成极大的负担。

发明内容

[0004] 有鉴于此，本发明提出了一种基于云的 CC 攻击的防护方法、装置及系统，主要目的在于解决对 CC 攻击进行防护时占用处理资源的问题。

[0005] 依据本发明的第一个方面，本发明提供了一种基于云的 CC 攻击的防护方法，包括：

[0006] 向云服务器获取白名单，白名单用于记录发起正常访问请求的网间协议 IP 地址；

[0007] 监测网站服务器的负载状态，判断负载状态是否超过设定的阈值；

[0008] 若当前的负载状态超过阈值，则获取访问请求对应的 IP 地址；

[0009] 判断 IP 地址是否记录在白名单中；

[0010] 允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。

[0011] 依据本发明的第二个方面，本发明提供了一种基于云的 CC 攻击的防护装置，该装置通常位于网关中，包括：

[0012] 获取单元，用于向云服务器获取白名单，白名单用于记录发起正常访问请求的网间协议 IP 地址；

[0013] 判断单元，用于监测网站服务器的负载状态，判断负载状态是否超过设定的阈值；

[0014] 获取单元还用于当判断单元判断当前的负载状态超过所述阈值时，获取访问请求对应的 IP 地址；

[0015] 判断单元还用于判断 IP 地址是否记录在白名单中；

[0016] 访问单元，用于允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。

[0017] 依据本发明的第三个方面，本发明提供了一种基于云的 CC 攻击的防护系统，该系统包括：

[0018] 云服务器和网关；其中，云服务器用于对白名单进行更新；网关包含如前第二个方面所述的装置。

[0019] 借由上述技术方案，本发明实施例提供的基于云的 CC 攻击的防护方法、装置及系统，能够向云服务器获取记录有发起正常访问请求的 IP 地址的白名单，并在监测到网站服务器的负载状态超过设定的阈值时开始获取访问请求对应的 IP 地址，判断该 IP 地址是否记录在白名单中，允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。与现有技术中需要针对每一次访问请求统计其频率，判断该访问请求是否为攻击行为的方式相比，本发明只需要在网站服务器的负载状态超过阈值时，仅仅通过判断访问请求的 IP 地址是否记录在白名单中来确定是否对访问请求进行阻止，从而通过较小的处理资源对 CC 攻击进行有效防护。

[0020] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0021] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0022] 图 1 示出了本发明实施例提供的一种基于云的 CC 攻击的防护方法的流程图；

[0023] 图 2 示出了本发明实施例提供的一种基于云的 CC 攻击的防护装置的组成框图；

[0024] 图 3 示出了本发明实施例提供的一种基于云的 CC 攻击的防护装置的组成框图；

[0025] 图 4 示出了本发明实施例提供的一种基于云的 CC 攻击的防护装置的组成框图；

[0026] 图 5 示出了本发明实施例提供的一种基于云的 CC 攻击的防护系统的组成框图。

具体实施方式

[0027] 下面将参照附图更加详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0028] 由于目前对 CC 攻击的防护大多是通过监测 IP 地址的请求频率来实现，当某个 IP 地址的请求频率过高，对网站服务器造成阻塞时，则判定该 IP 地址在对网站进行攻击。然而，为了对 CC 攻击进行防护，采用现有的方式就需要针对每一次访问请求统计其频率，判断该访问请求是否为攻击行为，这种实施方式无疑会占用网站服务器大量的处理资源，并会对用户正常的访问网站造成严重影响，同时对网站的运维造成极大的负担。

[0029] 为了解决对 CC 攻击进行防护时占用处理资源的问题，本发明实施例提供了一种基于云的 CC 攻击的防护方法，该方法主要用于网关一侧。如图 1 所示，该方法包括：

[0030] 101、向云服务器获取白名单。

[0031] 随着诸如大中小企业等用户群体的庞大及其业务的复杂,其对互联网主机应用的需求日益增加,用户在采用传统的服务器时,由于成本、运营商选择等诸多因素,不得不面对各种棘手的问题,而云服务器具有集中化的远程管理平台、多级业务备份、快速的业务部署与配置、规模的弹性扩展能力等优点,能够有效解决传统服务器的缺陷,为用户提供了完善的互联网基础设施服务。

