绿盟 WEB 应用防护系统 V6.0

产品白皮书

目录

一. 概述 1

二. 关键特性 1

2.1 客户资产视角 CUSTOMER ASSET PERSPECTIVE 1
2.2 优化的向导系统 OPTIMIZED CONFIGURATION WIZARD 2
2.3 细致高效的规则体系 MULTIPLE RULE-BASED INSPECTIONS 3
2.4 辅助 PCI-DSS 合规 PCI-DSS COMPLIANCE REPORT 4
2.5 多层次的防护机制 LAYERED SECURITY MECHANISM 4
2.6 智能自学习白名单 EFFECTIVE ANTO-LEARNING AND WHITE LIST 5
2.7 透明部署，即插即用 TRANSPARENT，DROP-IN DEPLOYMENT 6
2.8 智能补丁应急响应 EMERGENCY RESPONSE THROUGH CLOUD SECURITY SERVICE 7
2.9 绿盟安全管家 NSFOCUS SAFETY STEWARD 7
2.10 IP 信誉 IP REPUTATION 8
2.11 智能检测-机器学习与语义分析
INTELLIGENT DETECTION – MACHINE LEARNING & SEMANTIC ANALYSIS 8
2.12 满足大规模部署的集中管理能力 CENTRALIZED MANAGEMENT CAPABILITY FOR LARGE-SCALE DEPLOYMENT 8

三. 典型部署 8

四. 典型应用 10

4.1 网站访问控制 10
4.2 网页篡改在线防护 10
4.3 敏感信息泄漏防护 10
4.4 DDOS 联合防护 11
4.5 虚拟站点防护 12

五. 附录 12

5.1 业务资产定义 12
5.2 规则体系定义 13

插图索引

图表 1 WAF 的资产视角 2
图表 2 向导体系过滤站点规则 3
图表 3 资产分层及其防护层级 5
图表 4 防护体系 6
图表 5 智能补丁 7
图表 6 WAF 的典型部署 9
图表 7 绿盟 WAF 和绿盟 ADS 的 DDoS 联合防护方案 11
图表 8 站点的定义 12
图表 9 主机名的定义 12
图表 10 URI 及相关字段的定义 13

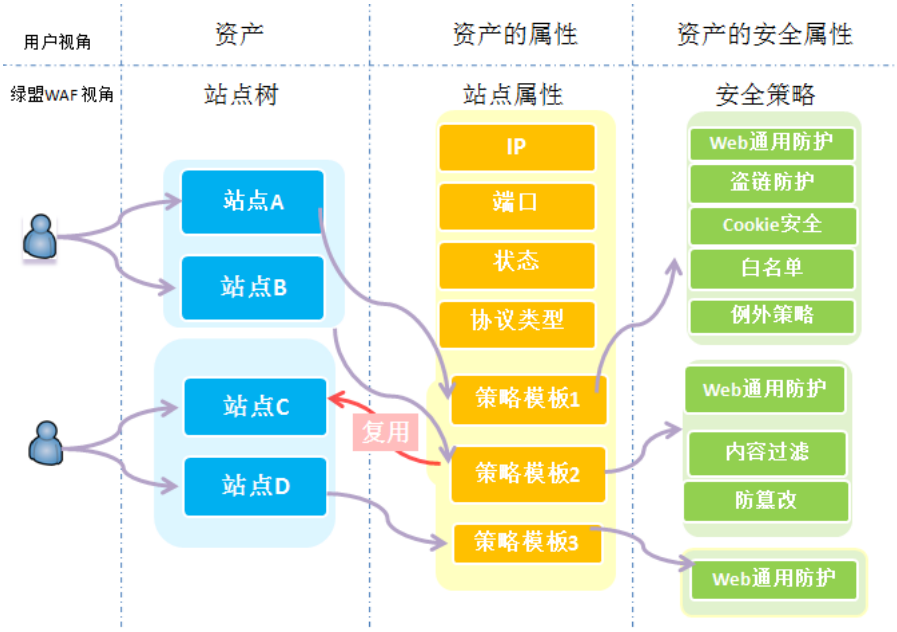
一. 概述

绿盟科技 Web 应用防火墙（简称 WAF）将客户资产作为组织 Web 安全解决方案的依据，用黑、白名单机制相结合的完整防护体系，通过精细的配置将多种 Web 安全检测方法连结成一套完整（COMPLETE）的解决方案，并整合成熟的 DDoS 攻击抵御机制，能够在 IPV4、IPV6 及二者混合环境中抵御 OWASP Top 10 等各类 Web 安全威胁和拒绝服务攻击，并以较低的运营成本为各种机构提供透明在线部署、路由旁路部署、镜像部署和云部署，能方便快捷的部署上线，保卫您的 Web 应用免遭当前和未来的安全威胁。

