H3C SecPath F1000-C-G 防火墙

产品概述

SecPath 系列产品是 H3C 公司为企业和运营商用户设计的专业网络安全产品，通过将强大安全抵御功能、专业 VPN 服务和智能网络特性无缝集成在一个硬件平台上，不但能为用户提供广泛和深入的安全防护和安全连接功能，同时可以降低与安全相关的总体拥有成本以及部署的复杂程度，是网络安全解决方案的理想选择。

SecPath 系列产品作为 H3C 公司 iSPN（智能安全渗透网络）解决方案的重要组成部分，已经成为 H3C 公司 IToIP 核心理念中的 IP 自适应安全网络的坚实基础。

SecPath F1000-C-G 是 H3C 公司面向大中型企业用户开发的新一代专业防火墙设备。支持外部攻击防范、内网安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能，能够有效的保证网络的安全；采用 ASPF（Application Specific Packet Filter）应用状态检测技术，可对连接状态过程和异常命令进行检测；提供多种智能分析和管理手段，支持邮件告警，支持多种日志，提供网络管理监控，协助网络管理员完成网络的安全管理；支持多种 VPN 业务，如 L2TP VPN、GRE VPN 、IPSec VPN、SSL VPN 等，可以构建多种形式的 VPN；提供基本的路由能力，支持 RIP/OSPF/BGP/路由策略及策略路由。

SecPath F1000-C-G 防火墙充分考虑网络应用对高可靠性的要求，采用互为冗余备份的双电源（1＋1 备份）模块，支持交、直流输入电源模块；支持双机状态热备，支持 Active/Active 和 Active/Passive 两种工作模式。提供机箱内部环境温度检测功能，并支持网管。

SecPath F1000-C-G 防火墙产品

产品特点

市场领先的基础安全防护功能

- 增强型状态安全过滤：支持基础、扩展和基于接口的状态检测包过滤技术，支持按照时间段进行过滤；支持 H3C 特有 ASPF 应用层报文过滤（Application Specific Packet Filter）协议，支持对每一个连接状态信息的维护监测并动态地过滤数据包，支持对 FTP、HTTP、SMTP、RTSP、H.323（包括 Q.931，H.245， RTP/RTCP 等）应用层协议的状态监控，支持 TCP/UDP 应用的状态监控。
- 抗攻击防范能力：包括多种 DoS/DDoS 攻击防范、ARP 欺骗攻击的防范、提供 ARP 主动反向查询、TCP 报文标志位不合法攻击防范、超大 ICMP 报文攻击防范、地址/端口扫描的防范、ICMP 重定向或不可达报文控制功能、Tracert 报文控制功能、带路由记录选项 IP 报文控制功能；静态和动态黑名单功能；MAC 和 IP 绑定功能；支持智能防范蠕虫病毒技术。
- 应用层内容过滤：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；支持应用层过滤，提供 Java/ActiveX Blocking 和 SQL 注入攻击防范。

- 多种安全认证服务：支持 RADIUS 和 HWTACACS 协议及域认证；支持基于 PKI /CA 体系的数字证书（X.509 格式）认证功能；在 PPP 线路上支持 CHAP 和 PAP 验证协议；支持用户身份管理，不同身份的用户拥有不同的命令执行权限；支持用户视图分级，不同级别的用户赋予不同的管理配置权限。
- 集中管理与审计：提供各种日志功能、流量统计和分析功能、各种事件监控和统计功能、邮件告警功能。
- 全面 NAT 应用支持：提供多对一、多对多、静态网段、双向转换 、Easy IP 和 DNS 映射等 NAT 应用方式；支持多种应用协议正确穿越 NAT，提供 DNS、FTP、H.323、NBT 等 NAT ALG 功能，能够有效解析报文内部所携带的 IP 地址并予以相应转换，保证 NAT 设备两端的应用层协议访问正常。

灵活可扩展的深度安全防护

- 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）、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 Kaspersky 公司的流引擎查毒技术，从而迅速、准确查杀网络流量中的病毒等恶意代码。
- 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。

专业 灵活的 VPN 服务

- 支持 L2TP VPN、GRE VPN、IPSec VPN、SSL VPN 等多种 VPN 业务模式。

技术领先的 IPv6

- 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 隧道等。
- 支持 IPv6 ACL、Radius 等安全技术。