[0032] 由于云服务器具有强大的计算统计能力,本发明中的云服务器经统计可以得到记录有发起正常访问请求的 IP 地址的白名单,记录在白名单中的 IP 地址通常为历史访问记录正常的 IP 地址,不具有发起 CC 攻击的嫌疑。因此,在执行本发明实施例提供的基于云的 CC 攻击的防护方法中,可以先执行步骤 101 向云服务器获取白名单。

[0033] 102、监测网站服务器的负载状态,判断负载状态是否超过设定的阈值。

[0034] 在网站服务器的正常工作状态下,其负载状态处于一个合理的范围,随着用户发送访问请求的数量的增加或降低,网站服务器的负载状态也随之增高或降低,即访问请求的数量与网站服务器的负载状态成正相关关系。

[0035] 由于 CC 攻击是通过控制或模拟多个客户端向网站发送大量的访问请求,使网站查询请求积累不能立即完成,资源无法释放,导致数据库请求连接过多,数据库阻塞,网站无法正常打开。因此,在理论上只要网站服务器的处理资源足够应对数量庞大的访问请求即可,可以不必考虑发送的访问请求是否是恶意请求,只要网站服务器的负载状态处于正常水平,则可以允许任何一个访问请求对网站进行访问。但是在实际情况下网站服务器的处理资源有限,当网站服务器的负载状态达到一定程度后,就会造成网站阻塞甚至瘫痪。

[0036] 因此,本发明实施例需要执行步骤 102 监测网站服务器的负载状态,判断负载状态是否超过设定的阈值。该阈值是根据网站服务器的综合性能并结合各种网络环境及带宽的条件,计算得到的一个负载状态的临界值,当网站服务器的负载状态超过这个临界值后,网站的运行就会阻塞,不能正常打开网页,无法满足用户的正常使用。

[0037] 103、获取访问请求对应的 IP 地址。

[0038] 当在步骤 102 中判断出当前的负载状态超过阈值后,其原因很可能是网站被进行了 CC 攻击,但是也有可能是有过多的用户正在访问网站,使其负载状态超过阈值。此时,本发明实施例不关注究竟是何种原因造成的,无论是何种原因,其最终目的是避免网站瘫痪,确保网站的正常运行,满足大部分用户的使用需求。因此,本实施例不针对每一个访问请求进行攻击行为的判定,只需要在判断出网站服务器当前的负载状态超过阈值后执行步骤 103 获取访问请求对应的 IP 地址即可。

[0039] 104、判断 IP 地址是否记录在白名单中。

[0040] 由于在步骤 101 中向云服务器获取了白名单,该白名单中记录有发起正常访问请求的 IP 地址。基于云服务器强大的统计计算能力,白名单中通常记录有近期大量的历史访问请求正常的 IP 地址,这些 IP 地址发送的访问请求通常没有攻击嫌疑,可以被允许对网站进行正常访问。因此,在步骤 104 中需要对步骤 103 获取的 IP 地址进行判断,确定其是否记录在白名单中,不再具体针对每一个访问请求判定其是否为攻击行为。

[0041] 105、允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。

[0042] 当判断 IP 地址记录在白名单中之后,可以允许该 IP 地址发起对网站服务器的访问请求。而那些未被允许对网站服务器发送访问请求的 IP 地址由于不能继续发送访问请

求,从而使得发送给网站服务器的访问请求数量降低,低于阈值后就能使网站服务器的负载状态恢复到正常水平。

[0043] 本发明实施例提供的基于云的CC攻击的防护方法,能够向云服务器获取记录有发起正常访问请求的IP地址的白名单,并在监测到网站服务器的负载状态超过设定的阈值时开始获取访问请求对应的IP地址,判断该IP地址是否记录在白名单中,允许记录在白名单中的IP地址发起对网站服务器的访问请求。与现有技术中需要针对每一次访问请求统计其频率,判断该访问请求是否为攻击行为的方式相比,本发明只需要在网站服务器的负载状态超过阈值时,仅仅通过判断访问请求的IP地址是否记录在白名单中来确定是否对访问请求进行阻止,从而通过较小的处理资源对CC攻击进行有效防护。

