(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 101902456 A
(43)申请公布日 2010.12.01

(21)申请号 201010110771.8

(22)申请日 2010.02.09

(71)申请人 北京启明星辰信息技术股份有限公司
地址 100193 北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦

(72)发明人 叶润国 周涛 胡振宇 孙海波

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 栗若木 王漪

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/12(2006.01)

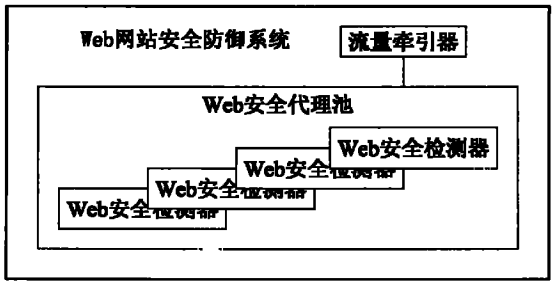
权利要求书 2 页 说明书 8 页 附图 4 页

(54)发明名称

一种 Web 网站安全防御系统

(57)摘要

一种 Web 网站安全防御系统，包括流量牵引器及 Web 安全检测器；所述流量牵引器与 DNS 服务器相连，用于从 DNS 服务器接收客户端的 DNS 域名解析请求，将该域名解析为所述 Web 安全检测器的 IP 地址，返回给所述客户端；所述 Web 安全检测器用于接收 HTTP 请求消息，对该 HTTP 请求消息进行入侵检测，如果未发现异常，则将该 HTTP 请求消息转发给该 HTTP 请求消息所指向的 Web 网站。本发明部署位置不受串行部署的限制，支持分布式部署，无需修改 Web 客户端和 Web 服务器配置，节省安全方面的成本，并且兼容性好，可伸缩性强。



CN 101902456 A

1. 一种 Web 网站安全防御系统，其特征在于，包括：

流量牵引器及 Web 安全检测器；

所述流量牵引器与 DNS 服务器相连，用于从 DNS 服务器接收客户端的 DNS 域名解析请求，将该域名解析为所述 Web 安全检测器的 IP 地址，返回给所述客户端；

所述 Web 安全检测器用于接收 HTTP 请求消息，对该 HTTP 请求消息进行入侵检测，如果未发现异常，则将该 HTTP 请求消息转发给该 HTTP 请求消息所指向的 Web 网站。

2. 如权利要求 1 所述的系统，其特征在于：

所述 Web 安全检测器包括一个或多个，各 Web 安全检测器的 IP 地址互不相同。

3. 如权利要求 2 所述的系统，其特征在于，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

所述流量牵引器保存各 Web 安全检测器的 IP 地址，从各 Web 安全检测器中选取负载最轻的 Web 安全检测器，将所述域名解析为该负载最轻的 Web 安全检测器的 IP 地址。

4. 如权利要求 2 所述的系统，其特征在于，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

所述流量牵引器保存各 Web 安全检测器的 IP 地址，将所述域名解析为所述各 Web 安全检测器所对应的 IP 地址的集合。

5. 如权利要求 2 所述的系统，其特征在于：

所述 Web 安全检测器分散部署在互联网中；

所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

所述流量牵引器保存各 Web 安全检测器的 IP 地址，将所述域名解析为距离发送所述 DNS 域名解析请求的客户端最近的 Web 安全检测器的 IP 地址。

6. 如权利要求 1 到 5 中任一项所述的系统，其特征在于：

所述 Web 安全检测器还用于接收 Web 网站返回的 HTTP 响应消息，对其中携带的 HTTP 文件对象进行内容安全扫描，如果未发现异常则将所述 HTTP 响应消息转发给该 HTTP 响应消息的目的客户端。

7. 如权利要求 1 到 5 中任一项所述的系统，其特征在于，还包括：

Web 安全日志库；

所述 Web 安全检测器还用于当发现异常时产生 Web 安全报警日志；

所述 Web 安全日志库用于接收来自 Web 安全检测器的 Web 安全报警日志并保存。

8. 如权利要求 1 到 5 中任一项所述的系统，其特征在于，所述 Web 安全检测器具体包括：

Web 代理模块，用于接收由客户端发往受保护 Web 服务器的 HTTP 请求消息，交给所述安全模块进行入侵检测，接收所述安全模块返回的入侵检测结果，如果该入侵检测结果为检测到 Web 攻击，则拒绝转发，否则转发该 HTTP 请求消息到该 HTTP 请求消息所指向的 Web 网站；以及当接收到来自 Web 网站的 HTTP 响应消息后，抽取出该 HTTP 响应消息中携带的 HTTP 文件对象，交给所述安全模块进行安全扫描，接收所述安全模块返回的安全扫描结果，如果该安全扫描结果为检测到恶意代码，则拒绝转发或用一个预先制作好的提示页面替换包含恶意代码的 HTML 页面后发给相应的客户端，否则转发该 HTTP 相应消息到相应的客户端；

所述安全模块用于当收到所述 Web 代理模块发送的 HTTP 请求消息时，对该 HTTP 请求

消息进行入侵检测，返回入侵检测结果；当收到所述Web代理模块发送的HTTP文件对象时，对该HTTP文件对象进行安全扫描，返回安全扫描结果。

9. 如权利要求1到5中任一项所述的系统，其特征在于，所述流量牵引器具体包括：

DNS服务模块及网站域名注册模块。

所述DNS服务模块用于从DNS服务器接收客户端发送来的DNS域名解析请求，将该域名解析为所述Web安全检测器的IP地址，返回给所述客户端；

所述网站域名注册模块用于对所有受保护的Web网站的注册，当一个受保护的Web网站被注册成功后，记录该Web网站的域名及其对应的IP地址。

10. 如权利要求9所述的系统，其特征在于，

所述Web安全检测器转发所述HTTP请求消息时，根据该HTTP请求消息中的目标域名查询所述网站域名注册模块的记录，找到该域名对应的IP地址，将所述HTTP请求消息转发到所找到的IP地址。

一种 Web 网站安全防御系统

技术领域

[0001] 本发明涉及网络安全领域，具体涉及一种 Web 网站安全防御系统。

背景技术

[0002] 中国互联网络信息中心 (CNNIC) 发布的《第 23 次中国互联网络发展状况统计报告》显示，截至 2008 年底，中国的网站数达到 287.8 万个。2008 年中国网站数较 2007 年增长 91.4%，是 2000 年以来增长最快的一年。截至 2008 年底，中国网页总数超过 160 亿个，较 2007 年增长 90%。网页的增长速度与网站的增速基本一致。

