(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112039846 B
(45)授权公告日 2023.08.15

(21)申请号 202010723766.8

(22)申请日 2020.07.24

(65)同一申请的已公布的文献号
申请公布号 CN 112039846 A

(43)申请公布日 2020.12.04

(73)专利权人 网宿科技股份有限公司
地址 200030 上海市徐汇区斜土路2899号甲光启文化广场A幢5楼

(72)发明人 王斌

(74)专利代理机构 上海晨皓知识产权代理事务所(普通合伙) 31260
专利代理师 成丽杰

(51)Int.Cl.
H04L 9/40(2022.01)

(56)对比文件
CN 104410702 A,2015.03.11
CN 108696568 A,2018.10.23
CN 109150821 A,2019.01.04
CN 101902456 A,2010.12.01
CN 104394163 A,2015.03.04
CN 107046518 A,2017.08.15
CN 111435393 A,2020.07.21
CN 103188255 A,2013.07.03
CN 109067772 A,2018.12.21
US 2015026757 A1,2015.01.22

审查员 郝凯利

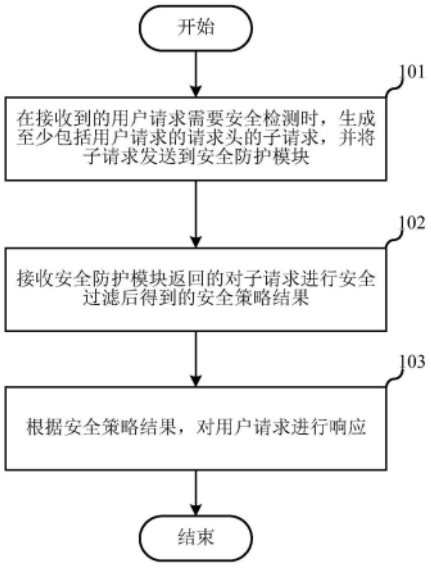
权利要求书2页 说明书9页 附图6页

(54)发明名称

请求处理方法与安全防护系统

(57)摘要

本发明实施例涉及网络安全技术领域，公开了一种请求处理方法与安全防护系统，请求处理方法包括：在接收到的用户请求需要安全检测时，生成至少包括用户请求的请求头的子请求，并将子请求发送到安全防护模块；接收安全防护模块返回的对子请求进行安全过滤后得到的安全策略结果；根据安全检测结果，对用户请求进行响应。本发明中，安全防护模块以旁路的方式提供安全防护服务，业务模块在执行自身业务时可以按需调用安全防护模块进行安全防护，提高了业务模块的利用率。



CN 112039846 B

1.一种请求处理方法,其特征在于,应用于安全防护系统的业务模块,所述安全防护系统还包括连接于所述业务模块的安全防护模块;所述方法包括:

在接收到的用户请求需要安全检测时,生成至少包括所述用户请求的请求头的子请求,并将所述子请求发送到所述安全防护模块;

接收所述安全防护模块返回的对所述子请求进行安全过滤后得到的安全策略结果;

根据所述安全策略结果,对所述用户请求进行响应;

所述生成至少包括所述用户请求的请求头的子请求,包括:

判断所述用户请求是否满足预设条件;

若所述用户请求满足预设条件,生成包括所述用户请求的请求头以及请求体的所述子请求;

若所述用户请求不满足预设条件,生成包括所述用户请求的请求头的子请求。

2.根据权利要求1所述的请求处理方法,其特征在于,所述预设条件包括所述用户请求支持请求体转发以及所述用户请求的请求体的大小小于或等于预设阈值。

3.根据权利要求1所述的请求处理方法,其特征在于,判断所述用户请求是否需要安全检测的方式为:

在接收到所述用户请求时,获取所述用户请求包含的目标域名的配置信息;

根据所述目标域名的配置信息,判断所述用户请求是否需要安全检测。

4.根据权利要求1所述的请求处理方法,其特征在于,所述根据所述安全策略结果,对所述用户请求进行响应,包括:

在所述安全策略结果表征所述用户请求处于通行状态时,将所述用户请求转发到目标服务器,并将接收到的所述目标服务器返回的响应内容作为所述用户请求的响应;

在所述安全策略结果表征所述用户请求处于拦截状态时,将预设的拦截页面作为所述用户请求的响应。

5.根据权利要求4所述的请求处理方法,其特征在于,所述将接收到的所述目标服务器返回的响应内容作为所述用户请求的响应,包括:

在接收到所述目标服务器返回的响应内容时,对所述响应内容进行安全检测,得到安全检测结果;

在所述安全检测结果表征所述响应内容为正常状态时,将所述响应内容作为所述用户请求的响应;

在所述安全检测结果表征所述响应内容为异常状态时,将预设的拦截页面作为所述用户请求的响应。

6.一种安全防护系统,其特征在于,包括:相互连接的业务模块与安全防护模块;

所述业务模块用于在接收到的用户请求需要安全检测时,生成至少包括所述用户请求的请求头的子请求,并将所述子请求发送到所述安全防护模块;

所述安全防护模块用于对所述子请求进行安全过滤,并将得到的安全策略结果发送到所述业务模块;

所述业务模块还用于根据所述安全策略结果,对所述用户请求进行响应;

所述业务模块用于判断所述用户请求是否满足预设条件;

所述业务模块用于在所述用户请求满足预设条件时,生成包括所述用户请求的请求头

以及请求体的所述子请求；

所述业务模块用于在所述用户请求不满足预设条件时，生成包括所述用户请求的请求头的子请求。

7.根据权利要求6所述的安全防护系统，其特征在于，所述预设条件包括所述用户请求支持请求体转发以及所述用户请求的请求体的大小小于或等于预设阈值。

8.根据权利要求6所述的安全防护系统，其特征在于，所述业务模块用于在接收到所述用户请求时，获取所述用户请求包含的目标域名的配置信息；

所述业务模块用于根据所述目标域名的配置信息，判断所述用户请求是否需要安全检测。

9.根据权利要求6所述的安全防护系统，其特征在于，

所述业务模块用于在所述安全策略结果表征所述用户请求处于通行状态时，将所述用户请求转发到目标服务器，并将接收到的所述目标服务器返回的响应内容作为所述用户请求的响应；

所述业务模块用于在所述安全策略结果表征所述用户请求处于拦截状态时，将预设的拦截页面作为所述用户请求的响应。

10.根据权利要求9所述的安全防护系统，其特征在于，所述业务模块中部署有安全组件；

所述业务模块还用于在接收到所述目标服务器返回的响应内容时，对所述响应内容进行安全检测，得到安全检测结果；

所述业务模块还用于在所述安全检测结果表征所述响应内容为正常状态时，将所述响应内容为所述用户请求的响应；

所述业务模块还用于在所述安全检测结果表征所述响应内容为异常状态时，将预设的拦截页面作为所述用户请求的响应。

11.根据权利要求6所述的安全防护系统，其特征在于，所述业务模块与所述安全防护模块均为基于nginx的模块。

12.根据权利要求6所述的安全防护系统，其特征在于，所述业务模块与所述安全防护模块部署在同一服务器中。

请求处理方法与安全防护系统

技术领域

[0001] 本发明实施例涉及网络安全技术领域,特别涉及一种请求处理方法与安全防护系统。

背景技术

[0002] Web应用防火墙(Web Application Firewall,简称WAF)系统主要用于对Web服务中遇到的入侵和攻击进行防护,例如DDOS防护、SQL注入、XML注入、XSS防护等。在CDN网络中,WAF系统是嵌入在边缘节点和父节点之间的专属节点中,从而能够利用WAF系统进行安全防护,WAF系统在对边缘节点发送的用户请求进行防护时,由WAF系统到父节点或源节点获取资源,并由边缘节点返回给用户。