[0044] 进一步的,为了更好的对上述图1所示的方法进行理解,作为对上述实施方式的细化和扩展,本发明实施例将针对图1中的步骤进行详细说明。

[0045] 在步骤102监测网站服务器的负载状态,判断负载状态是否超过设定的阈值中,可以通过不同的方式来判断网站服务器的负载状态。作为一种可选的实施方式,本实施例可以通过监测当前的请求并发数,判断请求并发数是否超过设定的访问请求上限来确定网站服务器的负载状态是否超过设定的阈值。其中,设定的访问请求上限就是设定的阈值,当发送的访问请求的并发数量超过访问请求上限的数量时,就说明网站服务器的负载状态过高,无法正常进行访问。

[0046] 同样的,作为另一种可选的实施方式,还可以通过监测网站服务器的CPU占用率,判断当前网站服务器的CPU占用率是否超过设定的CPU占用上限来确定网站服务器的负载状态是否超过设定的阈值。其中,设定的CPU占用上限就是设定的阈值,当网站服务器的CPU占用率超过CPU占用上限时,就说明网站服务器的负载状态过高,无法正常进行访问。

[0047] 这里需要说明的是,以上两种方式中的访问请求上限以及CPU占用上限都是根据网站服务器的综合性能并结合各种网络环境及带宽的条件,计算得到的一个负载状态的临界值,当网站服务器的负载状态超过这个临界值后,网站的运行就会阻塞,不能正常打开网页。同时,上述两种方式只是可选实施方式中的一种,当然也可以用其他参数来判断网站服务器的负载状态是否超过设定的阈值。

[0048] 进一步的,在步骤104判断IP地址是否记录在白名单中之后,若判断出IP地址未记录在白名单中,则可以将未记录在白名单中的IP地址记录在黑名单中,记录在黑名单中的IP地址将不能向网站服务器发送访问请求。通过这种实施方式,可以在后续发现网站服务器的负载状态超过设定的阈值时,不需要获取云服务器的白名单,直接禁止本地黑名单中的IP地址向网站服务器发送访问请求,即可降低向网站服务器发送访问请求的数量,确保网站服务器的负载状态恢复正常水平。

[0049] 由于在实际情况下,会存在一些未被记录在白名单中,但是正常发送访问请求的IP地址。对于这样的IP地址来说,如果由于未被记录在白名单中而导致被禁止向网站服务器发送访问请求,则会对这些IP地址的用户造成严重影响,使其无法访问网站服务器。

[0050] 因此,当网站服务器的负载状态恢复正常水平后,若监测到网站服务器的负载状态在正常水平下稳定运行了一段时间后,则可以允许所有IP地址发起对网站服务器的访问请求。这种实施方式可以避免那些虽然是用户的正常访问请求,但是由于IP地址未被记录在白名单中而导致无法对网站服务器进行访问的情况发生。

[0051] 进一步的,这里需要说明的是基于 CC 攻击防护机制的多样性,本发明实施例提供的基于云的 CC 攻击的防护方法既可以单独作为服务器的 CC 攻击防护机制,当然也可以与其他 CC 攻击防护机制相配合来防止服务器受到 CC 攻击。上述内容是对本实施例提供的基于云的 CC 攻击的防护方法单独作为服务器的 CC 攻击防护机制进行的说明,下面将针对本实施例提供的基于云的 CC 攻击的防护方法与其他 CC 攻击防护机制相配合作为防护场景,对 CC 攻击的防护进行说明。

