

H3C SecPath F1000-G5 系列防火墙

产品概述

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-G5 是面向分销市场的防火墙 VPN 集成网关产品，硬件上基于 MIPS/ARM 多核处理器架构，为 1U 的独立盒式防火墙。

在安全功能方面，作为一款 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、安全状态等多维度的策略控制功能。

图1-1 SecPath F1000-C-G5-LI 产品外观图

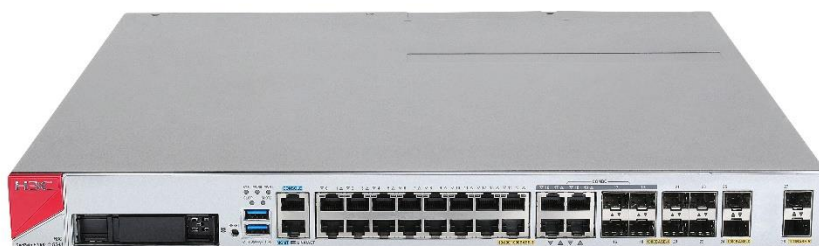
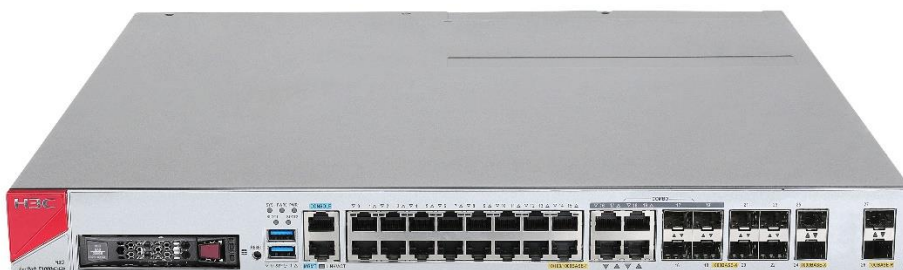


图1-2 SecPath F1000-C-G5 产品外观图



SecPath F1000-S-G5 产品外观图



图1-3 SecPath F1000-A-G5 产品外观图

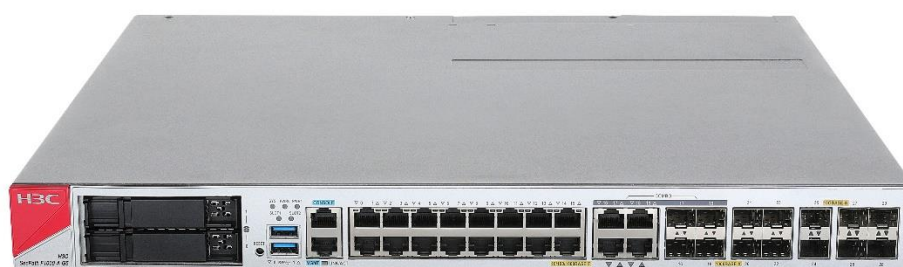


图1-4 SecPath F1000-E-G5 产品外观图



图1-5 SecPath F1000-H-G5 产品外观图



产品特点

集成 AC 控制器功能

- G5 全系列支持 AC 管理功能，最多可纳管 64 个无线 AP。通过防火墙、ACG、AC 控制器的多设备融合，简化网络拓扑，更快部署，节省投入。
- 实现集中式管理，接入安全管控，流量统计分析，点位灵活扩充。
- 防火墙性能无损耗，通过设备免费软件升级即可具备。

高性能的软硬件处理平台

- H3C SecPath F1000-G5 采用了先进的最新 **64 位多核高性能处理器**和**高速存储器**。

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、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-G5 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/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。

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：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 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。

专业的智能管理

- 支持智能安全策略：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 SecCenter SMP 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。

产品规格

产品型号	F1000-C-G5-LI/ F1000-C-G5	F1000-S-G5/ F1000-A-G5	F1000-E-G5/F1000-H-G5
接口	1个配置口（CON） 1MGM+16千兆电口+4千兆 Combo口+6千兆光口+2万兆光口	1个配置口（CON） 1MGM+16千兆电口+4千兆 Combo口+4千兆光口+6万兆光口	1个配置口（CON） 2MGM+14千兆电口+8千兆光口 +8万兆光口

USB接口	2	2	3 (含1Micro USB)
扩展槽位	2	2	4
存储介质	480G SSD	480G SSD	480G SSD
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报文标志位不合法超大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 协议 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		

