H3C SecPath F1000-AI 系列防火墙

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-AI 系列防火墙面向行业市场的高性能多千兆和超万兆防火墙 VPN 集成网关产品，硬件上基于多核多线程 MIPS/ARM 处理器+ASIC 硬件架构，为 1U 的独立盒式防火墙。该系列防火墙产品提供丰富的接口扩展能力，设备同时支持 Telemetry 和 Netconf 网络扩展协议，能够适应多种网络部署要求。作为 NGFW 产品，丰富的审计功能是必不可少的，所以产品系列可以扩展大容量硬盘，同时增加硬盘后还可以有效支持 web 缓冲等应用加速功能。

在安全功能方面，F1000-AI 系列作为 NGFW 产品，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、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、时间、地理位置、安全状态等多维度的策略控制功能。

产品系列集成了 AI 计算能力，针对未知威胁和 APT 攻击提供有力的防护。同时，基于 AI 技术，简化产品的运维体验。

在虚拟化和可靠性方面，基于 H3C 领先的 Comware V7 平台，支持多设备集群及 1:N 虚拟化。更好地适应云计算的要求的弹性扩展能力。

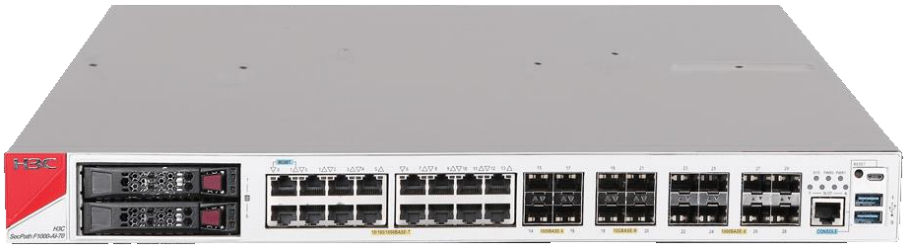
H3C SecPath F1000-AI-03 产品外观图

H3C SecPath F1000-AI-05 产品外观图

H3C SecPath F1000-AI-10/15 产品外观图

H3C SecPath F1000-AI-25/35/55 产品外观图

H3C SecPath F1000-AI-60 产品外观图



H3C SecPath F1000-AI-70 产品外观图

H3C SecPath F1000-AI-65/75 产品外观图

H3C SecPath F1000-AI-80/90 产品外观图

产品特点

人工智能特性

F1000-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。

F1000-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。

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。
- 虚拟化：支持虚拟防火墙的创建、启动、关闭、删除功能。

强大的安全防护功能

- 支持 IPv4/IPv6 双栈安全策略功能，支持基于五元组、安全域、时间段等多维度访问控制。
- 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、UPD Flood、ICMP Flood、DNS Flood 等常见 DDoS 攻击的检测防御。
- 最新支持 SOP 1:N 完全虚拟化。可在 H3C SecPath F1000-AI 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。
- 支持应用识别，且可以基于应用、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/HWTACACS+、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。
- 国密算法：支持国密 SM1/2/3/4 算法。

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。
- 实时的病毒防护：采用流引擎查毒技术，可迅速、准确查杀网络流量中的病毒等恶意代码。
- 海量 URL 分类过滤：设备支持根据 URL 类别实现 URL 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 公司拥有业界资深的攻击特征库团队，同时配备有专业的攻防实验室，紧跟网络安全领域的最新动态，从而保证特征库的及时准确更新。

业界领先的 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（IPV4&IPV6）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。支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略，且缺省动作支持黑名单。
- 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。支持基于文件协议、共享协议（NFS/SMB）的病毒功能。动作响应，可发现病毒发送的告警信息，支持用户编辑告警内容。
- 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。
- 深入的 WEB 安全防护 不局限于常规的 IPS/AV 防护，针对内网服务器，提供细致化的 web 应用防护，对于服务器最为头疼的 CC 攻击，异常外联，SQL 注入、HTTP 慢速攻击、跨站脚本等常见攻击行为，对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。
- 支持智能终端识别， 终端识别是建立物联网安全连接的重要前提，用于识别物联网中的终端，。当终端流量流经设备时，H3C 安全网关可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时向用户发送日志，提示用户。同时采用应用检测方式和 IPID 检测方式对通过 NAT 技术或代理技术进行共享上网的行为进行识别和管理。
- 资产扫描，支持资产发现功能，能够扫描发现内网主机开放的端口，服务，发现风险，识别威胁。
- 未知威胁检测 单靠特征分析已不足以应对复杂的网络环境，面对典型的 APT（Advanced Persistent Threat，高级持续性威胁）攻击沙箱技术是防御 APT 攻击最有效的方法之一，它用于构造隔离的威胁检测环境。H3C 安全网关通过将网络流量送入沙箱进行隔离分析，由沙箱给出是否存在威胁的结论。检测到某流量为恶意流量，设备将对流量实施阻断等处理。