[0052] 本实施例提供的基于云的 CC 攻击的防护方法可以作为一种备用防护机制,当监测到网站服务器运行异常缓慢的情况下,处于云防护的网站服务器在其他 CC 攻击防护机制生效后,若仍然存在超过负载状态阈值的大量访问请求,为了避免网站服务器资源耗尽而无法提供网络服务,则会启动备用防护机制,即本实施例提供的基于云的 CC 攻击的防护方法,优先允许白名单中记录的 IP 地址向网站服务器发送访问请求,如果后续网站服务器的负载状态恢复到正常水平,或者是 CPU、访问请求并发数、网络带宽等还有空余,则允许部分未记录在白名单中的 IP 地址向网站服务器发送访问请求。

[0053] 这种实施方式作为对其他 CC 攻击防护机制的一种补充机制,保证了在其他防护机制无法完全有效的情况下,网站服务器仍然能够正常工作,并且能够为部分正常访问请求提供服务,将损失最小化。

[0054] 进一步的,每当云服务器根据近期的历史运行状况对白名单进行更新后,还可以获取更新后的白名单,从而将那些未被记录在白名单中但是正常发送访问请求的 IP 地址记录在白名单中,同时将那些被发现进行了攻击行为但是还存在于白名单中的 IP 地址从白名单中删除,确保白名单中正常 IP 地址的准确性,从而使得当网站服务器的负载状态超过阈值后,最大程度的允许正常 IP 地址的用户访问网站服务器。

[0055] 本发明实施例通过本地生成黑名单的方式,直接禁止本地黑名单中的 IP 地址向网站服务器发送访问请求,即可降低向网站服务器发送访问请求的数量,确保网站服务器的负载状态恢复正常水平;当网站服务器的负载状态恢复正常水平后,允许所有 IP 地址发起对网站服务器的访问请求,避免那些虽然是用户的正常访问请求,但是由于 IP 地址未被记录在白名单中而导致无法对网站服务器进行访问的情况发生;同时对白名单进行更新,最大程度的允许正常 IP 地址的用户访问网站服务器。

[0056] 进一步的,作为对上述图 1 所示方法的实现,本发明实施例还提供了一种基于云的 CC 攻击的防护装置,该装置通常位于网关中。如图 2 所示,该装置包括:获取单元 21、判断单元 22 及访问单元 23,其中,

[0057] 获取单元 21,用于向云服务器获取白名单,白名单用于记录发起正常访问请求的网间协议 IP 地址;

[0058] 判断单元 22,用于监测网站服务器的负载状态,判断负载状态是否超过设定的阈值;

[0059] 获取单元 21 还用于当判断单元 22 判断当前的负载状态超过阈值时,获取访问请求对应的 IP 地址;

[0060] 判断单元 22 还用于判断 IP 地址是否记录在白名单中;

[0061] 访问单元 23,用于允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。

[0062] 进一步的,如图 3 所示,判断单元 22 包括:

