H3C SecPath F100/1000-X-HI 防火墙

产品概述

H3C SecPath F100-S-HI、F100-C-HI、F100-A-HI、F1000-C-HI 防火墙是新华三技术有限公司（以下简称 H3C 公司）面向中小企业的百兆、千兆防火墙 VPN 集成网关产品，硬件上基于多核处理器架构，为 1U 的独立盒式防火墙。支持应用审计功能，可以扩展硬盘。

在安全功能方面，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、安全状态等多维度的策略控制功能。

在虚拟化和可靠性方面，基于 H3C 领先的 ComwareV7 平台，支持 2 台设备集群及 1:N 虚拟化。更好地适应云计算的要求的弹性扩展能力。

图 1-1 SecPath F100-C-HI 产品外观图

图 1-2 SecPath F100-S-HI 产品外观图

图 1-3 SecPath F100-A-HI 产品外观图

图 1-4 SecPath F1000-C-HI 产品外观图

产品特点

高性能的软硬件处理平台

- H3C SecPath F100/1000-X-HI 系列防火墙采用了先进的多核高性能处理器和高速存储器。

全面的网络安全防护能力

- 支持安全区域管理，可基于接口、VLAN、IP、VM 名字划分安全域。
- 丰富的攻击防范技术。同时支持 IPV4 和 IPV6。支持状态防火墙安全隔离技术，针对异常报文攻击如 Land、smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、TCP 报文标志位不合法，地址欺骗攻击如 IP spoofing，扫描攻击如 IP 地址攻击、端口攻击，异常流量攻击如 Ack Flood、DNS Flood、Fin Flood、HTTP Flood、ICMP Flood、ICMPV6 Flood、Reset Flood、SYNACK Flood、SYN Flood、UDP Flood 等均能够提供有效防护。

丰富的 NAT 特性

- 支持源地址、目的地址 NAT。
- 静态 NAT：支持静态 1 对 1 NAT；支持静态 net-to-net NAT。
- NAT Fullcone 技术完美支持 NAT 网络中的 P2P 穿越
- NAT hairpin 技术解决同一 NAT 之后的 P2P 终端通信的同时，减少对出口带宽浪费。
- 支持多种协议状态检测如 FTP、DNS、TFTP、SQLNET、SIP、H.323、SCCP、RSH、MGCP、GTP、PPTP、QQ、MSN 等。
- 支持静态、动态 NAT444 技术，支持基于策略的多出口 NAT 特性。
- 支持高性能的 NAT 日志发送。

丰富的 VPN 应用

- CPU 内置高性能加密引擎，确保计算复杂的加解密操作不会对 CPU 处理其他防火墙业务造成影响，同时保证了 VPN 的处理性能。
- 支持 GRE VPN、L2TP VPN, IPSec VPN、DVPN、SSL VPN 及多种 VPN 技术的组合应用。
- 支持 IPV6 IPSec vpn、IPV6 GRE VPN。
- 支持多种 VPN 技术的组合使用 IPSec Over GRE，L2TP over IPSec 等。

完善的 IPv6 解决方案

- 支持 IPV6 静态路由、策略路由、OSPFV3、BGP4+、RIPng 等动态路由。
- 支持 IPV6 状态防火墙。
- 支持 IPV6 协议状态检测包括 DNS64、FTP、ICMPV6、SIP、RTSP、MGCP 等
- 支持 IPV6 地址对象及 IPV6 安全策略
- 支持 IPV6 攻击防范，包括 IPV6 DOS/DDOS 攻击、扫描攻击等
- 支持 IPV6 IPSec VPN
- 支持 DS-LITE、NAT64、IVI 及 IPV6 隧道等各种过渡技术。

- 支持 IPV6 管理、日志及审计。
- 支持 IPV6 虚拟防火墙。

电信级高可靠性

- 支持防火墙、NAT、攻击防护、VPN 业务的热备。
- 故障隔离：软件模块化技术使软件的各个部分做到故障隔离。Comware V7 的模块化设计，保证一个进程的异常不会影响其他进程以及内核的正常运行。软件的故障也可以通过自行恢复，不影响硬件的运行
- 进程级 GR：通过完善的进程级 GR 技术，保证异常进程可恢复，并且不影响系统业务。

全面的管理监控手段

- 支持通过 Web-GUI、CLI、SSH 等多种手段管理设备。
- 基于角色的功能授权机制，可以实现到功能、命令行、菜单级的权限控制。
- 统一的 SSM 管理平台，可以实现设备的配置管理、性能监控、日志审计。
- 丰富的 MIB 节点便于外部设备进行性能监控。

