(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105338017 A
(43)申请公布日 2016.02.17

(21)申请号 201410306976.1

(22)申请日 2014.06.30

(71)申请人 北京新媒传信科技有限公司
地址 100089 北京市海淀区万泉庄路28号万柳新贵大厦A座6层602室

(72)发明人 任宙 石海涛

(74)专利代理机构 北京市隆安律师事务所 11323
代理人 权鲜枝

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)

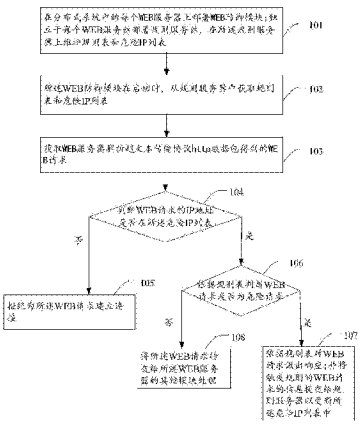
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种WEB防御方法和系统

(57)摘要

本发明公开了一种WEB防御方法和系统，该方法包括：在分布式系统中的每个WEB服务器上部署WEB防御模块；独立于每个WEB服务器部署规则服务器，在所述规则服务器上维护规则表和危险IP列表；所述WEB防御模块在启动时从规则服务器中获取规则表和危险IP列表；对WEB服务器解析http协议数据包得到的WEB请求，判断该WEB请求的IP是否在危险IP列表中；如果在，拒绝为WEB请求建立连接；如果不在，则继续依据规则表判断WEB请求是否为危险请求；如果是，依据规则表对WEB请求做出响应，并将触发规则的WEB请求的信息提交给规则服务器以更新IP列表中。本发明能够及时处理大流量的WEB请求。



CN 105338017 A

1. 一种 WEB 防御方法，其特征在于，在分布式系统中的每个 WEB 服务器上部署 WEB 防御模块；独立于每个 WEB 服务器部署规则服务器，在所述规则服务器上维护规则表和危险 IP 列表；其中，所述规则表配置有检测 WEB 请求是否为危险请求的规则，以及对触发规则的 WEB 请求做出的响应；所述危险 IP 列表包括一定数量的触发规则次数达到预设阀值的 WEB 请求的 IP；该方法包括：

所述 WEB 防御模块在启动时，从所述规则服务器中获取所述规则表和所述危险 IP 列表；

获取 WEB 服务器解析超文本传输协议 http 数据包得到的 WEB 请求；

判断所述 WEB 请求的 IP 是否在所述危险 IP 列表中；

如果在，拒绝为所述 WEB 请求建立连接；

如果不在，则继续依据所述规则表判断所述 WEB 请求是否为危险请求；

如果是，依据所述规则表对所述 WEB 请求做出响应，并将触发规则的所述 WEB 请求的信息提交给所述规则服务器以更新所述危险 IP 列表中；

如果不是，将所述 WEB 请求转交给所述 WEB 服务器的其他模块处理。

2. 根据权利要求 1 所述的方法，其特征在于，该方法还包括：

所述 WEB 防御模块周期性地从所述规则服务器中获取所述规则表和所述危险 IP 列表；以及，

当所述规则表或所述危险 IP 列表有更新时，接收所述规则服务器下发的更新后的规则表或危险 IP 列表。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，独立于所述规则服务器部署监控服务器，所述监控服务器用于向所述规则服务器下发新的规则以更新所述规则表；该方法还包括：

所述 WEB 防御模块接收所述监控服务器的 WEB 查询请求，并根据所述 WEB 查询请求将自身的运行状态上报给所述监控服务器。

4. 一种 WEB 防御方法，其特征在于，在分布式系统中的每个 WEB 服务器上部署 WEB 防御模块；独立于每个 WEB 服务器部署规则服务器，在所述规则服务器上维护规则表和危险 IP 列表；该方法包括：

所述规则服务器接收检测 WEB 请求是否为危险请求的规则，以及对触发规则的 WEB 请求做出的响应的配置信息；

根据所述规则和响应的配置信息建立或更新所述规则表；

接收所述 WEB 防御模块提交的触发所述规则表中规则的 WEB 请求的信息；

依据触发规则的所述 WEB 请求的信息做哈希表，哈希表的键包括所述 WEB 请求的 IP，对应的值为该 IP 的触发次数，其中，每触发规则一次，则触发次数加一；

从所述哈希表中获取一定数量的触发次数达到预设阀值的 WEB 请求的 IP 建立或更新所述危险 IP 列表；

在所述 WEB 防御模块启动时，发送所述规则表和所述危险 IP 列表到所述 WEB 防御模块，使得所述 WEB 防御模块根据所述规则表和所述危险 IP 列表对 WEB 请求进行防御。

5. 根据权利要求 4 所述的方法，其特征在于，该方法还包括：

当所述规则表或所述危险 IP 列表有更新时，下发更新后的规则表或危险 IP 列表到所

述 WEB 防御模块；以及，

根据所述 WEB 防御模块周期性发送的获取请求，将所述规则表和所述危险 IP 列表发送到所述 WEB 防御模块。

6. 根据权利要求 4 或 5 所述的方法，其特征在于，独立于所述规则服务器部署监控服务器，所述监控服务器用于向所述规则服务器下发新的规则以更新所述规则表；该方法还包括：

所述规则服务器接收所述监控服务器的 WEB 查询请求，并根据所述 WEB 查询请求将所述规则表和所述危险 IP 列表上报给所述监控服务器。

7. 一种 WEB 防御系统，其特征在于，该系统包括：至少一个 WEB 防御模块、一个规则服务器，其中，所述 WEB 防御模块部署在分布式系统中的每个 WEB 服务器上；所述规则服务器独立于每个 WEB 服务器部署，在所述规则服务器上维护规则表和危险 IP 列表；