专业的智能管理

- 支持智能安全策略：支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调

优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略，动态检测内网业务动态生成安全策略并推荐。

- 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，满足专业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。
- ISSU（In-Service Software Upgrade，不中断业务升级）是一种可靠性高的升级设备启动软件的方式。通过 ISSU 升级，能够确保在升级过程中业务不中断或者中断时间较短。
- 将 BLS、ATK、CFGLOG 细分为五类日志，支持真分页功能，增加清除功能，支持独立模块设置日志参数，分页查询和配置日志。

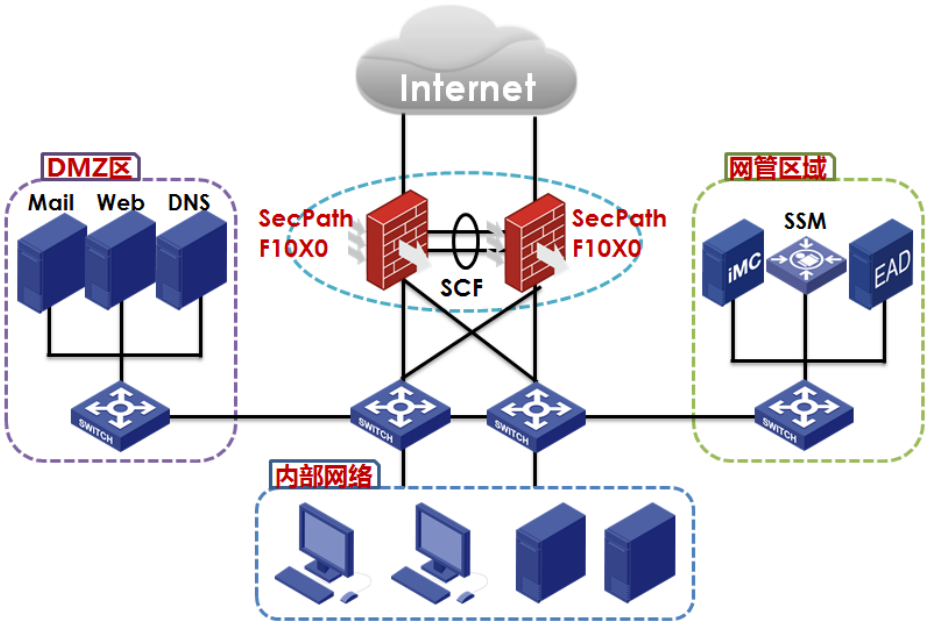
产品规格

项目	F1000-AI-05	F1000-AI-10/15	F1000-AI-25/35/55	F1000-AI-60/70	F1000-AI-65/75	F1000-AI-80/90
接口	1个配置口（CON） 2个USB接口 8个千兆以太电口 2个2Combo（含一个管理口） 2个Bypass接口	1个配置口（CON） 2个USB接口 2个MGMT接口 18个千兆以太电口 8个Combo接口 4个Bypass接口 2个万兆以太光口	1个配置口（CON） 2个USB接口 1个MGMT接口 16个千兆以太电口 4个Combo接口 6个千兆以太光口 2个万兆以太光口	1个配置口（CON） 1个Micro USB 接口 2个USB接口 2个MGMT接口 14个千兆以太电口 12个千兆以太光口 4个万兆以太光口	1个配置口（CON） 2个USB接口 1个MGMT接口 16个千兆以太电口 4个Combo接口 4个千兆以太光口 6个万兆以太光口	1个配置口（CON） 1个Micro USB 接口 2个USB接口 2个MGMT接口 14个千兆以太电口 8个千兆以太光口 8个万兆以太光口
扩展槽位	无	无	2	2/4	2	4
电源冗余	1个内置交流电源	1个内置交流电源/2个内置交流电源	2个可插拔交直流冗余电源模块	2个可插拔交直流冗余电源模块	2个可插拔交直流冗余电源模块	2个可插拔交直流冗余
风扇冗余	1	1/2个冗余风扇	4个冗余风扇	5个冗余风扇	4个冗余风扇	5个冗余风扇
存储	支持硬盘					