[0003] 然而,发明人发现现有技术至少存在以下技术问题:在CDN网络中,部署有WAF的边缘节点一般作为专属节点,仅用于对需要安全检测的客户请求进行处理,不支持普通客户请求的处理,导致机器部署灵活性低,并且利用率较低。

发明内容

[0004] 本发明实施方式的目的在于提供一种请求处理方法与安全防护系统,安全防护模块以旁路的方式提供安全防护服务,业务模块在执行自身业务时可以按需调用安全防护模块进行安全防护,提高了业务模块的利用率;同时,实现了安全防护服务与其他业务叠加,安全防护模块可以灵活部署;并且,子请求对内存占用较少,且不会一直占据进程资源,进一步减小了对资源的占用。

[0005] 为解决上述技术问题,本发明的实施方式提供了一种请求处理方法,应用于安全防护系统的业务模块,安全防护系统还包括连接于业务模块的安全防护模块;方法包括:在接收到的用户请求需要安全检测时,生成至少包括用户请求的请求头的子请求,并将子请求发送到安全防护模块;接收安全防护模块返回的对子请求进行安全过滤后得到的安全策略结果;根据安全策略结果,对用户请求进行响应。

[0006] 本发明的实施方式还提供了一种安全防护系统,包括:相互连接的业务模块与安全防护模块;业务模块用于在接收到的用户请求需要安全检测时,生成至少包括用户请求的请求头的子请求,并将子请求发送到安全防护模块;对所述子请求进行安全过滤,并将得到的安全策略结果发送到所述业务模块;业务模块还用于根据安全策略结果,对用户请求进行响应。

[0007] 本发明实施方式相对于现有技术而言,业务模块能够在接收到的用户请求需要安全检测时,生成至少包括用户请求的请求头的子请求,并将该子请求发送到安全防护模块,安全防护模块则能够对该子请求进行安全过滤,并将得到的安全策略结果发送到业务模块,继而业务模块可以根据安全策略结果,对用户请求进行响应,即安全防护模块以旁路的方式提供安全防护服务,业务模块在执行自身业务时可以按需调用安全防护模块进行安全防护,提高了业务模块的利用率;同时,实现了安全防护服务与其他业务叠加,安全防护模

块可以灵活部署;并且,子请求对内存占用较少,且不会一直占据进程资源,进一步减小了对资源的占用。

[0008] 另外,生成至少包括用户请求的请求头的子请求,包括:判断用户请求是否满足预设条件;若用户请求满足预设条件,生成包括用户请求的请求头以及请求体的子请求;若用户请求不满足预设条件,生成包括用户请求的请求头的子请求。本实施例中,务模块能够针对不同的用户请求,生成不同的子请求,以便于安全防护模块针对不同的用户请求进行不同的安全过滤。

[0009] 另外,预设条件包括用户请求支持请求体转发以及用户请求的请求体的大小小于或等于预设阈值。

[0010] 另外,判断用户请求是否需要安全检测的方式为:在接收到用户请求时,获取用户请求包含的目标域名的配置信息;根据目标域名的配置信息,判断用户请求是否需要安全检测。本实施方式提供了业务模块判断用户请求是否需要安全检测的一种具体实现方式。

[0011] 另外,根据安全策略结果,对用户请求进行响应,包括:在安全策略结果表征用户请求处于通行状态时,将用户请求转发到目标服务器,并将接收到的目标服务器返回的响应内容作为用户请求的响应;在安全策略结果表征用户请求处于拦截状态时,将预设的拦截页面作为用户请求的响应。本实施方式提供了一种根据安全策略结果,对用户请求进行响应的一种具体实现方式。

[0012] 另外,将接收到的目标服务器返回的响应内容作为用户请求的响应,包括:在接收到目标服务器返回的响应内容时,对响应内容进行安全检测,得到安全检测结果;在安全检测结果表征响应内容为正常状态时,将响应内容为用户请求的响应;在安全检测结果表征响应内容为异常状态时,将预设的拦截页面作为用户请求的响应。本实施方式中,利用业务模块对响应内容的安全检测,即业务模块无需通过安全防护模块便能够直接进行响应内容的安全检测,减少了响应内容的转发操作,简化了安全检测流程。

附图说明

[0013] 一个或多个实施例通过与之对应的附图中的图片进行示例性说明,这些示例性说明并不构成对实施例的限定,附图中具有相同参考数字标号的元件表示为类似的元件,除非有特别申明,附图中的图不构成比例限制。

[0014] 图1是根据本发明第一实施方式中的请求处理方法应用的安全防护系统的方框示意图;

[0015] 图2是根据本发明第一实施方式中的请求处理方法的具体流程图;

[0016] 图3是图4中步骤103的具体流程图;

[0017] 图4是根据本发明第一实施方式中的服务器、客户端以及目标服务器之间的交互时序图;

[0018] 图5是根据本发明第二实施方式中的请求处理方法的具体流程图;

[0019] 图6是根据本发明第二实施方式中的服务器、客户端以及目标服务器之间的交互时序图。

具体实施方式

[0020] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合附图对本发明的各实施方式进行详细的阐述。然而，本领域的普通技术人员可以理解，在本发明各实施方式中，为了使读者更好地理解本申请而提出了许多技术细节。但是，即使没有这些技术细节和基于以下各实施方式的种种变化和修改，也可以实现本申请所要求保护的技术方案。

[0021] 本发明的第一实施方式涉及一种请求处理方法，请参考图1，应用于安全防护系统中的业务模块1，安全防护系统还包括连接于业务模块1的安全防护模块2。本实施例中，业务模块1用于为用户提供加速、缓存等服务，可以为安装在服务器中业务系统软件；安全防护模块2用于为用户提供安全防护服务，可以为安装在服务器中WAF系统软件。其中，业务模块1与安全防护模块2可以均为基于nginx的模块，即业务系统软件与WAF系统软件均为基于nginx的软件。

[0022] 本实施方式的请求处理方法的具体流程如图1所示。

[0023] 步骤101，在接收到的用户请求需要安全检测时，生成至少包括用户请求的请求头的子请求，并将子请求发送到安全防护模块。

[0024] 具体而言，业务模块1所在的服务器的内存中预先加载有各域名的配置信息，配置信息包括各域名是否需要安全检测的设置，业务模块1接收到用户通过客户端3发送的目标域名的用户请求时，可以读取该目标域名的配置信息，并能够根据该目标域名的配置信息，来判断用户请求是否需要安全检测。