[0003] 但与此同时，国内 Web 网站的安全状况堪忧。据不完全统计，国内有 60%以上的网站都存在 Web 安全漏洞，包括各种 SQL 注入漏洞、跨站脚本攻击漏洞等，并且很多网站已经遭受到各种 Web 攻击，例如网页被挂马、网站 SQL 注入、网页被篡改等等，并且这种 Web 攻击趋势正在愈演愈烈。

[0004] 为保障 Web 网站的安全，有经济实力的企事业单位一般都购买和部署专门的 Web 安全网关（一般也成为 Web 应用防火墙，以下简称为 Web 应用防火墙）来防御针对其 Web 网站的安全攻击。Web 应用防火墙属于一种网关型设备，它作为 Web 服务器安全的最后一道防线，以串接方式部署在 Web 服务器的最前面，扫描进入 Web 服务器的所有 HTTP 请求，当发现针对 Web 服务器的恶意入侵时，将阻止该 HTTP 请求提交到后台的 Web 服务器，从而最大限度的保障 Web 服务器的安全。与此同时，一些 Web 应用防火墙还对返回给 Web 客户端的 HTML 页面进行内容扫描，当发现恶意代码时，将阻止该 HTML 页面发送到 Web 客户端，从而保障 Web 客户端免遭恶意代码的侵袭。

[0005] Web 应用防火墙能够在很大程度上保障 Web 网站的安全，但是，常见的 Web 应用防火墙都是网关设备，它以串行方式部署在 Web 服务器的前面，形成一种各自为政的 Web 网站安全防御架构（如图 1 所示）。

[0006] 但是，这种各自为政的 Web 网站安全防御架构在实际应用中会带来很多限制，这主要表现在以下几个方面：

[0007] 当前的 Web 应用防火墙都是网关设备，它必须以串行方式部署在 Web 网站的前面，这种部署上的限制在现实情况中导致很多不便；

[0008] 当前，很多企业为了业务上的方便，部署了多个 Web 网站，并且，这些 Web 网站分布在不同的地方，这样他们不得不为每个网站购买一个 Web 应用防火墙设备来保障其各个网站的安全，这将导致在安全方面的巨大开销；

[0009] 由于经费方面的限制，成千上万的企业是通过租用 IDC(Internet DataCenter，互联网数据中心）的 Web 空间来构建其 Web 网站的，没有财力去购买这种几万元的 Web 应用防火墙来保障其 Web 网站的安全。

发明内容

[0010] 本发明要解决的技术问题是提供一种 Web 网站安全防御系统，部署位置不受串行

部署的限制，支持分布式部署，无需修改 Web 客户端和 Web 服务器配置，节省安全方面的成本，并且兼容性好，可伸缩性强。

[0011] 为了解决上述问题，本发明提供了一种 Web 网站安全防御系统，包括：

[0012] 流量牵引器及 Web 安全检测器；

[0013] 所述流量牵引器与 DNS 服务器相连，用于从 DNS 服务器接收客户端的 DNS 域名解析请求，将该域名解析为所述 Web 安全检测器的 IP 地址，返回给所述客户端；

[0014] 所述 Web 安全检测器用于接收 HTTP 请求消息，对该 HTTP 请求消息进行入侵检测，如果未发现异常，则将该 HTTP 请求消息转发给该 HTTP 请求消息所指向的 Web 网站。

[0015] 进一步地，所述 Web 安全检测器包括一个或多个，各 Web 安全检测器的 IP 地址互不相同。

[0016] 进一步地，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

[0017] 所述流量牵引器保存各 Web 安全检测器的 IP 地址，从各 Web 安全检测器中选取负载最轻的 Web 安全检测器，将所述域名解析为该负载最轻的 Web 安全检测器的 IP 地址。

[0018] 进一步地，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

[0019] 所述流量牵引器保存各 Web 安全检测器的 IP 地址，将所述域名解析为所述各 Web 安全检测器所对应的 IP 地址的集合。

[0020] 进一步地，所述 Web 安全检测器分散部署在互联网中；

[0021] 所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

[0022] 所述流量牵引器保存各 Web 安全检测器的 IP 地址，将所述域名解析为距离发送所述 DNS 域名解析请求的客户端最近的 Web 安全检测器的 IP 地址。

[0023] 进一步地，所述 Web 安全检测器还用于接收 Web 网站返回的 HTTP 响应消息，对其中携带的 HTTP 文件对象进行内容安全扫描，如果未发现异常则将所述 HTTP 响应消息转发给该 HTTP 响应消息的目的客户端。

[0024] 进一步地，所述的系统还包括：

[0025] Web 安全日志库；

[0026] 所述 Web 安全检测器还用于当发现异常时产生 Web 安全报警日志；

[0027] 所述 Web 安全日志库用于接收来自 Web 安全检测器的 Web 安全报警日志并保存。

[0028] 进一步地，所述 Web 安全检测器具体包括：

[0029] Web 代理模块，用于接收由客户端发往受保护 Web 服务器的 HTTP 请求消息，交给所述安全模块进行入侵检测，接收所述安全模块返回的入侵检测结果，如果该入侵检测结果为检测到 Web 攻击，则拒绝转发，否则转发该 HTTP 请求消息到该 HTTP 请求消息所指向的 Web 网站；以及当接收到来自 Web 网站的 HTTP 响应消息后，抽取出该 HTTP 响应消息中携带的 HTTP 文件对象，交给所述安全模块进行安全扫描，接收所述安全模块返回的安全扫描结果，如果该安全扫描结果为检测到恶意代码，则拒绝转发或用一个预先制作好的提示页面替换包含恶意代码的 HTML 页面后发给相应的客户端，否则转发该 HTTP 相应消息到相应的客户端；

[0030] 所述安全模块用于当收到所述 Web 代理模块发送的 HTTP 请求消息时，对该 HTTP

请求消息进行入侵检测，返回入侵检测结果；当收到所述 Web 代理模块发送的 HTTP 文件对象时，对该 HTTP 文件对象进行安全扫描，返回安全扫描结果。

[0031] 进一步地，所述流量牵引器具体包括：

[0032] DNS 服务模块及网站域名注册模块。

[0033] 所述 DNS 服务模块用于从 DNS 服务器接收客户端发送来的 DNS 域名解析请求，将该域名解析为所述 Web 安全检测器的 IP 地址，返回给所述客户端；