二. 关键特性

2.1 客户资产视角 Customer Asset Perspective

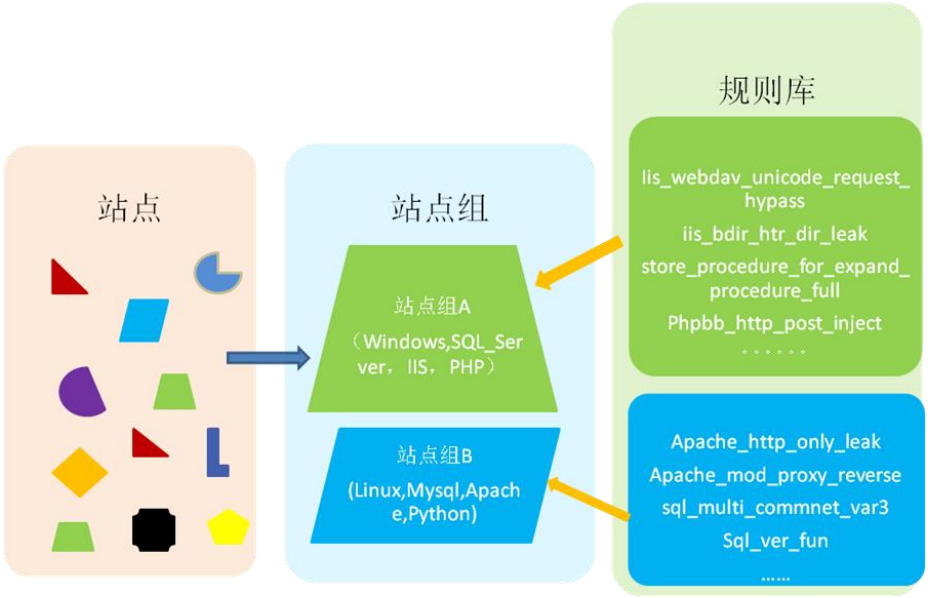
绿盟 WAF 将站点看做用户的客户资产，用站点树来展示资产列表，直观展示资产清单及各资产的属性，如状态、协议类型、IP 地址、端口等。同时，将资产所用的安全策略——各种安全规则的集合视为资产的属性之一，并以模板的方式保存。策略模版可以在 IP+端口不同、业务环境相似的站点之间被方便的复用，产品更贴近客户。



图表 1 WAF 的资产视角

2.2 优化的向导系统 Optimized Configuration Wizard

基于客户资产视角，绿盟WAF提供了一套优化的向导系统，在配置客户信息的过程中询问操作系统、数据库、Web 服务器及使用的编程语言信息，同时引入站点组概念，支持将 OS、Web Server 和应用程序相同或者类似的站点（IP 地址 + 端口号）纳入一个站点组，在构建站点资产的同时也完成了针对客户环境的规则过滤，实现了客户环境对规则体系中黑名单规则的精准利用，减少了误报，同时大大简化了配置操作。



图表 2 向导体系过滤站点规则

2.3 细致高效的规则体系 Multiple Rule-Based Inspections

规则是 WAF 识别和阻止已知攻击的基础检测方法，绿盟 WAF 规则库基于多年网络安全研究积累，已高度细化，基于规则的防护功能包括：

- Web 服务器漏洞防护
- Web 插件漏洞防护
- 爬虫防护
- 跨站脚本防护
- SQL 注入防护
- LDAP 注入防护
- SSI 指令防护
- XPATH 注入防护
- 命令行注入防护
- 路径穿越防护
- 远程文件包含防护