[0025] 当目标域名的配置信息表征该域名处于监控状态时，判定该用户请求需要进行安全检测，此时业务模块1生成至少包括用户请求的请求头的子请求，并将该子请求发送到安全防护模块2，由安全防护模块2对该子请求进行安全过滤。

[0026] 当目标域名的配置信息表征该域名处于拦截状态时，业务模块1则可以直接响应预设的拦截页面到客户端3。

[0027] 当目标域名的配置信息表征该域名处于正常状态时，判定该用户请求不需要进行安全检测，此时将用户请求发送到目标服务器4，并将接收到的目标服务器4返回的响应内容转发到客户端3，其中目标服务器4可以为业务模块1所在服务器的父节点或目标域名的源站。

[0028] 在一个例子中，业务模块1在生成至少包括用户请求的请求头的子请求时，还可以判断用户请求是否满足预设条件，若用户请求满足预设条件，则生成包括用户请求的请求头与请求体的子请求；若用户请求不满足预设条件，生成包括用户请求的请求头的子请求；即业务模块1能够针对不同的用户请求，生成不同的子请求，以便于安全防护模块2针对不同的用户请求进行不同的安全过滤。其中，预设条件包括用户请求支持请求体转发以及用户请求的请求体的大小小于或等于预设阈值。

[0029] 举例来说，业务模块1中可以配置需要进行安全检测的请求类型，例如GET请求、POST请求、HEAD请求等，从而在接收到的用户请求属于安全检测的请求类型时，判定用户请求需要进行安全检测，业务模块1中还配置了支持转发请求体的请求类型，例如为POST请求，业务模块1在判定用户请求需要进行安全检测时，先判断该用户请求的类型是否支持转发请求体，若该用户请求支持请求体转发，再判断用户请求的请求体的大小是否小于或等于预设阈值，若用户请求的请求体的大小小于或等于预设阈值，则生成包括该用户请求的

请求头以及请求体的子请求;反之,在用户请求不支持请求体转发或者用户请求的请求体的大小大于预设阈值时,则生成包括用户请求的请求头的子请求。

[0030] 步骤102,接收安全防护模块返回的对子请求进行安全过滤后得到的安全策略结果。

[0031] 具体而言,安全防护模块2作为WAF系统,在接收到业务模块1发送的子请求时,对该子请求进行安全过滤,检测方式包括URL的正则匹配、请求头的检验等等,从而能够检测出用户请求中是否存在SQL注入、XSS攻击、WEBSHELL攻击等等,并生成相应的安全策略结果,并将该安全策略结果返回到业务模块1。其中,安全策略结果可以表征用户请求处于通行状态或者是拦截状态,通行状态表示该用户请求中未包含攻击内容、拦截状态表示该用户请求中包含攻击内容,通行状态的安全策略结果中还可以包括重定向、限速等辅助策略;安全防护模块2可以在安全策略结果表征用户请求处于拦截状态时,生成攻击记录日志,该日志中包含完整的用户请求包、用户请求时间、请求IP、命中规则ID、攻击类型、规则库匹配到的攻击内容等信息,以便于后续对受到的攻击进行分析防范。

[0032] 步骤103,根据安全策略结果,对用户请求进行响应。

[0033] 请参考图3,步骤103包括以下子步骤:

[0034] 子步骤1031,在安全策略结果表征用户请求处于通行状态时,将用户请求转发到目标服务器,并将接收到的目标服务器返回的响应内容作为用户请求的响应。

[0035] 子步骤1032,在安全策略结果表征用户请求处于拦截状态时,将预设的拦截页面作为用户请求的响应。

[0036] 具体而言,业务模块1在安全策略结果表征用户请求处于通行状态时,继续进行加速、缓存业务流程,将用户请求发送到目标服务器4,并将接收到的目标服务器4返回的响应内容作为用户请求的响应,即将该响应内容转发给客户端3;业务模块1在安全策略结果表征用户请求处于拦截状态时,将预设的拦截页面作为用户请求的响应,即将该拦截页面发送到客户端3,其中拦截页面上还可以包括http状态码403。

[0037] 本实施例中,若业务模块1为基于nginx的模块,则业务模快1可以基于nginx HTTP框架对用户请求进行分解得到多个子请求,从而能够得到包括用户请求的请求头的子请求;然后在安全防护模块2返回的安全策略结果表征用户请求处于通行状态时,利用upstream机制访问目标服务器4,并将目标服务器4返回的响应内容发送给客户端3。

[0038] 在一个例子中,业务模块1与安全防护模块2可以部署在一个融合服务器中,即安全防护系统部署在一个融合服务器上,以业务模块1为安装在该融合服务器上的nginx业务系统软件、安全防护模块2安装在该融合服务器上的nginx的WAF系统软件为例,融合服务器在利用业务系统软件提供基础的业务服务时,将WAF系统软件作为业务系统软件的子服务。其中,由业务系统软件来判断用户请求是否需要进行安全检测,WAF系统软件仅用于提供安全过滤,从而仅需加载一份各域名的配置信息到服务器的内存中,WAF系统软件则无需加载各域名的配置信息到服务器的内存中,减少了对服务器内存的消耗,减小了部署在同一服务器中的WAF系统软件与业务系统软件之间的相互影响。

[0039] 在融合服务器中,将安全防护模块2作为业务模块1的子服务,来提供安全防护功能;并且安全防护模块2仅用于进行安全过滤,减小了安全防护模块2对融合服务器内存的消耗,降低了安全防护模块2与业务模块1之间的相互影响,使得同一服务器能够同时提供

多种服务。

[0040] 请参考图4，为服务器与客户端3以及目标服务器4之间的交互时序图，本实施例中，用户通过客户端3向业务系统软件发起请求，将用户请求发送到业务系统软件，业务系统软件在接收到用户请求后读取用户请求中包含的目标域名的配置信息，并根据该配置信息，判断用户请求是否需要进行安全检测。若配置信息表征用户请求处于正常状态，则判定用户请求不需要进行安全检测，将用户请求转发到目标服务器4，目标服务器4获取用户请求对应的响应内容，并将该响应内容发送到业务系统软件，业务系统软件则将该响应内容发送给客户端3；若配置信息表征用户请求处于监控状态，则判定用户请求需要进行安全检测，生成至少包括用户请求的请求头的子请求，并该子请求发送到WAF系统软件，WAF系统软件则对该子请求进行安全过滤，得到安全策略结果，并将该安全策略结果发送到业务系统软件。

[0041] 业务系统软件在该安全策略结果表征用户请求处于通行状态时，将该用户请求转发给目标服务器4，目标服务器4获取用户请求对应的响应内容，并将该响应内容发送到业务系统软件，业务系统软件则将该响应内容发送给客户端3；业务系统软件在该安全策略结果表征用户请求处于拦截状态时，将预设的拦截页面作为用户请求的响应发送到客户端3。

