PH F4100 系 NGFW 下一代防火墙产品

产品概述

PH F4100 系列是圃惠基于先进的 MIPS 嵌入式多核构架，搭载自主研发的操作系统的下一代防火墙产品。F4100 系列通过单路径并行处理的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、直观、有效的应用层一体化安全防护体系。

PHF4100 系列支持 4 层嵌套的带宽管理技术，结合智能路由等全面的网络层支撑以及双机热备高可靠性保障，可灵活的部署在透明、NAT、VPN、多出口、双链路等网络环境中，帮助用户方便安全的开展业务的同时简化网络安全架构，是下一代网络安全防护的最佳选择。

圃惠 F4100 系列防火墙包括可满足各行业不同级别的安全组网需要，为用户提供了多样化的选择。

主要特性

- **多业务高性能**

圃惠下一代防火墙采用先进的 MIPS 多核架构，结合圃惠自主知识产权的安全操作系统，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攻击技术，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。

- **精细的上网行为管理**

圃惠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可视化展现及有效管控。

系统支持 IP/MAC 绑定，同时可以基于 Radius、LDAP 认证，Portal 认证、微信认证、短信网关等多种身份识别。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。

- **全面的入侵防御**

圃惠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。

  - 超过 3000 种预定义攻击特征
  - 实时在线更新
  - 防蠕虫防攻击

- 保证基础网络安全
- 分级事件及操作配置
- 虚拟补丁管理
- 创造以人为本网络

- **专业的病毒查杀**

圃惠下一代防火墙拥有海量病毒特征库，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。查杀范围包括病毒、木马、蠕虫、后门、间谍软件、恶意程序以及HTTP\FTP\SMTP\POP3\IMAP 等主流应用协议，超过 200 万病毒特征全库模杀，特征库实时在线更新。针对纯扫描优化的产品架构，无系统监控，不占系统资源，是保护内网资源不受互联网病毒侵扰的最佳选择。

- **遏制带宽滥用**

圃惠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 即时通讯、在线视频、炒股、游戏等。将圃惠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**

内置专用的硬件 VPN 模块，支持 GRE、IPSec、SSL VPN 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。通过配置我司的集中管理软件，可对零散的 VPN 分支做集中式管理，可实现统一配置下发、告警集中处理、统一日志上报，有效减少管理员工作量。

- **组网方式灵活**

圃惠下一代防火墙支持 MCE、IPSEC、802.1Q、GRE、VPN track、反向路由注入等网络特性，并支持路由模式、透明模式、旁路模式和混合模式，可在任意复杂的网络环境中灵活组网。

- **配置维护简洁**

圃惠下一代防火墙的安全策略集成用户识别、应用控制，URL 过滤、入侵检测、防病毒、VPN 等，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，六大功能只需一条策略，灵活方便，维护简单，条理清晰，效果良好。在大规模部署时，可通过圃惠集中管理系统对分布部署的下一代防火墙进行统一的配置策略下发、攻击事件监控和攻击事件分析。

- **高度可靠性**

  圃惠下一代防火墙支持双机热备和软硬件 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。

软件功能

项目	PH F4100-AVG-M2030
硬件规格	1U，8 个千兆电口，2 个千兆光口，2 个万兆光口；标配 1T 硬盘；固化交流电源
网络功能	支持透明、路由、混合三种工作模式，支持链路捆绑 支持源 NAT、目的 NAT、端口 NAT、静态 NAT 支持 Vlan、VRF 支持 Wlan、3G 无线接入 支持 DHCP server 和 DHCP Relay、DNS sever 和静态 DNS 支持静态路由、策略路由、ISP 路由、源接口路由 支持基于应用的路由 支持动态路由 OSPF、RIP、OSPFv3 支持路由探测功能 支持 IPv6 静态路由、路由通告和隧道转换
防火墙	并发连接数 300 万，新建连接数 8 万 支持基于用户、应用、源目的接口、源目的 IP、服务和时间的八元组一体化策略 支持地址、服务、时间表、应用、用户资源化 支持基于策略的长连接 支持策略命中次数统计和清零 支持策略优先级调整 支持 IPv6 安全策略 支持会话统计、监控、临时阻断和全局会话限制
安全防护	支持 IP-MAC 绑定、ARP 欺骗防护和 ARP Flood 攻击防护 支持 IPv4 异常包攻击防护，包括：Ping of Death、Land-Base、Tear Drop、TCP Flag Winnuke、Smurf、Jolt2 等 支持端口扫描防护和 IP 扫描防护 支持基于接口和 IP 的 SYNFlood、UDPFlood、ICMPFlood、DNSFlood 攻击防护 支持手动、自动攻击防护的黑名单记录 支持 IPv6 异常包攻击防护，包括：Winnuke、Land-Base、TCP Flag、Fraggle、IP Spoof

	共享接入管理
VPN	支持各种标准的 IPSecVPN 协议及部署方式 支持基于策略和基于路由的 IPsecVPN 支持 CA 中心和 X.509 格式证书 支持 VPN Track 支持 SSLVPN 隧道模式 支持 GREVPN 支持 VPN 隧道下的安全防护和带宽管理
病毒防护	支持基于 HTTP\FTP\SMTP\POP3\IMAP 协议的病毒过滤 支持禁止特定文件类型通过 支持最大 20 层的压缩文件查毒 支持病毒库手动和自动更新 支持恶意 URL 过滤
入侵检测	支持协议自动识别 支持超过 3000 种预定义的攻击特征 支持特征库的自动和手动更新 支持对蠕虫、木马后门、网络钓鱼等的安全防护
上网行为管理	支持对 IM 软件登陆和收发消息的控制 支持对 P2P、流媒体等影响工作效率的软件控制 支持网络游戏控制 支持股票行情和交易的行为控制 支持电子邮件收发、附件大小过滤 支持设置行为审计策略 支持 URL 分类过滤
AC 功能	可对圃惠 AP 进行管理，默认主机配置 64 个 AP 管理授权
用户管理	支持防火墙本地用户认证 支持标准的 Radius、LDAP 等第三方用户认证 支持微信用户认证和短信网关 支持 Portal 用户认证 支持用户在线监控和超时管理 支持集中用户策略管理
流量管理	支持基于通道、接口、用户、应用的多级嵌套的带宽管理 支持带宽优先级管理 支持最大带宽限制、最小带宽保证和弹性带宽 支持每 IP 限速 支持排除策略
可视化	支持实时的 CPU、内存、接口流量等设备健康统计 支持饼图、柱图、趋势图等多种方式展现用户和应用的流量统计 支持用户和应用排名的实时展现

	支持系统事件和安全风险的实时告警
系统管理	支持系统管理员和只读管理员 支持管理员唯一性检查、超时管理 支持系统时间手动设定和 NTP 同步 支持双系统配置文件备份 支持系统文件手动升级 支持 SNMPv1/v2/v3 支持主备、主主两种模式的双机热备 支持接口状态同步和接口状态探测 支持 PING、TRACERT、TCPSYN 方式进行系统诊断 支持系统信息定期收集