智能网络集成及 QoS 保证

- 支持路由、透明及混合运行模式
- 支持静态路由协议
- 支持 RIP v1/2、OSPF、BGP 动态路由协议
- 支持路由策略及策略路由

- 支持基于 802.1q VLAN
- 支持 PPPoE Client
- DHCP Client/Server/Relay

电信级设备高可靠性

- 支持双机状态热备功能，支持 Active/Active 和 Active/Passive 两种工作模式，实现负载分担和业务备份。
- 支持机箱内部环境温度自动检测，并可通过网管自动采集告警信息。
- 双电源冗余备份。

极具性价比的多业务特性

- 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 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。

智能 图形化的管理

- 通过 Web 方式进行远程配置管理。
- 通过 H3C 网管软件实现与网络设备的统一管理。
- 支持基于 SNMP 和 TR-069 协议的管理。
- 通过 IMC IVM 组件对 VPN 进行动态和图形化的业务管理和状态监控。

产品规格

系统规格

项目	属性
接口	1 个配置口（CON） 12 个千兆光电 Combo 1 个 USB 口
插槽	2 个插槽，可选的接口模块有: 2GE 电口 4GE 光口
Flash	1GB Nand Flash
SDRAM	4GB
内置硬件加密引擎	是
外型尺寸（W×H×D）	442mm × 44.2mm × 442.6mm（带塑胶面板）
重量	5.5Kg
电源模块	交流主机：100-240V ； 50/60Hz

项目	属性
	直流主机：-48V－-60V
电源功率	150W
工作环境温度	0～45℃
环境相对湿度	5～95% （非凝露）
工作海拔高度	-60m～4km

功能特性规格

属性	说明	
运行模式	路由模式 透明模式 混合模式	
网络安全性	AAA 服务	RADIUS 认证 HWTACACS 认证 CHAP 验证 PAP 验证
	防火墙	包过滤 基础和扩展的访问控制列表 基于接口的访问控制列表 基于时间段的访问控制列表 动态包过滤 ASPF 应用层报文过滤 应用层协议：FTP、HTTP、SMTP、RTSP、H.323（Q.931，H.245， RTP/RTCP） 传输层协议：TCP、UDP 抗攻击特性 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、ARP 欺骗攻击防范 ARP 主动反向查询 TCP 报文标志位不合法攻击防范 超大 ICMP 报文攻击防范 地址/端口扫描的防范 DoS/DDoS 攻击防范 TCP Proxy 功能 ICMP 重定向或不可达报文控制功能 Tracert 报文控制功能 带路由记录选项 IP 报文控制功能 静态和动态黑名单功能 MAC 和 IP 绑定功能 透明防火墙

属性	说明	
		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 常等攻击的防御 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
	安全日志及统计	NAT 转换日志 攻击实时日志 黑名单日志 流量告警日志 流量统计和分析功能 全局/基于安全域连接数率监控 安全事件统计功能 E-MAIL 邮件实时告警功能 E-MAIL 邮件定期信息发布功能
	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

