安恒信息
DAS-security 安全中国

# 明御®Web 应用防火墙-信创版

V3.0.4.6

# 产品白皮书

文档版本：01

发布日期：2022-03

# 文档说明

| | | | |
|---|---|---|---|
| **产品名称** | | 明御®Web 应用防火墙 | |
| **适用平台/版本** | | V3.0.4.6 | |
| **拟制人** | | **评审组** | |
| **发布人** | | **备注** | 受控文档 |

# 修订记录

| 日期 | 修订版本 | 修改记录 | 修改人 |
|---|---|---|---|
| 2022-03 | 01 | 初次发布 | 谭琪（AH10382） |

# 目 录

# 前言

## 概述

感谢您选择安恒信息的网络安全产品。明御®Web 应用防火墙（简称“WAF”）是一款专注为网站、APP 等 Web 业务系统提供安全防护的专业应用安全防护产品。本手册主要对明御®Web 应用防火墙的背景信息、产品介绍、产品核心功能、产品形态和部署方式进行了详细说明。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

## 预期读者

本文档主要适用于期望了解明御®Web 应用防火墙的读者，包括服务工程师、系统管理员、网络管理员等。本文假设读者对以下领域的知识有一定了解：

- 网络安全相关知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。
- 安全防护策略、NAT 地址转换、VPN、各类路由协议的基本工作原理和配置。

## 获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

**联系信息**

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999

传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

# 1 背景信息

## 1.1 背景介绍

近年来，我国互联网事业快速发展，Web 类应用已广泛应用于政府、金融、教育、医疗、运营商等各行业。随着客户自身业务的发展，Web 业务系统越发复杂，其承载的企业数据也越发重要。由于数据的重要性、敏感性导致 Web 类应用成为黑客攻击的主要目标，Web 应用也面临严峻的安全挑战。

**挑战一：Web 类应用成为攻击的主要入口**

国家计算机网络应急技术处理协调中心（CNCERT/CC）发布的《2020 年中国互联网网络安全年报》中指出 2020 年接收的 Web 应用漏洞占比高达 29.5%（位居第二）。另外报告中指出 2020 年监测到国内约 5.3 万个网站被植入后门、约 10 万个网站发生被篡改的问题，从以上依据可以看出由于 Web 类应用漏洞数量之多、Web 类应用数量庞大则很容易成为黑客攻击的主要目标入口。

**挑战二：Web 类应用监管越发严格**

- 国家层面及各行业的法律法规相应颁布，明确要求 Web 类应用必须要加强安全防护措施，以防范网站被篡改、数据被泄露等安全性问题，包括《中华人民共和国网络安全法》《等保 2.0》《网上银行系统信息安全通用规范》《国办函〔2011〕40 号 国务院办公厅关于进一步加强政府网站管理工作的通知》《2017 年教育信息化工作要点》《卫生行业信息安全等级保护工作的指导意见》等法律法规。
- 每年国内重大活动及护网行动期间，Web 类应用成为重保及护网行动的重点防护对象，而 Web 类应用作为对外的主要入口成为攻击者第一选择的主要攻击目标。

**挑战三：传统安全防护手段难以满足客户需求**

- 采用传统网络安全设备（IPS 或者 NGFW），传统网络安全设备重点关注 2~4 层网络安全问题，而对于 7 层 HTTP 及 HTTPS 安全性问题则无法覆盖，导致 Web 应用攻击绕过。
- 采用传统 Web 应用防火墙，传统 Web 应用防火墙安全引擎采用基于正则静态签名的方式，该方式属于 Web 攻击的一种防护手段，但随着客户自身业务发展、客户业务系统越发复杂，此种方式会导致大量的规则误报，增加客户对于规则维护的工作量。另外，基于正则静态签名的方式无法防护未知攻击及 0day 的攻击行为，安全引擎的漏报率较高，难以满足客户对于安全防护能力的需求。

