H3C SecPath F100-E-G 新一代防火墙

产品概述

H3C SecPath F100-E-G 是 H3C 公司推出的新一代防火墙产品，能够满足中小企业不断变化的网络环境和日益丰富网络应用的需要。SecPath F100-E-G 继承 H3C 一贯的高性能、高可靠硬件平台，能够为用户提供线速、稳定的应用体验。SecPath F100-E-G 不但可以提供传统的基础安全功能，如状态检测、NAT、VPN、链路负载均衡等；同时通过统一的软件平台和处理引擎，SecPath F100-E-G 有效整合防火墙、入侵防御、应用层流量识别与控制、防病毒功能，为用户提供一体化的应用安全防护。

H3C SecPath F100-E-G 不仅能够通过 H3C SecCenter 安全管理中心进行设备管理和维护，同时还支持 SNMP 和 TR-069 网管方式，最大化减少设备运营成本和维护复杂性。

H3C SecPath F100-E-G 新一代防火墙

产品特点

市场领先的基础安全防护

- 全面的基础安全防护：提供安全区域划分、静态/动态黑名单功能、MAC 和 IP 绑定、访问控制列表（ACL）和攻击防范等基本功能，还提供基于状态的检测过滤、虚拟防火墙、VLAN 透传等功能。能够防御 ARP 欺骗、TCP 报文标志位不合法、Large ICMP 报文、SYN flood、地址扫描和端口扫描等多种恶意攻击
- 丰富的 VPN 特性：支持 L2TP VPN、GRE VPN、IPSecVPN 及 SSL VPN 等远程安全接入方式，同时设备集成硬件加密引擎实现高性能的 VPN 处理
- 专业的 NAT 应用：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

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

技术领先的 IPv6

- 国内率先支持 IPv6 状态防火墙，真正意义上实现 IPv6 条件下的防火墙功能，满足迫在眉睫的 IPv6 应用需求
- 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

电信级设备的高可靠性

- 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
- 支持双机状态热备功能，支持配置同步与 IPSecVPN 的状态备份，支持 Active/Active 和 Active/Passive 两种工作模式，实现负载分担和业务备份

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
- 作为分支机构的出口设备，支持广域网 EAD 解决方案

简单易用的智能管理

- 简单易用的 Web UI 管理
- 适合专业用户的全命令行管理
- 支持基于 SNMP 和 TR-069 协议的管理
- 通过 H3C SecCenter 安全管理中心实现统一管理

产品规格

系统规格

项目	描述
接口	1 个配置口（CON） 6GE
插槽	2 个 MIM 插槽，可通过该插槽扩展网络接口
DDR SDRAM	1GB

项目	描述	
CF 卡	标配 256M CF 卡	
外型尺寸（W ×H ×D）	442mm×400mm×44.2mm	
电源模块	输入额定电压	100VAC～240VAC；50/60Hz
	最大输入电流	1.6A
最大功率消耗	46W	
环境温度	工作：0～45℃ 非工作：-40～70℃	
环境湿度	工作：10～95%，无冷凝 非工作：5～95%，无冷凝	
重量	<6Kg	

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	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	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 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 动态包过滤 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

属性	说明	
		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
	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 支持对 BT 等 P2P/IM 识别和控制 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）
	URL 过滤	客户自定义 URL 过滤规则库 支持 Java Blocking、ActiveX Blocking 过滤
	安全日志及统计	系统操作日志 防火墙日志 攻击防护日志 黑名单日志 NAT 日志
	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	
	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
	SSL VPN	支持 Web Proxy 服务 支持 Telnet、Windows、VNC 远程桌面共享 支持 Outlook、Notes 支持固定服务端口的 TCP 应用程序

