SecPath F100-C-SI 防火墙

产品概述

SecPath F100-C-SI 是 H3C 公司面向小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 和动态 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、路由策略及策略路由；支持丰富的 QoS 特性，提供流量监管、流量整形及多种队列调度策略。

SecPath F100-C-SI 防火墙产品图片

产品特点

市场领先的安全防护功能

- 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 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，支持对应用层协议的状态监控。
- 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、超大 ICMP 报文攻击防范、地址/端口扫描的防范、Tracert 报文控制功能；静态和动态黑名单功能；MAC 和 IP 绑定功能。
- 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；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功能。
- 全面 NAT 应用支持：提供多对一、多对多、静态网段、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。

专业 灵活的 VPN 服务

- 支持 SSL VPN、L2TP VPN、GRE VPN、IPSec VPN 和动态 VPN 等多种 VPN 业务模式。
- 利用动态 VPN（DVPN）技术，简化 VPN 配置，实现按需动态构建 VPN 网络。

智能网络集成及 QoS 保证

- 支持流分类、流量监管、流量整形及接口限速
- 支持拥塞管理（FIFO、PQ、CQ、WFQ、CBWFQ、RTPQ）
- 支持拥塞避免（WRED）

智能 图形化的管理

- 通过 Web 方式进行远程配置管理。
- 通过 H3C IMC 网管软件实现与网络设备的统一管理。
- 通过 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。

产品规格

系统规格

项目	防火墙描述
固定接口	1 个配置口（CON） 1 个 USB 接口 2 个以太 WAN 接口 4 个以太 LAN 接口
FLASH	256MB
DDR SDRAM	256MB
外型尺寸（W×D×H）	230×160×43.6mm
重量	1.8kg
电源模块	额定范围（外置）：100～240V 50/60Hz
最大功耗	12W
工作环境温度	0～45℃
环境相对湿度	5～90%（不结露）

功能特性规格

属性	说明	
网络安全性	AAA 服务	RADIUS 认证 HWTACACS 认证 PKI/CA（X.509 格式）认证 域认证 CHAP 验证 PAP 验证

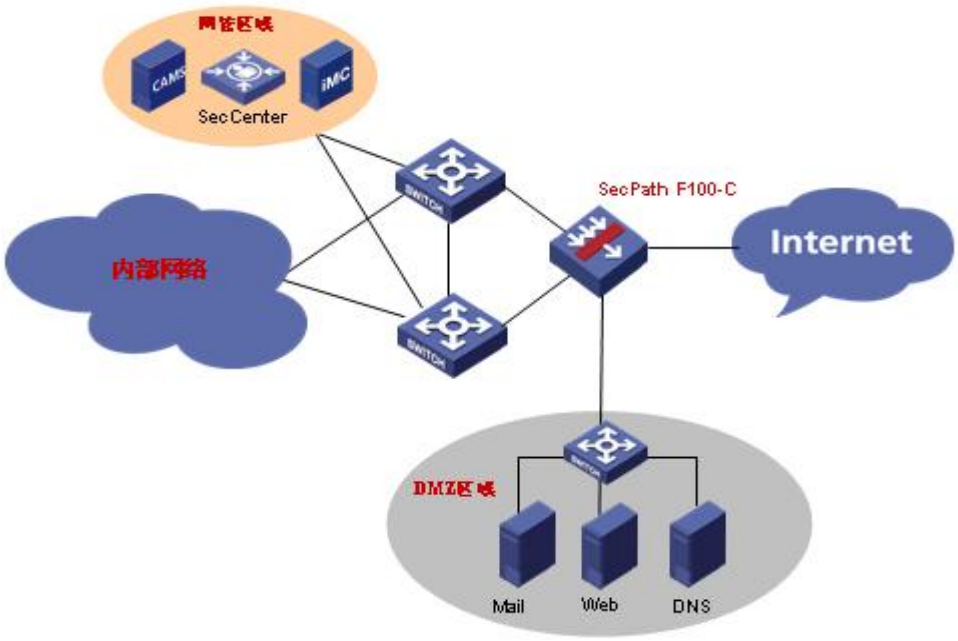
属性	说明	
	防火墙	包过滤 基础和扩展的访问控制列表 基于接口的访问控制列表 基于时间段的访问控制列表 ASPF 应用层报文过滤 应用层协议：FTP、HTTP、SMTP、RTSP、H.323 传输层协议：TCP、UDP 抗攻击特性 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、ARP 欺骗攻击防范 TCP 报文标志位不合法攻击防范 超大 ICMP 报文攻击防范 地址/端口扫描的防范 DoS/DDoS 攻击防范 ICMP 重定向或不可达报文控制功能 Tracert 报文控制功能 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
	安全日志及统计	NAT 转换日志 攻击实时日志 黑名单日志 流量统计和分析功能 安全事件统计功能
	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 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

