神州云科 Yunke China | DCN

DCFW-1800E-X 系列下一代防火墙彩页

全面防御下一代威胁的高性能应用层网关

产品概述

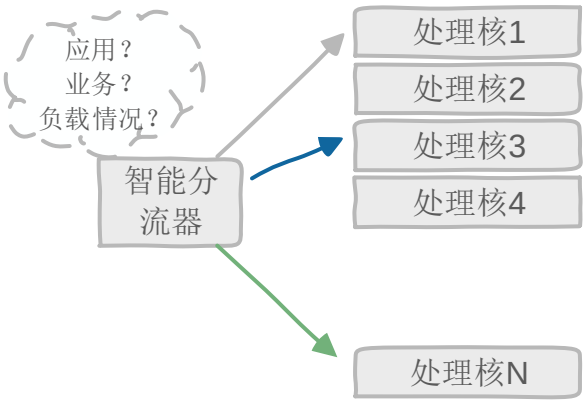
DCFW-1800E-X 系列下一代防火墙，是 DCN 自主研发的面向移动互联时代的全面保障 L2-L7 安全的新一代应用安全网关产品。该系列产品采用多核硬件平台，结合单路径并行处理的用户识别、应用识别和安全检测引擎，实现对用户、应用和内容的深入分析，为用户提供高性能、可视化、精准有效的应用层一体化安全防护体系。下一代防火墙以用户识别、应用识别为基础，提供应用层防火墙、入侵防护、防病毒、反 APT、VPN、智能带宽管理、多出口链路负载均衡、内容过滤、URL 过滤、威胁情报联动等多重安全功能。在软件架构上采用了控制与业务分离的设计，根据业务类型分为控制面（Control Plane，简称 CP）和数据面（Data Plane，简称 DP）两部分，CP 主要处理鉴权、配置、路由、日志和高可用性等管理业务，并提供 WebUI、命令行和 SDN API 等管理接口。DP 则处理网络层、应用层解析和防火墙各项策略的执行。每个 CP 或 DP 都与一个逻辑处理器进行绑定，避免由于系统调度对性能产生负面影响。

产品图片

产品特点

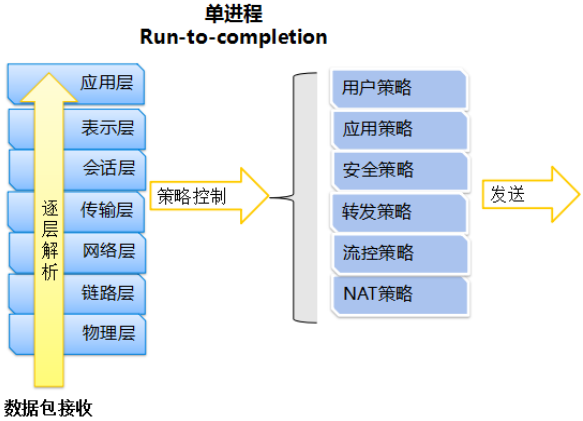
超高的性能

DCFW-1800E-X 系列下一代防火墙采用精于应用层复杂业务运算的多核架构，采用攻击特征库、病毒库树形存储、流扫描处理、零拷贝并行流处理等高效的防御技术，整个解析过程一次拆包，确保开启多重防护功能后依然保证高速度、低时延的安全防护。



一体化的安全引擎

DCFW-1800E-X 系列下一代防火墙为客户提供基于用户和应用的一体化安全防护，用户身份验证和 4 到 7 层的安全防护并行完成，让安全多维度，无死角。匹配数通引擎的数据经过一体化引擎可以根据用户设定并行通过威胁入侵检测、病毒扫描检测、web 安全分类以及内容过滤引擎，有效阻止木马、蠕虫、SQL 注入、XSS 攻击和溢出攻击等，保障文件传输安全，阻断对不良站点和非法链接的访问，并基于内容分析作出防范。



全面的入侵防御

DCN 团队经过多年在网络安全领域沉淀和积累，打造了一支资深的攻击特征库团队和安全服务团队，随时关注业界最新发现的安全漏洞和接收全球用户反馈的攻击特征，并在第一时间做出响应和提供更新，实时完善攻击特征库，提供最及时、最全面的入侵防御。系统支持超过 3000 种预定义攻击特征，可实时在线更新，有效防护蠕虫、SQL 注入、溢出等攻击，保证基础网络安全，通过分级事件及操作配置和虚拟补丁管理创造以人为本网络。

强大的 APT 防御

DCFW-1800E-X 系列下一代防火墙本地拥有 800 万+病毒特征库，配合先进的防病毒引擎，能够精准识别并清除流行木马和顽固病毒，对于未知威胁和 APT 事件，则上交云系统，进行高级模拟分析，获取检测结果和特征升级，为用户信息系统免遭互联网病毒侵扰打造全面立体的防护。

精确的上网行为管理与审计

DCFW-1800E-X 系列下一代防火墙将用户和应用作为安全防护的核心维度，采用先进的用户识别和应用识别技术，实现对用户和应用的精细管控和行为审计。

系统支持基于 IP/MAC 绑定、Radius、LDAP 认证，Portal 认证 等多种身份识别方式。支持上千种网络应用软件的识别和精确控制，包括主流应用、高风险应用和移动终端热点应用，通过对应用行为和内容的深入分析进行更加精细化和准确的管控，使网络管理更贴近用户预期。