[0042] 本实施方式相对于现有技术而言，业务模块能够在接收到的用户请求需要安全检测时，生成至少包括用户请求的请求头的子请求，并将该子请求发送到安全防护模块，安全防护模块则能够对该子请求进行安全过滤，并将得到的安全策略结果发送到业务模块，继而业务模块可以根据安全策略结果，对用户请求进行响应，即安全防护模块以旁路的方式提供安全防护服务，业务模块在执行自身业务时可以按需调用安全防护模块进行安全防护，提高了业务模块的利用率；同时，实现了安全防护服务与其他业务叠加，安全防护模块可以灵活部署；并且，子请求对内存占用较少，且不会一直占据进程资源，进一步减小了对资源的占用。

[0043] 本发明的第二实施方式涉及一种请求处理方法，本实施方式相对于第一实施方式来说，主要区别之处在于：增加了对响应内容的安全检测。

[0044] 本实施方式的请求处理方法的具体流程如图5所示。

[0045] 其中，步骤201、步骤202与步骤101、步骤102大致相同，在此不再赘述，主要不同之处在于，步骤203包括：

[0046] 子步骤2031，在安全策略结果表征用户请求处于通行状态时，将用户请求转发到目标服务器，并对接收到的目标服务器返回的响应内容进行安全检测，得到安全检测结果。

[0047] 具体而言，可以在业务模块1中部署有基于nginx动态模块机制的waflib库，业务模块1可以调用该waflib库对响应内容进行安全检测；请参考图6的服务器与客户端3以及目标服务器4之间的交互时序图，业务模块1在安全策略结果表征用户请求处于通行状态时，将该用户请求发送到目标服务器4，在接收目标服务器4返回的响应内容后，调用wiflib库对该响应内容进行安全检测，得到安全检测结果，安全检测结果表征响应内容为正常状态或异常状态。其中，安全检测内容包括：响应内容响应头以及响应体的增删改操作、web服务器响应错误信息(如服务器的版本等信息)、数据库名称等敏感信息、web程序异常抛出的敏感信息等。

[0048] 子步骤2032，在安全检测结果表征响应内容为正常状态时，将响应内容作为用户

请求的响应。

[0049] 子步骤2033,在安全检测结果表征响应内容为异常状态时,将预设的拦截页面作为用户请求的响应。

[0050] 具体而言,业务模块1在安全检测结果表征响应内容为正常状态时,将该响应内容作为用户请求的响应,即将该响应内容发送到客户端3;在安全检测结果表征响应内容为异常状态时,业务模块1则将预设的拦截页面发送到客户端3,并记录该响应内容的检测日志。

[0051] 子步骤2034,在安全策略结果表征用户请求处于拦截状态时,将预设的拦截页面作为用户请求的响应。

[0052] 本实施方式相对于第一实施方式而言,业务模块还可以对响应内容进行安全检测,即无需通过安全防护模块便能够直接进行响应内容的安全检测,减少了响应内容的转发操作,简化了安全检测流程。

[0053] 本发明第三实施方式涉及一种安全防护系统,如图1所示,安全防护系统包括相互连接的业务模块1与安全防护模块2,业务模块1用于为用户提供加速、缓存等服务,为业务系统软件;安全防护模块2用于为用户提供安全防护服务,例如为WAF系统软件。安全防护系统可以为CDN网络中边缘节点集群、或者单个边缘节点,若安全防护系统可以为CDN网络中单个边缘节点,则说明业务模块1与安全防护模块2部署在同一个服务器(本实施例以及之后的实施例中均以此为例)中,该服务器融合了加速、缓存等服务以及安全防护服务,即业务系统软件与WAF软件融合后部署在同一个服务器中,可以同时为用户提供多种服务,该服务器可以称为融合服务器,在融合服务器中,将安全防护模块2作为业务模块1的子服务,来提供安全防护功能;并且安全防护模块仅用于进行安全过滤,减小了安全防护模块对服务器内存的消耗,降低了安全防护模块2与业务模块1之间的相互影响。其中,业务模块1与安全防护模块2可以均为基于nginx的模块,即业务系统软件与WAF系统软件均为基于nginx的软件。

[0054] 业务模块1用于在接收到的用户请求需要安全检测时,生成至少包括用户请求的请求头的子请求,并将子请求发送到安全防护模块。

[0055] 具体的,融合服务器的内存中预先加载有各域名的配置信息,配置信息包括各域名是否需要安全检测的设置,业务模块1接收到用户通过客户端3发送的目标域名的用户请求时,可以读取该目标域名的配置信息,并能够根据该目标域名的配置信息,来判断用户请求是否需要安全检测。

[0056] 当目标域名的配置信息表征该域名处于监控状态时,判定该用户请求需要进行安全检测,此时业务模块1生成至少包括用户请求的请求头的子请求,并将该子请求发送到安全防护模块2,由安全防护模块2对该子请求进行安全过滤。

[0057] 当目标域名的配置信息表征该域名处于拦截状态时,业务模块1则可以直接响应预设的拦截页面到客户端3。

[0058] 当目标域名的配置信息表征该域名处于正常状态时,判定该用户请求不需要进行安全检测,此时将用户请求发送到目标服务器4,并将接收到的目标服务器4返回的响应内容转发到客户端3,其中目标服务器4可以为业务模块1所在服务器的父节点或目标域名的源站。

[0059] 业务模块1在生成至少包括用户请求的请求头的子请求时,还可以判断用户请求

是否满足预设条件，若用户请求满足预设条件，则生成包括用户请求的请求头与请求体的子请求；若用户请求不满足预设条件，生成包括用户请求的请求头的子请求；即业务模块1能够针对不同的用户请求，生成不同的子请求，以便于安全防护模块2针对不同的用户请求进行不同的安全过滤。其中，预设条件包括用户请求支持请求体转发以及用户请求的请求体的大小小于或等于预设阈值。

[0060] 举例来说，业务模块1中可以配置需要进行安全检测的请求类型，例如GET请求、POST请求、HEAD请求等，从而在接收到的用户请求属于安全检测的请求类型时，判定用户请求需要进行安全检测，业务模块1中还配置了支持转发请求体的请求类型，例如为POST请求，业务模块1在判定用户请求需要进行安全检测时，先判断该用户请求的类型是否支持转发请求体，若该用户请求支持请求体转发，再判断用户请求的请求体的大小是否小于或等于预设阈值，若用户请求的请求体的大小小于或等于预设阈值，则生成包括该用户请求的请求头以及请求体的子请求；反之，在用户请求不支持请求体转发或者用户请求的请求体的大小大于预设阈值时，则生成包括用户请求的请求头的子请求。