## 1.2 发展趋势

随着客户自身业务快速发展，传统安全防护手段已难以满足客户对于 Web 应用安全的防护的需求，一款专业优秀的 Web 应用防火墙需要具备以下能力：

- 低误报
- 低漏报
- 高性能

- 主动防护
- 简单易用

在此背景下，明御®Web 应用防火墙应运而生。

# 2 产品介绍

## 2.1 基本介绍

明御®Web 应用防火墙是一款专注为网站、APP 等 Web 应用提供安全防护的专业应用安全防护产品。能够对网站及 APP 业务流量进行多维度、深层次的安全检测和防护。系统内置五大安全引擎（包括语义分析引擎、机器学习引擎、威胁情报引擎、行为分析引擎、基础特征引擎），可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及 APP 业务安全、可靠运行。

## 2.2 国产化部署

采用中国自主知识产权的处理器，解决了芯片设计上存在的安全隐患；操作系统采用中国自主研发的操作系统，该系统具备强大的抗攻击能力，解决自身进程及文件被非法篡改和破坏；应用模块采用安恒信息自主研发的应用模块，真正实现硬件到软件、系统到芯片的完全自主，真正意义上的全国产化安全产品。

## 2.3 防护理念

- **主动防护**

解决传统安全设备仅依赖安全规则对流量进行检测的被动防护过程，逐步由被动防护实现主动防护，帮助客户主动发现前期存在的安全隐患。

- **智能感知**

主动发现、梳理现网环境中存在的 Web 应用并自动实现安全防护，通过威胁情报技术主动发现恶意 IP 对 Web 应用的踩点访问行为并通知客户采取相应的安全措施。

- **智能防护**

通过语义分析引擎、机器学习引擎、行为分析引擎、基础特征引擎、威胁情报引擎五大引擎联动实现对已知、未知、0day 攻击行为的检测。

- **智能联动**

与其他安全产品（如明御®APT 攻击预警平台、态势感知平台、AiLPHA 大数据智能安全平台等）实现联动防护，为客户提供全面的 Web 应用安全解决方案。


主动防护
智能感知
WAF
智能联动
智能防护

# 3 产品核心功能

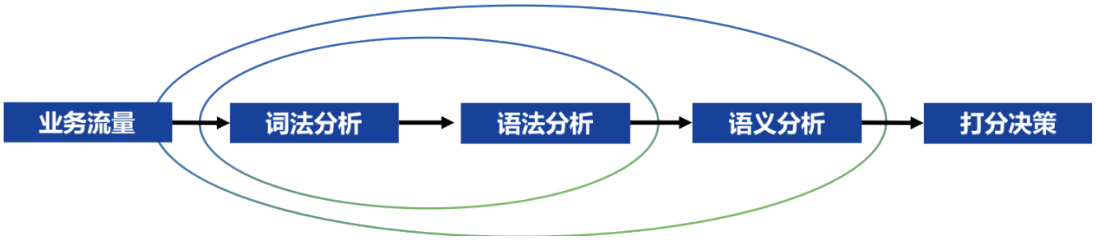
## 3.1 资产梳理及自动防护

明御®Web 应用防火墙可帮助客户主动发现现网环境中存在的 Web 应用系统，并对 Web 业务资产信息进行梳理，梳理的资产信息包括协议类型（HTTP/HTTPS、IPv4/IPv6）、服务器 IP、服务器端口、域名等信息。可让客户快速了解当前已存在的 Web 业务资产信息，并针对梳理的 Web 资产实现自动安全防护。

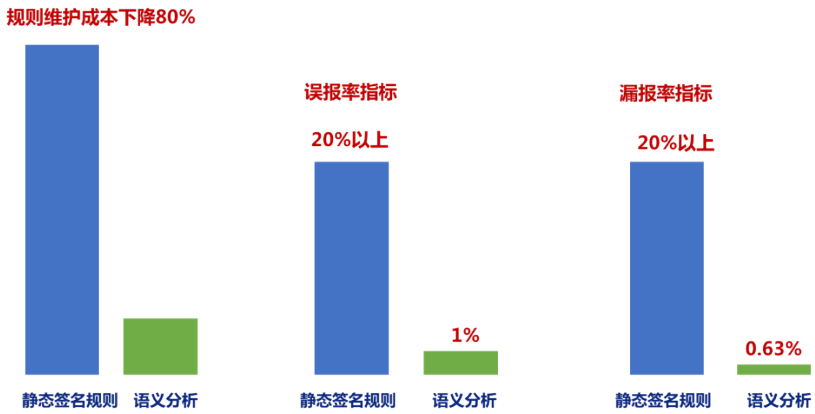
## 3.2 智能语义分析引擎

传统 WAF 安全引擎采用正则静态签名的方式实现对 SQL 注入、XSS、命令注入、WebShell 等 Web 攻击的安全检测，此方式安全引擎的误报率及漏报率较高，难以实现对未知攻击及 0day 的安全防护。