所述 WEB 防御模块，用于在启动时从所述规则服务器中获取所述规则表和所述危险 IP 列表；对 WEB 服务器解析 http 数据包得到的 WEB 请求，判断所述 WEB 请求的 IP 是否在所述危险 IP 列表中；如果在，拒绝为所述 WEB 请求建立连接；如果不在，则继续依据所述规则表判断所述 WEB 请求是否为危险请求；如果是，依据所述规则表对所述 WEB 请求做出响应，并将触发规则的所述 WEB 请求的信息提交给所述规则服务器以更新所述危险 IP 列表；如果不是，将所述 WEB 请求转交给所述 WEB 服务器的其他模块处理；

所述规则服务器，用于接收检测 WEB 请求是否为危险请求的规则，以及对触发规则的 WEB 请求做出的响应的配置信息，根据所述规则和响应的配置信息建立或更新所述规则表；根据 WEB 防御模块提交的触发规则的 WEB 请求的信息做哈希表，哈希表的键包括所述 WEB 请求的 IP，对应的值为该 IP 的触发次数，其中，每触发规则一次，则触发次数加一；从所述哈希表中获取一定数量的触发次数达到预设阀值的 WEB 请求的 IP 建立或更新所述危险 IP 列表。

8. 根据权利要求 7 所述的系统，其特征在于，

所述 WEB 防御模块，还用于周期性地从所述规则服务器中获取所述规则表和所述危险 IP 列表；和 / 或，

当所述规则表或所述危险 IP 列表有更新时，接收所述规则服务器下发的更新后的规则表或危险 IP 列表。

9. 根据权利要求 7 所述的系统，其特征在于，

所述规则服务器，还用于当所述规则表或所述危险 IP 列表有更新时，下发更新后的规则表或危险 IP 列表到所述 WEB 防御模块；和 / 或，

根据所述 WEB 防御模块周期性发送的获取请求，将所述规则表和所述危险 IP 列表发送到所述 WEB 防御模块。

10. 根据权利要求 7-9 任一项所述的系统，其特征在于，该系统还包括：

监控服务器，独立于所述规则服务器部署，用于向所述规则服务器下发新的规则以更新所述规则表；以及，向所述 WEB 防御模块发送 WEB 查询请求查询所述 WEB 防御模块的运行状态，向所述规则服务器发送 WEB 查询请求查询所述规则表和所述危险 IP 列表。

一种 WEB 防御方法和系统

技术领域

[0001] 本发明涉及互联网安全技术领域，特别是涉及一种 WEB 防御方法和系统。

背景技术

[0002] 随着互联网业务及 WEB 应用的迅猛发展，WEB 技术的更新换代，WEB 应用的攻击面在不断的扩大，各种漏洞层出不穷，WEB 应用的安全面临新的挑战。

[0003] 现有的 WEB 攻击大致可以分为两类：一种是利用 WEB 服务器的漏洞进行攻击，另一种是利用网页自身的安全漏洞进行攻击。在现有的防御 WEB 攻击方式中，网站应用级入侵防御系统 (WAF，Web Application Firewall)，会对 HTTP 的请求进行异常检测，拒绝不符合 HTTP 标准的请求。然而由于其网络架构的特点，主要用在小流量的 WEB 应用。在面对大流量的应用时，WAF 的网络架构存在网络实体负载过大，性能难以胜任的缺陷。

发明内容

[0004] 本发明提供了一种 WEB 防御方法和系统，以解决现有的 WEB 防御方式在处理大流量的 WEB 请求时不能及时处理的问题。

[0005] 本发明公开了一种 WEB 防御方法，在分布式系统中的每个 WEB 服务器上部署 WEB 防御模块；独立于每个 WEB 服务器部署规则服务器，在所述规则服务器上维护规则表和危险 IP 列表；其中，所述规则表配置有检测 WEB 请求是否为危险请求的规则，以及对触发规则的 WEB 请求做出的响应；所述危险 IP 列表包括一定数量的触发规则次数达到预设阀值的 WEB 请求的 IP；该方法包括：

[0006] 所述 WEB 防御模块在启动时，从所述规则服务器中获取所述规则表和所述危险 IP 列表；

[0007] 获取 WEB 服务器解析超文本传输协议 http 数据包得到的 WEB 请求；

[0008] 判断所述 WEB 请求的 IP 是否在所述危险 IP 列表中；

[0009] 如果在，拒绝为所述 WEB 请求建立连接；

[0010] 如果不在，则继续依据所述规则表判断所述 WEB 请求是否为危险请求；

[0011] 如果是，依据所述规则表对所述 WEB 请求做出响应，并将触发规则的所述 WEB 请求的信息提交给所述规则服务器以更新所述危险 IP 列表中；

[0012] 如果不是，将所述 WEB 请求转交给所述 WEB 服务器的其他模块处理。

[0013] 可选的，所述 WEB 防御模块周期性地从所述规则服务器中获取所述规则表和所述危险 IP 列表；以及，

[0014] 当所述规则表或所述危险 IP 列表有更新时，接收所述规则服务器下发的更新后的规则表或危险 IP 列表。

[0015] 可选的，独立于所述规则服务器部署监控服务器，所述监控服务器用于向所述规则服务器下发新的规则以更新所述规则表；该方法还包括：所述 WEB 防御模块接收所述监控服务器的 WEB 查询请求，并根据所述 WEB 查询请求将自身的运行状态上报给所述监控服

务器。

[0016] 依据本发明的另一方面，提供了一种WEB防御方法，在分布式系统中的每个WEB服务器上部署WEB防御模块；独立于每个WEB服务器部署规则服务器，在所述规则服务器上维护规则表和危险IP列表；该方法包括：

[0017] 所述规则服务器接收检测WEB请求是否为危险请求的规则，以及对触发规则的WEB请求做出的响应的配置信息；

[0018] 根据所述规则和响应的配置信息建立或更新所述规则表；

[0019] 接收所述WEB防御模块提交的触发所述规则表中规则的WEB请求的信息；

[0020] 依据触发规则的所述WEB请求的信息做哈希表，哈希表的键包括所述WEB请求的IP，对应的值为该IP的触发次数，其中，每触发规则一次，则触发次数加一；

[0021] 从所述哈希表中获取一定数量的触发次数达到预设阀值的WEB请求的IP建立或更新所述危险IP列表；

[0022] 在所述WEB防御模块启动时，发送所述规则表和所述危险IP列表到所述WEB防御模块，使得所述WEB防御模块根据所述规则表和所述危险IP列表对WEB请求进行防御。