[0061] 安全防护模块2用于对子请求进行安全过滤，并将得到的安全策略结果发送到业务模块。

[0062] 安全防护模块2作为WAF系统，在接收到业务模块1发送的子请求时，对该子请求进行安全过滤，检测方式包括URL的正则匹配、请求头的检验等等，从而能够检测出用户请求中是否存在SQL注入、XSS攻击、WEBSHELL攻击等等，并生成相应的安全策略结果，并将该安全策略结果返回到业务模块1。其中，安全策略结果可以表征用户请求处于通行状态或者是拦截状态，通行状态表示该用户请求中未包含攻击内容、拦截状态表示该用户请求中包含攻击内容，通行状态的安全策略结果中还可以包括重定向、限速等辅助策略；安全防护模块2可以在安全策略结果表征用户请求处于拦截状态时，生成攻击记录日志，该日志中包含完整的用户请求包、用户请求时间、请求IP、命中规则ID、攻击类型、规则库匹配到的攻击内容等信息，以便于后续对受到的攻击进行分析防范。

[0063] 业务模块1还用于根据安全策略结果，对用户请求进行响应。具体的，业务模块1在安全策略结果表征用户请求处于通行状态时，继续进行加速、缓存业务流程，将用户请求发送到目标服务器4，并将接收到的目标服务器4返回的响应内容作为用户请求的响应，即将该响应内容转发给客户端3；业务模块1在安全策略结果表征用户请求处于拦截状态时，将预设的拦截页面作为用户请求的响应，即将该拦截页面发送到客户端3，其中拦截页面上还可以包括http状态码403。

[0064] 本实施例中，若业务模块1为基于nginx的模块，则业务模快1可以基于nginx HTTP框架对用户请求进行分解得到多个子请求，从而能够得到包括用户请求的请求头的子请求；然后在安全防护模块2返回的安全策略结果表征用户请求处于通行状态时，利用upstream机制访问目标服务器4，并将目标服务器4返回的响应内容发送给客户端3。

[0065] 在一个例子中，业务模块1与安全防护模块2可以部署在一个融合服务器中，即安全防护系统部署在一个融合服务器上，以业务模块1为安装在该融合服务器上的nginx业务系统软件、安全防护模块2安装在该融合服务器上的nginx的WAF系统软件为例，融合服务器在利用业务系统软件提供基础的业务服务时，将WAF系统软件作为业务系统软件的子服务。其中，由业务系统软件来判断用户请求是否需要进行安全检测，WAF系统软件仅用于提供安

全过滤，从而仅需加载一份各域名的配置信息到服务器的内存中，WAF系统软件则无需加载各域名的配置信息到服务器的内存中，减少了对服务器内存的消耗，减小了部署在同一服务器中的WAF系统软件与业务系统软件之间的相互影响。

[0066] 服务器中部署有基于nginx动态模块机制的waflib库，该waflib库为业务系统软件与WAF系统软件之间交互的lib库，其用于用户请求的转发、拦截动作的执行以及响应拦截页面给客户端3等操作。

[0067] 在融合服务器中，将安全防护模块2作为业务模块1的子服务，来提供安全防护功能；并且安全防护模块2仅用于进行安全过滤，减小了安全防护模块2对融合服务器内存的消耗，降低了安全防护模块2与业务模块1之间的相互影响，使得同一服务器能够同时提供多种服务。

[0068] 请参考图4，为服务器与客户端3以及目标服务器4之间的交互时序图，本实施例中，用户通过客户端3向业务系统软件发起请求，将用户请求发送到业务系统软件，业务系统软件在接收到用户请求后读取用户请求中包含的目标域名的配置信息，并根据该配置信息，判断用户请求是否需要进行安全检测。若配置信息表征用户请求处于正常状态，则判定用户请求不需要进行安全检测，将用户请求转发到目标服务器4，目标服务器4获取用户请求对应的响应内容，并将该响应内容发送到业务系统软件，业务系统软件则将该响应内容发送给客户端3；若配置信息表征用户请求处于监控状态，则判定用户请求需要进行安全检测，生成至少包括用户请求的请求头的子请求，并该子请求发送到WAF系统软件，WAF系统软件则对该子请求进行安全过滤，得到安全策略结果，并将该安全策略结果发送到业务系统软件。

[0069] 业务系统软件在该安全策略结果表征用户请求处于通行状态时，将该用户请求转发给目标服务器4，目标服务器4获取用户请求对应的响应内容，并将该响应内容发送到业务系统软件，业务系统软件则将该响应内容发送给客户端3；业务系统软件在该安全策略结果表征用户请求处于拦截状态时，将预设的拦截页面作为用户请求的响应发送到客户端3。

[0070] 由于第一实施例与本实施例相互对应，因此本实施例可与第一实施例互相配合实施。第一实施例中提到的相关技术细节在本实施例中依然有效，在第一实施例中所能达到的技术效果在本实施例中也同样可以实现，为了减少重复，这里不再赘述。相应地，本实施例中提到的相关技术细节也可应用在第一实施例中。

[0071] 本实施方式相对于现有技术而言，业务模块能够在接收到的用户请求需要安全检测时，生成至少包括用户请求的请求头的子请求，并将该子请求发送到安全防护模块，安全防护模块则能够对该子请求进行安全过滤，并将得到的安全策略结果发送到业务模块，继而业务模块可以根据安全策略结果，对用户请求进行响应，即安全防护模块以旁路的方式提供安全防护服务，业务模块在执行自身业务时可以按需调用安全防护模块进行安全防护，提高了业务模块的利用率；同时，实现了安全防护服务与其他业务叠加，安全防护模块可以灵活部署；并且，子请求对内存占用较少，且不会一直占据进程资源，进一步减小了对资源的占用。

[0072] 本发明的第四实施方式涉及一种服务器，本实施方式相对于第三实施方式来说，主要区别之处在于：请参考图1与图6，在业务模块1中增加了对响应内容的安全检测。

[0073] 业务模块1还用于在接收到目标服务器4返回的响应内容时，对响应内容进行安全

检测,得到安全检测结果。

[0074] 本实施例中,可以在业务模块1中部署有基于nginx动态模块机制的waflib库,业务模块1可以调用该waflib库对响应内容进行安全检测。

[0075] 业务模块1还用于在安全检测结果表征响应内容为正常状态时,将响应内容作为用户请求的响应。

[0076] 业务模块1还用于在安全检测结果表征响应内容为异常状态时,将预设的拦截页面作为用户请求的响应。

[0077] 具体的,业务模块1在安全策略结果表征用户请求处于通行状态时,将该用户请求发送到目标服务器4,在接收目标服务器4返回的响应内容后,调用wiflib库对该响应内容进行安全检测,得到安全检测结果,安全检测结果表征响应内容为正常状态或异常状态。其中,安全检测内容包括:响应内容响应头以及响应体的增删改操作、web服务器响应错误信息(如服务器的版本等信息)、数据库名称等敏感信息、web程序异常抛出的敏感信息等。

[0078] 业务模块1在安全检测结果表征响应内容为正常状态时,将该响应内容作为用户请求的响应,即将该响应内容发送到客户端3;在安全检测结果表征响应内容为异常状态时,业务模块1则将预设的拦截页面发送到客户端3,并记录该响应内容的检测日志。

[0079] 由于第二实施例与本实施例相互对应,因此本实施例可与第二实施例互相配合实施。第二实施例中提到的相关技术细节在本实施例中依然有效,在第二实施例中所能达到的技术效果在本实施例中也同样可以实现,为了减少重复,这里不再赘述。相应地,本实施例中提到的相关技术细节也可应用在第二实施例中。