[0034] 所述网站域名注册模块用于对所有受保护的 Web 网站的注册，当一个受保护的 Web 网站被注册成功后，记录该 Web 网站的域名及其对应的 IP 地址。

[0035] 进一步地，所述 Web 安全检测器转发所述 HTTP 请求消息时，根据该 HTTP 请求消息中的目标域名查询所述网站域名注册模块的记录，找到该域名对应的 IP 地址，将所述 HTTP 请求消息转发到所找到的 IP 地址。

[0036] 本发明的技术方案不受传统 Web 应用防火墙部署位置的限制，允许为多个 Web 网站同时提供 Web 安全防护，可以大大节省企业在安全方面的开销；也允许有实力的安全服务公司部署一个公共的 Web 网站安全防御系统，使得成千上万的中小企业网站可以租用该公共 Web 安全防御系统提供的 Web 安全防御服务来保障其 Web 网站的安全，也可大大节约费用开支；而且本发明的 Web 网站安全防御系统对 Web 客户端和受保护的 Web 网站来说是透明的，无须对 Web 客户端和受保护的 Web 网站程序代码进行任何修改，兼容性好；另外，本发明所述开放式 Web 网站安全防御系统伸缩性强，可以根据需要本系统增加或减少 Web 安全检测器。

附图说明

[0037] 图 1 为传统的 Web 网站安全防御的架构示意图；

[0038] 图 2 为实施例一的 Web 网站安全防御系统的架构示意图；

[0039] 图 3 为实施例一的 Web 网站安全防御系统的结构示意图；

[0040] 图 4 为实施例一中包含 Web 安全日志库的 Web 网站安全防御系统的结构示意图；

[0041] 图 5 为实施例一的 Web 网站安全防御系统中 Web 安全检测器的结构示意图；

[0042] 图 6 为实施例一的 Web 网站安全防御系统中流量牵引器的结构示意图；

[0043] 图 7 为实施例一中，某 Web 客户端访问 Web 网站安全防御系统保护的 Web 网站的流程示意图；

[0044] 图 8 为实施例一中，某 Web 客户端访问受保护 Web 网站过程的实例。

具体实施方式

[0045] 下面将结合附图及实施例对本发明的技术方案进行更详细的说明。

[0046] 实施例一，一种 Web 网站安全防御系统，如图 2 所示，设置于公共互联网中、Web 客户端和受保护的 Web 网站之间，以使得 Web 客户端用户——不管是正常用户还是恶意用户——通过该 Web 网站安全防御系统来访问受保护的 Web 网站。

[0047] 本实施例的 Web 网站安全防御系统采用 DNS 接管技术来实现 HTTP 流量的流量牵引，使得原本直接发往受保护 Web 网站的所有 HTTP 流量必须先流经本实施例提供的 Web 网站安全防御系统后再发往受保护 Web 网站，这样，本实施例的 Web 网站安全防御系统有机会

对所有发往受保护 Web 网站的 HTTP 流量进行安全检测。由于采用了流量牵引技术，因此，在物理网络连接上并不要求该 Web 网站安全防御系统串联到 Web 客户端和受保护的 Web 网站之间，它可以部署在互联网上任何位置。

[0048] 本实施例的 Web 网站安全防御系统作为 Web 客户端和 Web 服务器之间的访问中介真实存在，但对 Web 客户端和 Web 服务器两端来说都是透明的，它犹如一朵漂浮在互联网络上的“云”，负责检测 Web 客户端和受保护 Web 网站之间的所有 HTTP 流量。本实施例的 Web 网站安全防御系统可以在传统的分布式计算平台上实施，也可以采用最新的基于互联网的分布式计算平台实现，比如“云计算”平台。

[0049] 本实施例的 Web 网站安全防御系统类似于一个 HTTP 流量的“集散中心”，采用 DNS 接管技术来实现对所有发往受保护 Web 网站的 HTTP 流量的“集散”，使得所有原本直接发往受保护 Web 网站的 HTTP 流量必须先在开放式 Web 网站安全防御系统“聚集”后，经过安全扫描再“分发”到受保护的 Web 网站；这样，将有机会对转发的 HTTP 请求消息和 HTTP 响应消息进行安全检查。

[0050] 本实施例的所述 Web 网站安全防御系统如图 3 所示，包括：

[0051] 流量牵引器及 Web 安全检测器；

[0052] 所述流量牵引器与 DNS 服务器相连，用于从 DNS 服务器接收客户端的 DNS 域名解析请求，将该域名解析为所述 Web 安全检测器的 IP 地址，返回给所述客户端；可以直接返回，也可通过所述 DNS 服务器或其它设备返回；

[0053] 所述 Web 安全检测器用于接收 HTTP 请求消息，对该 HTTP 请求消息进行入侵检测，如果未发现异常，则将该 HTTP 请求消息转发给该 HTTP 请求消息所指向的 Web 网站。

[0054] 本实施例的所述流量牵引器将原本从 Web 客户端直接发往受保护 Web 网站的 HTTP 流量“牵引”至本发明所述 Web 网站安全防御系统；所述 Web 安全检测器作为 Web 客户端和受保护 Web 网站之间的数据传输代理，基于应用层代理技术创建从 Web 客户端到指定的 Web 网站的数据传输通道，转发 Web 客户端和受保护 Web 网站之间的所有安全的 HTTP 流量。

[0055] 本实施例中的 Web 安全检测器并不同于传统的 Web 代理，传统的 Web 代理在使用时对用户来说是不透明的，需要 Web 客户端知道 Web 代理的 IP 地址。而本实施例中的 Web 安全检测器对 Web 客户端来说是透明的，无需 Web 客户端做任何配置的修改；在 Web 访问中，Web 客户端通过域名解析得到 Web 安全检测器的 IP 地址；因此，从 Web 客户的角度来看，Web 客户要访问的 Web 网站好像是在 Web 安全检测器上，可以像平常一样采用 HTTP 协议访问 Web 安全检测器。

[0056] 当使用了本实施例的 Web 网站安全防御系统后，为防止恶意 Web 客户端绕过该 Web 网站安全防御系统直接对受保护的 Web 网站发起攻击，Web 网站管理员可以对其 Web 网站服务器做一些限制措施，比如可以限制受保护的 Web 网站只接收来自本实施例的 Web 网站防御系统转发的 HTTP 请求消息，也可以限制受保护 Web 网站只接收携带了本实施例的 Web 网站防御系统签名的 HTTP 流量，从而对这些 Web 网站进行安全防御。

