云安全防护系统

网页防篡改功能技术白皮书

Ver1.0

青松智慧（北京）科技有限公司

一．前言

网页防篡改功能（以下代称为 WAM）是一款针对网站服务器应对篡改攻击的一款防护产品，主要功能是通过预先配置的保护目录，在文件层面对 web 服务器的网站源文件目录进行全方位的保护，防止黑客、病毒通过对网页和应用的漏洞进行的提权等操作对网站目录的文件进行未授权的修改和破坏。防篡改功能可以有效地保证网站的安全运行，保障业务的正常流转，维护企业、机构和政府形象，解决非法修改带来的一系列问题，同时工作在 SaaS 模式下更便于用户进行配置和维护，是一款高效、易用、安全的新一代防篡改功能产品。

本文档适用于对本功能和技术指标有了解需求的相关人员。

文档共五章，第一章前言，第二章系统简述，第三章系统的组成和功能特点，第四章主要技术实现，第五章使用部署事项。

二. 系统简述

近几年来我国网站建设以突飞猛进的速度进行，截止 2017 年 12 月我国域名总数已超过 4000 万个，仅.cn 的域名就达到 2085 万个，在信息发布，电子商务，日常生活，内容查询等各个方面网站均起到了至关重要的作用。以近些年政府服务逐渐云化为例，当前我国使用在线政务服务的用户达到 4.85 亿，可以说在电子政务、商务空前发展的今天，黑客的表现欲望，竞争对手的不正当攻击，不法势力的不正企图也愈发强烈。在这些威胁中，网页篡改事件影响极为恶劣。网页篡改事件传播速度快，事后影响大，难以追查责任，实时防护较难。而我国大多数网站的更新速度远跟不上攻击模式和方法的发展速度，尤其以信息、金融、政府类网站最易成为攻击目标。

青松网页防篡改功能使用简单，可靠性高，部署成本极低，使用新一代防篡改技术能够完全杜绝更改，灵活程度高，不依赖 web 结构和部署架构。青松网页防篡改功能可以应用在各类网站中，包括但不限于政府以及企业门户、信息发布交换、在线商务、高校机构等各行业网站。

由于 WAM 功能工作在专有的私有节点上，并且可以与 SaaS 管理平台直接进行数据和配置的交互，其配置的创新性和易用性以及 SaaS 式的管理操作为国内网页防篡改功能的先行者。

三. 系统组成及特点

3.1 系统组成

WAM 包含三个部分：监控器、私有节点恢复进程和管理平台，WAM 需要工作在私有节点上，私有节点的部署方法详见私有节点部署相关文档。各个部分功能说明如下：

管理平台部署在云端（无需用户部署），用户可以通过登录管理平台，切换到防篡改的功能页面对防篡改功能进行管理；

恢复进程、监控器部署在用户的私有节点，用户无需单独部署恢复进程，只需登录管理平台开启防篡改功能即可启用恢复进程；用户开启 web 服务器相关的目录权限和对应的防篡改功能之后，监控器也会自动运行。