在细化多种规则的同时，绿盟 WAF 也引入了众多机制保证规则的精准、有效。

1. 前导字符

网络中合法流量占主体，引入前导码机制，通过前导码的简单字符串的匹配，对流量进行预筛选，提高检测效率。

2. 不同检测位置

支持灵活的检测对象定义，包括任意的 HTTP 头部字段，HTTP BODY 字段，支持各种检测运算。

3. 多种检测条件的逻辑组合

支持多个检测条件的逻辑组合，以支持复杂规则的定义。

4. 自定义规则

提供贴近于自然语言、支持复杂场景描述的自定义规则，能作用于具体的 URL 上，大大提高了规则的有效性和精准度。

5. 独立的规则升级

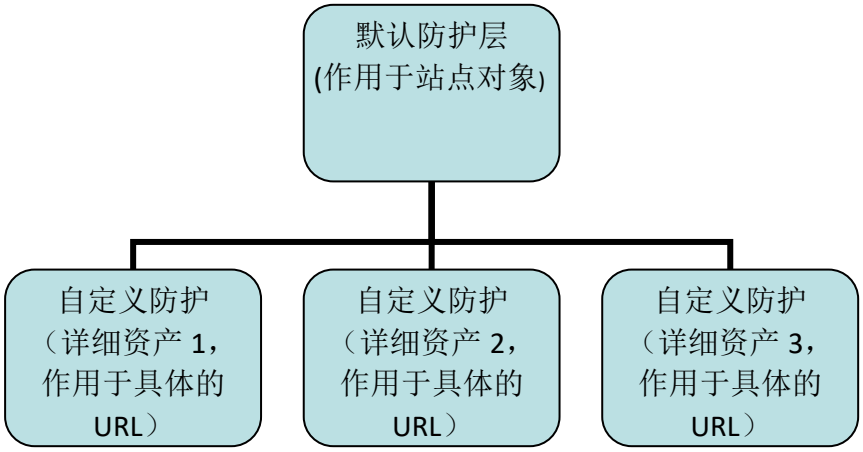
通过编译式运行的规则库，绿盟 WAF 还分离了规则升级和系统升级。

2.4 辅助 PCI-DSS 合规 PCI-DSS Compliance Report

随着业务的扩展，支撑业务的信息环境也日益复杂，通过满足各种安全合规标准成为了各行业规约和保证企业信息安全的一种手段。 支付卡行业（PCI：Payment Card Industry）数据安全标准（DSS：Data Security Standard），作为衡量金融机构、消费者等涉及支付卡业务的商家和服务提供者的数据资料安全基准，详细规约了对存储、处理或传输持卡人数据的商家和服务提供商的安全要求，已经在全球范围内获得了广泛的认可。 绿盟 WAF， 站在用户资产的视角，能够结合当前防护站点的安全配置，按照 PCI-DSS 的合规要求对用户资产环境做出是否合规的判断，并在此基础上提出满足 PCI-DSS 合规的配置建议，协助商家和服务提供商应对 PCI-DSS 合规检查和信息系统安全环境的加固。