- 明御®Web 应用防火墙的语义分析引擎，采用词法分析和语法分析，并结合上下文进行关联分析，解析异变的 Web 攻击，还原威胁，并通过打分决策模块实现对 Web 攻击的判断。




- 明御®Web 应用防火墙支持 SQL 注入、XSS、PHP 反序列、Java 代码注入、命令注入、ASP WebShell、PHP Webshell 等 13 种基于语义语法检测的 Web 攻击类型，采用语义分析检测方式其攻击检测的误报率和漏报率远远低于采用正则静态签名方式，可大大降低安全管理员对于规则维护的工作量。

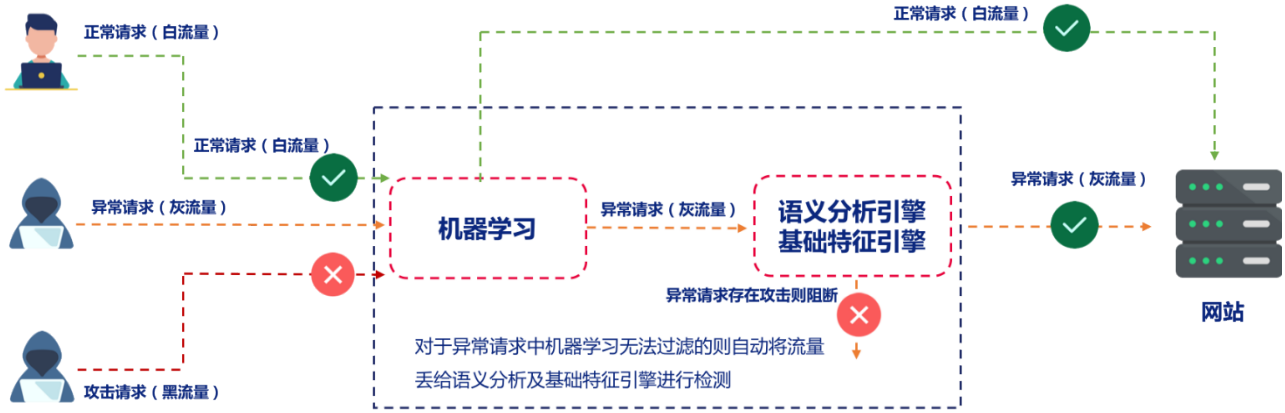



## 3.3 机器学习引擎

机器学习模型是采用统计学算法对网站流量进行学习、训练最终得到白名单业务模型，区别与传统 WAF

的自学习功能，机器学习模型建立的过程无需人工干预，自动进行模型建立和更新，学习的内容包括URL、参数、参数类型、参数长度、Cookie 等信息。

机器学习模型建立完成后，可将流量整体分为白（正常流量）、灰（异常流量）、黑（攻击流量）三大层。如果是正常流量或者攻击流量，由机器学习模型直接放行或者阻断；如果判断是异常流量，则会将流量发给其他安全引擎（语义分析、基础特征等）进一步匹配判断是否为攻击。通过机器学习自主完成已知攻击检测和防御，并具备感知未知威胁或误报漏报的能力，使用户脱离繁琐的规则维护工作。

