神州云科 Yunke China | DCN

DCFW-1800-WAF-P　WEB 应用防火墙系统

专注与 WEB 应用防护，提供 SSL 加速、抗 DDOS、应用负载均衡、WEB 漏洞扫描等安全模块，是一款多安全引擎、高性价比的 WEB 应用安全产品。

产品概述

DCFW-1800-WAF-P 实现了 IPV4/IPV6 双协议栈下的 HTTP/HTTPS 流量相关内容的实时分析检测、过滤，来精确判定并阻止各种入侵攻击、恶意代码与非法行为，阻断对 Web 服务器的恶意访问与非法操作，并提供实时在线的网站内容防篡改、内容防泄漏、防病毒与敏感信息发布过滤，适应 Web2.0 时代的主动实时监测过滤风险技术，将恶意代码、非授权篡改、应用攻击等众多因素结合在一起进行综合防范，从而做到对 Web 服务器的多重保护。

产品图片

产品特点

多维度的安全可视

从多个维度例如：Web 攻击、入侵防护、病毒防护、Web 访问数据统计等角度，通过攻击地图、柱状图、饼图等图形建模辅以各类数据环绕的方式，详细显示用户 Web 应用系统的安全和运行状态，同时更具备专用的威胁地图监控页面，融合地理识别功能，适合用户在各种运营中心进行安全展示，帮助客户做到安全的全方位可视化，对 Web 应用系统威胁能够做到从宏观到微观的深入全面了解。

WAF+IPS 双擎保护

内置轻量化的 IPS 引擎 ，可以帮助用户一站式解决 Web 应用系统环境中安全关联性较强的如操作系统、数据库系统、网络设备等方面的安全威胁问题，具体包括安全漏洞、溢出攻击等防御模块，同时更具备自定义策略功能，用户可根据自身业务安全需求灵活定制专有的 WAF 及 IPS 策略。

协议安全+内容安全

从协议合规及传输内容安全的角度出发，除了常规的特征库检测手段之外还包括 HTTP 协议内容长度检查、请求及行为方法控制、溢出检查、cookie 过滤、上传/下载类型检测、URL 访问控制、盗链防护、网站隐身、敏感信息过滤等多项可控安全功能，全方位覆盖 OWASP TOP10 威胁内容。

病毒上传过滤

除了 Web 攻击与入侵防御的防御手段之外，还具备 FTP 和 HTTP 协议的文件上传病毒过滤功能，内置实时更新的病毒特征库，从恶意程序和协议识别角度保护用户 HTTP 和 FTP 业务服务器的文件健康，有效避免重要服务器成为病毒程序的扩散源，造成水坑攻击效果，有效防御病毒攻击。

双栈协议支持

在 IPV4 地址资源逐渐枯竭的今天，越来越多的校园网、科研单位网络正在向 IPV6 组网跨越，YK-WAF 满足各类双栈部署环境，同时双向支持 IPV4 及 IPV6 协议栈，帮助用户轻松组建实验网络或帮助从 IPV4 到 IPV6 的过渡，并支持 IPV6 地址的安全检测。

内置 Web 漏洞扫描功能

通过扫描计划任务，周期性的对自己的站点进行高效可靠的扫描工作，尽量在信息安全事件发生前感知 Web 应用系统的漏洞和弱点，及时部署相应的安全保护措施。扫描器可支持的扫描项目包括：SQL 注入漏洞、XSS 脚本漏洞、Web 后门、网页挂马、程序错误信息、内部目录泄露、邮箱地址泄露、无效链接、代码泄露、目录遍历、入侵广告、目录浏览、内部文件泄露、WebDAV 启用、典型登录页面、内部 IP 泄露。

网络及应用层 DOS 攻击防护

针对 Web 应用系统的网络层和应用层攻击防护功能，可以根据多种参数组合方式拦截各类 flood 攻击、cc 攻击，保障正常访问业务连接，阻断异常或非法的请求连接，有效抵御流量及连接型 dos 攻击，保障业务可用。

冗余与业务逃生

支持 HA-active&active 与 HA-active&standby 部署方式，辅以多种探测机制消除单点故障，保障用户 Web 业务稳定可靠运行；支持软件和硬件 bypass，在单机部署时，也可根据合理有效的参数设定快速切换至逃生状态，保障用户业务优先。

Webshell 侦测与阻断

实时监测过滤 WebShell 攻击命令，阻止 WebShell 发起的各种攻击例如：挂马、文件下载、端口扫描、内容篡改等，同时配套专用的 Webshell 监测工具（绿色、操作简单、无需额外组件、支持畸形文件夹文件名、扫描速度快）。

旁路阻断

通过接收交换机镜像流量进行流量分析，不会对真实业务流量产生任何阻止动作及性能瓶颈影响，是最快速易用的部署模式。还支持旁路阻断功能，可以通过设置专用的阻断端口实现 TCPreset 功能，在侦测模式下完成威胁流量的防御拦截。

多种部署模式

根据用户组网需求，YK-WAF 支持多种部署模式，包括对网络拓扑影响最小的透明模式，可以隐藏网站真实 IP 的高安全性反向代理模式，适于快速部署和业务学习的侦测模式，复杂环境中的混合模式，消除单体故障的 HA 主主与 HA 主备模式，充分满足用户的各类组网环境需求。

合规报表

在进行安全事件记录的同时，也可记录所有 Web 访问行为的日志，为调查工作提供完整的追查依据，符合国家网络监管要求，并可进行深度挖掘和关联分析,为用户提供网站应用优化及防御的报表数据支撑。

功能规格

项目	DCFW-1800-WAF-P
网络部署	支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式
	支持 IPv4、IPv6 双栈防护；支持旁路镜像模式下，对检测到的攻击进行旁路阻断
	支持通过 BGP 方式对流量进行牵引，并在清洗攻击后回注，回注过程支持设置 SNAT 策略
Web 安全防御	支持 HTTPS 防护，支持上传证书及密钥；识别和阻断注入攻击；支持防扫描陷阱；支持爬虫防护
	支持文件上传、下载过滤；识别阻断跨站脚本(XSS)攻击；识别阻断跨站请求伪造攻击
	非法上传检测阻断，包括恶意 WebShell 防护；对网页请求/响应内容中的非法关键字进行检测、过滤
虚拟补丁	支持虚拟补丁功能，支持导入 appscan 等第三方扫描器的扫描结果生成 WAF 的规则，对此类网站漏洞直接防护
智能部署	支持网站自学习建模，可通过学习 URL、host 等信息展示网站结构树形图，并支持对 URL 的访问量和响应健康度进行图形化统计；支持自定义防护模板，提供通用、增强、专家的初始防护策略模板；
移动管理	支持通过移动终端管理，实现网站快速应急处置；
威胁情报	支持利用威胁情报规则进行防护，并支持基于威胁情报的日志查询；
应用加速	系统内嵌应用加速模块，通过对各类页面文件高速缓存，提高访问速度
Web 漏洞扫描	提供 Web 站点安全扫描功能；
监控及报表	支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示

选配信息

项目	DCFW-1800-WAF-P
机型	1U ,440mm*330mm*44mm
主板	RIS-191，板载 6 电,
CPU	Intel Celeron　J1900 2.0Ghz
内存	8GB DDR3L
插槽	1 个扩展插槽
网络	6*10/100/1000M
硬盘	1T HDD
电源	75W