- [0063] 监测模块 221,用于监测当前的请求并发数；
[0064] 判断模块 222,用于判断请求并发数是否超过设定的访问请求上限。
[0065] 进一步的,监测模块 221 用于监测网站服务器的 CPU 占用率；
[0066] 判断模块 222 用于判断网站服务器的 CPU 占用率是否超过设定的 CPU 占用上限。
[0067] 进一步的,如图 4 所示,该装置还包括：
[0068] 记录单元 24,用于将未记录在白名单中的 IP 地址记录在黑名单中；
[0069] 访问单元 23 还用于禁止记录在黑名单中的 IP 地址发起对网站服务器的访问请求。
[0070] 进一步的,访问单元 23 还用于当判断单元 22 监测到网站服务器的负载状态未超过设定的阈值时,允许所有 IP 地址发起对网站服务器的访问请求。
[0071] 进一步的,该装置还包括：
[0072] 更新单元 25,用于通过云服务器更新白名单。
[0073] 本发明实施例提供的基于云的 CC 攻击的防护装置,能够向云服务器获取记录有发起正常访问请求的 IP 地址的白名单,并在监测到网站服务器的负载状态超过设定的阈值时开始获取访问请求对应的 IP 地址,判断该 IP 地址是否记录在白名单中,允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。与现有技术中需要针对每一次访问请求统计其频率,判断该访问请求是否为攻击行为的方式相比,本发明只需要在网站服务器的负载状态超过阈值时,仅仅通过判断访问请求的 IP 地址是否记录在白名单中来确定是否对访问请求进行阻止,从而通过较小的处理资源对 CC 攻击进行有效防护。
[0074] 此外,本发明实施例通过本地生成黑名单的方式,直接禁止本地黑名单中的 IP 地址向网站服务器发送访问请求,即可降低向网站服务器发送访问请求的数量,确保网站服务器的负载状态恢复正常水平;当网站服务器的负载状态恢复正常水平后,允许所有 IP 地址发起对网站服务器的访问请求,避免那些虽然是用户的正常访问请求,但是由于 IP 地址未被记录在白名单中而导致无法对网站服务器进行访问的情况发生;同时对白名单进行更新,最大程度的允许正常 IP 地址的用户访问网站服务器。
[0075] 进一步的,作为对上述方法的实现以及上述装置的应用,本发明实施例还提供了一种基于云的 CC 攻击的防护系统,如图 5 所示,该系统包括：云服务器 51 和网关 52;其中,云服务器 51 用于对白名单进行更新;网关 52 包含如图 2 和 / 或图 3 和 / 或图 4 所示的装置。
[0076] 本发明实施例提供的基于云的 CC 攻击的防护系统,能够向云服务器获取记录有发起正常访问请求的 IP 地址的白名单,并在监测到网站服务器的负载状态超过设定的阈值时开始获取访问请求对应的 IP 地址,判断该 IP 地址是否记录在白名单中,允许记录在白名单中的 IP 地址发起对网站服务器的访问请求。与现有技术中需要针对每一次访问请求统计其频率,判断该访问请求是否为攻击行为的方式相比,本发明只需要在网站服务器的负载状态超过阈值时,仅仅通过判断访问请求的 IP 地址是否记录在白名单中来确定是否对访问请求进行阻止,从而通过较小的处理资源对 CC 攻击进行有效防护。
[0077] 此外,本发明实施例通过本地生成黑名单的方式,直接禁止本地黑名单中的 IP 地址向网站服务器发送访问请求,即可降低向网站服务器发送访问请求的数量,确保网站服务器的负载状态恢复正常水平;当网站服务器的负载状态恢复正常水平后,允许所有 IP 地

址发起对网站服务器的访问请求,避免那些虽然是用户的正常访问请求,但是由于 IP 地址未被记录在白名单中而导致无法对网站服务器进行访问的情况发生;同时对白名单进行更新,最大程度的允许正常 IP 地址的用户访问网站服务器。

[0078] 本发明的实施例公开了:

[0079] A1、一种基于云的 CC 攻击的防护方法,其特征在于,所述方法包括:

[0080] 向云服务器获取白名单,所述白名单用于记录发起正常访问请求的网间协议 IP 地址;

[0081] 监测网站服务器的负载状态,判断所述负载状态是否超过设定的阈值;

[0082] 若当前的负载状态超过所述阈值,则获取访问请求对应的 IP 地址;

[0083] 判断所述 IP 地址是否记录在所述白名单中;

[0084] 允许记录在所述白名单中的 IP 地址发起对所述网站服务器的访问请求。

[0085] A2、根据权利要求 A1 所述的方法,其特征在于,所述监测网站服务器的负载状态,判断所述负载状态是否超过设定的阈值,包括:

[0086] 监测当前的请求并发数;

[0087] 判断所述请求并发数是否超过设定的访问请求上限。

[0088] A3、根据权利要求 A1 所述的方法,其特征在于,所述监测网站服务器的负载状态,判断所述负载状态是否超过设定的阈值,包括:

[0089] 监测所述网站服务器的中央处理器 CPU 占用率;

[0090] 判断所述网站服务器的 CPU 占用率是否超过设定的 CPU 占用上限。

[0091] A4、根据权利要求 A1 所述的方法,其特征在于,若所述 IP 地址未记录在所述白名单中,则所述方法还包括:

