H3C SecPathM9000-S 系列多业务安全网关

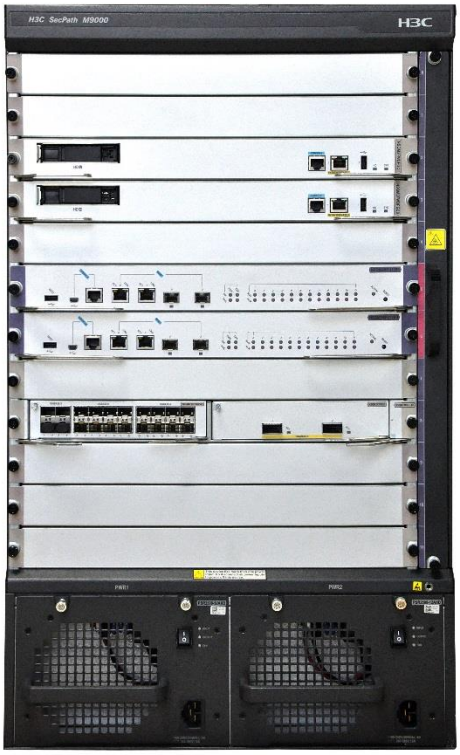
产品概述

H3C SecPathM9000-S 系列是新华三技术有限公司（以下简称 H3C 公司）结合云计算、IPv6、大数据及高性能计算的发展趋势，针对云计算数据中心、运营商 CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。

H3C SecPathM9000-S 系列全面支持攻击防范、抗 DDoS、访问控制、安全域划分、黑名单、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；支持多种 VPN 业务，如 L2TP VPN、GRE VPN 、IPSec VPN、SSL VPN、MPLS VPN 等，满足多种高性能 VPN 接入的需求；支持业界最丰富的 NAT 特性，满足各大运营商的 NAT 需求；提供丰富的路由能力，支持静态路由、RIP/OSPF/BGP/ISIS 路由策略及策略路由；全面支持 IPv4/IPv6 双协议栈。

H3C SecPathM9000-S 系列多业务安全网关充分考虑网络应用对高可靠性的要求，采用领先的多核全分布式架构。主控引擎 1+1 冗余，提供整机统一配置管理，支持安全集群；业务引擎和接口单元支持混插，可以根据性能需求灵活进行选择；风扇模块冗余，风扇框支持风扇状态监控，风扇支持无级调速，可以根据环境温度、单板配置自动分组调速；电源模块 M+N 备份，交、直流电源模块支持热插拔，多电源模块负载分担，可灵活根据系统功耗配置模块数量，保证模块高效工作。设备所有单元均支持热插拔，充分满足网络维护、升级、优化的需求。

SecPath M9008-S 产品外观图



SecPath M9012-S 产品外观图

产品特点

高性能的软硬件处理平台

- 采用控制、业务、数据相分离的全分布式架构，控制引擎、交换引擎、业务引擎及接口单元硬件分离，解耦合系统关键部件，提高系统可靠性；独立的硬件交换引擎，支撑高性能安全业务无阻塞处理及转发
- 独立的高性能控制引擎，实现系统统一配置管理和安全集群
- 安全业务引擎采用最新多核高性能处理器，单板卡高速处理安全业务性能业界最高；一块硬件板卡上可同时提供 L2～L7 的全面安全防御，包括防火墙、NAT、LB、IPS、AV、ACG、VPN 等；内置专业硬件 TCAM，保证大容量策略表项的高速检索
- 内置模块化软件系统，支持多进程的调度，进程间运行空间隔离，单个进程的异常不会影响系统其他部分，提高系统可靠性；支持权限管理功能，基于特性、命令行、系统资源、WEB 管理等级别定义用户读写权限，提高系统安全性；支持热补丁、支持 ISSU，不中断业务的情况下实现系统升级，提高系统易用性