2.5 多层次的防护机制 Layered Security Mechanism

基于用户资产分层的特性，绿盟 WAF 将防护层级也进行了细分：默认防护层作用于站点对象；自定义防护层则作用于详细资产，即具体的 URL。



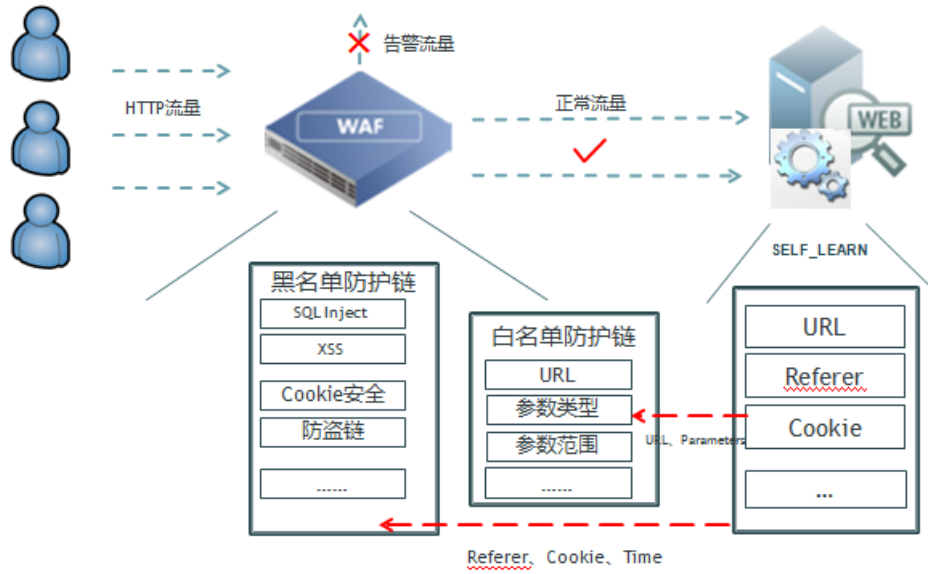
图表 3 资产分层及其防护层级

此外，绿盟 WAF 在专注于 Web 应用防护的同时，还应用了自主研发的抗 DDoS 算法和多种应用层抗 DDoS 技术，可防护各类带宽资源耗尽型 DDoS 和应用层 DDoS，实时阻断攻击流量，从网络层面确保 Web 业务的可用性及连续性。在 DDoS 攻击流量超过绿盟 WAF 的处理能力时，绿盟 WAF 和绿盟的专业 Anti-DDoS 设备 ADS 还能形成联合防护方案，借助 ADS 的专业防护能力完成攻击流量的牵引和清洗。

2.6 智能自学习白名单 Effective Anto-learning and White List

黑名单规则即内置及自定义的规则是绿盟 WAF 在防护 Web 安全时的强大知识依托，然而，黑名单体系固有的“事后更新”特点使其仅仅能解决已知问题，在应对 0day 漏洞防护时显得略为滞后，且由于未参考客户环境的业务逻辑，在防护效果上也无法做到精准。

绿盟 WAF 引入的自学习+白名单机制，弥补了黑名单防护体系的固有缺点，有效增强了 0day 漏洞的防护能力和精准防护能力。WAF 基于统计学方法的自学习技术，分析用户行为和指定 URL 的 HTTP 请求参数，能将站点的业务逻辑完整的呈现出来，协助管理员构建正常的业务流量模型，形成白名单规则。



图表 4 防护体系

在防护顺序上，绿盟 WAF 先利用黑名单规则解决已知安全风险，在用自学习、白名单作为黑名单规则的补充解决业务逻辑层面的安全风险， 使绿盟 WAF 的安全防护体系更完整，进一步贴近了客户业务环境，在应对 0day 漏洞时也更加快速、精准、有效。而这种防护顺序的设计，避免了依赖白名单机制而带来的设备上线需要长时间的学习业务、且业务模型变动时策略调整频繁等缺点，上线就能即插即用、零配置防护。

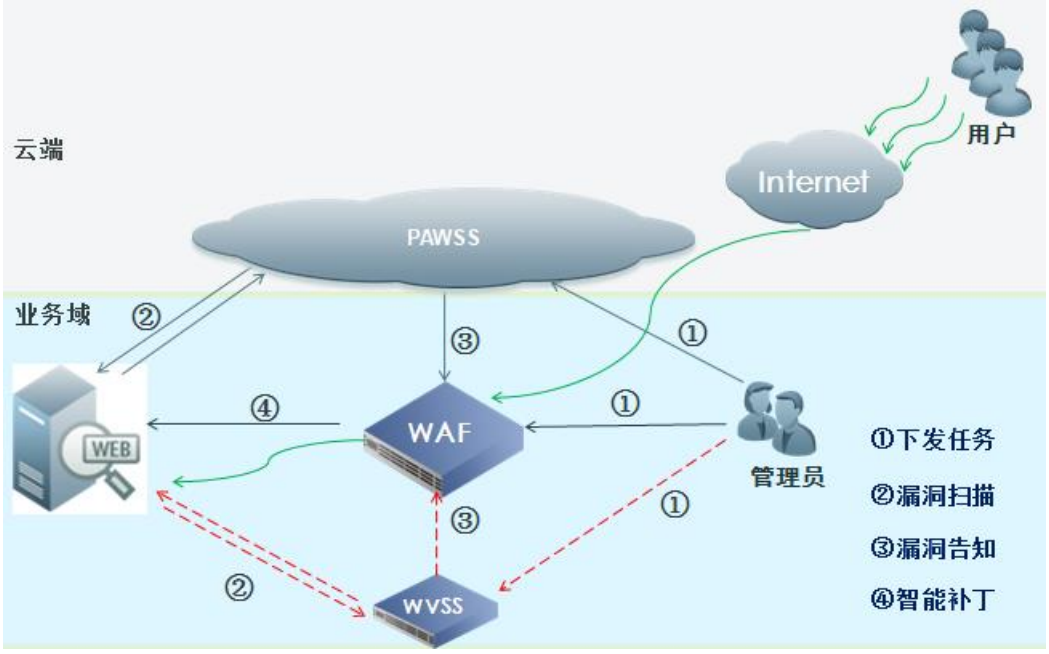
2.7 透明部署，即插即用 Transparent，Drop-in Deployment