[0092] 将未记录在所述白名单中的 IP 地址记录在黑名单中;

[0093] 禁止记录在所述黑名单中的 IP 地址发起对所述网站服务器的访问请求。

[0094] A5、根据权利要求 A1 所述的方法,其特征在于,在所述允许记录在所述白名单中的 IP 地址发起对所述网站服务器的访问请求之后,所述方法还包括:

[0095] 当监测到所述网站服务器的负载状态未超过设定的阈值时,允许所有 IP 地址发起对所述网站服务器的访问请求。

[0096] A6、根据权利要求 A1 至 A5 中任一项所述的方法,其特征在于,所述方法还包括:通过所述云服务器更新白名单。

[0097] B7、一种基于云的 CC 攻击的防护装置,其特征在于,所述装置包括:

[0098] 获取单元,用于向云服务器获取白名单,所述白名单用于记录发起正常访问请求的网间协议 IP 地址;

[0099] 判断单元,用于监测网站服务器的负载状态,判断所述负载状态是否超过设定的阈值;

[0100] 所述获取单元还用于当所述判断单元判断当前的负载状态超过所述阈值时,获取访问请求对应的 IP 地址;

[0101] 所述判断单元还用于判断所述 IP 地址是否记录在所述白名单中;

[0102] 访问单元,用于允许记录在所述白名单中的 IP 地址发起对所述网站服务器的访问请求。

- [0103] B8、根据权利要求 B7 所述的装置，其特征在于，所述判断单元包括：
- [0104] 监测模块，用于监测当前的请求并发数；
- [0105] 判断模块，用于判断所述请求并发数是否超过设定的访问请求上限。
- [0106] B9、根据权利要求 B7 所述的装置，其特征在于，所述判断单元包括：
- [0107] 监测模块，用于监测所述网站服务器的中央处理器 CPU 占用率；
- [0108] 判断模块，用于判断所述网站服务器的 CPU 占用率是否超过设定的 CPU 占用上限。
- [0109] B10、根据权利要求 B7 所述的装置，其特征在于，所述装置还包括：
- [0110] 记录单元，用于将未记录在所述白名单中的 IP 地址记录在黑名单中；
- [0111] 所述访问单元还用于禁止记录在所述黑名单中的 IP 地址发起对所述网站服务器的访问请求。
- [0112] B11、根据权利要求 B7 所述的装置，其特征在于，所述访问单元还用于当所述判断单元监测到所述网站服务器的负载状态未超过设定的阈值时，允许所有 IP 地址发起对所述网站服务器的访问请求。
- [0113] B12、根据权利要求 B7 至 B11 所述的装置，其特征在于，所述装置还包括：
- [0114] 更新单元，用于通过所述云服务器更新白名单。
- [0115] C13、一种基于云的 CC 攻击的防护系统，其特征在于，所述系统包括：
- [0116] 云服务器和网关；其中，所述云服务器用于对白名单进行更新；所述网关包含如权利要求 B7 至权利要求 B12 中任一项所述的装置。
- [0117] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。
- [0118] 可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施例的优劣。
- [0119] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。
- [0120] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。
- [0121] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。
- [0122] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0123] 本领域那些技术人员可以理解,可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件,以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和 / 或过程或者单元中的至少一些是相互排斥之外,可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述,本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0124] 此外,本领域的技术人员能够理解,尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征,但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如,在下面的权利要求书中,所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0125] 本发明的各个部件实施例可以以硬件实现,或者以在一个或者多个处理器上运行的软件模块实现,或者以它们的组合实现。本领域的技术人员应当理解,可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的发明名称(如确定网站内链接等级的装置)中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如,计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上,或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到,或者在载体信号上提供,或者以任何其他形式提供。

[0126] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制,并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中,不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中,这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

