H3C F1000-AK1030防火墙

产品名称	H3C F1000-AK1030防火墙
公司名称	山东神州四季通信技术有限公司
价格	.00/个
规格参数	H3C:H3C 型号:F1000-AK1030 产地:杭州
公司地址	济南数码港大厦A-1007（山大路47号）
联系电话	0531-81819991 18653187795

产品详情

H3C SecPath F1000-AK1030防火墙设备：1U机架式设备，8个千兆电口+2对Combo口

随着网络技术的不断普及与发展，网络攻击行为出现得越来越频繁。通过各种攻击软件，只要具有一般计算机常识的初学者也能完成对网络的攻击，同时，各种网络病毒的泛滥，也加剧了网络被攻击的危险。

H3C SecPath F1000-AK系列AI防火墙是面向商业市场的高性能、多千兆和超万兆的智慧型安全网关产品，硬件上基于多核处理器架构，实现了业务高速处理能力，并提供丰富的接口扩展能力。同时作为NGFW（下一代防火墙）的升级产品，不仅支持丰富的安全审计功能，而且增加硬盘后还可以有效支持WEB缓冲等多种应用加速功能。

在功能方面，H3C SecPath F1000-AK系列AI防火墙除支持安全控制、VPN、NAT、DOS/DDOS防御等防火墙安全功能外，还一体化地集成了IPS、AV、WAF、应用控制、DLP、URL分类及自定义过滤等深度安全防御的功能，实现了基于用户、应用等多维度的策略控制功能，能有效的保障网络的安全。H3C SecPath F1000-AK系列AI防火墙还集成了AI计算能力，针对未知威胁和APT攻击能够提供有力的防护。同时，基于AI技术，能有效提高产品

的运维体验效果。

在虚拟化和可靠性方面，基于H3CComwareV7平台，多系列支持多设备集群及1:N虚拟化，更好地适应云计算要求的弹性扩展能力。

人工智能特性

H3C SecPath F1000-AK系列AI防火墙是集成了AI分析引擎的新一代防火墙，在有效应对传统网络安全威胁的基础上还能够：

识别加密和新型应用，提供更加准确、精细和灵活的安全管控策略；

识别恶意的加密流量，发现隐藏在正常加密流量中的恶意行为；

识别异常、威胁和攻击等安全风险，为应急响应提供决策和依据；

与云端和态势感知等平台相结合，提供全方位的协同防御。

H3C SecPath F1000-AK系列AI防火墙是一个持续演进的产品，是AI综合网络安全解决方案中的关键部分，也是网络安全主动防御体系中的必要环节，将朝着弹性架构、加密分析、AI赋能、协同防御的方向不断推进。

高性能的软硬件处理平台

H3C SecPath F1000-AK1000系列采用了先进的64位多核高性能处理器和高速存储器。

H3C SecPath F1000-AK1000系列采用CPU+Switch架构，CPU进行安全业务处理，Switch实现多业务端口的扩展。

电信级设备高可靠性

采用H3C公司拥有自主知识产权的软、硬件平台。产品应用从电信运营商到中小企业用户，经历了多年的市场考验。

支持H3C SCF虚拟化技术，可将多台设备虚拟化为一台逻辑设备，对外呈现为一个网络节点，资源统一管理，完成业务备份同时提高系统整体性能。

强大的安全防护功能

支持丰富的攻击防范功能。包括：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP分片报文、ARP欺骗、ARP主动反向查询、TCP报文标志位不合法、超大ICMP报文、地址扫描、端口扫描等攻击防范，还包括针对SYN Flood、UDP Flood、ICMP Flood、DNS Flood等常见DDoS攻击的检测防御。

支持SOP 1:N完全虚拟化。可在H3C SecPath F1000-AK12X2/AK13X2设备上划分多个逻辑的虚拟防火墙，基于容器化的虚拟化技术使得虚拟系统与实际物理系统特性一致，并且可以基于虚拟系统进行吞吐、并发、新建、策略等性能分配。

支持安全区域管理。可基于接口、VLAN划分安全区域。

支持包过滤。通过在安全区域间使用标准或扩展访问控制规则，借助报文中UDP或TCP端口等信息实现对数据包的过滤。此外，还可以按照时间段进行过滤。

支持基于应用、用户的访问控制，将应用与用户作为安全策略的基本元素，并结合深度防御实现下一代的访问控制功能。

支持应用层状态包过滤（ASPF）功能。通过检查应用层协议信息（如FTP、HTTP、SMTP、RTSP及其它基于TCP/UDP协议的应用层协议），并监控基于连接的应用层协议状态，动态的决定数据包是被允许通过防火墙或者是被丢弃。

支持验证、授权和计帐（AAA）服务。包括：基于RADIUS/HW TACACS+、CHAP、PAP等的认证。

支持静态和动态黑名单。

支持NAT和NAT多实例。

支持VPN功能。包括：支持L2TP、IPSec/IKE、GRE、SSL等，并实现与智能终端对接。
支持丰富的路由协议。支持静态路由、策略路由，以及RIP、OSPF等动态路由协议。
支持安全日志。
支持流量监控统计、管理。