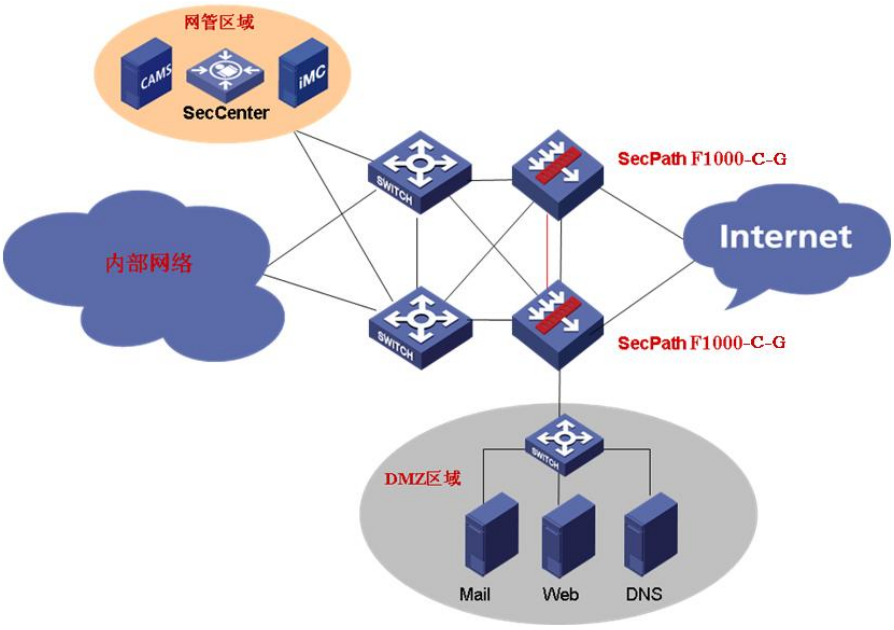
属性	说明	
		支持内部地址直映射到接口公网 IP 地址 支持 DNS 映射功能 可配置支持地址转换的有效时间 支持多种 NAT ALG，包括 DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP 等
VPN	L2TP VPN	支持根据 VPN 用户完整用户名、用户域名向指定 LNS 发起连接 支持为 VPN 用户分配地址 支持进行 LCP 重协商和二次 CHAP 验证
	GRE VPN	
	SSL VPN	支持域认证
	IPSec/IKE	支持 AH、ESP 协议 支持手工或通过 IKE 自动建立安全联盟 ESP 支持 DES、3DES、AES 多种加密算法 支持 MD5 及 SHA-1 验证算法 支持 IKE 主模式及野蛮模式 支持 NAT 穿越 支持 DPD 检测
网络互连	局域网协议	Ethernet_II Ethernet_SNAP 802.1q VLAN
	链路层协议	PPPoE Client
网络协议	IP 服务	ARP 域名解析 IP UNNUMBERED DHCP 中继 DHCP 服务器 DHCP 客户端
	IP 路由	静态路由 RIP v1/2 OSPF BGP 路由策略 策略路由
IPv6	IPv6 安全	RADIUS
	IPv6 基础特性	支持 Ipv6 地址管理 支持 ICMPv6 协议 支持 ND 协议 支持 PMTU
	IPv6 应用	DHCPv6 Client

属性	说明	
		DHCPv6 Relay NTP6 Ping6 DNS6 Tracert6 Telnet6
	IPv6 路由	RIPng OSPFv3 MP-BGP Ipv6 Unicast MP-BGP Ipv6 Multicast Ipv6 静态路由 IPv6 策略路由
	IPv6 组播	MLDv1、MLDv2 PIM SM/DM SSM Ipv6 MC over Ipv4 Tunnels 组播静态路由 BSR
	过渡技术	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 DS-LITE NAT64
负载均衡	调度算法：轮转、加权轮转、最小连接、加权最小连接、随机、加权随机、源地址散列、源地址端口散列、目的地址散列 健康性检测算法：ICMP、TCP Half Open ISP 表项匹配 链路繁忙保护 基于策略的选路 链路阀值保护 持续性算法：基于源 IP、基于目的 IP	
高可靠性	双机状态热备,Active/Active 和 Active/Passive 两种工作模式,支持负载分担和会话业务、IPSec 业务双机热备 远端链路状态监测（NQA） 关键部件冗余设计 支持 VRRP 机箱温度自动检测	

属性	说明	
服务质量保证（QoS）	流量监管：CAR	
配置管理	命令行接口	通过 Console 口进行本地配置 通过 Telnet 或 SSH 进行本地或远程配置 配置命令分级保护，确保未授权用户无法侵入设备 提供全中文的提示和帮助信息 详尽的调试信息，帮助诊断网络故障 提供网络测试工具，如 Tracert、Ping、HWPing 命令等，迅速诊断网络是否正常 用 Telnet 命令直接登录并管理其它设备 FTP Server/Client，可以使用 FTP 下载、上载配置文件和应用程序 支持 TFTP 上传下载文件 支持日志功能 文件系统管理 User-interface 配置，提供对登录用户多种方式的认证和授权功能。
	支持标准网管 SNMPv3，并且兼容 SNMP v2c、SNMP v1 支持 NTP 时间同步	
	支持 Web 方式进行远程配置管理 支持 H3C BIMS 系统进行设备管理 支持 H3C IMC IVM 系统进行 VPN 业务管理和监控	