介质	
环境温度	工作：0～45℃ 非工作：-40～70℃
运行模式	路由模式、透明模式、混杂模式
AAA服务	Portal认证、RADIUS认证、HWTACACS认证、PKI /CA（X.509格式）认证、域认证、CHAP验证、PAP验证
防火墙	SOP虚拟防火墙技术，支持CPU、内存、存储等硬件资源划分的完全虚拟化 安全区域划分 可以防御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 位不合法超大ICMP报文、地址扫描、端口扫描、SYN Flood、UPD Flood、ICMP Flood、DNS Flood等多种恶意攻击 基础和扩展的访问控制列表 基于时间段的访问控制列表 基于用户、应用的访问控制列表 ASPF应用层报文过滤 静态和动态黑名单功能 MAC和IP绑定功能 基于MAC的访问控制列表 支持802.1q VLAN 透传
病毒防护	基于病毒特征进行检测 支持病毒库手动和自动升级 报文流处理模式 支持 HTTP、FTP、SMTP、POP3、IMAP 协议等 支持的病毒类型：Backdoor、Email-Worm、IM-Worm、P2P-Worm、Trojan、AdWare、Virus 等 支持病毒日志和报表
深度入侵防御	支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、DoS/DDoS 等常见的攻击防御 支持缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御 支持攻击特征库的分类（根据攻击类型、目标机系统进行分类）、分级（分高、中、低、提示四级） 支持攻击特征库的手动和自动升级（TFTP 和 HTTP） 支持对 BT 等 P2P/IM 识别和控制
邮件/网页/应用层过滤	邮件过滤 SMTP 邮件地址过滤 邮件标题过滤 邮件内容过滤 邮件附件过滤 网页过滤 HTTP URL 过滤 HTTP 内容过滤 应用层过滤 Java Blocking ActiveX Blocking SQL 注入攻击防范
NAT	支持多个内部地址映射到同一个公网地址

	支持多个内部地址映射到多个公网地址 支持内部地址到公网地址一一映射 支持源地址和目的地址同时转换 支持外部网络主机访问内部服务器 支持内部地址直接映射到接口公网 IP 地址 支持 DNS 映射功能 可配置支持地址转换的有效时间 支持多种 NAT ALG，包括 DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP 等
VPN	L2TP VPN、IPSec VPN、GRE VPN、SSL VPN
IPv6	基于 IPv6 的状态防火墙及攻击防范 IPv6 协议：IPv6 转发、ICMPv6、PMTU、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay 等 IPv6 路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由、PIM-SM、PIM-DM 等 IPv6 安全：NAT-PT、IPv6 Tunnel、IPv6 Packet Filter、Radius、IPv6 域间策略、IPv6 连接数限制等
高可靠性	支持 SCF 2:1 虚拟化 支持双机状态热备（Active/Active 和 Active/Backup 两种工作模式） 支持双机配置同步 支持 IPSec VPN 的 IKE 状态同步 支持 VRRP
易维护性	支持基于命令行的配置管理 支持 Web 方式进行远程配置管理 支持 H3C SSM 安全管理中心进行设备管理 支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2 智能安全策略
环保与认证	支持欧洲严格的 RoHS 环保认证

典型组网



H3C SecPath F1000-AI 系列组网应用示意图

- SCF 2:1 虚拟化技术，高可靠网络设计
- 具有强大的处理能力，支持 GE、10GE 组网
- 丰富路由协议，实现安全与网络融合
- 具有强大的 VPN 加密处理能力
- 全面深度安全防御阻止恶意攻击，同时能够实现邮件、网页、文件过滤
- 丰富路由协议，实现安全与网络融合

订购信息

（1）主机选购一览表

项目	数量	备注
H3C SecPath F1000-AI主机	1	必配

（2）插卡模块选购一览表

	描述	备注
4GE PFC电口模块	4端口千兆PFC接口模块	选配
4GE光口模块	4端口千兆光接口模块	选配
6*10GE光口模块	6端口万兆光接口模块	选配
综合日志审计平台模块	H3C SecCenter CSAP-SA-C 综合日志	选配，F1000-AI-25及以上款型支持，

	描述	备注
	审计平台插卡模块	具体信息可联系产品经理

（3）电源模块选购一览表

电源模块	备注
交流电源模块	必配，F1000-AI-05/10/15 为内置电源，不需要额外配置电源。
直流电源模块	必配，F1000-AI-05/10/15 为内置电源，不需要额外配置电源。

（4）硬盘选购一览表

硬盘	描述	备注
硬盘模块	1T HDD 480G SSD	选配

说明：

“必配”表示所描述项目是设备正常运行的最小配置。

“选配”表示所描述项目是用户根据实际使用需要可选择配置。

新华三技术有限公司
北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504