属性	说明	
		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
	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
	SSL	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 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
网络互连	局域网协议	Ethernet_II Ethernet_SNAP 802.1q VLAN
	链路层协议	PPPoE
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

属性	说明	
		路由策略 策略路由
高可靠性	远端链路状态监测 支持 VRRP	
服务质量保证（QoS）	流量监管	CAR
	拥塞管理	FIFO、PQ、CQ、WFQ、CBWFQ、RTPQ
	拥塞避免	WRED
	流量整形	GTS
	接口速率限制	LR
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、NQA 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 VPN Manager 系统进行 VPN 业务管理和监控	

典型组网

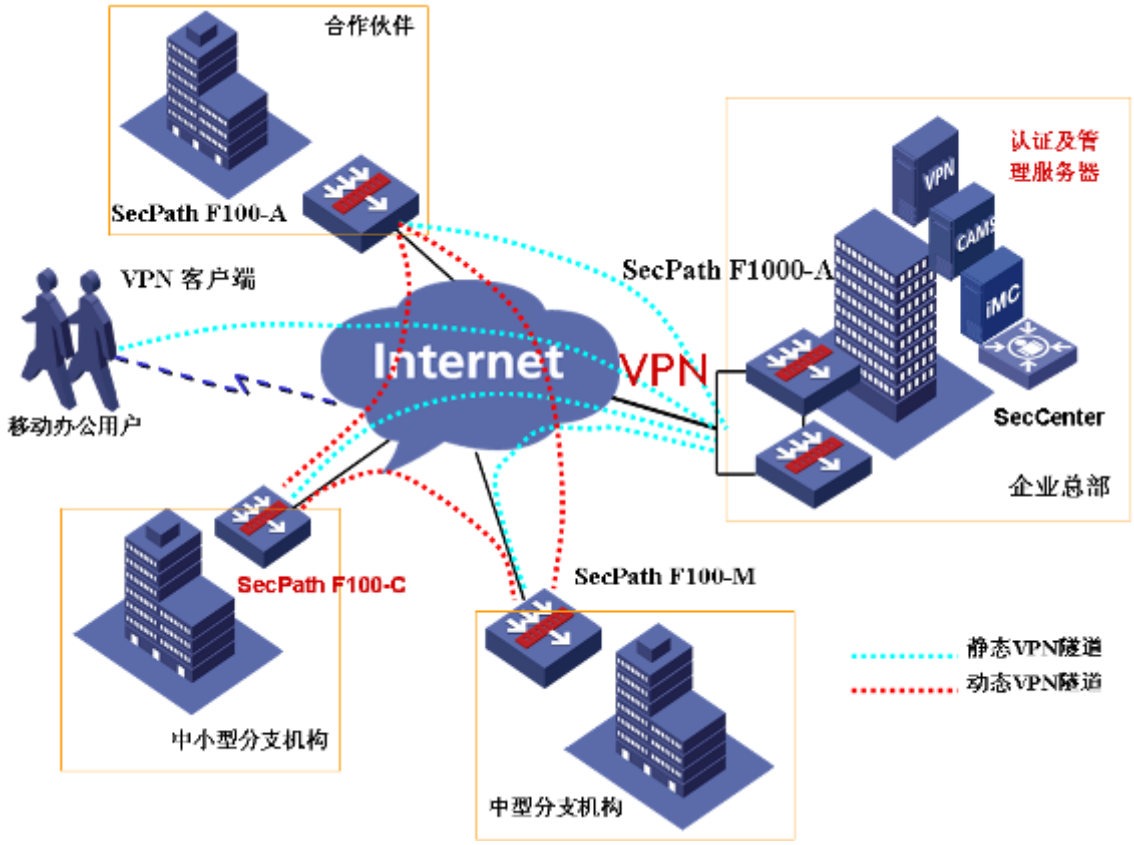
一、防火墙应用方案



SecPath F100-C-SI 防火墙应用典型部署图

- 灵活组网，可按需扩展，具有强大的处理能力
- 丰富路由协议，实现安全与网络融合
- 阻止各种攻击，如 DOS 攻击和 ARP 攻击

二、防火墙结合 VPN 应用方案



SecPath F100-C-SI 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/X.509 格式数字证书认证
- 具有强大的 VPN 加密处理能力
- 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

订购信息

（1）主机选购一览表

项目	数量	备注
SecPath F100-C-SI	1	必配

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。