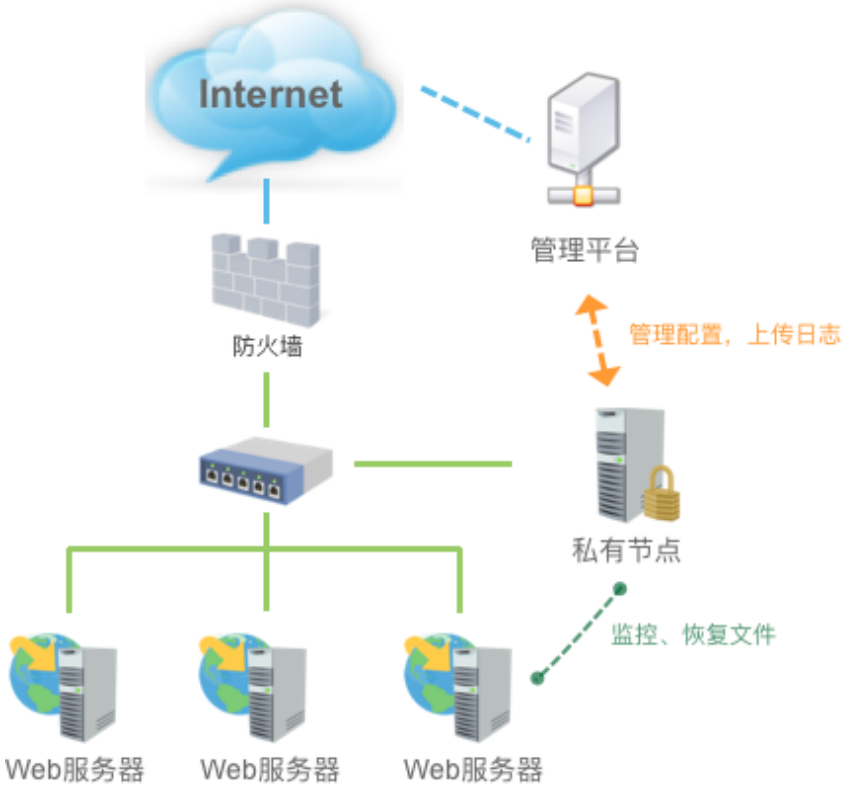

图 3-1 系统结构示意图

由于恢复进程和监控器均部署在私有节点上，不存在传输数据被窃取的问题；管理中心向节点进行的配置下发和传输均采用加密传输，确保通信的保密

性；用户使用 nfs 等网络共享协议进行目录的共享和挂载，直接与用户系统相挂钩，不依赖于 web 结构。

3.2 系统功能

WAM 会通过监视器实时监测被观察目录的文件（包括静态网页、动态脚本、图片等）的属性状态，一旦发现目录中文件出现了文件篡改操作，系统会直接通知相关告警对象，并且自动从可信的文件备份端进行有效文件恢复，保证网站相关目录的文件不被修改。

由于在线业务的不断扩大，如出现网页内容的未授权更改，可能会出现虚假消息的发布，或者反动内容的展示，这不仅会带来经济和形象的损失，可能会连带出现一系列法律责任风险，消除这些风险和影响的时间和经济损失巨大，因此，防篡改功能逐渐会成为各行各业网站的必备安全要素。

WAM 功能具备的技术内容归纳如下：

（1）工作在完全自主研发的私有节点系统中，内核稳定，高效；

（2）文件加密水印监测，安全可靠

（3）无需在服务器端部署软件，对服务器资源占用可忽略不计

（4）采用 SaaS 管理模式进行配置，操作简易，可视，方便；

（5）不限制 web 服务器类型，不限制保护文件类型，可用性范围大；

（6）可指定多种监控告警方案，第一时间反馈用户处理；

（7）随时可开关操作，随时可新增减少监控目录，配置灵活，配即生效。

3.3 主要技术功能

1.多重防护，纵深防御

- 实时阻断：实时性阻断非法操作对受保护目录文件的写操作，杜绝篡改的可能
- 事件触发：根据篡改情况触发后续的保护性措施，根据不同目录设置不同的告警规则

- 指纹技术：使用数字指纹技术验证对外发布文件的合法性，确保非授权指纹文件不被发布到外网，从根本降低篡改网页被浏览的可能性
- 防注入攻击：防篡改功能还可以联动私有节点的其他功能形成防护策略网络，比如针对性设置多层级防篡改目录，设置多种类别的防护规则，根据提交内容设置关键词审查，预先进行可疑内容的审查防范。

2.结合私有节点的网站安全运行保障

- 保护网站的内容不被篡改
- 保证网站免收应用层攻击以及资源耗尽攻击的危害
- 支持实时的数据监测的流量检测
- 支持历史数据的分析和导出

四．实现原理与优势

4.1 实现原理

WAM 实际把用户网站目录映射到私有节点的路径上进行防护，监视器会在指定目录上生成对应的水印，除了目录水印，每个目录下被监测的文件（包括静态资源文件，动态脚本以及其他文件）都会有其对应的水印。并且在私有节点上维护一个水印的列表，对其实时进行监测，当文件出现篡改时，会及时从节点的安全目录中恢复备份的对应文件，并使用校验方式验证整个目录的完整性和可靠性，这个过程是完全自动的，并且系统会把整个恢复过程的处理流程和操作日志上报到管理平台，这样使得网站即使遭到篡改，也能保证访问者看到正常的网站页面，使得网站的公信力和名誉得到保证。

实际校验时，校验的指纹信息中包含了目标文件的指纹 ID，大小，创建时间，所有权以及对应目录的指纹 ID，大小，创建时间，所有权，当指纹出现任何可疑情况时系统都会从可信备份目录进行实时的文件恢复，确保文件真实可靠。

