神州云科 Yunke China | DCN

DCFW-1800-WAF WEB 应用防火墙产品

产品型号：DCFW-1800-WAF-LAB

产品概述

随着计算机技术的发展和网络及其应用的普及，网络安全日益成为影响网络效能的重要问题。而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，也对网络安全提出了更高的要求。WEB 应用作为最流行的网络应用，在极大方便了人们的办公、信息获取、业务办理的同时，也给攻击者留下了更多的可乘之机，带来了很大的安全隐患。据国家计算机网络应急技术处理协调中心（简称 CNCERT）监测，2015 年中国大陆有近 25 万个网站被黑客攻击，其中我国政府网站被入侵 21674 次，较 2014 年增长 36.7%。作为专业的应用层安全防护产品-WEB 应用安全网关，由于其针对性强、易于实施和管理维护等特点，已经成为实现网站安全防护最重要和最有效的安全网关产品。

神州数码网络有限公司作为国内知名的网络设备供应商，始终关注网络安全的发展。在努力提高网络设备安全性的同时，神州数码网络有限公司依托多年网络产品的研发经验，整合神州数码集团的资源优势，投入到网络安全领域并取得了重大技术突破，DCFW-1800-WAF 系列 WEB 应用安全网关（以下简称 DCNWAF）就是神州数码网络 10 年磨一剑的力作。

神州数码 DCFW-1800-WAF-LAB WEB 应用安全网关是神州数码研究开发的面向教育实验室的新一代高性能应用层网络安全网关。能够为入门型 WEB 应用提供立体化安全防护解决方案.

主要功能

WEB 攻击防护

DCNWAF 使用业界领先的细粒度多核防护引擎，能够实时识别和防护多种针对 WEB 的应用层攻击。例如 SQL 注入、XSS 跨站脚本、代码注入、会话劫持、跨站请求伪造、网站挂马、恶意文件执行、非法目录遍历等攻击手段。

盗链爬虫防护

DCNWAF 能帮助网站防止盗链。盗链大大消耗了网站宝贵的带宽和服务器资源，DCNWAF 能智能识别正常访问和通过盗链网站过来的访问，阻止盗链访问。

网站伪装

DCNWAF 是应用层安全网关，应用层安全防护的重要特性就是会话内容的深度解析。基于这个特性，DCNWAF 修改客户端和网站的交互内容，隐藏网站的有价值信息，以防止这些信息被攻击者利用。

服务器状态监测

DCNWAF 监控网站服务器的访问情况。当网站不能访问时，通过邮件、短信等手段及时通知管理员。

网页防篡改

DCNWAF 对网站的静态页面做镜像备份。当服务器上的网页被篡改时，防篡改功能记录篡改前后的页面内容、篡改时间等信息，作为证据保留日志，并自动恢复被篡改网页和报警。

WEB 应用扫描

DCNWAF 支持漏洞扫描功能，检查网站的漏洞并生成报告。网页内容是在不断更新的，新的网页因为开发者的习惯和水平问题，可能有应用层的漏洞，容易被攻击者利用，造成千里之堤毁于蚁穴的惨剧。

敏感信息过滤

DCNWAF 支持对网站上敏感信息的检查和过滤，防止网站上存在不良信息，防止网站上核心数据等内容的泄露。

DDoS 攻击防护

DCNWAF 采用行为建模和特征相结合的智能 DDoS 攻击识别技术，可防护多种类型的 DDoS 攻击，有效区分正常访问流量和攻击流量，保证正常访问流量的畅通，过滤掉攻击流量。

Cache 加速

DCNWAF 支持 cache 加速功能。当多个客户端在短时间内访问同一个网站页面时，DCNWAF 缓存页面，绝大多数的客户端访问看到的是 DCNWAF 的缓存，加快了网站访问体验。