[0057] 本实施例中，所述 Web 安全检测器包括一个或多个，各 Web 安全检测器的 IP 地址互不相同；可以但不限于采用 Web 安全检测器池存放该一个或多个 Web 安全检测器。

[0058] 本实施例中，所述 Web 安全检测器池中的 Web 安全检测器可以根据需要进行添加和删除，而不影响本 Web 网站安全防御系统的正常工作，只要保证至少存在一个 Web 安全检

测器即可。

[0059] 本实施例的一种实施方式中，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

[0060] 所述流量牵引器保存各 Web 安全检测器的 IP 地址，从各 Web 安全检测器中选取负载最轻的 Web 安全检测器，将所述域名解析为该负载最轻的 Web 安全检测器的 IP 地址。

[0061] 本实施例的另一种实施方式中，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

[0062] 所述流量牵引器保存各 Web 安全检测器的 IP 地址，将所述域名解析为所述各 Web 安全检测器所对应的 IP 地址的集合。

[0063] 本实施例的又一种实施方式中，所述 Web 安全检测器可以分散部署在互联网中；该实施方式中，所述流量牵引器将域名解析为所述 Web 安全检测器的 IP 地址具体包括：

[0064] 所述流量牵引器保存各 Web 安全检测器的 IP 地址，将所述域名解析为距离发送所述 DNS 域名解析请求的客户端最近的 Web 安全检测器的 IP 地址，从而提高整个系统的工作效率。

[0065] 在本实施例中，为实现将距离最近的 Web 安全检测器的 IP 地址返回给发送所述 DNS 域名解析请求的客户端，可以依据公知的 IP 地址分配表来实现，原则是尽量确保发送 DNS 域名解析请求的客户端和为其服务的 Web 安全检测器在同一个网络管理域中。比如，如果发现该 DNS 请求来自中国电信网络，并且在中国电信网络上存在本实施例中所述的 Web 安全检测器，则返回部署在中国电信网络上的某一个或多个 Web 安全检测器的对应 IP 地址作为本次 DNS 域名解析结果。

[0066] 本实施例中，所述 Web 安全检测器还用于接收 Web 网站返回的 HTTP 响应消息，对其中携带的 HTTP 文件对象进行内容安全扫描，如果未发现异常则将所述 HTTP 响应消息转发给相应的客户端，即该 HTTP 响应消息的目的客户端。

[0067] 所述 HTTP 文件对象包括 HTML 网页和任何可能包含恶意代码的文件或文档。所述 Web 安全检测器可以采用公知的任意恶意代码检测技术对文件内容进行扫描。

[0068] 本实施例中，所述 Web 安全检测器在对接收到的来自 Web 客户端的 HTTP 请求进行入侵检测时，检测内容包括但不限于 SQL 注入攻击和跨站脚本攻击等内容。在具体实施时，可以采用公知的任意 SQL 注入攻击和跨站脚本攻击检测算法来实现。

[0069] 本实施例中，如果所述 Web 安全检测器在进行安全扫描 / 入侵检测时发现异常，则不进行转发。所述 Web 安全检测器当发现 HTTP 响应消息中包含的 HTML 页面包含恶意代码时，也可以用一个提示页面替换原先的包含恶意代码的 HTML 页面，还可以进一步可通过电子邮件等方式通知该 Web 网站管理人员，以便该 Web 网站管理人员能够及时对该 HTML 页面进行修复。

[0070] 本实施例中，如图 4 所示，所述 Web 网站安全防御系统还可以包括一个 Web 安全日志库；

[0071] 所述 Web 安全检测器还用于当发现异常时产生 Web 安全报警日志；

[0072] 所述 Web 安全日志库用于接收并保存来自 Web 安全检测器的 Web 安全报警日志，并允许受保护 Web 网站的网站管理员获取其 Web 网站相关的安全日志记录信息，从而在其 Web 网站出现安全问题时，可以基于这些 Web 安全日志进行事后的取证分析。

[0073] 本实施例中，所述 Web 安全检测器如图 5 所示，包括：安全模块和 Web 代理模块；

[0074] 所述 Web 代理模块用于接收由客户端发往受保护 Web 服务器的 HTTP 请求消息，交给所述安全模块进行入侵检测，接收所述安全模块返回的入侵检测结果，如果该入侵检测结果为检测到 Web 攻击，则拒绝转发，否则转发该 HTTP 请求消息到该 HTTP 请求消息所指向的 Web 网站；以及当接收到来自 Web 网站的 HTTP 响应消息后，抽取出该 HTTP 响应消息中携带的 HTTP 文件对象，交给所述安全模块进行安全扫描，接收所述安全模块返回的安全扫描结果，如果该安全扫描结果为检测到恶意代码，则拒绝转发或用一个预先制作好的提示页面替换包含恶意代码的 HTML 页面后发给相应的客户端，否则转发该 HTTP 相应消息到相应的客户端；

[0075] 所述安全模块用于当收到所述 Web 代理模块发送的 HTTP 请求消息时，对该 HTTP 请求消息进行入侵检测，返回入侵检测结果；当收到所述 Web 代理模块发送的 HTTP 文件对象时，对该 HTTP 文件对象进行安全扫描，返回安全扫描结果。

[0076] 本实施例中，所述流量牵引器如图 6 所示，包括：DNS 服务模块及网站域名注册模块。

[0077] 所述 DNS 服务模块用于模拟一个标准的 DNS 服务，并执行对所有受保护 Web 网站域名的 DNS 解析任务；从外部的 DNS 服务器接收客户端发送来 DNS 域名解析请求，将该域名解析为所述 Web 安全检测器的 IP 地址，然后返回给所述客户端。

[0078] 与标准 DNS 服务不同的是，所述 DNS 服务模块在解析受保护 Web 网站域名时，返回的并不是该 Web 网站域名所对应的真实 IP 地址，而是 Web 安全检测器池中某一 Web 安全检测器所对应的单个 IP 地址或者是一组 Web 安全检测器所对应的 IP 地址集合，这样，任何 Web 客户端使用 Web 网站域名访问受保护 Web 网站时，会把原本直接发往受保护 Web 网站的 HTTP 流量首先发给某一 Web 安全检测器，这样该 Web 安全检测器有机会对提交到受保护 Web 网站的 HTTP 请求消息进行入侵检测，以及对返回的 HTTP 响应消息中携带的 HTTP 文件对象进行内容安全检测。