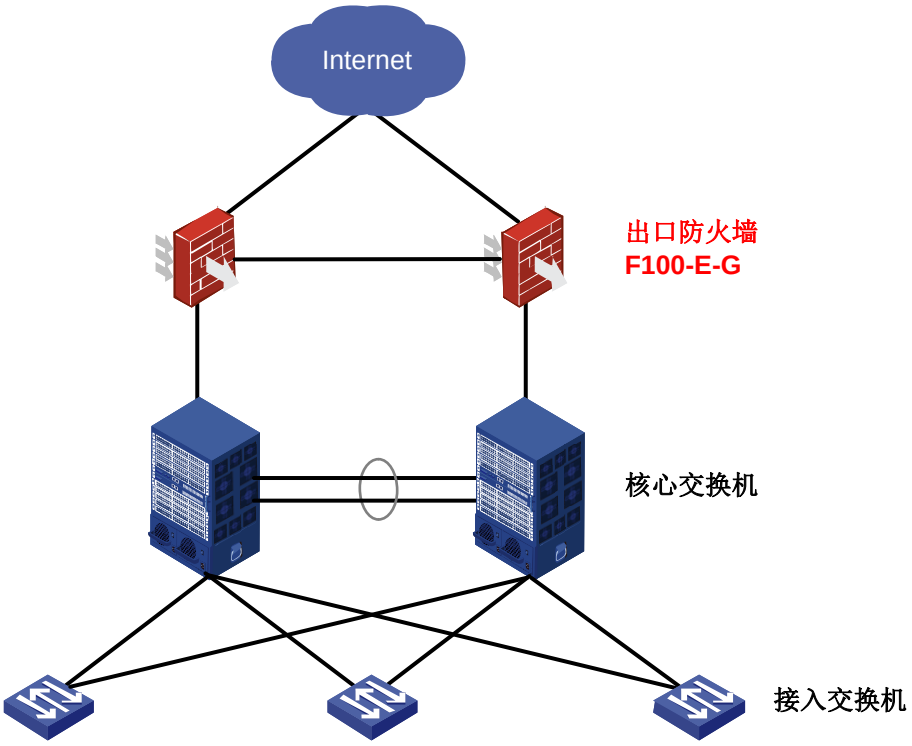
属性	说明	
		支持路由模式的 IP 互连 支持客户端隧道分离 支持对可访问网段的限制 支持对 TCP、UDP 和 ICMP 报文的过滤 支持使用私有协议对客户端虚网卡 IP 地址的分配 支持 SSL VPN 客户端之间的通讯 客户端支持 WINS 服务和 DNS 服务 支持本地认证、RADIUS 认证、LDAP 认证、AD 认证、PKI 证书认证和双因子认证 支持对操作系统、浏览器、用户证书、指定文件和指定进程的检查 支持清除缓存的网页、Cookie、客户端程序和客户端配置
	DVPN	支持 UDP 封装 支持动态 IP 地址构建 VPN 支持加密保护（注册控制报文，会话控制报文，策略报文） 支持多个 DVPN 域 支持分支自动建立 VPN 隧道 支持 Server 对分支隧道的策略控制 Server 对 Client 的 AAA 身份认证 Client 对 Server 的身份验证
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	IPv4 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 策略路由
高可靠性	VRRP 支持双机状态热备（Active/Active 和 Active/Backup 两种工作模式） 支持负载分担和业务备份	
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

属性	说明	
		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 SNMP、TR069 网管协议 支持 H3C SecCenter 安全管理中心进行设备管理	
认证	公安部销售许可证	

典型组网

中小企业 Internet 出口安全

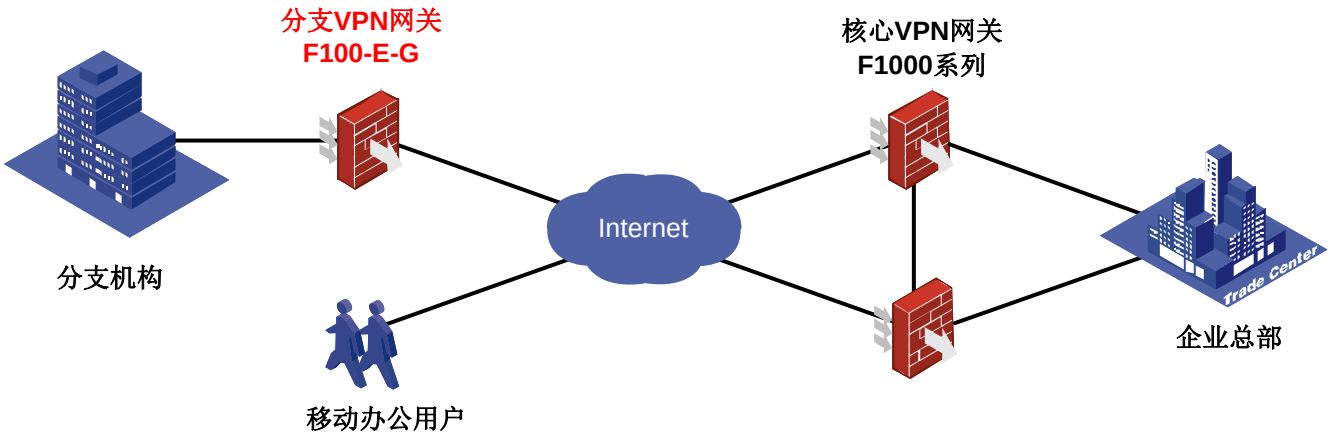
H3C SecPath F100-E-G 支持完整的基础安全防护和深度安全防御功能，为企业提供专业的安全防护；F100-E-G 能够支持完整的 IPv6 状态防火墙，满足马上到来的 IPv6 时代的安全防护需求；同时 F100-E-G 还内置了链路负载均衡、SSL VPN 等丰富特性，能够满足当前互联网出口多 ISP 链路和移动办公的业务需求。



F100-E-G 中小企业 Internet 出口应用示意图

分支机构互联 VPN

H3C SecPath F100-E-G 一体化集成 IPsecVPN 和 SSL VPN 功能，既能满足分支机构网络通过 IPsecVPN 接入总部网络的技术要求，同时提供 SSL VPN 技术满足移动办公用户远程办公的技术要求。



F100-E-G 分支机构互联 VPN 应用示意图

订购信息

项目	数量	备注
主机（交流主机）	1	必配

项目	数量	备注
接口插卡（2GE 电）	0-2	选配
接口插卡（4GE 光）	0-2	选配
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。