[0080] 本实施方式相对于第三实施方式而言,利用业务模块对响应内容的安全检测,即业务模块无需通过安全防护模块便能够直接进行响应内容的安全检测,减少了响应内容的转发操作,简化了安全检测流程。

[0081] 本领域的普通技术人员可以理解,上述各实施方式是实现本发明的具体实施例,而在实际应用中,可以在形式上和细节上对其作各种改变,而不偏离本发明的精神和范围。

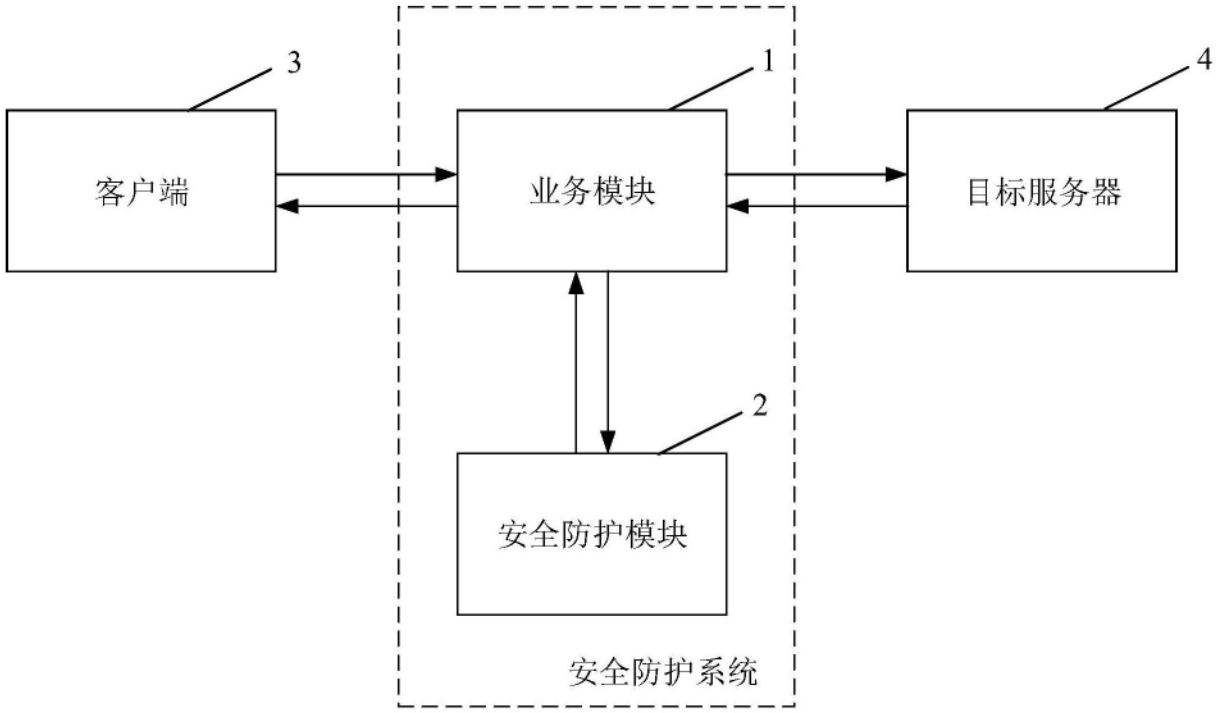


图1

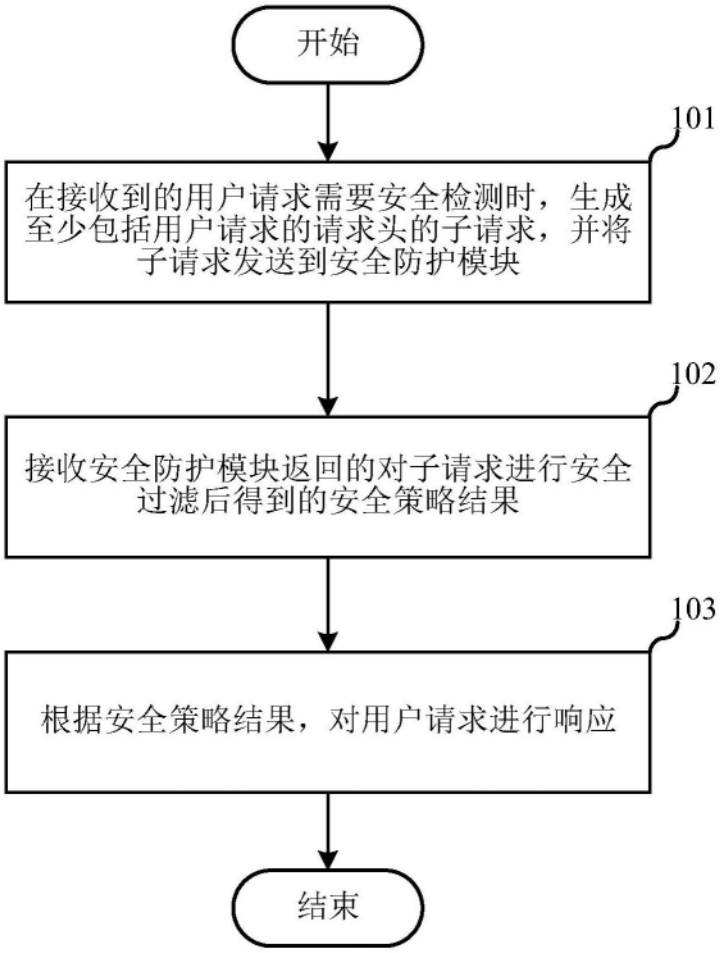

开始
101
在接收到的用户请求需要安全检测时，生成至少包括用户请求的请求头的子请求，并将子请求发送到安全防护模块
102
接收安全防护模块返回的对子请求进行安全过滤后得到的安全策略结果
103
根据安全策略结果，对用户请求进行响应
结束