[0023] 可选的，当所述规则表或所述危险IP列表有更新时，下发更新后的规则表或危险IP列表到所述WEB防御模块；以及，根据所述WEB防御模块周期性发送的获取请求，将所述规则表和所述危险IP列表发送到所述WEB防御模块。

[0024] 可选的，独立于所述规则服务器部署监控服务器，所述监控服务器用于向所述规则服务器下发新的规则以更新所述规则表；该方法还包括：所述规则服务器接收所述监控服务器的WEB查询请求，并根据所述WEB查询请求将所述规则表和所述危险IP列表上报给所述监控服务器。

[0025] 依据本发明的另一方面，提供了一种WEB防御御系统，该系统包括：至少一个WEB防御模块、一个规则服务器，其中，所述WEB防御模块部署在分布式系统中的每个WEB服务器上；所述规则服务器独立于每个WEB服务器部署，在所述规则服务器上维护规则表和危险IP列表；

[0026] 所述WEB防御模块，用于在启动时从所述规则服务器中获取所述规则表和所述危险IP列表；对WEB服务器解析http数据包得到的WEB请求，判断所述WEB请求的IP是否在所述危险IP列表中；如果在，拒绝为所述WEB请求建立连接；如果不在，则继续依据所述规则表判断所述WEB请求是否为危险请求；如果是，依据所述规则表对所述WEB请求做出响应，并将触发规则的所述WEB请求的信息提交给所述规则服务器以更新所述危险IP列表；如果不是，将所述WEB请求转交给所述WEB服务器的其他模块处理；

[0027] 所述规则服务器，用于接收检测WEB请求是否为危险请求的规则，以及对触发规则的WEB请求做出的响应的配置信息，根据所述规则和响应的配置信息建立或更新所述规则表；根据WEB防御模块提交的触发规则的WEB请求的信息做哈希表，哈希表的键包括所述WEB请求的IP，对应的值为该IP的触发次数，其中，每触发规则一次，则触发次数加一；从所述哈希表中获取一定数量的触发次数达到预设阀值的WEB请求的IP建立或更新所述危险IP列表。

[0028] 可选的，所述WEB防御模块，还用于周期性地从所述规则服务器中获取所述规则表和所述危险IP列表；和/或，当所述规则表或所述危险IP列表有更新时，接收所述规则

服务器下发的更新后的规则表或危险 IP 列表。

[0029] 可选的，所述规则服务器，还用于当所述规则表或所述危险 IP 列表有更新时，下发更新后的规则表或危险 IP 列表到所述 WEB 防御模块；和 / 或，根据所述 WEB 防御模块周期性发送的获取请求，将所述规则表和所述危险 IP 列表发送到所述 WEB 防御模块。

[0030] 可选的，该系统还包括：监控服务器，独立于所述规则服务器部署，用于向所述规则服务器下发新的规则以更新所述规则表；以及，向所述 WEB 防御模块发送 WEB 查询请求查询所述 WEB 防御模块的运行状态，向所述规则服务器发送 WEB 查询请求查询所述规则表和所述危险 IP 列表。

[0031] 综上所述，本发明的技术方案，由于 WEB 防御模块单独部署在 WEB 服务器上，任何一个宕机不会影响到其他的服务器和业务，稳定易用并且便于扩充，克服了传统单一节点部署的性能瓶颈和单点故障。此外，由于 WEB 防御模块是对 WEB 服务器解析 http 数据包得到的 WEB 请求进行处理，能够充分利用 WEB 服务器的资源，解析效率和处理性能得以兼顾，因此能够及时处理大流量的 WEB 请求。

附图说明

[0032] 图 1 是本发明实施例提供的一种 WEB 防御方法的流程图；

[0033] 图 2 是本发明实施例提供的另一种 WEB 防御方法的流程图；

[0034] 图 3 是本发明实施例提供的一种 WEB 防御系统的结构示意图。

具体实施方式

[0035] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0036] 图 1 是本发明实施例提供的一种 WEB 防御方法的流程图。如图 1 所示，该方法包括如下步骤。

[0037] 步骤 101，在分布式系统中的每个 WEB 服务器上部署 WEB 防御模块；独立于每个 WEB 服务器部署规则服务器，在所述规则服务器上维护规则表和危险 IP 列表。

[0038] 在步骤 101 中，为了更好的防御来自 WEB 的攻击，在分布式系统的每个 WEB 服务器上都部署 WEB 防御模块。由于每个 WEB 服务器上的 WEB 防御模块相互独立，因此单个服务器上的 WEB 防御模块出现宕机不会影响该分布式系统中的其他 WEB 服务器上的 WEB 防御模块的正常工作。

[0039] 此外，独立于每个 WEB 服务器部署规则服务器，在所述规则服务器上维护规则表和危险 IP 列表；规则表中配置有检测 WEB 请求是否为危险请求的规则，以及对触发规则的 WEB 请求做出的响应；所述危险 IP 列表包括一定数量的触发规则次数达到预设阀值的 WEB 请求的 IP。由于 WEB 防御模块与规则服务器是相互独立的，因此规则服务器的宕机并不会影响 WEB 防御模块的正常工作，WEB 防御模块仍可以根据已有的规则表和危险 IP 列表对 WEB 请求进行防御。

[0040] 步骤 102，WEB 防御模块在启动时，从所述规则服务器中获取所述规则表和所述危险 IP 列表。

[0041] 在步骤 102 中，WEB 防御模块是以 WEB 服务器模块的形式部署在各个 WEB 服务器

上的，因此可以通过 WEB 服务器加载配置文件的方式以激活该 WEB 防御模块。并且在 WEB 防御模块启动时，会向规则服务器发送获取请求，从规则服务器中获取规则表和危险 IP 列表。