绿盟科技 WAF 提供灵活的部署模式，包括常见使用的“即插即用-透明部署”，这种模式下不需要对当前网络和应用环境进行任何改变，部署方便快捷。同时，在这种模式下，WAF 还提供缺省防护策略和缺省网络接口配置等功能，可以将设备上线时间缩短至半小时之内。

此外，绿盟 WAF 还提供路由旁路；流量牵引模式和反向代理模式。路由旁路流量牵引模式能减少单点故障，没有额外的流量转发开销，能达到性能最优；反向代理模式的部署位置灵活，WAF 和 Web 服务器可以不在一个安全区域中，该模式已经被国内外用户运用在云 WAF 业务模式中。

2.8 智能补丁应急响应 Emergency Response through Cloud Security Service

通过与绿盟科技云安全平台的 Web 漏洞扫描服务（PAWSS）或者 WEB 应用漏洞扫描系统（WVSS）联合防护，绿盟 WAF 能获取被防护站点的漏洞扫描报告，并根据自身已有的规则自动生成一套新的规则即智能补丁，应用于被保护站点。当被防护站点打上了智能补丁之后，之前被扫描出的 Web 应用漏洞将无法重现。



图表 5 智能补丁

智能补丁，借助了绿盟科技云安全平台中 Web 漏洞扫描服务和 WEB 应用漏洞扫描系统对 Web 漏洞的感知能力，又很好利用了绿盟 WAF 自身的规则体系，在不用更改被防护站点配置、不为其设备提供额外负担的情况下，有效减少了一些站点因无法频繁打补丁、业务频繁升级而引入漏洞带来的安全风险，还能及协助客户满足安全合规要求。

2.9 绿盟安全管家 Nsfocus Safety Steward

客户可在 AppStore 中下载绿盟科技安全管家 APP，通过 WAF 与云的联动，可以把 APP 与 WAF 进行绑定，时刻获取设备的运行的状态，包括设备的 cpu、内存、规则库版本等信息，一旦设备出现问题，可通过 APP 上一键联系绿盟安全人员对设备进行维护。运营实时化，大大降低了运维难度。

2.10 IP 信誉 IP Reputation

WAF 与 NSFOCUS NTI 对接后，获取不同攻击类型的高危信誉 IP，在 WAF 上自动生成防护策略。通过启用 IP 信誉功能，可有效防止撞库、羊毛党（刷单、刷积分）的问题，同时有效减少疑似攻击行为的告警噪音，达到提升告警精度的效果。

2.11 智能检测-机器学习与语义分析 Intelligent Detection – Machine Learning & Semantic Analysis

基于规则和表达式对攻击行为进行判断和过滤的安全设备已无法满足当下复杂多变的网络环境，漏报和误报的情况难免会发生。绿盟科技 WAF 通过使用机器学习方法的攻击检测机制，对海量的攻击样本进行学习构建模型，引入误报率更低、性能更优的智能检测引擎，降低传统规则防护难以调和的漏报率和误报率。

2.12 满足大规模部署的集中管理能力 Centralized management capability for large-scale deployment

随着 WEB 相关业务的不断增长，单台 WAF 可能已经无法满足庞大业务防护需求，后续扩容之后对设备集中管理提出了新的要求。绿盟科技 WAF 可以通过集中管理平台（ESPC）对多台设备进行统一管理，可对设备统一接入、防护策略批量下发、设备状态集中监控等功能，满足大规模部署环境下的集中管理需求。