图2

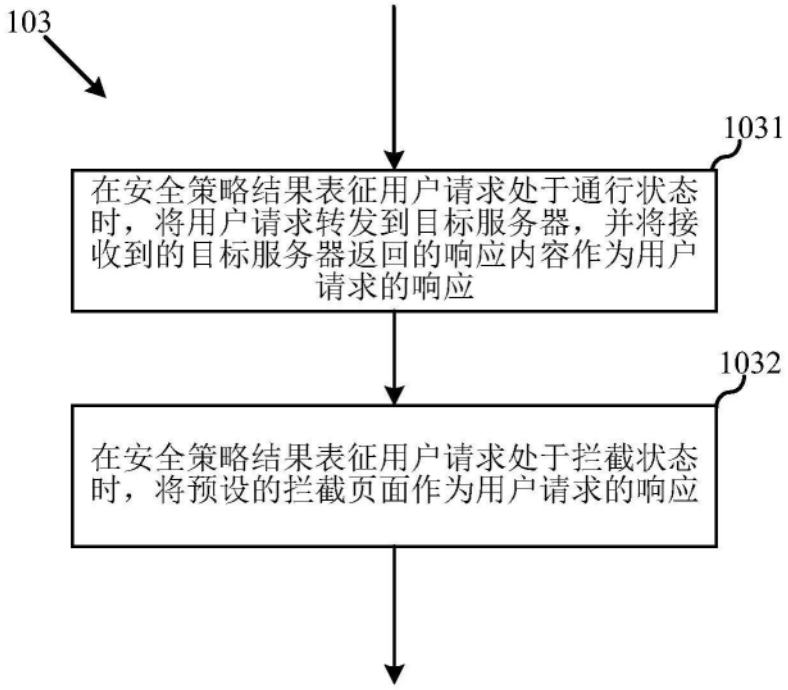

103
1031
在安全策略结果表征用户请求处于通行状态时，将用户请求转发到目标服务器，并将接收到的目标服务器返回的响应内容作为用户请求的响应
1032
在安全策略结果表征用户请求处于拦截状态时，将预设的拦截页面作为用户请求的响应

图3

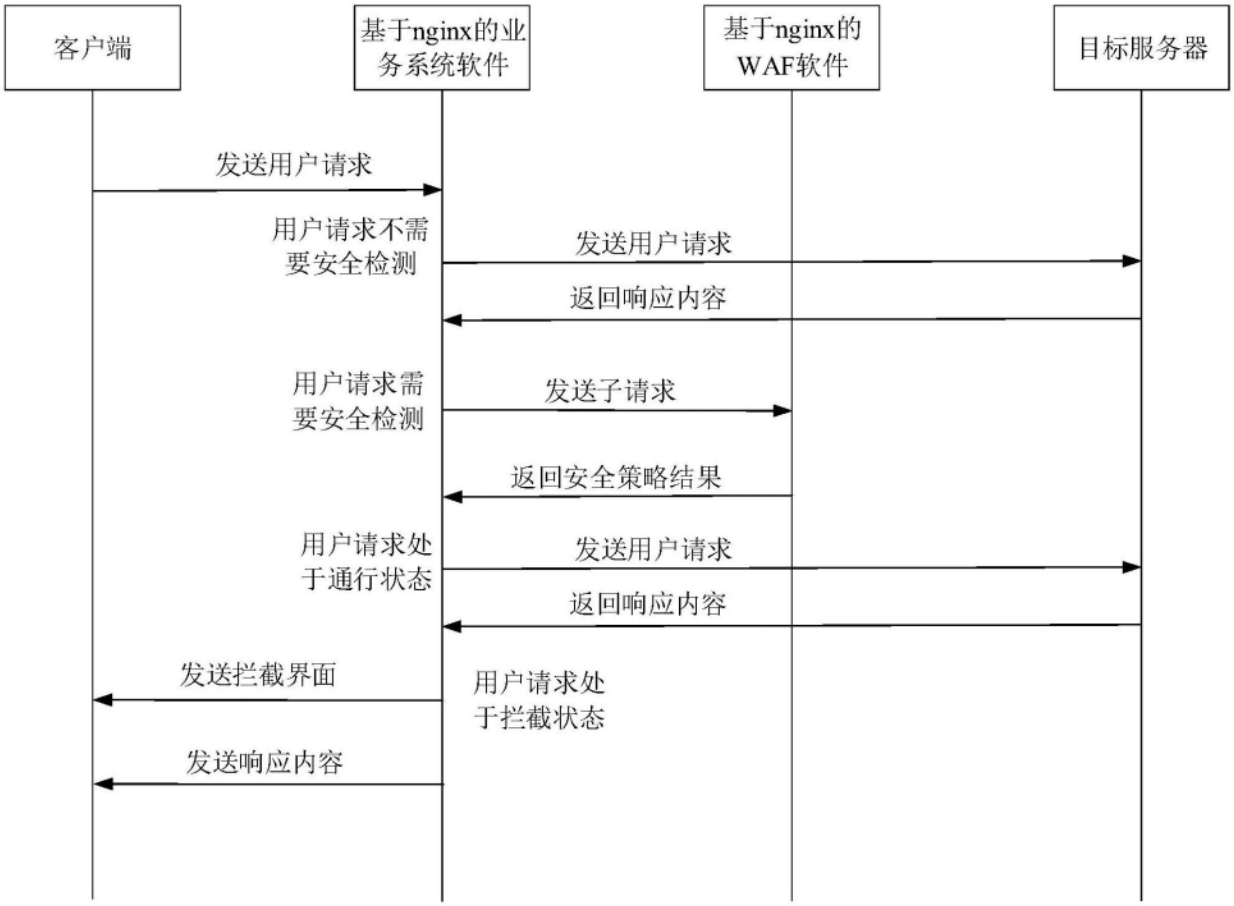

客户端
基于nginx的业务系统软件
基于nginx的WAF软件
目标服务器
发送用户请求
用户请求不需要安全检测
发送用户请求
返回响应内容
用户请求需要安全检测
发送子请求
返回安全策略结果
用户请求处于通行状态
发送用户请求
返回响应内容
发送拦截界面
用户请求处于拦截状态
发送响应内容