电信级设备高可靠性

- 采用 H3C 公司拥有自主知识产权的软、硬件平台。产品应用从大中型企业用户到各大电信运营商，经历了多年的市场考验
- 支持状态 1:1 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
- 支持状态 N:N 热备功能，实现负载分担和业务备份，大幅提高系统可靠性
- 支持 SCF（安全集群系统），支持多框集群和异构集群，实现灵活管理和弹性扩展。

强大的安全防护功能

- 支持丰富的攻击防范功能。包括：Land、Smurf、UDP Snork attack、UDP Chargen DoS attack (Fraggle)、Large ICMP Traffic 、Ping of Death、Tiny Fragment 、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、端口扫描等攻击防范，还包括针对 SYN Flood、UPD Flood、ICMP Flood、DNS Flood、CC 等常见 DDoS 攻击的检测防御。
- 支持统一管理。主机+多业务引擎始终作为一个网元进行统一管理，无需对每块插卡进行 IP 地址规划，在节省用户的 IP 地址的同时大量减少部署的复杂度，并且可以对设备实现全面的配置管理、性能监控和日志审计。
- 支持智能分流（IFF）。部署多业务插卡后，流量自动在多个业务板卡内负载分担从而实现分布式处理。
- 支持安全集群框架（SCF）。全面突破机框的限制，在简化管理和部署的基础上同时实现了安全业务和安全性能的弹性扩展。支持异构集群，M9008-S 和 M9012-S 相互之间可集群，集群系统更灵活和多样化。
- 支持安全 ONE 平台（SOP）。采用创新的基于容器的虚拟化技术实现了真正意义上的虚拟防火墙：
    - SOP 之间实现了基于进程的真正相互隔离
    - SOP 通过统一的 OS 内核可以对系统的静态及动态的资源进行细粒度的划分

- SOP 数量可以按照系统需求的变化动态调整
- SOP 能力可以根据用户需求动态的进行调整

- 支持安全区域管理。可基于接口、VLAN 划分安全区域
- 支持包过滤。通过在安全区域间使用标准或扩展访问控制规则，借助报文中 UDP 或 TCP 端口等信息实现对数据包的过滤，支持按照时间段进行过滤
- 支持应用层状态包过滤（ASPF）功能。通过检查应用层协议信息（如 RAWIP/ICMP/ICMPV6/UDP-LITE/SCTP 及其它基于 TCP/UDP 协议的应用层协议），并监控基于连接的应用层协议状态，动态的决定数据包是被允许通过多业务安全网关或者是被丢弃
- 支持验证、授权和计帐（AAA）服务。包括：基于 RADIUS/HWTACACS+/ LDAP(AD)、CHAP、PAP 等的认证
- 支持静态和动态黑名单
- 支持静态 NAT、源地址 NAT、目的地址 NAT
- 支持静态及动态运营商 CGN NAT
- 支持 Fullcone、Hairpin 等 P2P 穿越技术
- 支持 NAT ALG
- 支持 VPN 功能。包括：支持 L2TP、手工/自动方式 IPSec、GRE、MPLS VPN 等
- 支持丰富的路由协议。支持 IPv4、IPv6 静态路由、等价路由、策略路由，以及 BGP、RIPv2、OSPF、ISIS 等动态 IPv4 路由协议，支持 BGP4+、OSPFv3、ISISV6 等动态 IPv6 路由协议
- 支持组播技术。支持 IGMP v1/v2/v3，PIM-SM、PIM-DM
- 支持安全日志。支持操作日志、域间策略匹配日志、攻击防范日志；支持 DS-LITE 日志；支持 NAT444 日志，支持电信、联通、移动格式；
- 支持流量监控统计、管理。

灵活可扩展的一体化深度安全

- 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。
- 迅捷的 URL 分类过滤：提供基础的 URL 黑白名单过滤同时，可以配置 URL 分类过滤服务器在线查询。
- 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。