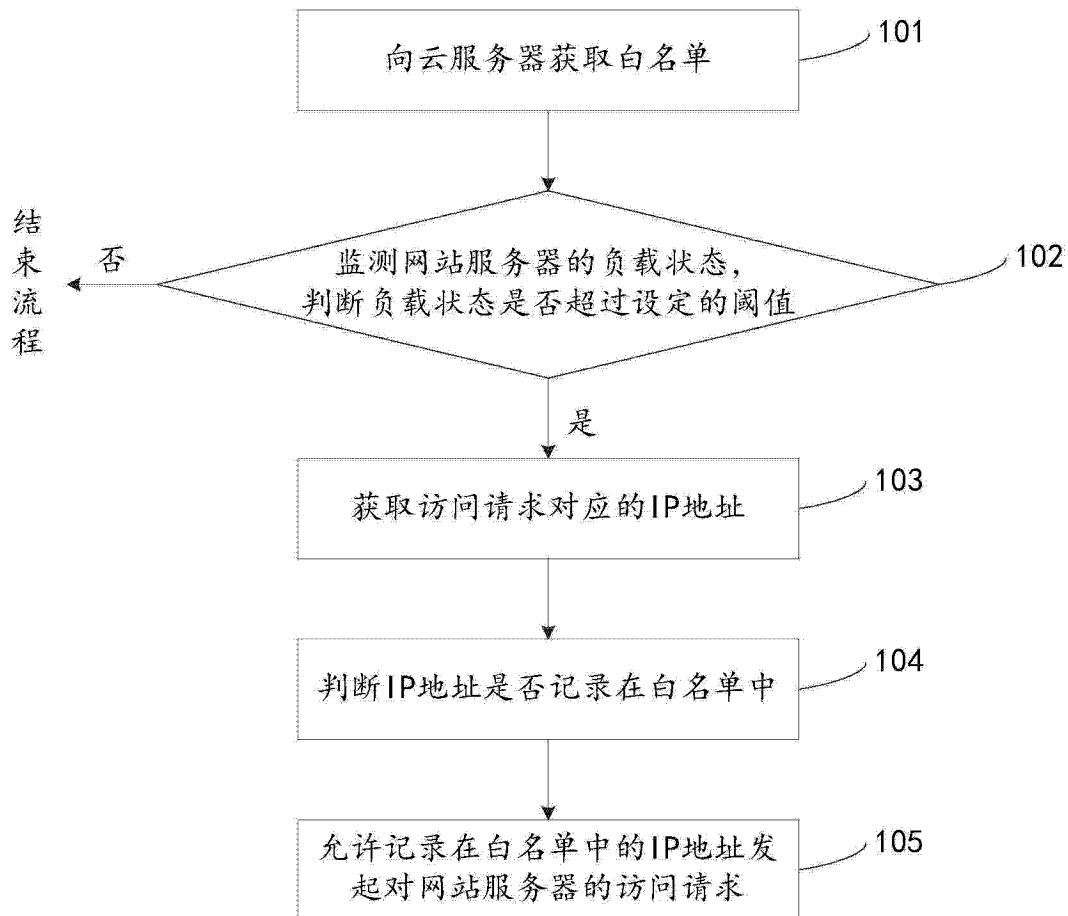


图 1

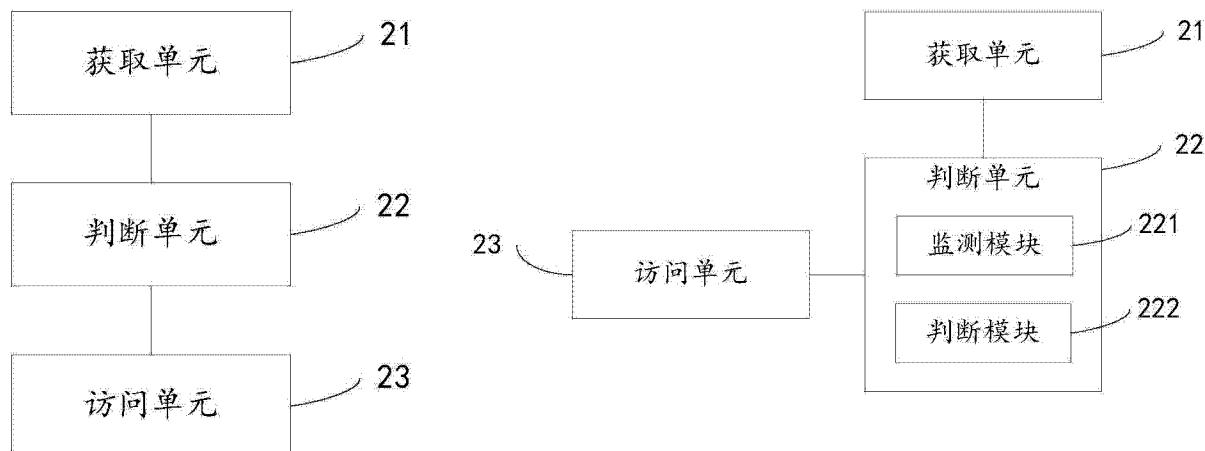


图 3

