H3CNS-SecPathF100-C防火墙

产品名称	H3CNS-SecPathF100-C防火墙
公司名称	北京龙鑫在线科技有限公司
价格	2300.00/个
规格参数	品牌:H3C 型号:H3CNS-SecPathF100-C-AC VPN:支持VPN
公司地址	中国 北京市海淀区 北京市海淀区海淀中街16号中关村公馆E座900室
联系电话	86 010 62684231 18611365515

产品详情

h3c secpath f100 系列防火墙

稳定可靠 功能全面

h3c secpath防火墙/vpn是业界功能最全面、扩展性最好的防火墙/vpn产品，集成防火墙、vpn和丰富的网络特性，为用户提供安全防护、安全远程接入等功能。

h3c secpath f100系列防火墙包括secpath f100-c/secpath f100-c-ei/secpath f100-s/secpath f100-m/secpath f100-a-si/secpath f100-a/secpath f100-e等七款产品，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、动态vpn等；支持rip/ospf/bgp/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。

产品特点

扩展性最强

基于h3c 先进的oaa开放应用架构，secpath防火墙能灵活扩展病毒防范、网络流量监控和ssl vpn等硬件业务模块，实现2-7层的全面安全。

强大的攻击防范能力

能防御dos/ddos攻击（如cc、syn flood、dns query flood、syn flood、udp flood等）、arp欺骗攻击、tcp报文标志位不合法攻击、large icmp报文攻击、地址扫描攻击和端口扫描攻击等多种恶意攻击，同时支持黑名单、mac绑定、内容过滤等先进功能。

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。

丰富的vpn特性

集成ipsec、l2tp、gre和ssl等多种成熟vpn接入技术，保证移动用户、合作伙伴和分支机构安全、便捷的接入。

应用层内容过滤

可以有效的识别网络中各种p2p模式的应用，并且对这些应用采取限流的控制措施，有效保护网络带宽；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。

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。

全面的认证服务

支持本地用户、radius、tacacs等认证方式，支持基于pki/ca体系的数字证书（x.509格式）认证功能。支持基于用户身份的管理，实现不同身份的用户拥有不同的命令执行权限，并且支持用户视图分级，对于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。

产品规格

f100系列功能特性列表

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 pki /ca（x.509格式）认证 域认证

		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 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 基于mac的访问控制列表 支持802.1q vlan透传
	邮件/网页/应用层过	邮件过滤

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 支持与外部服务器(第三方如surfcontrol)进行集成联动提供url网页过滤的解决方案，有效控制和管理用户的web访问行为 应用层过滤 java blocking activex blocking sql注入攻击防范
安全日志及统计	用户行为流日志 nat转换日志 攻击实时日志 黑名单日志 地址绑定日志 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 全局/基于安全域协议报文比例监控 安全事件统计功能 e-mail邮件实时告警功能 e-mail邮件定时告警功能
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 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
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 bgp 路由策略 策略路由
高可靠性	双机状态热备,active/active和active/passive两种工作模式,支持负载分担和业务备份 远端链路状态监测（l3 monitor） 关键部件冗余设计 接口模块热插拔 机箱温度自动检测	
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、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 vpn manager系统进行vpn业务管理和监控	

组网应用

防火墙组网应用方案

secpath f100系列防火墙应用典型部署图

- u 灵活组网，可按需扩展
- u 双机状态热备技术，高可靠网络设计
- u 具有强大的处理能力
- u 丰富路由协议，实现安全与网络融合
- u 支持p2p流量检测和应用层过滤
- u 阻止恶意攻击，能够实现邮件、网页过滤

防火墙结合vpn组网应用方案

secpath f100-a防火墙结合vpn应用典型部署图

u 支持动态/点对点/远程访问等vpn组网应用

u 支持用户名/口令/seckey/x.509格式数字证书认证

u 具有强大的vpn加密处理能力

u 双机状态热备技术，高可靠网络设计

u 基于用户接入控制，对流量进行监控和过滤

u 丰富路由协议，实现安全与网络融合

u 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

u 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

选配信息

(1) secpath f100-e主机选购一览表

项目	数量	备注
主机-双交电源(4fe/1slot)	1	必配
mim插卡	1	选配

(2) secpath f100-a主机选购一览表

项目	数量	备注
主机(7fe/1slot)	1	必配
mim插卡	1	选配

(3) secpath f100-a-si主机选购一览表

项目	数量	备注
主机(6fe/1slot)	1	必配
mim插卡	1	选配

(4) secpath f100-m主机选购一览表

项目	数量	备注
主机(3fe/1slot)	1	必配
mim插卡	1	选配

(5) secpath f100-s主机选购一览表

项目	数量	备注
主机-交流电源(4fe)	1	必配

(6) secpath f100-c主机选购一览表

项目	数量	备注
主机(4fe)	1	必配

(7) secpath f100-c-ei主机选购一览表

项目	数量	备注
主机(5fe)	1	必配

(8) 接口模块选购一览表

接口模块	描述	备注
2fe	2端口10/100base-tx模块	选配
4fe	4端口10/100base-tx模块	选配
1gbe	1端口10/100/1000base-t接口模块	选配
2gbe	2端口10/100/1000base-t接口模块	选配
1gef	1端口1000base-x接口模块	选配，须另配sfp模块
2gef	2端口1000m以太网光接口模块	选配，须另配sfp模块
ndecii	ipsec加密卡	选配

本产品的品牌是H3C，型号是H3CNS-SecPathF100-C-AC，VPN是支持VPN，用户数限制是200用户，产品类型是中型企业级，NAT是支持NAT，质保是一年（年），OEM是不可OEM