[0042] 步骤 103，获取 WEB 服务器解析 http 数据包得到的 WEB 请求。

[0043] 在步骤 103 中，WEB 服务器在接收到 http 数据包时，对接收到的 http 数据包进行解析，得到相应的 WEB 请求。并将该 WEB 请求发送给所述 WEB 防御模块；其中，对 http 数据包进行解析能够得到对应的 WEB 请求中包括：URL 地址、与 IP 对应的 cookie，以及 http 头等信息。

[0044] 步骤 104，判断所述 WEB 请求的 IP 是否在所述危险 IP 列表中；如果是则进行步骤 105，如果否则进行步骤 106。

[0045] 在步骤 104 中，WEB 防御模块对 WEB 服务器解析 http 数据包得到的 WEB 请求，根据危险 IP 列表判断发送该 WEB 请求的 IP 是否在危险 IP 列表中。

[0046] 在本发明的一种具体实施例中，危险 IP 列表中保存有危险 IP 以及与该危险 IP 对应的 cookie。通过危险 IP 列表中的 cookie 能够区别出发起攻击的主机是该 IP 下的某个具体主机，用于解决一个 IP 下具有多台主机，发起攻击的可能仅仅是其中一台主机的情况。

[0047] 步骤 105，在判断发送该 WEB 请求的 IP 在危险 IP 列表中时，拒绝为所述 WEB 请求建立连接。

[0048] 步骤 106，在判断发送该 WEB 请求的 IP 不在危险 IP 列表中时，则继续依据规则表判断所述 WEB 请求是否为危险请求。如果是进行步骤 107，如果否进行步骤 108。

[0049] 在步骤 106 中，WEB 防御模块根据规则表对 WEB 请求进行判断，在检测到该 WEB 请求中包含规则表中任意一条规则中的关键字时，则表明该 WEB 请求触发了该规则，即判断该 WEB 请求为危险请求。

[0050] 步骤 107，依据所述规则表对所述 WEB 请求做出响应，并将触发规则的所述 WEB 请求的信息提交给所述规则服务器以更新所述 IP 列表中。

[0051] 在步骤 107 中，在判断 WEB 请求为危险请求之后，WEB 防御模块依据与触发的规则相对应的响应操作做出响应；举例为，如果对触发某规则的 WEB 请求的响应动作为拒绝，则停止处理所述 WEB 请求，即不将该 WEB 请求转交给 WEB 服务器的其他模块处理；如果对触发某规则的 WEB 请求的响应动作为记录日志，则将触发该规则的 WEB 请求记录到规则服务器中的日志中。规则表中还包括其他响应操作，并且各响应操作可以同时进行，举例为，响应操作为拒绝和记录日志，在此不一一赘述。

[0052] 步骤 108，在判断该 WEB 请求不是危险请求时，将所述 WEB 请求转交给所述 WEB 服务器的其他模块处理。

[0053] 在上述的步骤 103 中，WEB 防御模块获取 WEB 服务器对 http 数据包进行解析后得到的 WEB 请求。由于该 WEB 防御模式是部署在 WEB 服务器上的，对 WEB 层的解包只需要进行一次，因此能够充分利用 WEB 服务器的资源，不需要额外的成本开销，即 WEB 防御模块不需要对 http 数据包进行单独的解析，只需要对 WEB 服务器解析后的结果进行分析即可，因此提高了对 http 数据包处理的效率。与现有技术相比，能够更加效率的处理 WEB 请求。

[0054] 在本发明的一种具体实施例中，为了能够更好地防御来自 WEB 的攻击，WEB 防御模块周期性地向规则服务器发送获取请求，从规则服务器中获取规则表和危险 IP 列表；即通

过设置WEB防御模块每隔一定周期从规则服务器中获取规则表和危险IP列表。WEB防御模块依据新获取到的规则表和危险IP列表对WEB请求进行防御，同时根据新获取到的规则表和危险IP列表对本地保存的规则表和危险IP列表进行更新。

[0055] 在本发明的其他实施例中，还可以在规则服务器中设置周期性地向每个WEB防御模块下发规则表和危险IP列表。

[0056] 较佳的，为了能够更快、更及时地让WEB防御模块更新本地的规则表和危险IP列表。在本发明中，当所述规则表或所述危险IP列表有更新时，规则服务器将更新后的规则表或所述危险IP列表发送给WEB防御模块，即规则服务器中的规则表或者危险IP列表中任意有更新时，立即将更新后的规则表或者危险IP列表下发给WEB防御模块。

[0057] 在上述实施例中，当有新的安全风险或者新的WEB攻击方式出现时，通过在规则服务器中设置新的规则表，并及时下发给WEB防御模块，使得WEB防御模块对WEB攻击的防御更加具有时效性。

[0058] 由上述可知，WEB防御模块能够周期性地从规则服务器中获取规则表和危险IP列表，以及规则服务器及时地将更新后的规则表或所述危险IP列表发送给WEB防御模块，保证WEB防御模能够及时地获取到最新的规则表和危险IP列表，实现对最新WEB攻击的防御。

[0059] 在本发明的一种具体实施例中，独立于所述规则服务器部署监控服务器，监控服务器用于向所述规则服务器下发新的规则以更新所述规则表。在本实施例中，监控服务器可以跨网络进行部署，即监控服务器与规则服务器并不在同一个局域网内。在上述实施例中，还可以通过监控服务器对规则服务器进行查看或配置。举例为：查看或配置规则服务器上的规则表，查看或配置规则服务器上的危险IP列表。还可以通过监控服务器查看某段时间内的保存的日志。

[0060] 在本发明的一种具体实施例中，为了能够更加直观地对WEB防御模块的运行状态进行监控。WEB防御模块接收监控服务器的WEB查询请求，并根据所述WEB查询请求将自身的运行状态上报给所述监控服务器。具体为，WEB防御模块接收跨网络部署的监控服务器的发送的WEB查询请求，根据所述WEB查询请求将自身的运行状态上报给所述监控服务器。举例为：监控服务器可以以WEB访问的方式查看WEB服务器上的WEB防御模块的运行状态，查看那条规则被触发的次数最多，查看有多少个IP发动攻击，以及IP所在的物理地址。