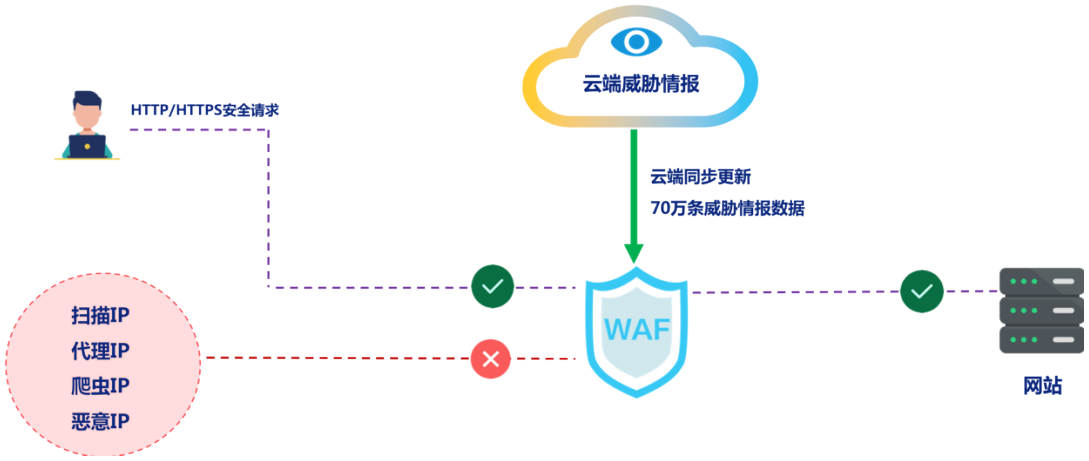



## 3.4 行为分析引擎

明御®Web 应用防火墙采用独创的行为检测算法（已申请国家专利），实现对应用层 DDoS、暴力破解等自动化攻击行为的识别检测拦截。基于 URL、请求头字段、目标 IP、请求方法等多种组合条件进行检测，在独创的检测算法中，采用请求速率、请求集中度、请求离散度等多重检测算法确保检测的准确性。

## 3.5 威胁情报引擎

明御®Web 应用防火墙可与云端威胁情报进行联动，威胁情报数据包括扫描器 IP、代理 IP、C&C 等恶意 IP。威胁情报数据会实时更新，主动发现可疑访问行为，帮助客户快速定位潜在威胁。



## 3.6 IPv4 和 IPv6 双协议栈

透明串接、反向代理、旁路镜像多种部署下均支持 IPv4 和 IPv6 双协议栈，可同时对 IPv4 和 IPv6 的 Web 业务系统进行安全防护，目前产品资质已获得 IPv6 金牌认证。