开放的系统接口

- 开放接口：传统的网络操作系统为封闭的系统，有专用的系统概念和处理流程，缺乏开放性。而 Comware V7 使用通用的 Linux 操作系统，回归了主流的软件实现方式。提供开放的标准编程接口，可供用户利用 Comware V7 提供的基础功能，实现自己的专用功能，目前主要基于 Netconf 接口。
- TCL 脚本：Comware V7 内嵌了 TCL 脚本执行功能，用户可以利用 TCL 脚本语言直接编写脚本，利用 Comware V7 提供的命令行、SNMP Get、SET 操作，以及 Comware V7 公开的编程接口等实现所需功能。
- EAA：可以在系统发生变化时执行预定义动作。在提高系统可维护性的同时，满足用户一些个性化需求。

产品规格

项目	F100-C-HI/F100-S-HI	F100-A-HI	F1000-C-HI
接口	8GE+2GE(bypass)+2Combo 1配置口（Con）+2USB口	16GE+8SFP 1配置口（Con）+2USB口	16GE+8SFP 1配置口（Con）+2USB口
扩展槽位	无	1个扩展插槽，用于PFC接口模块、光接口模块、加密卡	2个扩展插槽，用于PFC接口模块、光接口模块、加密卡
扩展板卡类型	无	4*GE PFC电口模块、 4*GE光口模块、 4*10GE光口模块	4*GE PFC电口模块、 4*GE光口模块、 4*10GE光口模块
存储介质	1个硬盘扩展插槽，支持扩展1块SATA硬盘		
环境温度	工作：无硬盘0～45℃，带硬盘5～40℃ 非工作：-40～70℃	工作：无硬盘0～45℃，带硬盘5～40℃ 非工作：-30～70℃	工作：无硬盘0～45℃，带硬盘5～40℃ 非工作：-30～70℃

环境湿度	工作：10～95%，无冷凝 非工作：5～95%，无冷凝	工作：10～80% 非工作：5～95%，无冷凝	工作：10～80% 非工作：5～95%，无冷凝
运行模式	路由模式、透明模式、混杂模式		

功能特性表

属性	说明	
网络安全性	验证、授权和计帐（AAA）服务	本地认证 RADIUS认证，支持PAP和CHAP验证方式 HWTACACS认证 AD/LDAP认证 PKI证书认证
	防火墙	基本ACL和高级ACL 基于安全区域的访问控制 基于时间段的访问控制 ASPF状态防火墙 DOS/DDOS攻击防范：包括SYN Flood、UDP Flood、ICMP Flood、ACK Flood、RST Flood，DNS Flood、HTTP Flood 畸形包攻击如：Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、IP分片报文攻击、分片报文攻击、TCP报文标志位不合法攻击、超大ICMP报文攻击、ICMP重定向或不可达报文 扫描窥探攻击防范：端口扫描、地址扫描、IP路由记录选项报文、Tracert报文 IP Spoofing攻击防范 静态和动态黑名单功能 连接数限制 支持N:1 SCF集群技术 • 支持多台设备集群 • 集群设备统一管理 • 集群设备业务分布式处理 支持1:N虚拟防火墙技术 • 容器化的虚拟化技术，虚拟防火墙特性与物理墙特性一致 • 虚拟防火墙独立 GUI/CLI 管理 • 虚拟防火墙独立配置文件 • 虚拟防火墙独立日志主机及日志审计 • 虚拟防火墙资源分配：吞吐、并发、新建、策略 • 虚拟防火墙接口共享 • N:1:M 虚拟化：先将多台设备集群，然后再进行虚拟防火墙划分

属性	说明	
	NAT	源地址NAT • 支持根据策略指定转换后的地址池； • 支持 PAT、支持 NO-PAT • 支持无限连接 • 支持 IP 持续性，保证同一源转换后的地址不变 • 支持 Easy IP 目的地址NAT • 支持地址+端口的一对一映射 • 支持多个公网地址转换为同一个私网地址 • 支持基于策略的目的 NAT 支持静态NAT • 支持一对一静态 NAT • 支持 net-to-net 静态 NAT 支持 NAT444 • 支持静态 NAT444 • 支持动态 NAT444 支持 Fullcone，解决 P2P 穿越问题 支持 C/S 方式、P2P 方式的 Hairpin 技术 支持端口块增量分配 支持DNS Mapping 支持多种ALG，包括FTP、DNS、TFTP、SQLNET、SIP、RTSP、H323、SCCP、RSH、MGCP、GTP、PPTP、QQ、MSN
	DPI	支持IPS 支持应用控制及应用带宽管理 支持telnet、FTP、SMTP/POP3、HTTP内容过滤
VPN	L2TP VPN	支持LNS 支持Auto-Initiated LAC L2TP支持VRF
	GRE VPN	GRE Over IPV4 GRE Over IPV6 GRE 支持VRF GRE P2MP(规划中)