典型组网

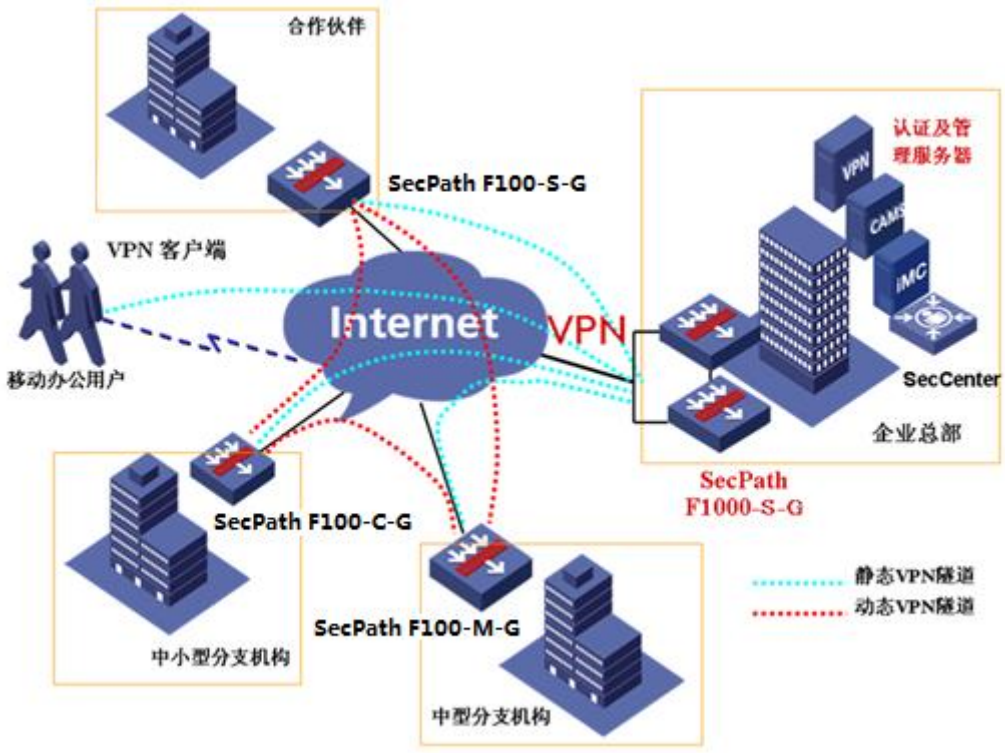
一、防火墙应用方案



SecPath F1000-C-G 防火墙应用典型部署图

- 灵活组网，可按需扩展
- 双机状态热备技术，高可靠网络设计
- 具有强大的处理能力
- 丰富路由协议，实现安全与网络融合
- 阻止恶意攻击，能够实现邮件、网页过滤

二、防火墙结合 VPN 应用方案



SecPath F1000-C-G 防火墙结合 VPN 应用典型部署图

- 支持动态/点对点/远程访问等 VPN 组网应用
- 支持用户名/口令/SecKey/X.509 格式数字证书认证
- 具有强大的 VPN 加密处理能力
- 双机状态热备技术，高可靠网络设计
- 基于用户接入控制，对流量进行监控和过滤
- 丰富路由协议，实现安全与网络融合
- H3C BIMS 系统对数量众多、位置分散的设备提供智能和高效管理
- H3C VPN Manager 系统对 VPN 进行动态和图形化的业务管理和状态监控

订购信息

（1）主机选购一览表

项目	数量	备注
F1000-C-G 主机（不带电源）	1	必配
MIM 插卡	2	选配

（2）接口模块选购一览表

接口模块	描述	备注

接口模块	描述	备注
2GBE	2 端口 10/100/1000Base-T 接口模块	选配
4GEF	4 端口 1000Base-X 接口模块	选配，须另配 SFP 模块

（3）电源模块选购一览表

接口模块	备注
交流电源模块	选配
直流电源模块	选配

（4）多功能 License 选购一览表

功能 License	数量	备注
病毒特征库升级-1 年	0-1	选配
IPS 特征库升级-1 年	0-1	选配
应用控制特征库升级-1 年	0-1	选配

📖 说明：

“必配”表示所描述项目直接随选购的主机提供，不需要用户选择购买。

“选配”表示所描述项目需要用户选择购买。