业界领先的 IPv6

- 支持 IPv6 基础协议。支持 TCP6,UDP6，RAWIP6，ICMPV6，PPPoEv6、DHCPV6 Server、DHCPv6 Client、DHCPV6 Relay、DNSv6、RADIUS6 等协议；
- 支持 IPv6 路由协议。支持静态路由、BGP4+\OSPFv3\ISISV6 路由策略和策略路由；
- 支持 IPv6 ASPF。
- 支持 IPV6 攻击防范。
- 支持 IPv6 Multicast。
- 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、NAT444、DS-Lite 等。

下一代多业务特性

- 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、短信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。
- DLP 基础功能支持，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；支持网络传输协议的文件过滤；支持应用层过滤，提供 Java/ActiveX Blocking 和 SQL 注入攻击防范。

专业的智能管理

- 支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2
- 可通过命令行界面进行设备管理及安全业务配置，满足专业管理和大批量配置需求
- 支持图形化界面，提供简单易用的 Web 管理
- 通过 H3C iMC 实现统一管理，集安全信息与事件收集、分析、响应等功能为一体，解决了网络与安全设备相互孤立、网络安全状况不直观、安全事件响应慢、网络故障定位困难等问题，使 IT 及安全管理员脱离繁琐的管理工作，能够集中精力关注核心业务，极大提高工作效率
- 基于先进的深度挖掘及分析技术，采用主动收集、被动接收等方式，为用户提供集中化的日志管理功能，并对不同类型格式（Syslog、二进制流日志等）的日志进行归一化处理。同时，采用高聚合压缩技术对海量事件进行存储，并可通过自动压缩、加密和保存日志文件到 DAS、NAS 或 SAN 等外部存储系统，避免重要安全事件的丢失
- 提供丰富的报表，主要包括基于应用的报表、基于网流的分析报表等
- 支持以 PDF、HTML、WORD 和 TXT 等多种格式输出
- 可通过 Web 界面进行报告定制，定制内容包括数据的时间范围、数据的来源设备、生成周期以及输出类型等

安全认证

- 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，可以防止低权限用户非法获取或修改配置信息等。M9008-S 设置了如下四种身份的用户：访问（Visit）级、监控（Monitor）级、配置（Config）级和管理（Manage）级用户。
- 视图分级保护。由于四种不同身份的用户拥有的配置权限不同，级别低的用户不能进入更高级的视图。
- 在 PPP 线路上支持 CHAP 和 PAP 验证协议。
- 支持基于 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）的 AAA（Authentication，Authorization，Accounting，认证、授权、计费）服务，可以与 RADIUS 服务器配合实施对接入用户的验证、授权和计费安全服务，防止非法访问。
- 支持基于 PKI/X.509 的证书认证功能。
- 路由协议 OSPF、RIP2 都具有 MD5 认证功能，确保所交换路由信息的可靠性。

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

属性	M9008-S	M9012-S
主控板槽位数	2	2
业务板槽位数	6	10
冗余设计	主控、电源、风扇	主控、电源、风扇
外型尺寸（W ×D ×H）	机箱：436*420*575mm(13RU)	机箱：436*420*708mm (16RU)
整机功耗	2800W（Max）	5000W（Max）
环境温度	工作：0～45℃ 非工作：-40～70℃	
运行模式	路由模式	
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	
多业务安全网关	虚拟多业务安全网关 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、DNS 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 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）	

属性	M9008-S	M9012-S
	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	
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、IPSec VPN、GRE VPN、MPLS VPN、SSL VPN	
IPv6	IPV6 状态防火墙 IPV6 域间策略 IPV6 攻击防范 IPV6 连接数限制 IPv6 协议： ICMPv6、PMTU、Ping6、DNS6、TraceRT6、Telnet6、DHCPv6 Client、DHCPv6 Relay 等 IPv6 路由：RIPng、OSPFv3、BGP4+、静态路由、策略路由、PIM-SM、PIM-DM 等 IPv6 过渡技术：NAT-PT、IPv6 Tunnel、NAT64(DNS64)、DS-LITE 等	
高可靠性	支持双机状态热备（Active/Active 和 Active/Backup 两种工作模式） 支持集群统一配置管理 支持非对称路径 支持 IPSec VPN 的 IKE 状态同步 支持 VRRP 支持静态及动态链路聚合 支持 BFD 支持不间断升级 ISSU	