灵活可扩展的一体化DPI深度安全

与基础安全防护高度集成的一体化安全业务处理平台。
全面的应用层流量识别与管理：通过H3C长期积累的状态机检测、流量交互检测技术，能精确检测Thunder/Web Thunder（迅雷/Web迅雷）、BitTorrent、eMule（电骡）/eDonkey（电驴）、微信、微博、QQ、MSN、PPLive等P2P/IM/网络游戏/炒股/网络视频/网络多媒体等应用；支持P2P流量控制功能，通过对流量采用深度检测的方法，即通过将网络报文与P2P协议报文特征进行匹配，可以精确的识别P2P流量，以达到对P2P流量进行管理的目的，同时可提供不同的控制策略，实现灵活的P2P流量控制。
高精度、高效率的入侵检测引擎。采用H3C公司自主知识产权的FIRST（Full Inspection with Rigorous State Test，基于精确状态的全面检测）引擎。FIRST引擎集成了多项检测技术，实现了基于精确状态的全面检测，具有极高的入侵检测精度；同时，FIRST引擎采用了并行检测技术，软、硬件可灵活适配，大大提高了入侵检测的效率。
程序。
海量URL分类过滤：支持本地+云端方式，139个分类库，超2000万条URL规则。
全面、及时的安全特征库。通过多年经营与积累，H3C公司拥有业界攻击特征库团队，

同时配备有攻防实验室，紧跟网络安全领域的动态，从而保证特征库的及时准确更新。H3C公司是中国国家信息安全漏洞库（CNNVD）一级技术支撑单位和国家信息安全漏洞共享平台（CNVD）技术组成员。

业界IPv6

支持IPv6状态防火墙，真正意义上实现IPv6条件下的防火墙功能，同时完成IPv6的攻击防范。

支持IPv4/IPv6双协议栈，并支持IPv6数据报文转发、静态路由、动态路由及组播路由等功能。

支持IPv6各种过渡技术，包括NAT-PT、IPv6 Over IPv4 GRE隧道、手工隧道、6to4隧道、IPv4兼容IPv6自动隧道、ISATAP隧道、NAT444、DS-Lite等。

支持IPv6 ACL、Radius等安全技术。

下一代多业务特性

集成链路负载均衡特性，通过链路状态检测、链路繁忙保护等技术，有效实现企业互联网出口的多链路自动均衡和自动切换。

一体化集成SSL VPN特性，满足移动办公、员工出差的安全访问需求，不仅可结合USB-Key、短信进行移动用户的身份认证，还可与企业原有认证系统相结合、实现一体化的认证接入。

数据防泄漏（DLP），支持邮件过滤，提供SMTP邮件地址、标题、附件和内容过滤；支持网页过滤，提供HTTP
URL和内容过滤；支持网络传输协议的文件过滤；支持应用层过滤，提供Java/ActiveX Blocking和SQL注入攻击防范。

入侵防御（IPS），支持Web攻击识别和防护，如跨站脚本攻击、SQL注入攻击等。

防病毒（AV），高性能病毒引擎，可防护500万种以上的病毒和木马，病毒特征库每日更新。

未知威胁防御，借助态势感知平台，NGFW可以快速发现攻击、定位问题，确保一旦单点受到攻击，全网实施策略升级及综合预警、响应。

智能管理

支持智能安全策略：一体化安全策略、实现策略冗余检测、策略匹配优化建议、动态检测内网业务动态生成安全策略。

支持标准网管 SNMPv3，并且兼容SNMP v1和v2。

提供图形化界面，简单易用的Web管理。

可通过命令行界面进行设备管理与防火墙功能配置，满足管理和大批量配置需求。

通过H3C IMC SSM安全管理中心实现统一管理，集安全信息与事件收集、分析、响应等功能为一体，解决了网络与安全设备相互孤立、网络安全状况不直观、安全事件响应慢、网络故障定位困难等问题，使IT及安全管理员脱离繁琐的管理工作，极大提高工作效率，能够集中精力关注核心业务。

基于先进的深度挖掘及分析技术，采用主动收集、被动接收等方式，为用户提供集中化的日志管理功能，并对不同类型格式（Syslog、二进制流日志等）的日志进行归一化处理。同时，采用高聚合压缩技术对海量事件进行存储，并可通过自动压缩、加密和保存日志文件到DAS、NAS或SAN等外部存储系统，避免重要安全事件的丢失。

提供丰富的报表，主要包括基于应用的报表、基于网流的分析报表等。

支持以PDF、HTML、WORD和TXT等多种格式输出。

可通过Web界面进行报告定制，定制内容包括数据的时间范围、数据的来源设备、生成

周期以及输出类型等。