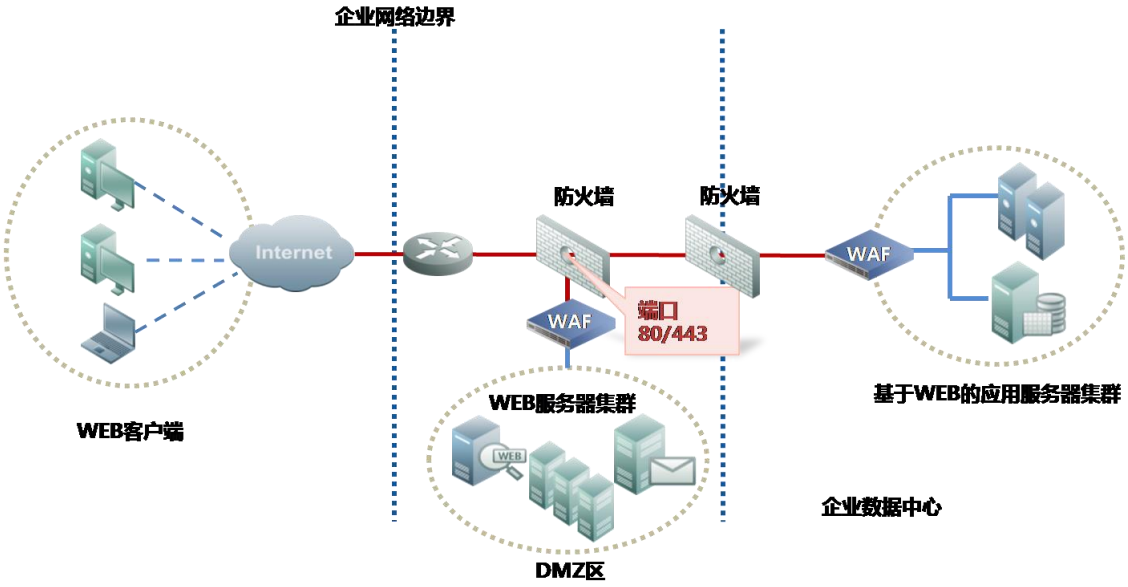
三. 典型部署

绿盟 WAF 提供多种灵活的部署方式，包括透明部署模式、反向代理模式和旁路模式。

串联部署模式下，绿盟 WAF 在内核模块实现从 TCP/IP 协议栈的透明代理，极大地提高网络适应能力、确保产品在网络中即插即用而无需修改网络及服务器配置，降低了部署、维护开销。而反向代理模式，需要改动服务器 IP 地址以及 DNS 解析；桥模式下，用 Web 服务器的 IP 地址作为 VIP，牺牲了一部分功能（如 SSL 功能）。

在部署了多业务网段服务器的网络环境中，WAF 设备也可以采用旁路方式部署，提供一种逻辑在线防护机制。该种部署灵活性较好，可以实现业务分流，对核心系统影响较小。旁路方式部署的技术原理如下：

1. **流量牵引**：通过路由方式，将原来去往目标网站 IP 的流量牵引至 WAF 设备。被牵引的流量为攻击流量与正常流量混杂的 HTTP 流量；
2. **流量检测和过滤**：WAF 设备通过多层的攻击流量识别与净化功能，将 Web 攻击流量从混合流量中过滤；
3. **流量注入**：经过 WAF 过滤之后的合法流量被重新注入回网络，最终到达目的网站。
4. **对返回流量检测**：网站响应的 HTTP 流量在返回给客户端之前，仍然需要流经 WAF 设备，WAF 可提供安全检测，经 WAF 检测后的流量最终返回给客户端。



图表 6 WAF 的典型部署

对于只需要 WAF 做检测不做阻断的用户，绿盟 WAF 提供了镜像部署方式，客户通过对交换机配置镜像，把流量镜像到 WAF 上进行攻击检测，不对客户流量造成任何影响。

四. 典型应用

4.1 网站访问控制

针对某些 Web 网站的部分路径只允许某些 IP 访问，某些路径不受访问 IP 限制的用户场景，绿盟 WAF 在串联部署、旁路部署和反向代理部署时均提供了 HTTP 访问控制功能。用户通过使用 HTTP 访问控制，不仅可以达到权限控制的效果，还可以做到误报纠正：例如某些 URI（见附录定义）直接放过而不检测。