图4

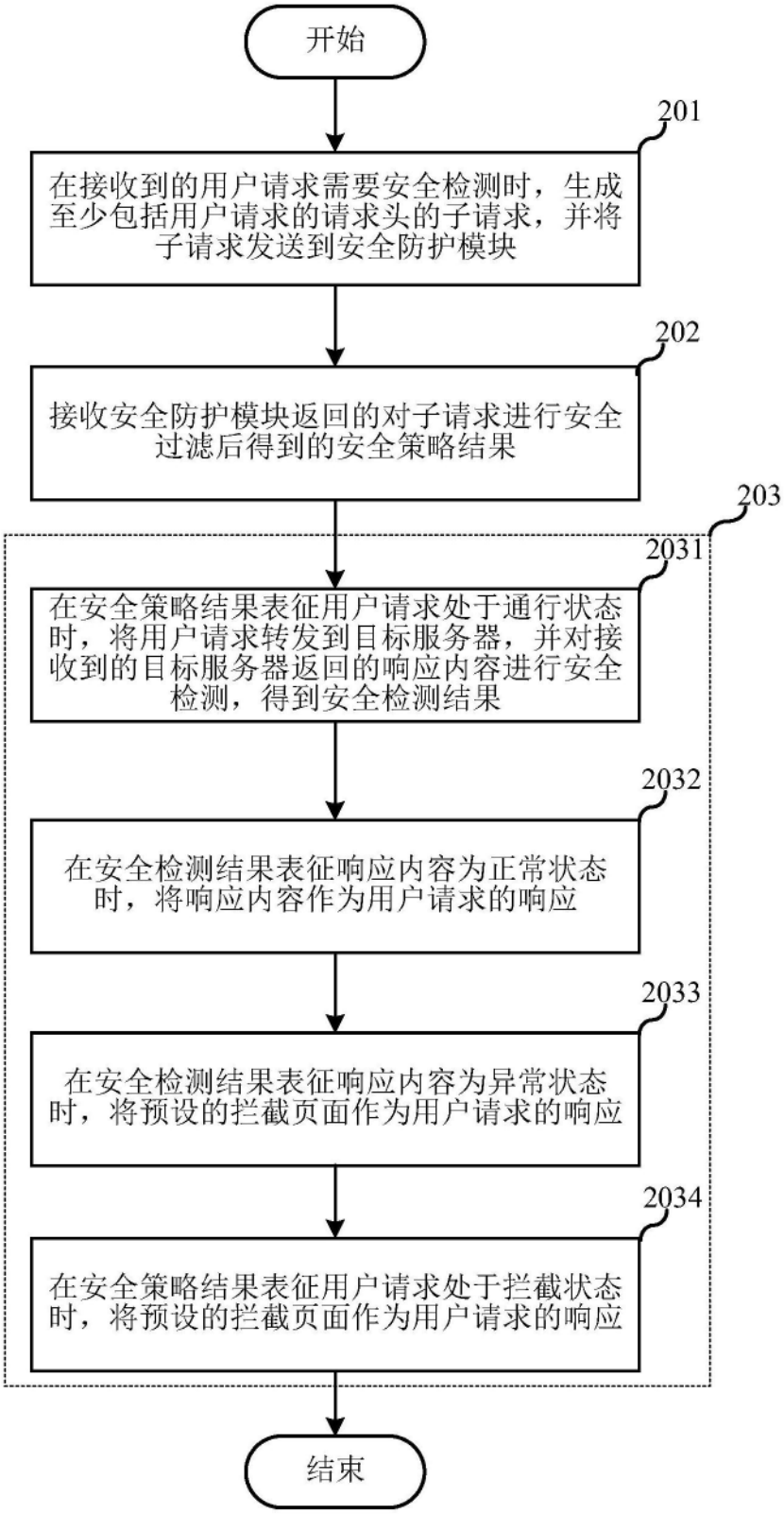

开始
201
在接收到的用户请求需要安全检测时，生成至少包括用户请求的请求头的子请求，并将子请求发送到安全防护模块
202
接收安全防护模块返回的对子请求进行安全过滤后得到的安全策略结果
203
2031
在安全策略结果表征用户请求处于通行状态时，将用户请求转发到目标服务器，并对接收到的目标服务器返回的响应内容进行安全检测，得到安全检测结果
2032
在安全检测结果表征响应内容为正常状态时，将响应内容作为用户请求的响应
2033
在安全检测结果表征响应内容为异常状态时，将预设的拦截页面作为用户请求的响应
2034
在安全策略结果表征用户请求处于拦截状态时，将预设的拦截页面作为用户请求的响应
结束

图5

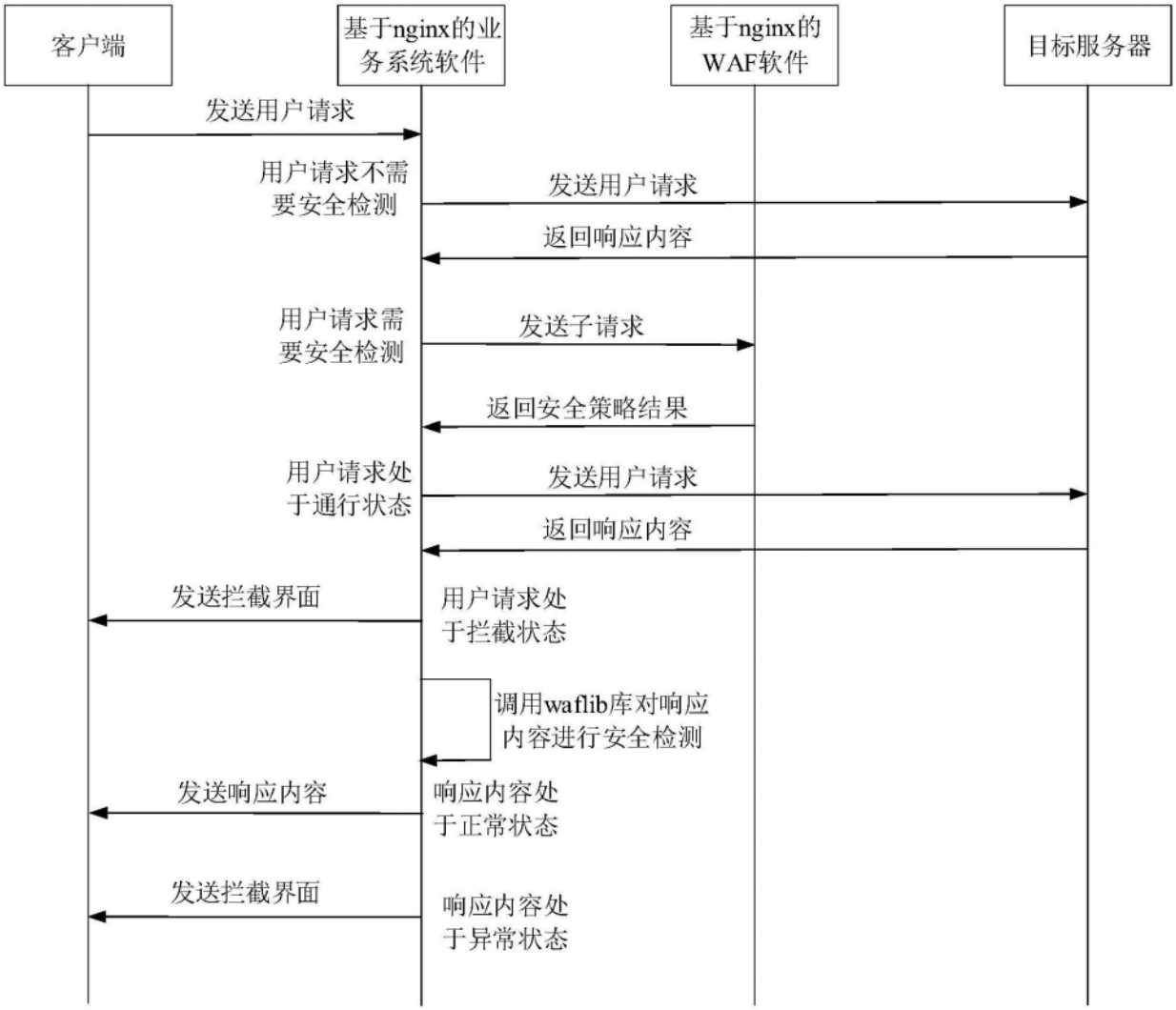

客户端
基于nginx的业务系统软件
基于nginx的WAF软件
目标服务器
发送用户请求
用户请求不需要安全检测
发送用户请求
返回响应内容
用户请求需要安全检测
发送子请求
返回安全策略结果
用户请求处于通行状态
发送用户请求
返回响应内容
发送拦截界面
用户请求处于拦截状态
调用waflib库对响应内容进行安全检测
发送响应内容
响应内容处于正常状态
发送拦截界面
响应内容处于异常状态

图6