[0079] 具体实施过程中，所述 DNS 服务模块在解析受保护 Web 网站域名时，可以采用两种实施方式：1) DNS 服务模块将 Web 安全检测器池中所有 Web 安全检测器的 IP 地址列表作为 DNS 域名解析结果返回给 Web 客户端，由 Web 客户端从中挑选一个 Web 安全检测器执行本次 Web 访问任务；2) 流量牵引器通过与 Web 安全检测器池通信，得到当前 Web 安全检测器池中负载最轻的 Web 安全检测器、或距离发送所述 DNS 域名解析请求的客户端最近的 Web 安全检测器，然后将该 Web 安全检测器的 IP 地址作为 DNS 域名解析结果返回给 Web 客户端。

[0080] 所述网站域名注册模块用于对所有受保护的 Web 网站的注册管理。网站域名注册模块负责完成对所有受保护网站的注册工作；可以维护一个“域名 - 真实 IP 列表”，当一个受保护的 Web 网站被注册成功后，网站域名注册模块为该 Web 网站在所述“域名 - 真实 IP 列表”中创建一条记录，记录该 Web 网站的域名及其对应的真实 IP 地址。实际应用时，可以用“域名 - 真实 IP 列表”之外的方式来记录 Web 网站的域名及其对应的真实 IP 地址。

[0081] 实际应用中，也可以采用其它形式保存网站域名所对应的真实 IP 地址。

[0082] 所述 Web 安全检测器在转发发往受保护 Web 网站的 HTTP 请求消息时，根据所述 HTTP 请求消息中的 HOST 字符串得到该 HTTP 请求消息所指向的 Web 网站的域名；查询所述“域名 - 真实 IP 列表”，以得到该域名对应的真实 IP 地址，这样，Web 安全检测器就能够转

发所述 HTTP 请求消息到所找到的 IP 地址，即：Web 安全检测器创建到该 HTTP 请求消息所指向的 Web 网站的 TCP 连接，然后再转发所述 HTTP 请求消息到该 HTTP 请求消息所指向的 Web 网站。

[0083] 为了确保针对受保护 Web 网站域名的所有 DNS 域名解析请求能够转发到本发明所述流量牵引器中的 DNS 服务模块，需要简单地调整原先负责解析受保护 Web 网站域名的外部 DNS 服务器的配置，要求该外部 DNS 服务器将所有针对受保护 Web 网站域名的 DNS 请求转发到本发明所述流量牵引器中的 DNS 服务模块。

[0084] 本实施例的一种实施方式中，所述流量牵引器还用于保存各受保护 Web 网站的域名，从所述外部 DNS 服务器接收所有 DNS 域名解析请求，接收后先判断请求解析的域名是否与所保存的受保护 Web 网站的域名之一匹配；如果匹配，则进行解析；否则返回给 DNS 服务器解析。

[0085] 如图 7 所示，一个 Web 客户端使用 Web 网站域名访问受保护 Web 网站实例的具体流程如下：

[0086] 701、Web 客户端向原先的负责解析受保护 Web 网站域名的外部 DNS 服务器发送 DNS 域名解析请求；

[0087] 702、该外部 DNS 服务器将当前 DNS 域名解析请求转发到所述流量牵引器；

[0088] 703、所述流量牵引器中的 DNS 服务模块负责对该受保护 Web 网站域名进行解析，它与 Web 安全检测器池通信，获得当前池中负载最轻的 Web 安全检测器，并将该 Web 安全检测器所对应的 IP 地址作为本次 DNS 域名解析结果返回给 Web 客户端；

[0089] 704、Web 客户端建立起到所选 Web 安全检测器的 TCP 连接，并发送 HTTP 请求消息到所选 Web 安全检测器；

[0090] 705、所选 Web 安全检测器接收到 HTTP 请求消息后，对当前 HTTP 请求消息执行入侵检测；

[0091] 706、所选 Web 安全检测器依据入侵检测结果执行下一步动作：如果发现 Web 攻击，则执行步骤 712；否则执行步骤 707；

[0092] 707、所选 Web 安全检测器从当前 HTTP 请求消息的“HOST”域中取出 Web 客户端需要访问的 Web 网站域名，查找流量牵引器中维护的“域名 - 真实 IP 列表”得到该 Web 网站域名所对应的真实 IP 地址，创建到该 Web 网站所在服务器的 TCP 连接，并转发当前 HTTP 请求消息到该 Web 网站所在服务器；

[0093] 708、所选 Web 安全检测器等待并接收从受保护 Web 网站服务器返回的 HTTP 响应消息，并从当前 HTTP 响应消息中抽取出 HTTP 文件对象，对其进行内容安全扫描；

[0094] 709、依据扫描结果决定下一步动作：如果没有检测到恶意代码，则执行步骤 710；如果检测到恶意代码，则执行步骤 711；

[0095] 710、直接转发当前 HTTP 响应消息到 Web 客户端，结束；

[0096] 711、丢弃当前 HTTP 响应消息，转发一个包含有预先制作的带有警告信息的 HTML 页面的 HTTP 响应消息给 Web 客户端，结束；

[0097] 712、拒绝转发该 HTTP 请求消息，终止当前 TCP 连接，结束。

[0098] 图 8 给出了另一个实例，举例说明某 Web 客户端是如何通过受保护 Web 网站域名访问受保护 Web 网站的。这里假设受本文所述开放式 Web 网站安全防御系统保护的两个

Web 网站的域名分别为 www.abc.com 和 www.def.com，这两个 Web 网站所对应的真实 IP 地址分别为 3.3.3.3 和 4.4.4.4；假设负责这两个 Web 网站域名解析的 DNS 服务器为图 8 中的“外部 DNS 服务器”；在该实例中存在两台 Web 安全检测器，其 IP 地址分别为 1.1.1.1 和 2.2.2.2。为了使得“Web 网站 1”和“Web 网站 2”能够受到本发明所述开放式 Web 安全防御系统的保护，它们的网站管理员将这两个 Web 网站的网站域名和网站服务器的真实 IP 地址信息向本发明所述 Web 网站安全防御系统中的流量牵引器进行注册，并修改了原先负责为“Web 网站 1”和“Web 网站 2”进行 DNS 域名解析的“外部 DNS 服务器”的配置，使得针对“Web 网站 1”和“Web 网站 2”网站域名的所有 DNS 域名解析请求都发送到本发明所述开放式 Web 安全防御系统中的流量牵引器。

[0099] 现在来看看某客户端是如何使用 Web 网站域名访问受本发明所述开放式 Web 网站安全防御系统保护的“Web 网站 1”（假设其网站域名为 www.abc.com）。