事实上，多数有访问控制需求的 Web 服务器都已经配置了一定的安全策略，但大多数安全策略可能会忽略对主机名的严格检测，从而存在安全防护策略被绕过的隐患。 绿盟 WAF 通过显式配置只允许指定的主机名访问，从安全策略配置层面避免了这一隐患引发的权限滥用，访问控制更加严格。

4.2 网页篡改在线防护

按照网页篡改事件发生的时序，绿盟 WAF 提供事中防护以及事后补偿的在线防护解决方案。事中，实时过滤 HTTP 请求中混杂的网页篡改攻击流量（如 SQL 注入、XSS 等）；事后，自动监控网站所有需保护页面的完整性，检测到网页被篡改，第一时间对管理员进行短信告警，对外仍显示篡改前的正常页面，保证用户可正常访问网站。

4.3 敏感信息泄漏防护

绿盟 WAF 可以识别并更正 Web 应用错误的业务流程，识别并防护敏感数据泄漏，满足合规与审计要求，具体如下：

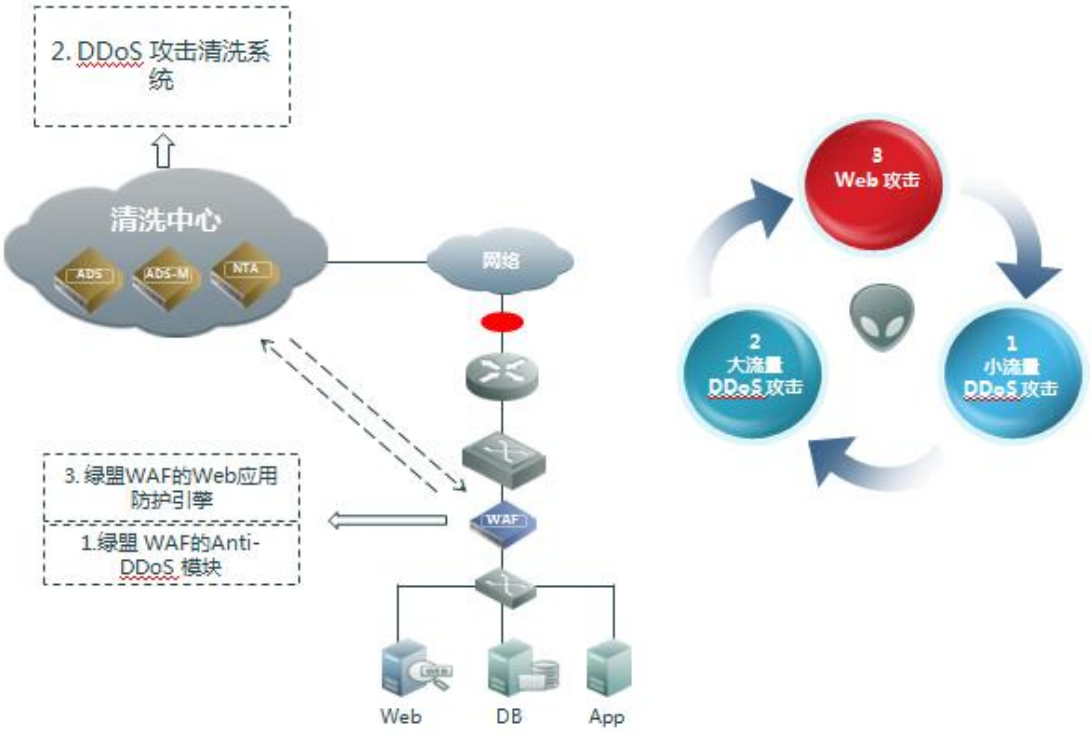
1. 可自定义非法敏感关键字，对其进行自动过滤，防止非法内容发布为公众浏览。
2. Web 站点可能包含一些不在正常网站数据目录树内的 URL 链接，比如一些网站拥有者不想被公开访问的目录、网站的 WEB 管理界面入口及以前曾经公开过但后来被隐藏的链接。WAF 提供细粒度的 HTTP 访问控制，防止对这些链接的非授权访问。