[0061] 由上可知，在本发明中，用户能够通过监控服务器及时地对规则服务器中的规则表进行配置，还能实时查看WEB防御模块的运行状态，便于用户根据监控服务器的展示进行实际的操作。

[0062] 图2是本发明实施例提供的另一种WEB防御方法的流程图，如图2所述，该方法包括如下步骤：

[0063] 步骤201，在分布式系统中的每个WEB服务器上部署WEB防御模块；独立于每个WEB服务器部署规则服务器，在所述规则服务器上维护规则表和危险IP列表。

[0064] 在步骤201中，部署WEB防御模块和规则服务器的方式同图1中的步骤101。

[0065] 步骤202，所述规则服务器接收检测WEB请求是否为危险请求的规则，以及对触发规则的WEB请求做出的响应的配置信息。

[0066] 在步骤202中，所述配置信息可以是用户手动在规则服务器上配置，也可以是通

过监控服务器进行配置。即规则服务器接收用户手动输入的配置信息，或者规则服务器接收用户通过监控服务器发送的配置信息。

[0067] 步骤 203，根据规则和响应的配置信息建立或更新规则表。

[0068] 在步骤 202 中，将接收的配置信息以 xml 格式存储为规则表。如下是本发明的一种 xml 格式的规则表的示例。

[0069]

```
<filterRule Name="ruleSQLInject" actionType="Deny Log">
    <filterWords>
        <filterWord
Value="insert,update,select,union,and,or,having,substr,datadir,drop,create,grant,load_file,sleep,
benchmark,case,when,concat,cast,ascii,char,floor,min,max,group_concat,bit_and,bit_or,bit_xor,
substring_index,substring,set,current_user,length,bit_length,match,against,like,hex,unhex,left,ri
ght,REVERSE,quote,locate,instr,FIND_IN_SET,CONCAT_WS(),NULLIF,IFNULL,INTERVA
L,between,is_srvrolemember,WAITFOR,declare,EXEC,HOST_NAME,DELAY,system_user ,I
NTERVAL"/>
    </filterWords>
</filterRule>
```

[0070] 该示例表示与 WEB 请求匹配的防注入规则，模式为拦截和记录日志。当 WEB 请求中包含此处的任何一个关键字时，就触发了本规则。

[0071] 步骤 204，接收 WEB 防御模块提交的触发所述规则表中规则的 WEB 请求的信息。

[0072] 在步骤 204 中，在 WEB 防御模块检测到有 WEB 请求触发了规则表中规则时，将该触发了规则的 WEB 请求的信息发送给规则服务器。

[0073] 步骤 205，依据触发规则的所述 WEB 请求的信息做哈希表，哈希表的键包括所述 WEB 请求的 IP，对应的值为该 IP 的触发次数，其中，每触发规则一次，则触发次数加一；

[0074] 在步骤 205 中，规则表依据触发规则的 WEB 请求的信息做哈希表；其中，将规则服务器以发送该 WEB 请求的 IP 和 cookie 做哈希为键，该 IP 触发的规则的触发次数为值的键值对，保存到缓存或者数据库中的哈希表中。其中，每触发规则一次，该哈希表中的对应的值加一。

[0075] 步骤 206，从所述哈希表中获取触发次数达到预设阀值的 WEB 请求的 IP 建立或更新危险 IP 列表。

[0076] 在步骤 206 中，当触发次数的值达到预设的阀值时，将该触发次数对应的 IP 和 cookie 加载到危险 IP 列表中，即实现对危险 IP 列表的更新。

[0077] 步骤 207，在 WEB 防御模块启动时，发送规则表和危险 IP 列表到 WEB 防御模块，使得 WEB 防御模块根据规则表和危险 IP 列表对 WEB 请求进行防御。

[0078] 在本发明的一种实施例中，为了保证 WEB 防御模块的时效性，采用触发更新方式，

即当规则表或危险 IP 列表有更新时，规则服务器会直接下发更新后的规则表或危险 IP 列表到各个 WEB 防御模块。

[0079] 在本发明的一种实施例中，规则服务器还可以根据 WEB 防御模块周期性发送的获取请求，将规则表和危险 IP 列表发送到 WEB 防御模块。

[0080] 在本发明的一种具体实施例中，独立于规则服务器部署监控服务器；其中，监控服务器用于向规则服务器下发新的规则以更新规则表。规则服务器接收监控服务器发送的 WEB 查询请求，根据该 WEB 查询请求将本地的规则表和危险 IP 列表上报给监控服务器。即在本实施例中，监控服务器以 WEB 的方式访问规则服务器，查看该规则服务器上的规则表和危险 IP 列表，还可以对规则服务器列表中的规则表进行配置，举例为：增加或修改其中的规则。

[0081] 本发明还公开了一种 WEB 防御系统，图 3 是本发明中一种 WEB 防御系统的结构示意图。如图 3 所示，该系统包括：至少一个 WEB 防御模块 301、规则服务器 302。其中，WEB 防御模块 301 部署在分布式系统中的每个 WEB 服务器 304 上，所述规则服务器 302 独立于每个 WEB 服务器 304 部署，在规则服务器 302 上维护规则表和危险 IP 列表。

[0082] WEB 防御模块 301，用于在启动时从规则服务器 302 中获取规则表和危险 IP 列表；对 WEB 服务器解析 http 数据包得到的 WEB 请求，判断所述 WEB 请求的 IP 是否在所述危险 IP 列表中；如果在，拒绝为所述 WEB 请求建立连接；如果不在，则继续依据所述规则表判断所述 WEB 请求是否为危险请求；如果是，依据所述规则表对所述 WEB 请求做出响应，并将触发规则的所述 WEB 请求的信息提交给所述规则服务器以更新危险 IP 列表；如果不是，将所述 WEB 请求转交给所述 WEB 服务器的其他模块处理。