[0100] 801、Web 客户端向原先的“外部 DNS 服务器”发起针对“Web 网站 1”域名 (www.abc.com) 的 DNS 域名解析请求；

[0101] 802、该 DNS 域名解析请求被转发到本发明所述开放式 Web 网站安全防御系统中的流量牵引器；

[0102] 803、所述流量牵引器中的 DNS 服务模块接收到针对受保护 Web 网站域名的 DNS 域名解析请求后，与所述系统中的 Web 安全检测器池进行通信，获得当前系统中负载最轻的 Web 安全检测器为“Web 安全检测器 1”，于是将“Web 安全检测器 1”的 IP 地址 (1.1.1.1) 作为本次域名解析结果返回给 Web 客户端；

[0103] 804、Web 客户端发起对“Web 安全检测器 1”的 TCP 连接请求，在 TCP 连接请求建立成功后，发送一个 HTTP 请求消息给“Web 安全检测器 1”；

[0104] 805、“Web 安全检测器 1”接收到该 HTTP 请求消息后，首先对该 HTTP 请求消息进行入侵检测，检测结果为没有发现 Web 攻击，因此，“Web 安全检测器 1”从当前 HTTP 请求消息的 HOST 域中提取“Web 网站 1”的真实域名 (www.abc.com)，然后查找所述系统中流量牵引器的“域名 - 真实 IP 列表”，得到 www.abc.com 域名所对应的真实 IP 地址为 3.3.3.3，最后，“Web 安全检测器 1”创建到“Web 网站 1”主机（地址为 3.3.3.3）的 TCP 连接，并将当前 HTTP 请求消息转发给“Web 网站 1”。

[0105] 806、“Web 安全检测器 1”接收从“Web 网站 1”服务器返回的 HTTP 响应消息，提出其中携带的 HTTP 文件对象，并对其进行内容安全扫描，扫描结果提示发现恶意代码，因此替换该 HTTP 文件对象为一个包含告警信息的 HTML 页面；