属性	说明	
	IPSec/IKE	安全协议支持AH/ESP 支持传输和隧道模式 ESP支持DES、3DES和AES三种加密算法 支持MD5及SHA-1验证算法 支持通过manual或IKE方式建立SA 支持防重放攻击 支持IPSec策略模版 支持IPSec反向路由注入 支持IKEV1 支持IKE主模式及野蛮模式 支持通过预共享密钥和证书方式验证IKE Peer身份 支持DPD 支持IKE Keppalive 支持NAT穿越(野蛮模式和主模式) VRF aware：通过IKE peer对端信息确定所属的VPN 支持IPSec双机热备(规划中) 支持IKEV2（规划中）
网络协议	局域网协议	Ethernet_II 802.1Q
	二层协议	STP MSTP
网络协议	IP服务	ARP • 静态 ARP • 动态 ARP • ARP 代理 • 免费 ARP DNS • 本地静态域名 • DNS Client • DNS Proxy • DDNS 动态域名服务 DHCP • DHCP 中继 • DHCP 服务器 • DHCP 客户端 NTP • NTP Client • NTP Server

属性	说明	
	IP路由	静态路由管理 策略路由 动态路由 • RIP-1/RIP-2 • OSPF • BGP • ISIS • 路由策略 组播 • IGMP • PM-SM • PM-DM
高可靠性	支持集群部署(最多8台) 支持集群内1:1备份 支持集群内N:N备份 支持选择性开启状态热备 VRRP/VRRP6V3 支持静态链路聚合、支持动态链路聚合、支持跨设备链路聚合 链路质量探测NQA 支持BFD 热补丁	
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 支持基于RBAC的细粒度权限控制，可以控制具体命令的权限 User-interface配置，提供对登录用户多种方式的认证和授权功能
	WEB网管接口	支持通过WEB方式进行配置 支持WEB管理员的超时下线。 支持WEB用户的登录和鉴权 支持基于RBAC的细粒度权限控制，可以控制具体web菜单的操作权限
	支持标准网管SNMP	支持SNMPV1、V2c和SNMPV3
	外部管理平台集成	支持通过IMC SSM组件对设备进行状态监控和安全策略、攻击防范、NAT等安全配置管理 IMC SSM组件可以和桌面终端联动、发现攻击用户后，自动使用户下线 IMC SSM组件可对设备攻击日志进行审计，对攻击进行分类统计，可以统计攻击源、攻击对象 IMC SSM组件可以实现对设备会话信息统计，可以基于源、目的展示TopN会话信息 支持通过IMC BIMS对设备进行远程配置管理

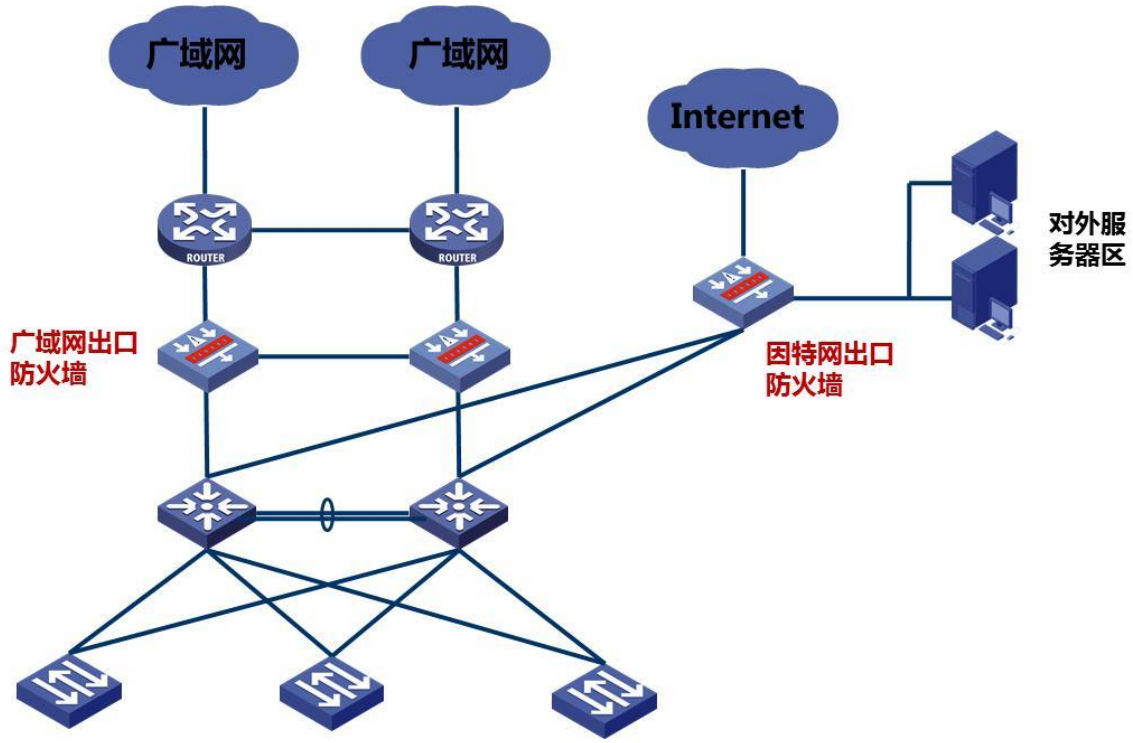
属性	说明	
	安全审计	攻击实时日志 域间策略匹配日志 黑名单日志 连接数限制日志 会话日志 NAT日志 流量统计和分析功能 安全事件统计功能
IPV6	IPV6业务	TELNET/FTP/RADIUS 域名解析 DHCP Server DHCP中继 DHCP客户端
	IPV6路由	静态路由 策略路由 RIPng OSPFv3 BGP4+ ISIS6
	IPV6安全	IPV6 对象 IPV6安全策略 IPV6 状态防火墙 IPV6攻击防范 IPV6 ALG IPV6连接数限制 IPV6 URPF IPV6虚拟分片重组 IPV6 IPSec VPN IPV6虚拟防火墙
	IPV6过渡技术	NAT-PT NAT64\IVI DS-LITE隧道 ISATAP隧道 IPv6 Over IPv4 GRE隧道