[0083] 规则服务器 302，用于接收检测 WEB 请求是否为危险请求的规则，以及对触发规则的 WEB 请求做出的响应的配置信息，根据所述规则和响应的信息建立或更新所述规则表；根据 WEB 防御模块 301 提交的触发规则的 WEB 请求的信息做哈希表，哈希表的键包括所述 WEB 请求的 IP，对应的值为该 IP 的触发次数，其中，每触发规则一次，则触发次数加一；从所述哈希表中获取一定数量的触发次数达到预设阀值的 WEB 请求的 IP 建立或更新危险 IP 列表。

[0084] 在本发明的一种具体实施例中，WEB 防御模块 301 周期性地从规则服务器 302 中获取规则表和危险 IP 列表。即 WEB 防御模块 301 周期性地向规则服务器 302 发送获取请求的方式从规则服务器 302 中获取规则表和危险 IP 列表。当规则表或危险 IP 列表有更新时，WEB 防御模块 301 还会接收规则服务器 302 下发的更新后的规则表或危险 IP 列表。

[0085] 在本发明的一种具体实施例中，当规则表或危险 IP 列表有更新时，规则服务器 302 下发更新后的规则表或危险 IP 列表到 WEB 防御模块 301。规则服务器 302 根据 WEB 防御模块 301 周期性发送的获取请求，将规则表和危险 IP 列表发送到 WEB 防御模块。

[0086] 如图 3 所示，该系统还包括：监控服务器 303。该监控服务器 303 独立于规则服务器 302 部署。

[0087] 在本发明的一种实施例中，监控服务器 303 向规则服务器 302 下发新的规则以更新规则表。具体为：监控服务器 303 向规则服务器 302 发送 WEB 配置请求，所述 WEB 配置请求中包括待更新的规则表或危险 IP 列表。监控服务器 303 以 WEB 的方式访问规则服务器 302，根据 WEB 配置请求对规则服务器 302 中的规则表和危险 IP 列表进行配置。

[0088] 在本发明的一种实施例中，监控服务器 303 向 WEB 防御模块发送 WEB 查询请求查询 WEB 防御模块 301 的运行状态。在本实施例中，监控服务器 303 向 WEB 防御模块 301 发送 WEB 查询请求，接收 WEB 防御模块 301 根据 WEB 查询请求上报的自身的运行状态。举例为：监控服务器能够以 WEB 的方式访问 WEB 防御模块 301，进而查看那些规则被触发的次数最多，发起 WEB 攻击的 IP，以及该 IP 的物理地址等信息。

[0089] 在本发明的一种实施例中，监控服务器 303 向规则服务器 302 发送 WEB 查询请求，查询规则服务器 302 上的规则表和危险 IP 列表。在本实施例中，监控服务器 303 以 WEB 的方式访问规则服务器 302，进而查看规则服务器 302 中配置的规则表和危险 IP 列表。还可以查看保存在规则服务器 302 中日志。

[0090] 在本发明的一种具体实施例中，监控服务器 303，能跨网络进行部署，即监控服务器 303 与 WEB 服务器 304 以及规则服务器 302 不在同一个局域网中，监控服务器 303 能够以 WEB 的方式运行，通过 WEB 的方式访问规则服务器 302 和 WEB 防御模块 301。

[0091] 在本发明的一种具体实施例中，规则服务器 302 接收 WEB 防御模块 301 提交的触发规则表中规则的 WEB 请求的信息；依据触发规则的 WEB 请求的信息做哈希表，哈希表的键包括所述 WEB 请求的 IP，对应的值为该 IP 的触发次数，其中，每触发规则一次，则触发次数加一。从该哈希表中获取触发次数达到预设阀值的 WEB 请求的 IP 建立危险 IP 列表；将规则表和危险 IP 列表下发到 WEB 防御模块 301。

[0092] 参见图 3 所示，本发明提供的系统可以划分为三层架构，WEB 防御模块、规则服务器和监控服务器。任意一层的宕机不会影响其他层的正常工作。其中，WEB 防御模块 301 部署在分布式系统的各个 WEB 服务器 304 中，单个 WEB 防御模块 301 的宕机并不会影响其他 WEB 防御模块 301 的正常工作，也不会影响其他 WEB 服务器和业务的正常工作。因此克服了传统单一节点部署的性能瓶颈和单点故障。并且，上述系统具有稳定易用，便于扩充的优点，即在新增加的 WEB 服务器上部署 WEB 防御模块，再从规则服务器中获取规则表和危险 IP 列表，快捷灵活的配置新的风险的规则。

[0093] 综上所述，本发明通过在分布式系统中的每个 WEB 服务器上部署 WEB 防御模块；在启动时从规则服务器中获取规则表和危险 IP 列表；根据规则表和危险 IP 列表对 WEB 请求是否存在攻击进行检测，并根据判断结果进行相应的操作的技术方案，本发明提供的技术方案中，WEB 防御模块单独部署在 WEB 服务器上，稳定易用并且便于扩充。此外，在处理大流量的 WEB 请求时，由于 WEB 防御模块只是对 WEB 服务器解析 http 数据包得到的 WEB 请求进行处理，能够充分利用 WEB 服务器的资源，解析效率和处理性能得以兼顾，因此能够及时处理大流量的 WEB 请求。

[0094] 进一步的，本发明提供的技术方案采用相对独立的 WEB 防御模块、规则表和监控服务器三层架构。单层的宕机不会影响其他层的正常工作，即监控服务器的宕机不会影响 WEB 防御模块或者规则服务器的正常工作；规则服务器的宕机不会影响 WEB 防御模块的正常工作，WEB 防御模块可以根据之前保存的规则表和危险 IP 列表进行防御。因此具有高可用性和可靠稳定性的优点。

[0095] 进一步的，通过监控服务器实现对规则服务器上的规则表进行实时配置，并将新配置的规则表及时下发给各 WEB 防御模块，实现对新出现的安全风险和新的 WEB 攻击方式的实时抵御。