[0106] 807、“Web 安全检测器 1”转发替换后的 HTTP 响应消息到 Web 客户端，整个过程结束。

[0107] 当然，本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明的权利要求的保护范围。

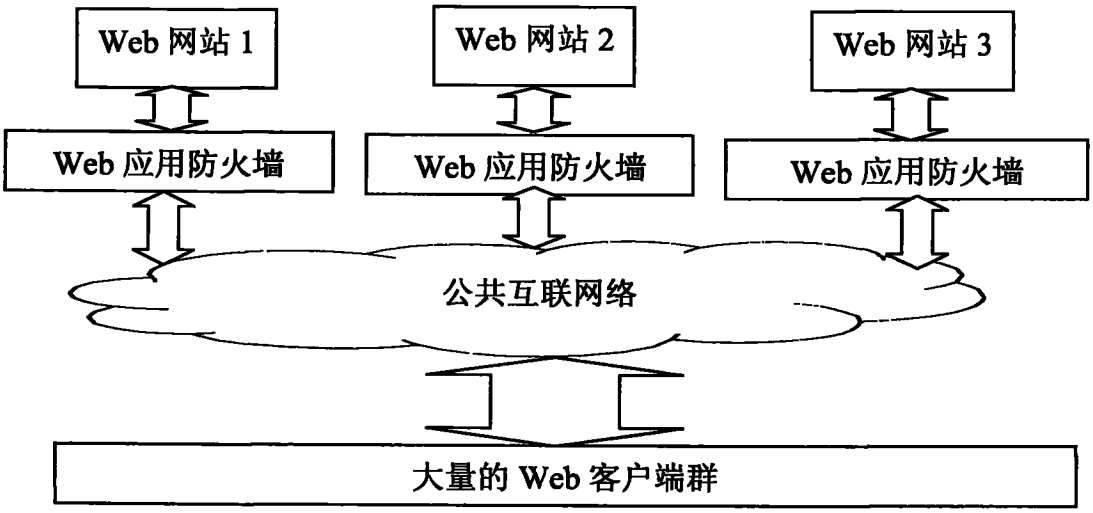

Web 网站 1
Web 网站 2
Web 网站 3
Web 应用防火墙
Web 应用防火墙
Web 应用防火墙
公共互联网络
大量的 Web 客户端群

图 1

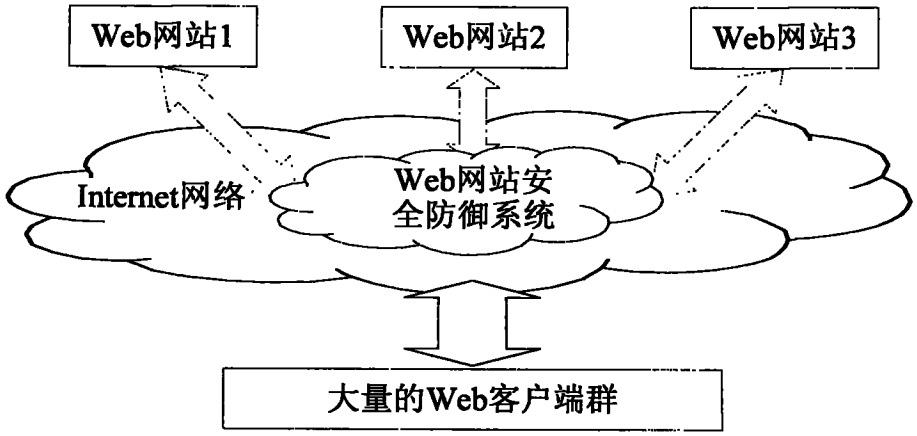

Web网站1
Web网站2
Web网站3
Internet网络
Web网站安全防御系统
大量的Web客户端群

图 2

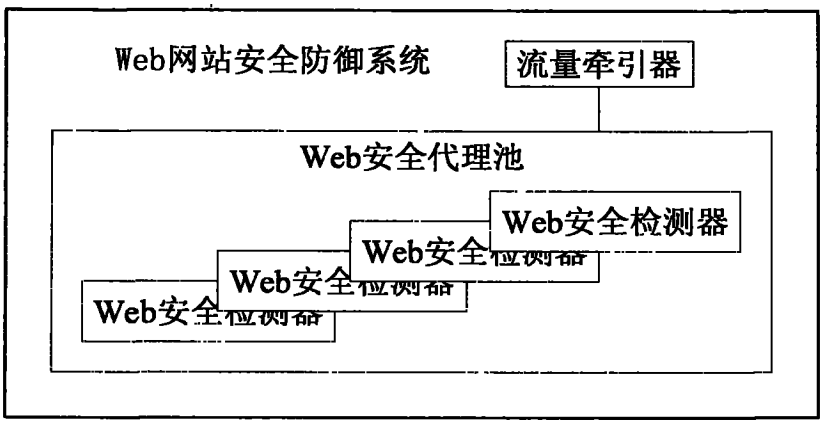

Web网站安全防御系统
流量牵引器
Web安全代理池
Web安全检测器

图 3

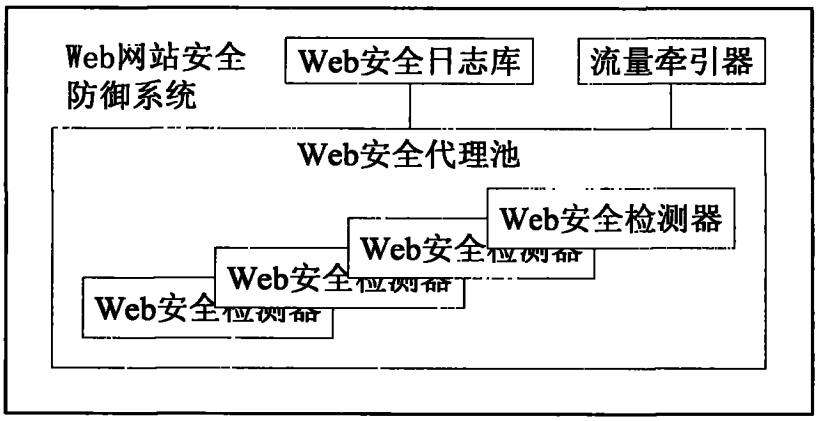

Web网站安全
防御系统
Web安全日志库
流量牵引器
Web安全代理池
Web安全检测器

图 4

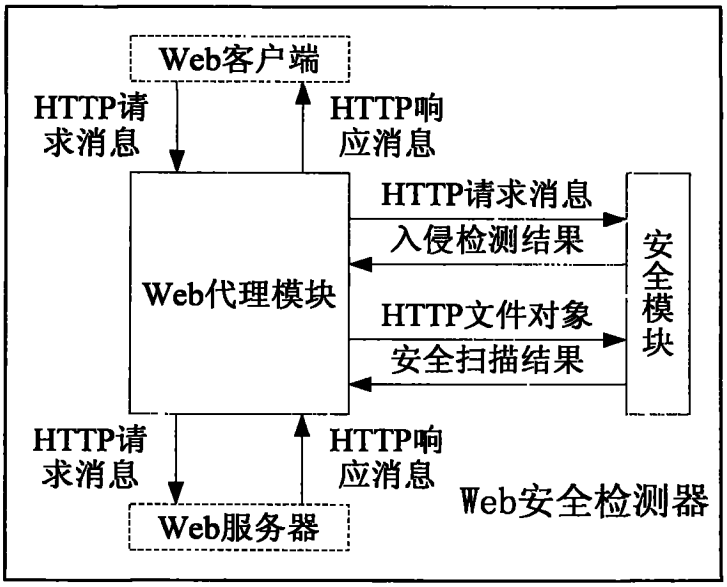

Web客户端
HTTP请求消息
HTTP响应消息
HTTP请求消息
入侵检测结果
Web代理模块
HTTP文件对象
安全扫描结果
安全模块
HTTP请求消息
HTTP响应消息
Web服务器
Web安全检测器