负载均衡

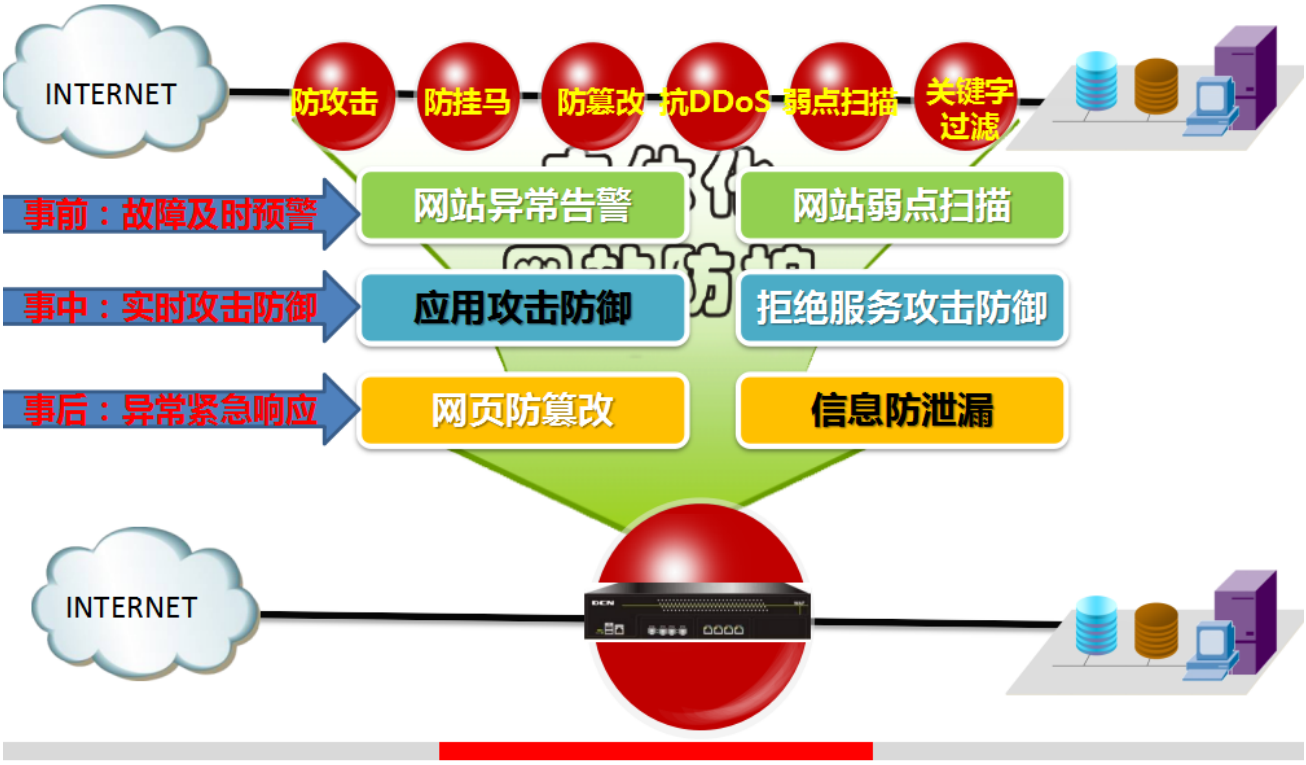
DCNWAF 支持服务器负载均衡功能，能根据 URL 访问请求智能分配会话所访问的网站服务器，是应用层负载均衡。

网站访问统计

DCNWAF 支持网站访问统计功能。从网站流量、访问客户端和被访问页面两个方面做多方面的详细的访问统计。为管理员展示出网站的动态量化数据，为管理员有针对性的优化网站提供很好的参考作用。

主要特性

DCNWAF 如下图，具有立体防御的能力



及时权威的攻击特征库

DCN 应用防御中心监控和分析国内政府、教育、企业行业客户的网站和应用系统出现的漏洞和攻击情况，及时形成 DCNWAF 的检测特征库。通过特征库的不断升级和更新，使 DCNWAF 能够有效检测和防御各种最新的攻击。

强大灵活的策略模板

DCNWAF 具备强大灵活的策略模板机制。在保护多个网站、多个服务器的情况下，能为每个网站和服务器的自身特点自定义不同的防护策略。

安全可靠的产品系统

DCNWAF 采用专用 DCNOS 实时并行操作系统，其并行的处理能力和模块化的结构易于集成和扩展安全功能。并针对多核并行处理进行了全面的优化和安全加固，极大地提高了系统的处理效率、系统稳定性和安全性。