[0096] 以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

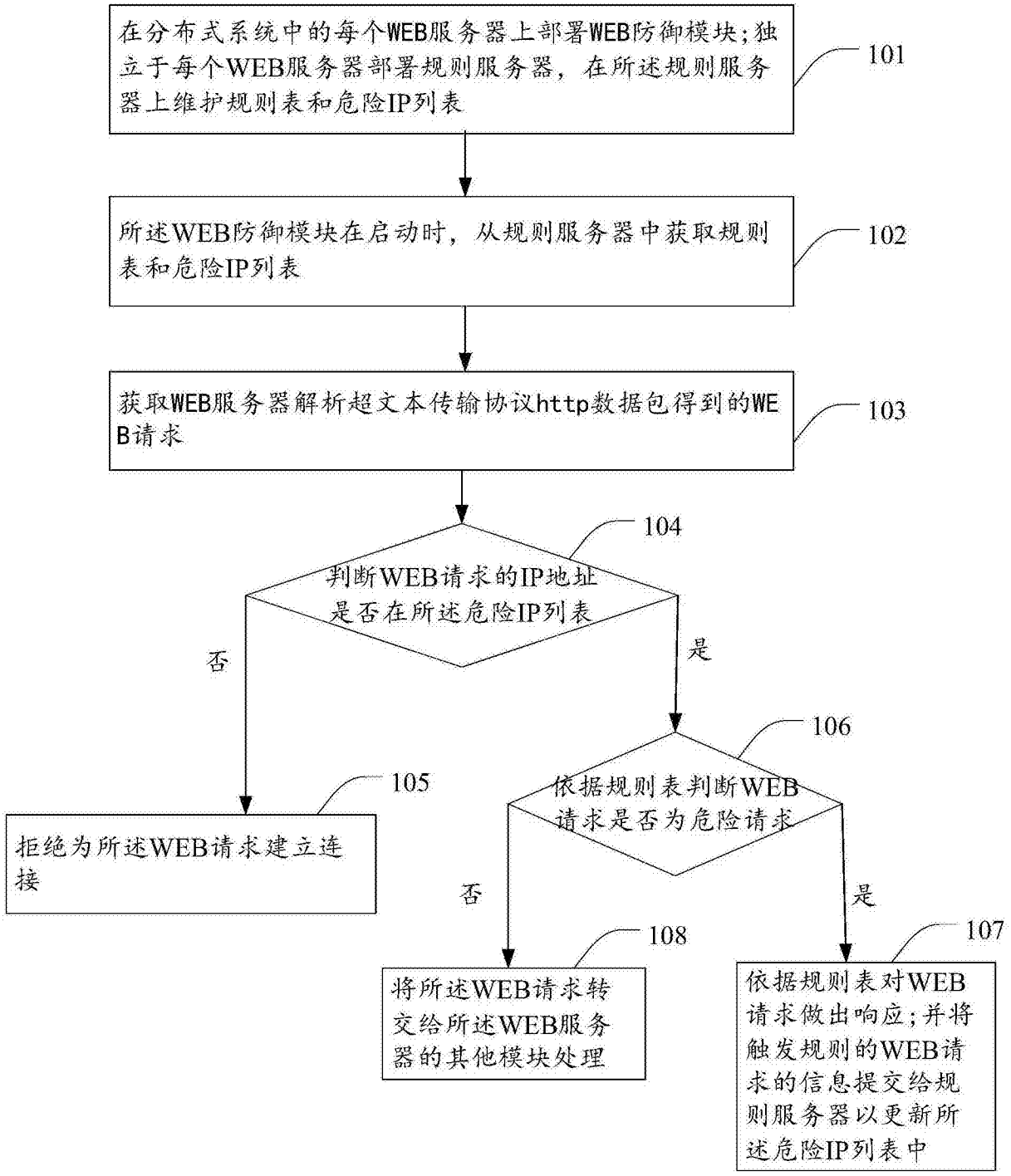

在分布式系统中的每个WEB服务器上部署WEB防御模块;独立于每个WEB服务器部署规则服务器，在所述规则服务器上维护规则表和危险IP列表
101
所述WEB防御模块在启动时，从规则服务器中获取规则表和危险IP列表
102
获取WEB服务器解析超文本传输协议http数据包得到的WEB请求
103
判断WEB请求的IP地址是否在所述危险IP列表
104
否
是
拒绝为所述WEB请求建立连接
105
依据规则表判断WEB请求是否为危险请求
106
否
是
将所述WEB请求转交给所述WEB服务器的其他模块处理
108
依据规则表对WEB请求做出响应;并将触发规则的WEB请求的信息提交给规则服务器以更新所述危险IP列表中
107