智能的带宽管理

DCFW-1800E-X 系列下一代防火墙能够全面识别互联网常见应用，包括经常造成带宽滥用、工作效率降低的 P2P 下载、IM 及时通讯、在线视频、炒股、游戏等。将 DCFW-1800E-X 系列下一代防火墙部署于网络的出口，可以有效地遏制各种应用抢夺宝贵的带宽和 IT 资源，从而确保网络资源的合理配置和关键业务的服务质量，显著提高网络的整体性能。

独立的 VPN 模块

DCFW-1800E-X 系列下一代防火墙内置专用的硬件 VPN 模块，支持 GRE、IPSec、SSL 等多种 VPN 业务模式，支持多种平台移动终端 VPN 接入。 支持对 VPN 隧道内的数据流进行管理，规范 VPN 隧道内上网行为并消除管理盲区。

灵活的组网方式

DCFW-1800E-X 系列下一代防火墙支持 MCE\IPSEC、802.1Q、GRE、VPN track 等网络特性，并支持 PPPoE、DHCP、Vlan、Trunk 等多种接入方式，可以灵活部署在路由模式、透明模式和混合模式的网络中。系统支持 IPv4/IPv6 双协议栈，支持 NAT64、NAT46、NAT66 等地址转换技术，可以方便的部署在 v6、v4 网络边界，为更新升级过程中的网络提供安全方案。

简洁的配置维护

DCFW-1800E-X 系列下一代防火墙的安全策略采用集中展示，独立配置，一体化检测的方案，为用户提供清晰可见的策略展现，最大程度的提升用户配置和查看的体验。防火墙策略、应用控制策略、审计策略、安全防护策略、入侵检测策略、防病毒策略、VPN 策略、流控策略集中展示，独立配置， 管理者可以根据不同的管控需求，为不同的用户定制不同的管理策略，灵活方便，维护简单，条理清晰，效果良好。

超高的可靠性

DCFW-1800E-X 系列下一代防火墙支持双机热备、VRRP 和软硬件 bypass 功能，不会成为网络瓶颈和故障点，确保网络高可靠性。当设备 CPU、内存等参数高于一定阈值时，自动 bypass 设备，让整个设备变为纯透明转发，保证业务不中断。

灵活的虚拟化扩展

DCFW-1800E-X 系列下一代防火墙支持虚拟化技术，DCFOS 安全操作系统可以运行在 KVM、XEN、Vmware 等开源虚拟系统之上，CPU、内存、接口、存储等核心资源全部独立分开，实现真正的资源隔离和管理隔离，根据虚拟资源的分配可以灵活的实现性能提升和平台扩展，是虚拟化和云系统的最佳安全实践。

产品规格

功能类别	功能细项
网络	支持透明、路由、混合三种工作模式
	支持旁路工作模式
	支持物理口、BVI 口、VLAN 口、聚合口、隧道口、环回口
	支持 GRE 接口、GER-KEY
	支持安全域
	支持 PPPoE 客户端
	支持 DHCP 服务器和中继
	支持 DHCP 客户端
	支持静态 ARP、IP-MAC 绑定
	支持 DNS 客户端、服务器
	支持静态路由、基于源地址保持和五元组的等价路由
	动态路由（RIP、OSPF、BGP4）
	支持基于应用和用户的策略路由
	支持基于策略路由的多路径选择、健康检查
	支持源 NAT、目的 NAT、静态 NAT
	支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL * NET
	支持 FTP、TFTP 协议非标准端口 ALG
访问控制	支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙策略
	支持常见 DOS 攻击防护
	支持基于 TCP、UDP 和 ICMP 的扫描防护
	支持智能 TCP Flood 防御
	支持 IPv6/IPv4 TCPFlood、UDP Flood、ICMP Flood、DNS Flood、HTTP FLOOD 攻击防护
	支持基于协议的长连接管理
上网行为控制	支持应用特征和行为的访问控制策略,可对 IM、流媒体、P2P、游戏、股票等应用行为控制
	支持 IM 登陆控制和黑白名单
	支持网页内容和关键字过滤
	支持邮件主题、正文关键字、收件人、发件人过滤
	支持基于 URL 分类库的过滤、URL 查询
	支持 URL 阻断
	支持 URL 阻断提示
上网行为审计	IM 账号、用户名、应用名称和收发消息等行为审计
	内容搜索审计，记录用户、账号、搜索内容
	社区论坛（BBS、博客、微博）账号、内容审计
	邮件账号、收发地址、主题、内容审计
	支持邮件内容记录
	支持电子商务在线购物内容搜索审计
	文件传输命令、文件名审计
	支持基于 URL 分类库的网站访问审计
	支持基于用户和 IP 地址的审计白名单
	支持基于源、目的、规则集的入侵检测。