3. 网站隐身：过滤服务器侧出错信息，如错误类型、出现错误脚本的绝对路径、网页主目录的绝对路径、出现错误的 SQL 语句及参数、软件的版本、系统的配置信息等，避免这些敏感信息为攻击者利用、提升入侵的概率。
4. 对数据泄密具备监管能力。能过滤服务器侧响应内容中含有的敏感信息，如身份证号、信用卡号等。

4.4 DDoS 联合防护

绿盟 WAF 本身提供 TCP Flood 防护功能，当 DDoS 攻击超过了本身防护阈值的情况下，还能跟由绿盟科技的专业抗拒绝服务攻击产品 ADS 组成的清洗中心联动，达到分层清洗的目的。绿盟 WAF 与 DDoS 清洗中心联动的工作场景如下：

1. 绿盟 WAF 的 TCP Flood 防护功能对一定阈值的拒绝服务攻击进行防护。
2. 当攻击流量超过了绿盟 WAF 本身的防护阈值时，WAF 向上游的 ADS 清洗中心发出通告，请求上游的 ADS 牵引并清洗到达 WAF 防护站点的攻击流量。
3. ADS 牵引并清洗成功后，WAF 退出本身的 TCP Flood 防护。
4. 当 WAF 发现到达上游 ADS 的攻击流量小于通告值时，申请取消上游 ADS 对流量的牵引和清洗，同时将自身的 TCP Flood 防护开启。



图表 7 绿盟 WAF 和绿盟 ADS 的 DDoS 联合防护方案

联合防护方案的实现，解决了 WAF 上游带宽被大流量 DDoS 攻击堵死且自身防护能力一无法满足清洗需求的问题，并能根据攻击流量大小自动判断和控制清洗层次，按需、合理调用 WAF 自身 Anti-DDoS 模块和清洗中心的清洗资源，是绿盟科技 Web 安全解决方案中重要的一环。

4.5 虚拟站点防护

随着数据中心不断发展和其用户托管网站业务的多样化，被托管网站使用一个 IP 对应多个不同域名的虚拟站点场景被越来越广泛的应用，对 WAF 也提出了支持虚拟站点场景的新要求。绿盟 WAF 能在 IP+端口定义的站点基础上，配置 IP 对应的不同域名，并针对不同域名的虚拟站点做不同的防护策略配置，使策略的配置完全切合用户业务场景。在保障托管用户 WEB 安全的基础上，也为数据中心用户提供了向其托管网站提供 WEB 安全增值服务的业务机会，已被应用于多个国内外客户中。

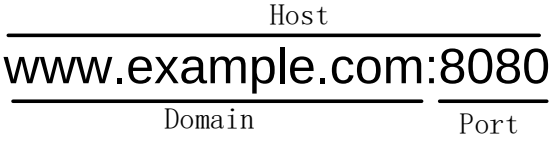
五. 附录

5.1 业务资产定义

1. **站点**的定义：

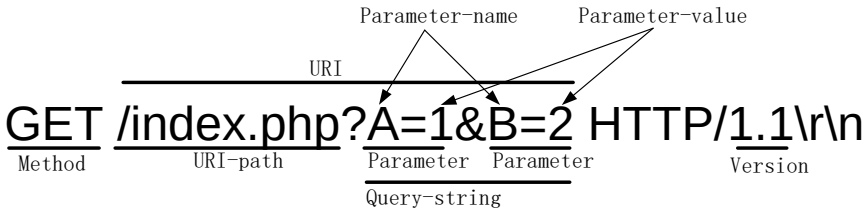
图表 8 站点的定义

2. **主机名（Host）**的定义：



图表 9 主机名的定义

3. **URI** 的定义：



图表 10 URI 及相关字段的定义

5.2 规则体系定义

以下介绍 WAF 规则体系的定义。

1. **规则**：基于 HTTP 流量的特定对象进行特征检测的字符串。
2. **策略**：规则集及规则集动作的定义，可定义策略例外。
3. **规则集**：一系列规则的集合，可为不同类型规则。
4. **策略例外**：定义对特定对象具有攻击特征的允许，允许策略中特定规则。
5. **白名单规则**：站点合法流量的特征描述，自学习引擎学习被防护站点流量特征生成或者自定义。
6. **智能补丁规则**：基于被防护站点的漏洞信息，由智能补丁系统生成的具有针对性的自定义规则。
7. **前导码**：规则特征串的简单字符串子串。