图 1

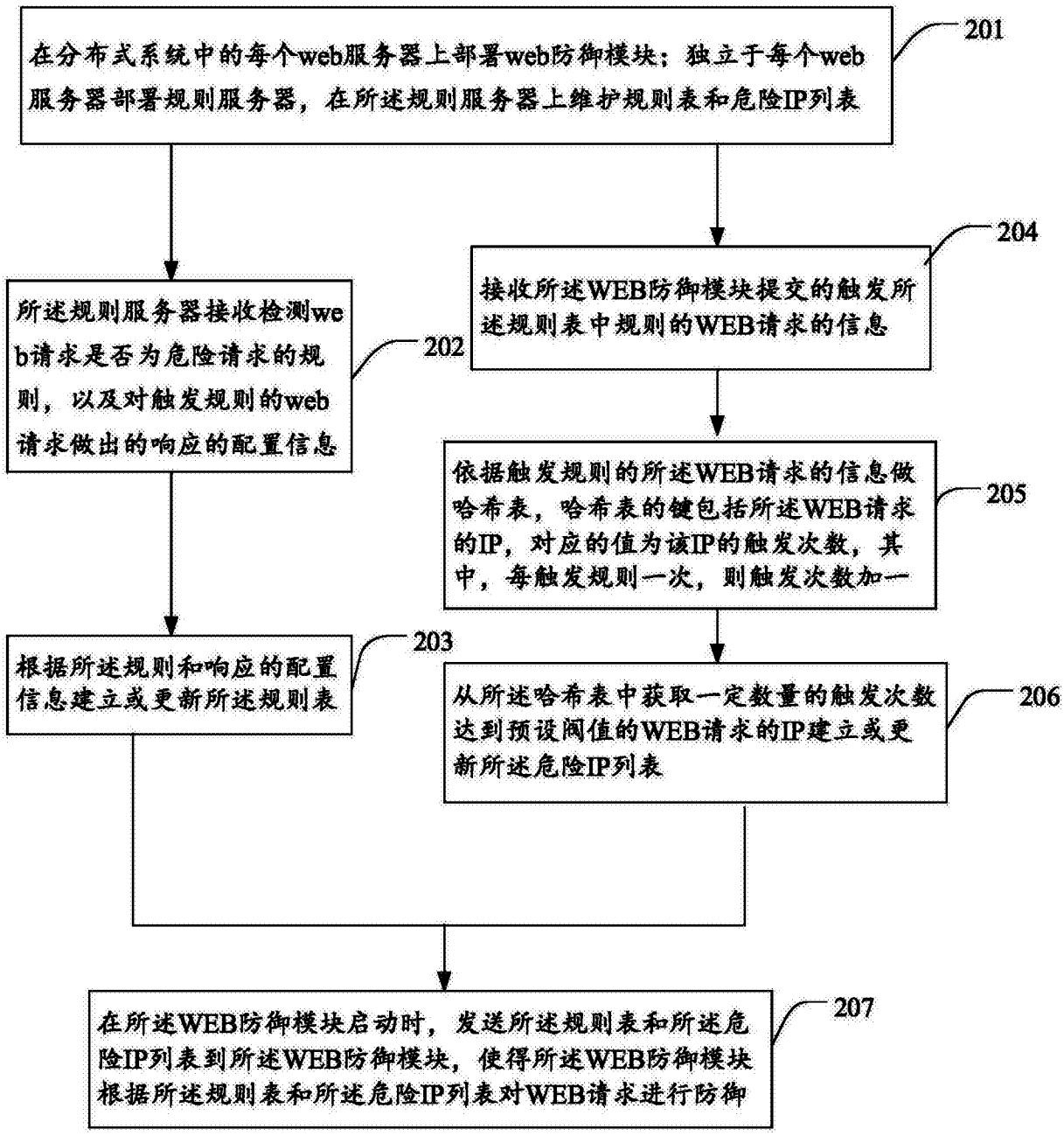

在分布式系统中的每个web服务器上部署web防御模块；独立于每个web服务器部署规则服务器，在所述规则服务器上维护规则表和危险IP列表
201
所述规则服务器接收检测web请求是否为危险请求的规则，以及对触发规则的web请求做出的响应的配置信息
202
根据所述规则和响应的配置信息建立或更新所述规则表
203
接收所述WEB防御模块提交的触发所述规则表中规则的WEB请求的信息
204
依据触发规则的所述WEB请求的信息做哈希表，哈希表的键包括所述WEB请求的IP，对应的值为该IP的触发次数，其中，每触发规则一次，则触发次数加一
205
从所述哈希表中获取一定数量的触发次数达到预设阈值的WEB请求的IP建立或更新所述危险IP列表
206
在所述WEB防御模块启动时，发送所述规则表和所述危险IP列表到所述WEB防御模块，使得所述WEB防御模块根据所述规则表和所述危险IP列表对WEB请求进行防御
207

图 2

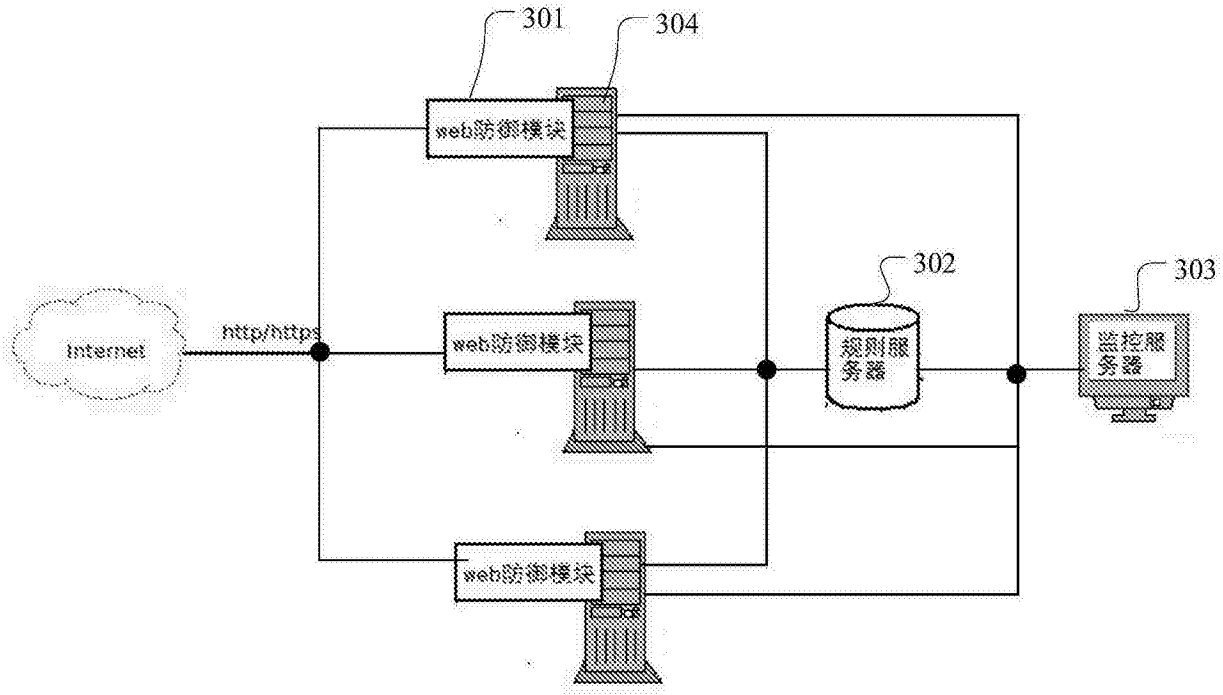

301
304
web防御模块
302
303
Internet
http/https
web防御模块
规则服务器
监控服务器
web防御模块

图 3