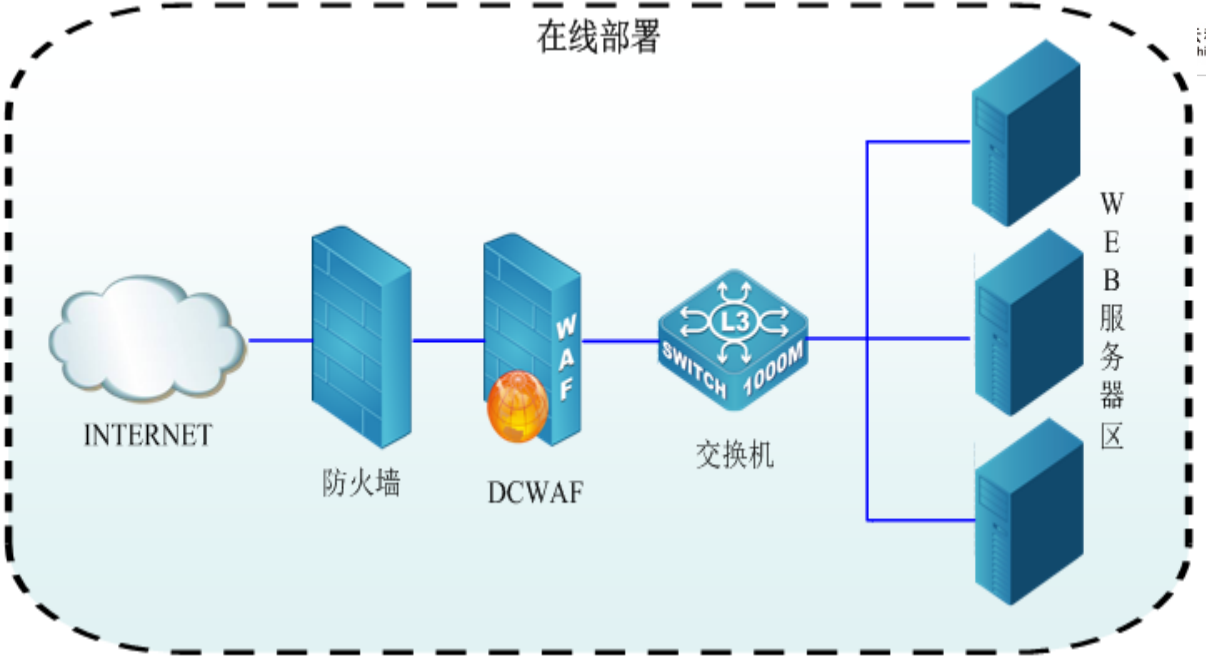
DCNWAF 支持双机热备和 bypass 功能，不会成为网络上的故障点，能够在最大程度上确保企业关键业务的不间断运行。

部署方式

1、无需更改服务器的 IP 地址，需要在 WAF 设备上配置桥 IP

2、WAF 与服务器为同一网段地址，且都是外网地址

3、若 WAF 与服务器不是同一网段的外网地址，只要保证 WAF 到服务器是通的即可。



产品规格

项　目	DCFW-1800-WAF-LAB
网络适应性	支持透明模式、反向代理模式
	支持 802.1q 协议标准 vlan 设置
	支持特定接口组桥时硬件 bypass 功能
	支持静态路由、策略路由配置
WEB 防护功能	支持对指定客户端的 IP 或 URI 进行黑白名单设置
	支持对 http 请求的各个参数进行设置，实现对 http 协议内容的完整性检验
	支持对站点敏感参数进行设置，实现敏感参数的细粒度防护；提供对上传文件格式检查功能
	支持对特定页面或者目录访问的访问控制
	支持对常见攻击如 SQL 注入，跨站脚本，目录遍历，系统命令注入等防护，支持对 OWASP 攻击类型防护
	支持暴力浏览防护
	支持 HTTP CC 防护
	支持通过 http 回复头的处理，实现对网站信息的隐藏
	支持对 http 回复内容敏感信息过滤和隐藏
	支持错误代码过滤功能
	支持对请求体和回复体敏感关键字过滤（如可以过滤色情，发动等关键字）的功能

	PCI DSS6.6 合规
漏洞扫描	支持对指定 WEB 站点进行漏洞扫描
	防篡改
	支持静态页面的 HTTP 方式防篡改
	支持指定目录的 FTP 方式防篡改
告警	支持 WEB 攻击告警、设备状态告警、服务状态告警、漏洞扫描告警、关键字过滤告警
	支持短信及邮件两种告警方式
应用交付	支持 HA 部署
	详尽的日志
	支持系统日志（包含系统日志）、访问日志（包含服务访问日志）、事件日志（包含主机监控日志、告警日志）、防护日志（包含 web 防护日志、防篡改日志、漏洞扫描日志）四大类
丰富的报表	支持时段综合统计、服务访问统计、服务综合统计、Web 攻击统计
	支持柱状，饼状，折线显示

选配信息

型　号	描述
DCFW-1800-WAF-LAB	神州数码 DCFW-1800-WAF-LAB 神州数码 WEB 应用安全网关百兆低端 物理参数：1U 标准机箱，内置 6 个 10/100/1000 以太网电口