# DCFW-1800-E5 系列下一代防火墙

## 全面防护下一代威胁的高性能应用层网关

## 产品概述

DCFW-1800-E5 系列下一代防火墙，可精确识别数千种网络应用，并提供详尽的应用风险分析和灵活的策略管控。内置先进的威胁检测引擎及专业的 WEB 服务防护，能够抵御病毒、木马、SQL 注入、XSS 跨站脚本、CC 攻击等网络攻击，有效保护 WEB 服务器安全。可广泛适用于教育、政府、企业等行业，为网络提供基于角色、深度应用安全的访问控制、IPSec/SSL VPN、应用带宽管理、病毒过滤、入侵防护、上网行为管理等安全服务。

产品图片

## 产品特色

### 精细化应用管控

神州数码下一代防火墙支持深度应用识别技术，可根据协议特征、行为特征及关联分析等，准确识别数千种网络应用，其中包括 200 余种移动应用。在此基础上，神州数码下一代防火墙为用户提供了精细而灵活的应用安全管控功能。

- 应用多维可视化及风险分析。除应用所在分类外，用户可了解到包括应用背景信息、应用风险级别、潜在风险描述、所用技术等详尽信息，如该应用是否大量消耗带宽、是否能够传输文件、是否存在已知漏洞等等。通过多维度的详尽应用分析，用户可制定针对性的安全策略以避免特定应用威胁网络安全。
- 精准应用筛选。神州数码下一代防火墙提供了精细化的应用筛选机制。用户可根据应用名称、应用类别、应用子类别、风险级别、所用技术、应用特征等 6 大条件。精确筛选出感兴趣的应用类型，如具备文件传输功能的通讯软件，或存在已知漏洞、基于浏览器的 WEB 视频应用等等，从而实现精细化的应用管控。
- 灵活应用控制。基于深度应用识别及精细化的应用筛选，神州数码下一代防火墙支持灵活的安全控制功能。包括策略阻止、会话限制、流量管控、应用引流或时间限制等。

### 全面威胁检测与防护

神州数码下一代防火墙提供了基于深度应用、协议检测和攻击原理分析的入侵防御技术，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，为用户提供 L2-L7 层网络安全防护。

- 优化的攻击识别算法。能够有效抵御如 SYN Flood、UDP Flood、HTTP Flood 等 DoS/DDoS 攻击，保障网络与应用系统的安全可用性。

● 专业 Web 攻击防护功能。支持 SQL 注入、跨站脚本、CC 攻击等检测与过滤，避免 Web 服务器遭受攻击破坏；支持外链检查和目录访问控制，防止 Web Shell 和敏感信息泄露，避免网页篡改与挂马，满足用户 Web 服务器深层次安全防护需求。

● 高性能的病毒过滤功能。领先的基于流扫描技术的检测引擎可实现低延时的高性能过滤。支持对 HTTP、FTP 及各种邮件传输协议流量和压缩文件（zip，gzip，rar 等）中病毒的查杀。

● 超过 2000 万条分类库的 URL 过滤功能，可帮助网络管理员轻松实现网页浏览访问控制，避免恶意 URL 带来的威胁渗入。

## 强大的网络适应性

神州数码下一代防火墙具备强大的网络适应能力，具备复杂环境下的安全部署能力，满足用户多样化的网络功能需求。

● 智能链路负载均衡功能。其出站动态探测和入站 SmartDNS 等功能允许网络访问流量在多条链路上实现智能分担，极大提升链路利用效率和用户网络访问体验。

● 内置 VPN 加速芯片。可显著提升 IPSec/SSL VPN 性能，支持大规模网络环境中 VPN 部署。结合 iOS 及 Android 平台下的 VPN 客户端，可为用户提供移动终端远程接入解决方案。

● 支持虚拟防火墙技术。可将一台物理防火墙在逻辑上划分成多个虚拟防火墙，每个虚拟防火墙拥有独立系统资源和独立配置管理平台，可根据不同业务系统的安全需求为不同租户提供专属安全防护，还可对租户间互访的东西向流量进行安全隔离和策略防护。

## 全并行高性能安全

神州数码下一代防火墙在具备全面安全防护的同时，更为用户提供业界领先的安全性能，最大可提供 40Gbps 吞吐能力、50 万新建连接速率（HTTP）及 1200 万并发连接数，其高吞吐、低延时、高并发等高性能优势，可为用户带来更快速的安全体验。

● 一次解析，并行检测。神州数码下一代防火墙采用单次报文解析技术，报文经一次解包后，由各个安全模块并行检测。有效保障在开启多种威胁防护功能时的综合安全性能。

● 全并行软硬件架构。神州数码下一代防火墙基于多核硬件处理架构和拥有自主知识产权的 64 位操作系统 DCFOS，实现软硬件全并行操作。专有算法可在每个 CPU 核上处理所有安全功能，并可将会话负载均分到所有内核，实现最优化的多核并行处理。