入侵防御	支持 5 种自定义动作
	可记录攻击日志和报警。
	支持系统规则库手动、自动升级。
	系统定义超过 2000 条规则，包含 Backdoor，bufferoverflow，dosddos，im，p2p，vulnerability，scan，webcgi，worm，game。
	支持 SQL 注入、XSS 攻击防御
	支持 IDS 联动
防病毒	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀
	查杀邮件正文/附件、网页及下载文件中包含的病毒
	支持 800 万余种病毒的查杀，病毒库定期与及时更新
	支持启发式扫描查杀未知病毒
	支持 ZIP/RAR 等压缩文件的病毒查杀
	支持 TAR 等多种打包文件的病毒查杀
流量管理	支持基于线路和通道嵌套的带宽管理
	支持基于接口的上下行带宽管理
	支持高、中、低优先级通道设置
	支持应用、用户、源地址、服务、时间的通道匹配
	支持带宽限制、带宽保障和弹性带宽
	支持每 IP 限速
	支持自动流量整形
	支持基于用户、地址排除策略
用户	支持用户自动识别
	支持本地静态绑定、web 用户认证
	支持 Portal 用户认证
	支持第三方用户认证服务器认证：Radius ladp
	支持基于源接口 / 安全域，目的接口 / 安全域，源 / 目的地址，时间的用户策略
	支持在线用户监控和管理
IPv6	支持 IPv4/IPv6 双协议栈
	支持路由、透明、混合模式部署
	支持 NAT66，支持跨协议转换 NAT64 和 NAT46
	支持 DNSv6 服务器
	支持 IPv6 静态路由
	支持 Ipv6 包过滤
	支持 Ipv6 MAC 绑定和扩展头过滤（命令行）
	支持 Ipv6 策略路由
	支持 Ipv6 隧道；DS - LITE（命令行）
	支持 DHCPv6 服务器（命令行）
	支持设备管理和维护协议：PING、HTTP、HTTPS、SSH、TELNET
VPN	支持标准协议的 IPSecVPN 协议
	支持 SSL VPN 协议，X7160、X8430 支持，X3005 不支持
	支持 FQDN 标识
	支持基于与共享密钥/证书的协商认证方式
	支持网关到网关和远程接入部署模式
	支持地址、ISP 地址对象、服务、时间计划对象化

对象管理	支持应用对象化，含应用对象、应用类
	支持关键字对象化，含网页关键字、应用账号关键字、URL 关键字、邮件关键字等
	支持用户对象，用户静态绑定
	支持第三方用户认证服务器：LDAP、RADIUS
	支持内置 URL 分类库，支持 URL 库在线升级或本地升级
	支持自定义 URL 分类
	支持 1000 多种应用并定期更新
	支持默认自带 3000+入侵防御事件
系统管理	支持网络健康检查模板
	支持 WEB（HTTP/HTTPS）、命令行、Console 进行管理配置
	支持管理员权限划分，可自定义管理员角色，支持只允许授权管理员访问日志
	支持对授权管理员的口令鉴别、U-KEY 双因子认证
	支持管理员用户的第三方用户认证，RADIUS/LDAP
	支持 SNMP v1、v2、v3
	支持 NTP 时钟同步和认证
	支持本地双配置文件
	支持系统资源异常使用监控
虚拟防火墙	支持 web 图形方式的网络调试、诊断命令和抓包
	支支持 L2-L7 业务的完全虚拟化，各虚拟系统独立运行，并且具有独立的管理员配置
高可用性	支持 CPU，内存，网络 I/O 计算资源按需分配
	支持主-主和主-备模式
	备机可通过配置带外管理 IP 进行管理
	支持接口联动
	支持标准的 VRRP 协议
	支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑
	支持 HA 设备之间的会话自动同步，确保 HA 切换时业务不发生任何中断
日志和监控	支持设置抢占优先级，高优先级设备可自动抢占主设备状态
	支持本地系统日志、操作日志、攻击实时日志、应用控制日志、网侵防御日志，病毒防护日志
	支持 Syslog 系统日志、操作日志、NAT 日志、策略日志、应用控制日志、入侵防护日志、病毒防护日志
	支持本地审计日志：IM 日志、搜索日志、社区 / BBS 日志、邮件日志、文件传输日志、电子商务搜索日志、网站访问日志、其他应用审计日志
	支持本地导出为 excel、txt、xml 格式
	支持本地日志存储耗尽机制
	支持弹窗、邮件告警
	支持日志外发
	支持实时流量统计和分析功能
	支持应用流量报表导出 PDF
	支持在线用户监控、查询、冻结
	支持系统会话状态监控
	支持接口状态监控，接口收发包、接口转发速率等
	支持入侵防护统计、病毒防护统计
	支持 URL 访问统计分析、热门网站排名、活跃用户排名、访问分布、访问趋势统计
	支持 Top10 应用的流量统计和趋势绘图

	支持 Top10 用户的流量统计和趋势绘图

选配信息

DCFW-1800E-X3005	DCFW-1800E-X6020	DCFW-1800E-X7160	DCFW-1800E-X8430
MFW-1800X-4GE4SFP	MFW-1800X-8GE	MFW-1800X-8SFP	MFW-1800X-4SFP