在不需要文件防篡改功能时，用户可以随时登录管理平台，选择关闭某个监控路径的监测，这样能够灵活的根据实际更新网站的需求和频次选择使用监控目录。

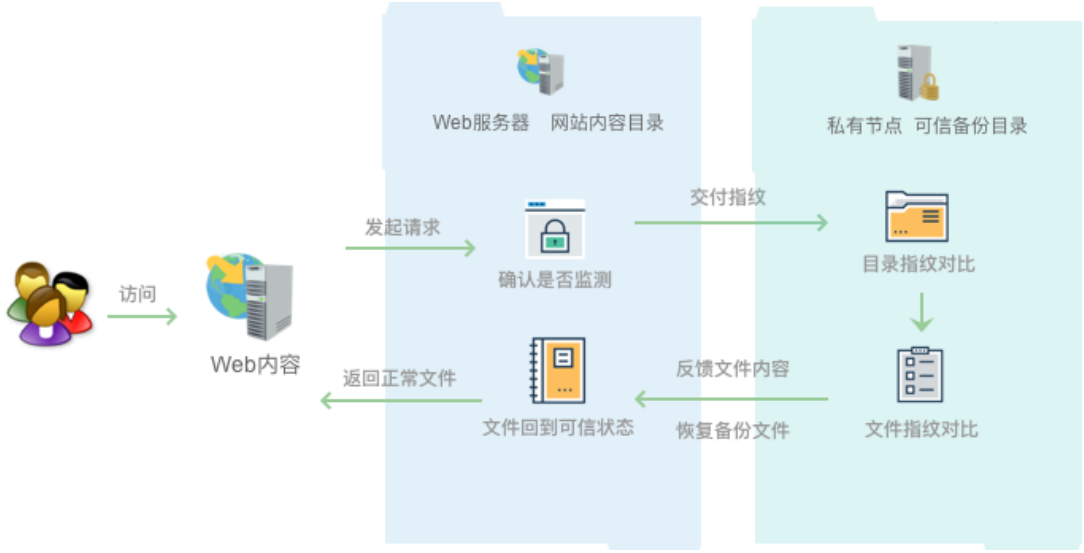

图 4-1 校验实现原理图

4.2 核心优势描述

1. 自研发底层可靠防护系统

私有节点为自研发，高定制化的底层防御系统，处理性能高，执行效率快，能够在系统资源低损耗的情况下进行防篡改的监测、恢复和告警动作，并且能够实时性上报执行动作的相关日志。由于部署在我私有节点，并不依赖于目标系统的工作环境，系统的工作可靠性还有自身的监控和保障程序实现，不必担心由于系统稳定性带来的无法恢复之类的问题。

2. 无需单独部署，SaaS 在线管控

用户无需部署复杂的设备，配置系统相关参数，在部署私有节点之后，直接通过管理平台操作，配置相关选项即可使用对应的功能，并且由于使用全 SaaS 的管理平台，即使用户不在机房的网络环境中，也可以通过云端的管理平台对防篡改的选项进行配置的管理，对于防护的路径也可以随时变更，按需配置。

3.不影响原有架构

由于系统部署的轻量性，不依赖目标系统的类型，除了私有节点之外不需要用户单独部署任何软件，不仅降低用户投资，也减少了部署成本，用户也无需变更原有的网络结构，只需做一部分基本操作和配置即可。

4.支持多目录监控

用户可根据需求设置多层级目录的防篡改监测，也可以自行设置备份路径，并且在多子目录，多级目录的设置下并不会影响原有系统的实际性能。

5.实时监控日志，支持日志导出查询

如果出现了任何篡改行为或者非授权的变动，管理平台都会记录相关的日志信息，并且这些日志支持导出查询， 用户可以筛选出对应类别的日志导出分析，了解整个系统的工作状态和情况。这些日志包括：

（1）对目录文件进行操作的日志；

（2）防篡改功能的配置操作日志；

（3）出现恢复的告警日志；

当出现告警信息时，也可以根据预先设置的告警目标和联系人进行消息的推送。

五．部署结构

5.1 基本部署

WAM 功能的部署并不依赖于用户的网络环境和结构，但是需要用户预先进行私有节点的部署，私有节点的部署方法详见私有节点部署方案及相关文档。

5.2 配置操作

当私有节点部署完成并且正常托管网站之后，用户需要登录管理平台进行防篡改功能的配置。

（1）添加监测路径：用户需要指定防篡改的网站，系统会自动识别其对应的私有节点；在指定节点以及网站之后，需要继续指定监测的目录，完成后防篡改的基本配置会被下发到对应的私有节点上。

（2）配置相关权限，生成水印：用户可以选择使用多种方式将预备监测路径映射到私有节点上，例如 NFS 的方法，使用 nfs 开启目录的共享操作，把目录映射挂载到私有节点对应配置的路径上，之后系统会生成目录以及内部文件的相关水印信息。

（3）开启监测：开启监测之后，系统即对目录中文件进行实时的监测以及防篡改操作。

5.3 部署事项

在部署时，需要保证私有节点和目标 web 服务器的网络通信畅通。