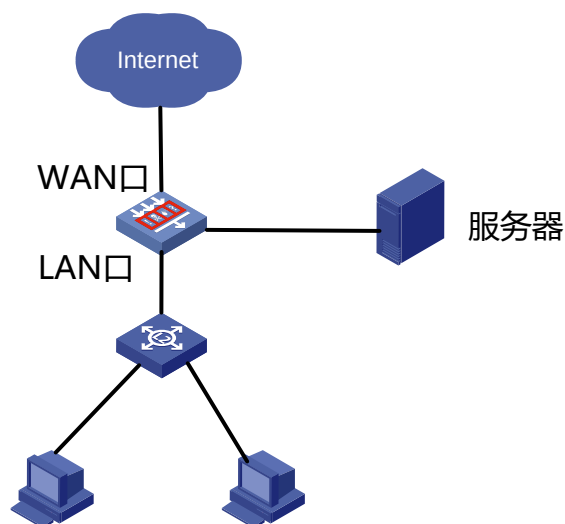
	网页过滤 HTTP URL 过滤 HTTP 内容过滤 应用层过滤 Java Blocking ActiveX Blocking SQL 注入攻击防范
NAT	支持多个内部地址映射到同一个公网地址 支持多个内部地址映射到多个公网地址 支持内部地址到公网地址一一映射 支持源地址和目的地址同时转换 支持外部网络主机访问内部服务器 支持内部地址直接映射到接口公网IP地址 支持DNS映射功能 可配置支持地址转换的有效时间 支持多种NAT ALG，包括DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP等
VPN	L2TP VPN、IPSec VPN、GRE VPN、SSL VPN
IPv6	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

防火墙应用

防火墙部署在 Internet 出口提供对外访问的安全控制及 NAT，同时通过防火墙的攻击防范及深度安全防护功能保护 DMZ 区的服务器。

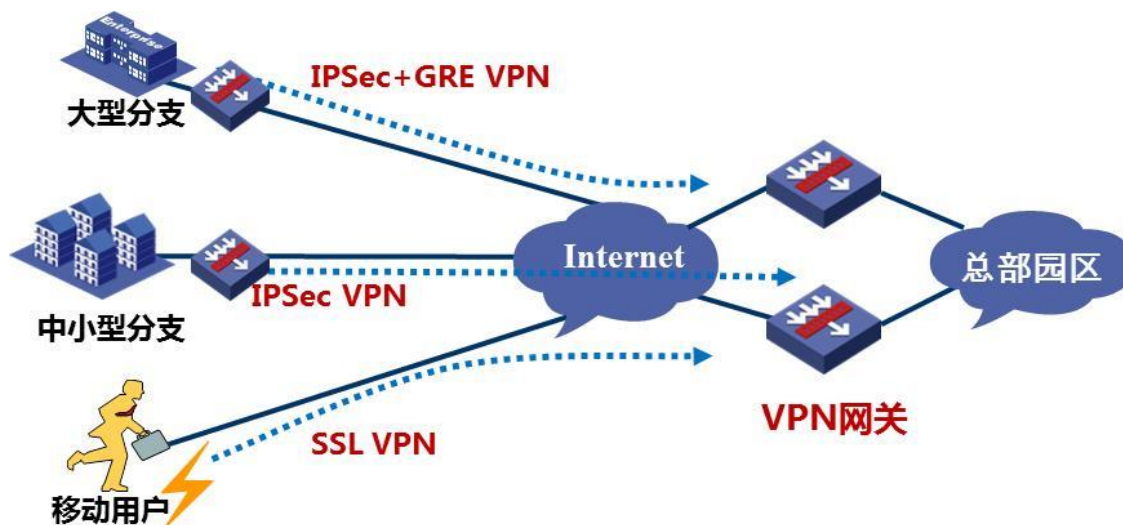
图1-6 出口安全防护



VPN 应用

防火墙集成了丰富的 VPN 功能，包括 IPsec VPN、SSL VPN、L2TP VPN 等，可以作为中小型企业出口网关设备提供移动用户的 SSL VPN 接入，也可以作为广域网组网的分支或二级中心设备提供 site-to-site 的 IPsec VPN 接入。

图1-7 VPN 应用组网图



订购信息

(1) 主机选购一览表

模块	数量	备注
SecPath F1000-C-G5-LI主机	1	必配
SecPath F1000-C-G5主机	1	必配
SecPath F1000-S-G5主机	1	必配
SecPath F1000-A-G5主机	1	必配
SecPath F1000-E-G5主机	1	必配
SecPath F1000-H-G5主机	1	必配

(2) 电源选购一览表

电源	描述	备注
PSR150-A1-B	150W交流电源模块	必配
PSR150-D1-B	150W直流电源模块	必配
注：主机F1000-C-G5-LI、F1000-C-G5、F1000-S-G5、F1000-A-G5、F1000-A-G5可选配2个可插拔150W电源。		
PSR250-12A1	250W 交流电源模块	必配
PSR450-12AHD	450W交流电源模块/450W高压直流电源模块	必配
PSR450-12D	450W 直流电源模块	必配
注：主机F1000-E-G5、F1000-H-G5可选配2个可插拔250W交流/450W交流/450W直流电源模块。		