典型应用

防火墙应用

SecPath F100/1000-X-HI 系列防火墙部署在广域网出口及 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御功能保护 DMZ 区的服务器。

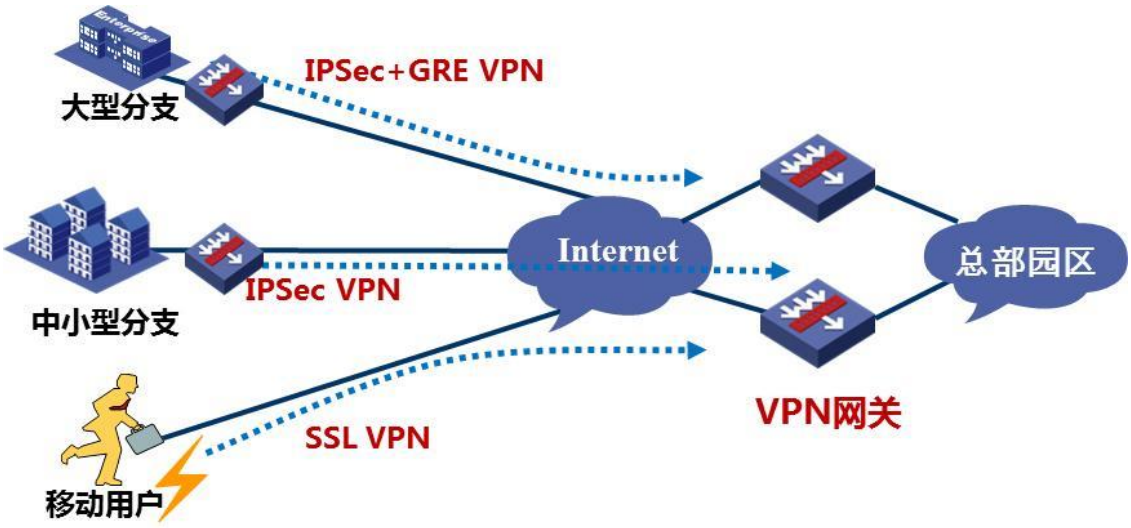
图1-1 出口安全防护



VPN 应用

SecPath F100/F1000-X-HI 系列集成了丰富的 VPN 功能，包括 IPSec VPN、SSL VPN、 L2TP VPN 等，可以作为中小型企业的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二三级中心设备提供 site-to-site 的 IPSec VPN 接入。IPSEC 业务和 SSLVPN 业务支持采用国密算法。

图1-2 VPN 应用组网图



订购信息

（1）主机选购一览表

项目	数量	备注
SecPath F1000-C-HI	1	必配
SecPath F100-A-HI	1	必配
500GB SATA HDD 硬盘模块	1	选配
PFC模块	1	选配
4SFP接口卡	1	选配
4SFP+接口卡	1	选配

项目	数量	备注
SecPath F100-C-HI/F100-S-HI	1	必配
500GB SATA HDD 硬盘模块	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。

新华三技术有限公司

杭州基地
杭州市高新技术产业开发区之江科技工业园六和路 310 号
邮编：310053
电话：0571-86760000
传真：0571-86760001

北京分部
北京市海淀区知春路 7 号致真大厦 B 座 21 层
邮编：100191
电话：010-63108666
传真：010-63108777

http://www.h3c.com.cn

客户服务热线
400-810-0504
800-810-0504

版本：20120316-V1.0