图 5

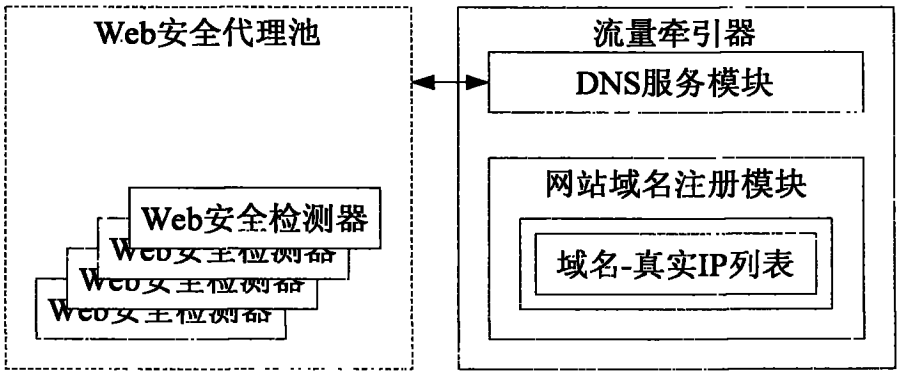

Web安全代理池
Web安全检测器
流量牵引器
DNS服务模块
网站域名注册模块
域名-真实IP列表

图 6

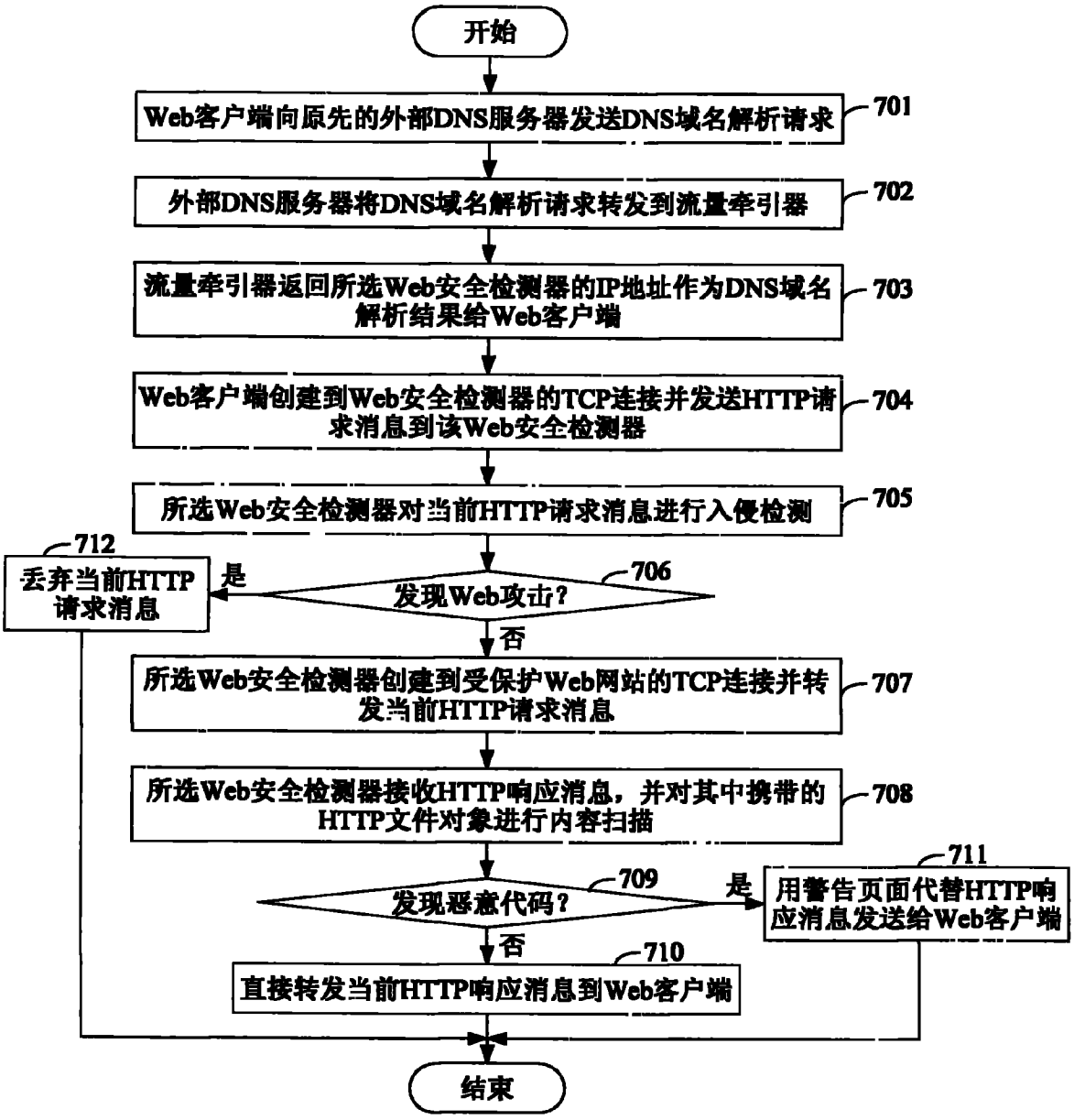

开始
Web客户端向原先的外部DNS服务器发送DNS域名解析请求
701
外部DNS服务器将DNS域名解析请求转发到流量牵引器
702
流量牵引器返回所选Web安全检测器的IP地址作为DNS域名解析结果给Web客户端
703
Web客户端创建到Web安全检测器的TCP连接并发送HTTP请求消息到该Web安全检测器
704
所选Web安全检测器对当前HTTP请求消息进行入侵检测
705
712
丢弃当前HTTP请求消息
是
发现Web攻击?
706
否
所选Web安全检测器创建到受保护Web网站的TCP连接并转发当前HTTP请求消息
707
所选Web安全检测器接收HTTP响应消息，并对其中携带的HTTP文件对象进行内容扫描
708
711
发现恶意代码?
709
是
用警告页面代替HTTP响应消息发送给Web客户端
否
710
直接转发当前HTTP响应消息到Web客户端
结束

图 7

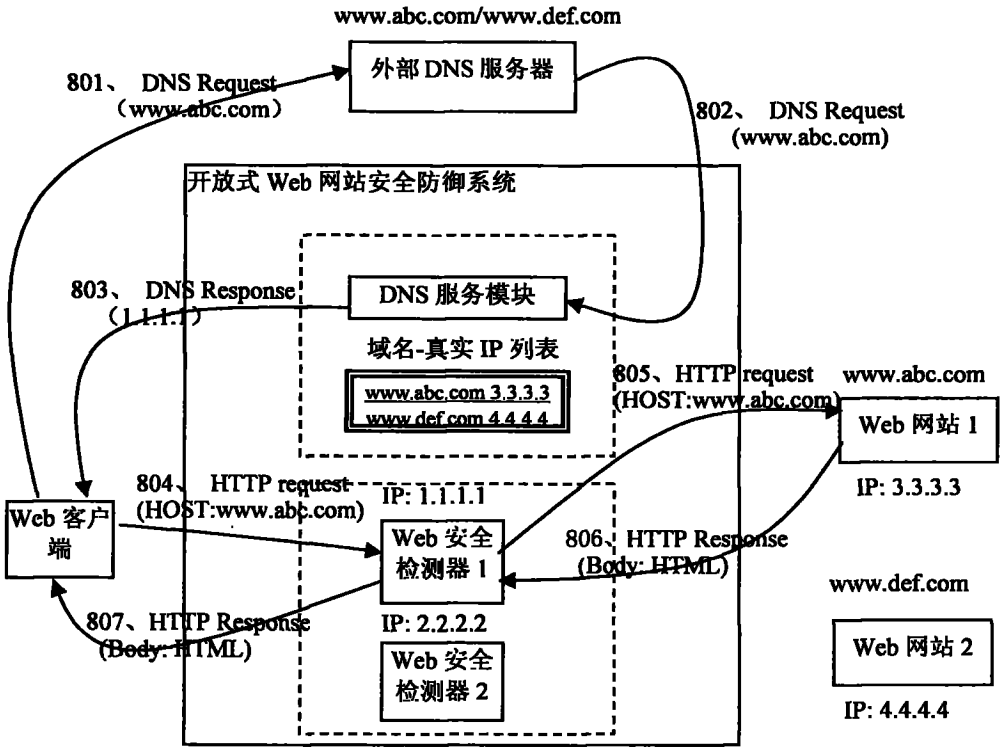

www.abc.com/www.def.com
外部 DNS 服务器
801、 DNS Request
（www.abc.com）
802、 DNS Request
(www.abc.com)
开放式 Web 网站安全防御系统
803、 DNS Response
（1.1.1.1）
DNS 服务模块
域名-真实 IP 列表
www.abc.com 3.3.3.3
www.def.com 4.4.4.4
805、HTTP request
(HOST:www.abc.com)
www.abc.com
Web 网站 1
IP: 3.3.3.3
804、 HTTP request
(HOST:www.abc.com)
IP: 1.1.1.1
Web 客户端
Web 安全检测器 1
806、HTTP Response
(Body: HTML)
www.def.com
807、HTTP Response
(Body: HTML)
IP: 2.2.2.2
Web 安全检测器 2
Web 网站 2
IP: 4.4.4.4

图 8