(3) 接口模块选购一览表

接口模块	描述	备注
NSQM1GT4PFC	H3C SecPath F1000系列 4千兆电PFC接口卡	选配
NSQM1GP4FBA	H3C SecPath F1000系列,4千兆光SFP接口模块	选配
NSQM1F1KGMC	H3C SecPath F1000国密办网络数据加密C模块	选配

(4) 硬盘选购一览表

硬盘	描述	备注
NS-SSD-480G-SATA-SFF	H3C SecPath 系列,480GB 2.5inch SATA SSD 硬盘模块	选配
NS-HDD-1T-SATA-SFF	H3C SecPath 系列,1TB 2.5inch SATA HDD 硬盘模块	选配

(5) 适配 AP 型号一览表

BOM	型号	产品描述
9801A48C	WA6520H-LI	H3C WA6520H-LI 内置天线双频四流 802.11ax/ac/n 面板型无线接入点-FIT
9801A3PM	WA6522H-LI	H3C WA6522H-LI 内置天线双频四流 802.11ax/ac/n 面板型无线接入点-FIT
9801A4RV	WA6522H-D	H3C WA6522H-D 内置天线双频四流 802.11ax/ac/n 面板型无线接入点-FIT
9801A3DT	WA6520-C	H3C WA6520-C 内置天线双频四流 802.11ax/ac/n 无线接入点-FIT
9801A3PK	WA6520S-C	H3C WA6520S-C 内置天线双频四流 802.11ax/ac/n 无线接入点-FIT
9801A48B	WA6520S-D	H3C WA6520S-D 内置天线双频四流 802.11ax/ac/n 无线接入点-FIT
9801A3PG	WA6520S-E	H3C WA6520S-E 内置天线双频三流 802.11ax/ac/n 无线接入点-FIT
9801A34A	WA6320S-E	H3C WA6320S-E 内置天线双频三流 802.11ax/ac/n 无线接入点-FIT
9801A3DA	WA6320S-C	H3C WA6320S-C 内置天线双频四流 802.11ax/ac/n 无线接入点-FIT
9801A3DS	WA6522-C	H3C WA6522-C 内置天线双频四流 802.11ax/ac/n 无线接入点-FIT
9801A2LB	WA5320S-E	H3C WA5320S-E 内置天线双频三流 802.11ac/n Wave 2 无线接入点-FIT
9801A18Q	WA5320-C	H3C WA5320-C 内置天线双频四流 802.11ac/n

BOM	型号	产品描述
		Wave 2 无线接入点-FIT
9801A2VX	WA6530-LI	H3C WA6530-LI 内置天线三频六流 802.11ax/ac/n 无线接入点-FIT
9801A2DQ	WA6338	H3C WA6338 内置天线三频八流 802.11ax/ac/n 无线接入点-FIT
9801A1LH	WA6528	H3C WA6528 内置天线双频八流 802.11ax/ac/n 无线接入点-FIT
9801A3Q3	WA6520XS-LI	H3C WA6520XS-LI 内置天线双频四流 802.11ax/ac/n 增强型无线接入点-FIT
9801A2XD	WA6620X-LI	H3C WA6620X-LI 内置天线双频四流 802.11ax/ac/n 工业级无线接入点-FIT
9801A2XE	WA6620XE-LI	H3C WA6620XE-LI 自带外置全向天线双频四流 802.11ax/ac/n 工业级无线接入点-FIT

(6) 无线 LIS 授权一览表

BOM	型号	产品描述
3130A1L9	LIS-WX-1-BE	增强型无线控制器 license 授权函-管理 1AP-企业网专用-V7V9
3130A2HB	LIS-WX-4-BE	增强型无线控制器 license 授权函-管理 4AP-企业网专用-V7V9
3130A1LA	LIS-WX-8-BE	增强型无线控制器 license 授权函-管理 8AP-企业网专用-V7V9
3130A1LC	LIS-WX-32-BE	增强型无线控制器 license 授权函-管理 32AP-企业网专用-V7V9

 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

Copyright ©2023 新华三技术有限公司保留一切权利

免责声明: 虽然 H3C 试图在本资料中提供准确的信息, 但不保证资料的内容不含有技术性误差或印刷性错误, 为此 H3C 对本资料中的不准确不承担任何责任。
H3C 保留在没有通知或提示的情况下对本资料的内容进行修改的权利。