DPtech FW1000 系列应用防火墙

杭州迪普科技股份有限公司

产品概述

防火墙作为网络安全的重要防护设备主要应用于以下场景：

区域隔离：通常部署于网络边界，通过不同区域之间的访问控制来实现区域间的安全互访；

分支安全互联（VPN）：通常部署于总部出口和分支机构出口，通过建立连接两端的加密隧道，实现总部 与分支之间的安全互联，避免传输内容被窃取及非授权人员的访问；

地址转换（NAT）：通常部署于互联网出口，通过将私网地址转化成公网地址，解决公网地址不足的问题。

随着互联网的不断发展，应用程序也不断推陈出新。根据第三方权威机构统计，光苹果开发者平台 App Store 一个月之内，就有 47533 款新 App 上线，全部 App 更新 144172 次，而应用程序本身以及使用模式的不断变化正在威胁传统防火墙曾经提供的安全保护。许多应用程序使用非标准端口、动态端口或加密技术来简化用户访问流程。并且用户经常从任意位置访问任意应用程序，以便完成他们的工作。网络犯罪分子充分利用这种不受约束的应用程序以及使用模式威胁企业安全，而依赖端口和协议的传统防火墙无法继续识别和控制网络中的应用程序和威胁。

迪普科技下一代应用防火墙，采用具有自主知识产权的高性能硬件平台 APP-X 及 L2~L7 融合操作系统 Conplat ，两者的结合使得迪普下一代应用防火墙在具备区域隔离、VPN、地址转换 NAT、应用控制、入侵防御、URL 过滤等丰富安全防护功能的同时，还具备高性能、虚拟化、强组网、IPv6、功能和性能弹性扩展等特性。DPtech FW1000 系列应用防火墙拥有从百兆到 T 级，从盒式到框式的各类产品款型，可应用于互联网出口、数据中心、分支机构安全互联等复杂场景，满足各类用户需求。

产品特点

■ **基于用户的应用访问控制**

防火墙作为网络最基本的安全设备，访问控制策略是实现安全防护的基本手段。而基于用户的应用访问控制策略，能够保证不论接入人员物理位置如何变化，只要其用户权限不变，安全策略就能始终作用在该用户身上，防止越权访问，并且管理人员不再需要实时地添加或修改控制策略，极大的减轻了工作量。同时基于应用的识别能力，使得对用户的访问控制能够精确到应用，防护更加灵活准确。

■ **独创的 N:M 虚拟化，应用能力按需调度**

虚拟化技术是目前业界最受关注的技术之一，越来越多的网络和服务器都已采用虚拟化技术，而针对应用虚拟化的要求，迪普科技具有独创的 N:M 虚拟化技术，可将多台设备虚拟化成一台设备或将一台设备虚拟化成多台设备，用户可将应用能力资源池化，并根据业务要求灵活的按需调度。

■ **支持丰富功能特性，提供全面防护能力**

具备区域隔离、NAT、VPN 功能的同时，还支持应用控制、URL 过滤、入侵防御、链路负载均衡等丰富功能。一台设备满足绝大部分的建设需求，简化网络结构的同时节约用户的建设成本。

■ **智能生成安全策略**

DPtech FW1000 系列下一代应用防火墙能够对一定时间内的日志数据进行分析和统计，自动学习和发现会话日志中的访问流量，从而智能生成符合当前网络状态的安全策略。此外，DPtech FW1000 还能统计一定时间内安全策略的命中数量，帮助运维人员发现无用的安全策略，迅速完成策略梳理。

■ **灵活组网能力，适应各种网络环境**

DPtech FW1000 系列应用防火墙支持丰富的网络特性，支持静态路由、策略路由、RIP v1/v2、OSPF、BGP 等多种路由协议，支持 MPLS VPN，支持组播协议，支持 IPv6；同时，DPtech FW1000 产品可支持路由模式、透明模式、混合模式组网，可适应各种复杂组网环境。