# 技术规范

| 功能类别 | 功能细项 |
| --- | --- |
| **应用识别** | 全新一代基于应用特征、行为和关联信息的应用识别<br>支持基于应用风险程度、特征的呈现、控制和审计<br>多达上千种的应用特征库，200+移动应用<br>独立的应用簿和服务簿管理<br>应用特征库通过网络实时更新，升级周期两周<br>支持多种 Web 视频高效引流 |
| **防火墙** | 基于深度应用识别的访问控制<br>基于应用 / 角色的安全策略<br>丰富的路由特性（静态路由、动态路由、ISP 路由、策略路由、BFD 等）<br>强大的 NAT （SNAT、DNAT、NAT444 等）<br>支持各种应用协议的 NAT 穿越 |

| | |
|---|---|
| **攻击防护** | 多种畸形报文攻击防护<br>SYN Flood、DNS Query Flood 等多种 DoS/DDoS 防<br>ARP 欺骗攻击防护<br>支持常见 IP 欺骗和 IP 扫描攻击<br>支持 Ping of Death 和 IP smurf 攻击防护支持攻击防护白名单 |
| **入侵防御** | 基于状态、精准的高性能攻击检测和防御<br>实时攻击源阻断、IP 屏蔽、攻击事件记录<br>支持针对 HTTP、SMTP、IMAP、POP3、VOIP\NETBIOS、TCP、UDP 等近 20 种协议和应用的攻击检测和防御<br>支持缓冲区溢出、SQL 注入和跨站脚本、外链、Web 访问攻击的检测和防护<br>支持超过 3000 种特征的攻击检测和防御，支持特征库实时在线及本地更新<br>支持全局黑名单<br>支持专业的 Web Server 防御及 CC 攻击防御等 |
| **病毒过滤** | 基于流、低延时、高并发、高性能的病毒过滤<br>支持大病毒文件及压缩文件的扫描<br>超过 200 万的病毒特征库，病毒库可以在线及本地实时更新<br>实时病毒连接阻断，病毒事件记录<br>支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描<br>支持在安全域和安全策略上绑定检测防护规则 |
| **网页访问控制** | 基于角色、时间、优先级等条件的 Web 网页访问策略控制<br>基于网页分类类别控制，控制对不良网站访问<br>支持自定义 Web 页面类别<br>总数几千万条域名的分类 Web 页面库，支持 Web 页面库实时更新 |
| **带宽流量管理** | 根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息划分管道<br>对多层级管道进行最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证<br>基于时间和优先级的差分服务，支持带宽均分策略<br>对剩余带宽根据优先级进行弹性分配 |
| **链路负载均衡** | 在多链路环境下，同时提供了入方向和出方向的负载均衡功能<br>Outbound 相关功能包括：基于策略的路由（PBR）、ECMP 及权重、内置 ISP 路由和动态探测<br>Inbound 相关功能包括：SmartDNS（支持 DNS A 记录解析）和动态探测<br>可根据带宽占用及时延情况自动进行链路切换<br>链路健康检查支持通过 ARP、PING、DNS 等方法来检测 |
| **服务器负载均衡** | 支持服务器健康检查和服务器会话保护、支持会话保持<br>支持加权哈希、加权轮询、加权最小会话数等算法<br>支持服务器会话状态的监控 |
| **VPN** | 支持标准 IPSec VPN/L2TP VPN 协议及各种部署方式<br>支持 SSL VPN（可选 USB-key)<br>创新的 PnPVPN( 即插即用 VPN)<br>支持 L2TP over IPSec VPN<br>支持 XAuth<br>支持针对 Android、IOS 等移动设备的 VPN 安全接入 |
| **IPv6** | IPv4/IPv6 双栈 |

| | |
|---|---|
| | NAT64/DNS64<br>IPv6 in IPv4 隧道<br>IPv4 in IPv6 隧道<br>基于 IPv6 的攻击防护<br>支持 IPv6 HA<br>支持记录 IPv6 相关日志 |
| **高可用性（HA)** | 主/主模式（A/A）和主/备模式（A/P)<br>支持 HA Peer Mode 模式<br>配置同步<br>会话同步<br>关键部件冗余 |
| **虚拟系统（VSYS)** | 支持对每个 VSYS 分配系统资源<br>支持 CPU 虚拟化<br>支持防火墙功能<br>支持 IPsec VPN<br>支持统计报表 |
| **日志报表** | 支持用户行为流日志、NAT 转换日志、攻击实时日志、流量警告日志、上网行为管理日志、网络入侵监测日志<br>支持地址绑定协议<br>支持实时流量统计和分析功能<br>支持安全事件统计功能<br>支持基于实名制的日志审计 |

地址 ：北京市海淀区上地九街九号数码科技广场三层 邮箱 ：dcn_support @digitalchina.com
网站 ：www.dcnetworks.com.cn 热线 ：+86 400-810-9119