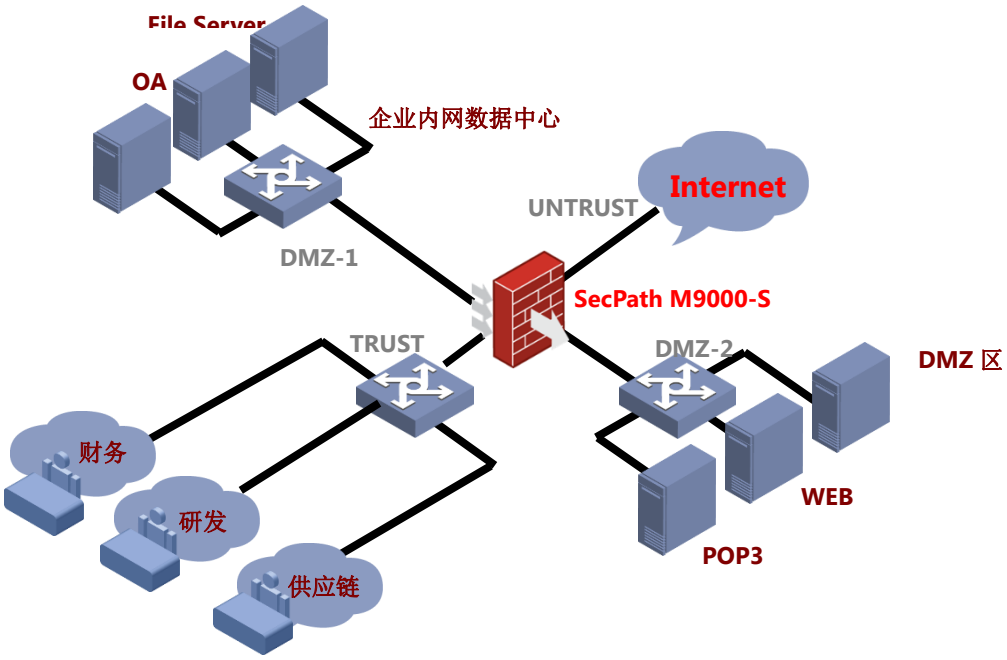
属性	M9008-S	M9012-S
	支持热补丁技术	
易维护性	支持基于命令行的配置管理 支持 Web 方式进行远程配置管理 支持 H3C iMC 管理平台进行设备管理 支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2	
环保与认证	支持欧洲严格的 RoHS 环保认证	