图 2

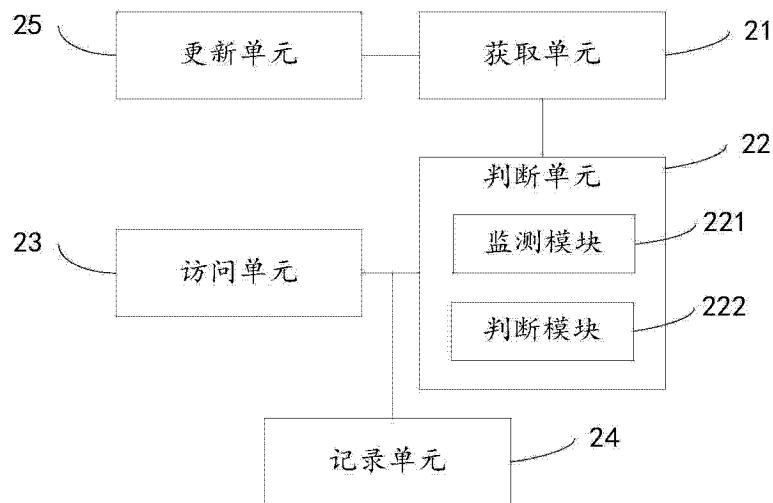


图 4

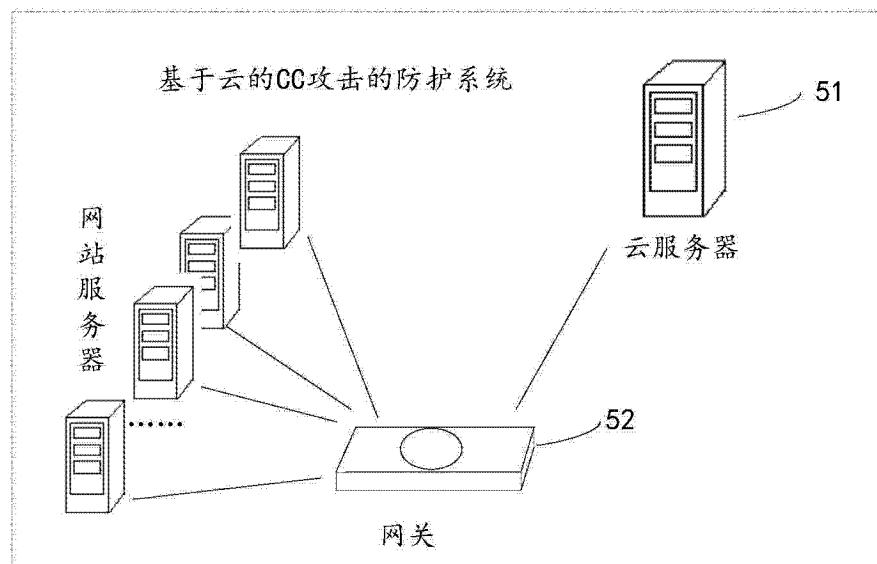


图 5