# 4 产品形态及部署方式

## 4.1 产品形态

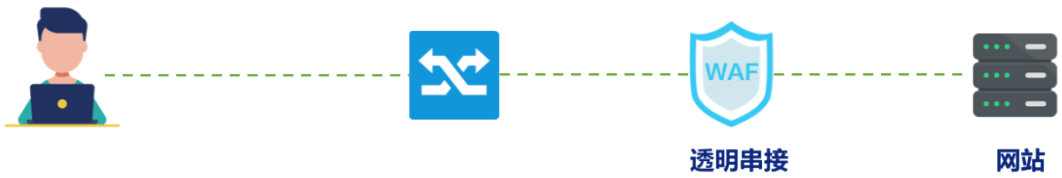
明御®Web 应用防火墙-信创版的产品形态为硬件 WAF。

## 4.2 部署方式

硬件 WAF 支持的部署模式包括：透明代理、反代代理（代理模式）、反向代理（牵引模式）、桥模式、旁路镜像模式。

◆ **透明代理模式**

透明代理模式下，WAF 串接在用户网络中，WAF 业务口无需配置 IP 地址，同时对于经过 WAF 的流量也不会修改源目 IP 地址。

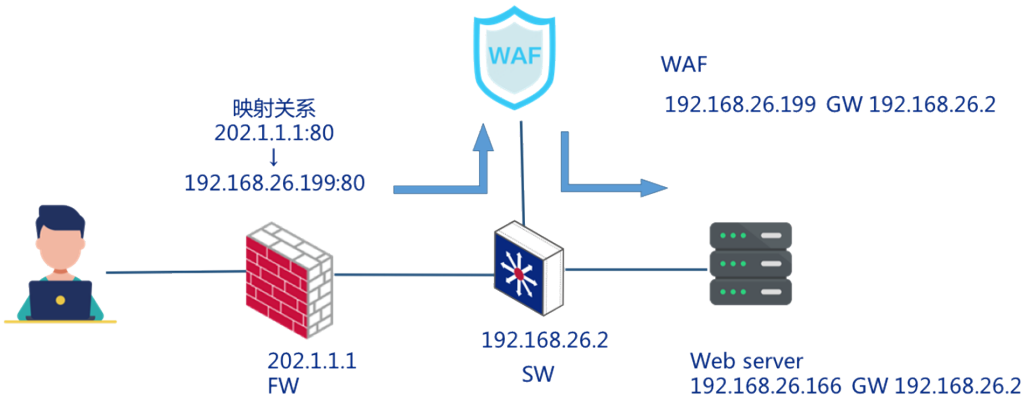



**部署特点：**

a) 不需要改变用户的网络结构。
b) 安全防护能力强。
c) 支持硬件 BYPASS 和软件 BYPASS，故障恢复快。

◆ **反向代理（代理模式）**

适用于现有网络无法串接的环境，部署时需要将公网地址映射到 WAF 前端地址上。客户端与 WAF 前端链路地址建立通讯，WAF 后端链路地址与 Server 建立通讯。

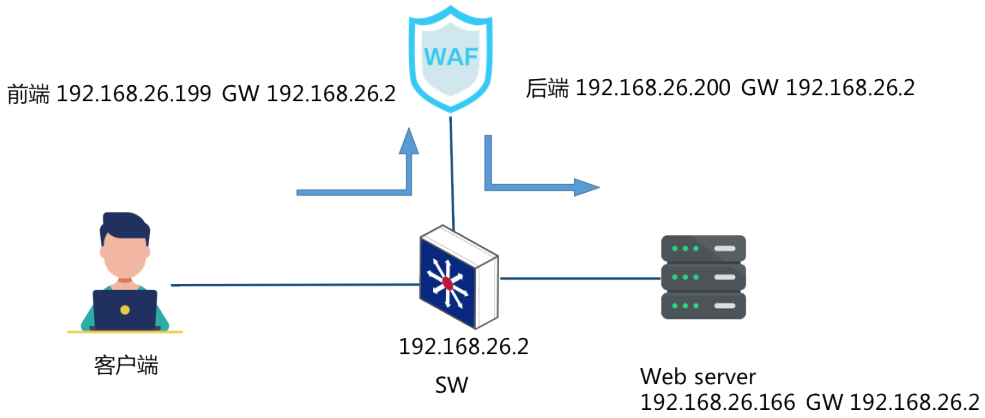



**部署特点：**

a) 旁路部署，防护能力强。
b) 支持 VRRP 主备。
c) 需要改变访问的目的 IP 地址。
d) 不支持硬件 BYPASS，故障恢复速度慢。

◆ **反向代理（牵引模式）**

需要在交换机上单独将用户访问 Server 的 Web 流量通过策略路由的方式牵引到 WAF，策略路由的下一跳地址为 WAF 的前端地址。

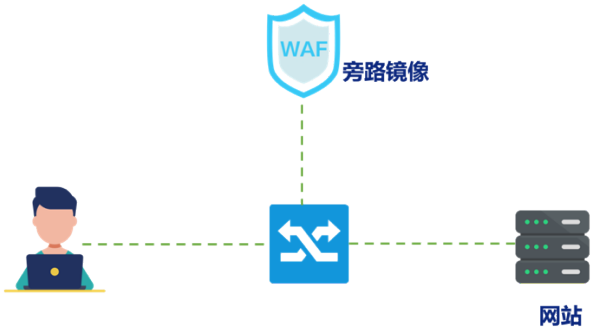



**部署特点：**

a) 旁路部署，防护能力强。
b) 支持 VRRP 主备。
c) 不改变访问的目的服务器 IP。
d) 不支持硬件 BYPASS，故障恢复速度慢。

◆ **旁路镜像模式**

通过交换机将流量镜像到 WAF，部署时不影响在线业务，对于应用流量只进行检测和日志审计，不进行拦截防护。




**部署特点：**

a) 旁路部署，只对流量检测告警不拦截。
b) 部署简单，无需改变现有网络拓扑。

c) 出现故障时不会影响在线业务。