■ **专业的数据流分析工具，迅速排查网络故障**

迪普科技为 DPtech FW1000 系列下一代应用防火墙专门配置了数据流分析工具，能够模拟一个数据包从设备入接口到出接口所经过的所有功能模块，通过设备反馈的处理情况，用户能够详细了解数据包的处理过程，准确定位数据包状态，迅速排查网络故障。

■ **网络高可靠性保障**

DPtech FW1000 支持关键部件冗余及热插拔，可支持 N+1 业务板卡冗余，实现 RAID 级的网络高可靠性*,同时还支持基于状态的双机热备，设备发生故障后确保原有的网络连接不会中断，实现真正的无缝切换。

■ **高效处理能力**

相较于传统防火墙，迪普科技 FW1000 应用防火墙基于自主研发的高性能硬件架构平台，保障了在大带宽和高并发的背景下，仍能够提供稳定高效的安全防护能力，不再成为网络瓶颈。

产品系列


FW1000-TE-17N


FW1000-TA-N


FW1000-Blade-EI


FW1000-Blade-AI


FW1000-Blade-S


FW1000-TA-A


FW1000-TM-E


FW1000-TS-E


FW1000-TS-A


FW1000-GE-N


FW1000-GA-E


FW1000-GM-A


FW1000-GM-E


FW1000-GM-N


FW1000-GS-N


FW1000-GC-N


FW1000-ME-N


FW1000-MA-N


FW1000-MS-N


FW1000-NG

功能价值

技术优势	功能价值
部署灵活	支持路由模式、透明模式、混合模式
基于用户的访问控制	基于用户部署应用访问控制策略，保证不论用户物理位置如何变化，使用什么种类的应用程序，只要其用户权限不变，安全策略就始终紧跟用户
丰富的 NAT 能力	支持一对一、地址池等 NAT 方式；支持多种应用协议，如 FTP、H.323、RAS、RTSP、SIP、ICMP、DNS、PPTP、NBT 的 NAT ALG 功能，支持组播 NAT*
虚拟化	支持 N:M 虚拟化，可将 N 台设备虚拟成一个资源池，再将资源池按需分成 M 台逻辑设备，实现云计算环境下资源池的动态调度
优异性能	可提供超过 2.56Tbps 单设备性能*，并可通过 N:M 虚拟化进行性能聚合，实现性能的倍增
全内置 VPN	支持 IPSec VPN、L2TP VPN、GRE VPN、SSL VPN，并且全内置硬件加密芯片，减少安全建设投入
广泛网络特性	支持 IPv4/IPv6，支持静态路由、策略路由、RIP v1/2、OSPF、BGP 等多种路由协议，支持 MPLS VPN，支持组播协议
入侵防御能力	可提供专业的入侵防御（IPS）能力，实现深入的应用层攻击防护；专业漏洞库团队提供实时可灵活升级的攻击特征库；支持配置入侵防御还原点，备份 IPS 规则、自定义 IPS 特征、接口 IPS 策略、全局 IPS 策略、IPS 黑名单联动、IDS 联动、协议防护策略、IPS 协议端口、IP 仿冒的配置信息
上网行为管理	支持 5000 条专业协议库，超过 8000 万条 URL 库，可识别主流应用及网站，实现细粒度的上网行为管理
高可靠性	N:M 虚拟化、双机状态热备、静默双机、VRRP 多主等多种模式，关键部件冗余及热插拔，支持 N+1 业务板卡冗余以及独创的应用 Bypass 技术*，真正的网络高可靠性

日志与报表	支持独立的日志服务器，日志可自动定时备份；内置数百种报表，可图形化的查询、审计、统计、检索内网用户的各种网络行为日志，方便管理者了解和掌控网络，支持通过对日志的统计整理，智能生成包过滤策略
设备管理	提供便捷的图形化管理界面，支持 Web GUI、SSH、串口 Console，并支持通过 UMC 网管平台集中管理；支持 NTP 协议，可作为 NTP Server，也可作为 Client 设备

* 此特性仅在高端框式设备上支持