典型组网

防火墙应用

SecPath M9000-S 提供强大的过滤功能和优秀的管理能力，部署在内网出口，防范各种来自外部的攻击，也可作为内网访问控制设备隔离不同安全等级的区域。

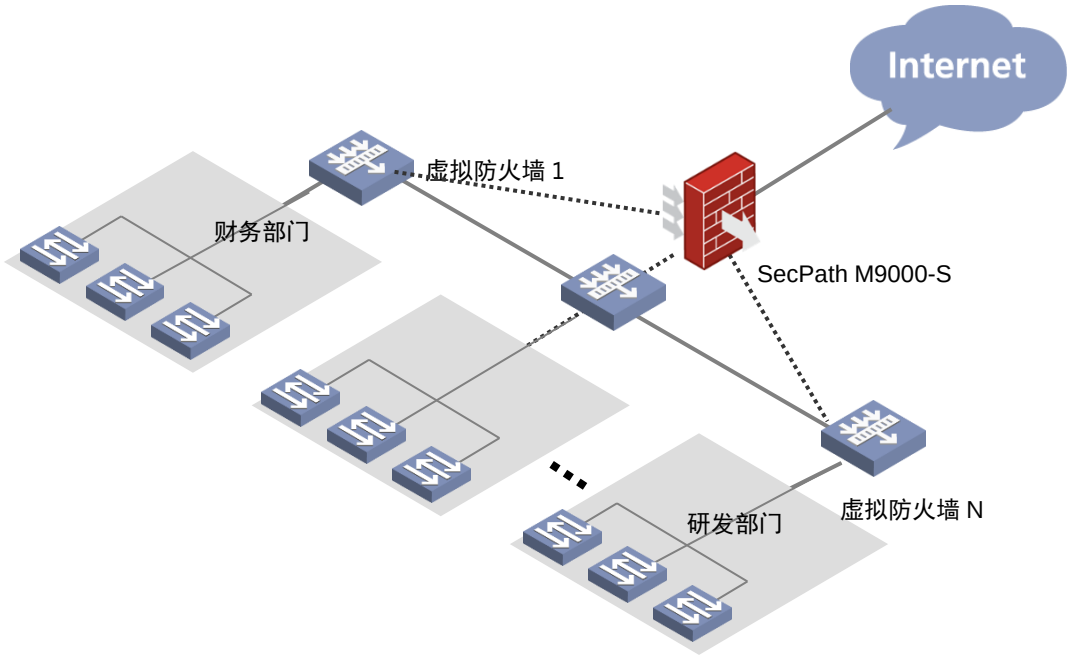
防火墙应用组网图



虚拟防火墙应用

SecPath M9000-S 不但提供强大的防火墙/VPN 功能，还可支持虚拟防火墙功能，一台 SecPath M9000-S 可虚拟成多台逻辑上的防火墙，每个虚拟防火墙有自己的策略且可进行独立管理。

虚拟防火墙功能应用组网图



选配信息

主机选购一览表

模块	数量	备注
SecPath M9008-S主机	1	选配
SecPath M9012-S主机	1	选配
SecPath M9008-S 主控交换模块	1-2	必配
SecPath M9012-S 主控交换模块	1-2	必配

安全业务引擎选购一览表

安全业务模块	描述	备注
防火墙业务板	依据机箱线卡槽位数	可选
应用交付业务板	依据机箱线卡槽位数	可选
入侵防御业务板	依据机箱线卡槽位数	可选

接口单元选购一览表

接口模块	描述	备注
48 端口千兆以太网电接口	48 端口千兆以太网电接口	选配
48 端口增强型千兆以太网光接口	48 端口增强型千兆以太网光接口	选配
16 端口千兆以太网光口(SFP,LC)+8 端口千兆以太网 Combo 口+2 端口万兆以太网光接口	16 端口千兆以太网光口(SFP,LC)+8 端口千兆以太网 Combo 口+2 端口万兆以太网光接口	选配
4 端口万兆以太网光接口模块	4 端口万兆以太网光接口模块	选配
8 端口万兆以太网光接口模块	8 端口万兆以太网光接口模块	选配
32 端口万兆以太网光接口模块	32 端口万兆以太网光接口模块	选配
4 端口 40G 以太网光接口板	4 端口 40G 以太网光接口板	选配
2 端口 100G 以太网光接口板	2 端口 100G 以太网光接口板	选配

电源模块选购一览表

电源模块	备注
交流电源模块,1400W	必选 1 个电源，最多可选 2 个，根据设备供电情况选择电源模块
直流电源模块,1400W	必选 1 个电源，最多可选 2 个，根据设备供电情况选择电源模块
交流电源模块,2500W	必选 1 个电源，最多可选 2 个，根据设备供电情况选择电源模块

电源模块	备注
直流电源模块,2500W	必选 1 个电源，最多可选 2 个，根据设备供电情况选择电源模块

新华三技术有限公司

北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市高新技术产业开发区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504