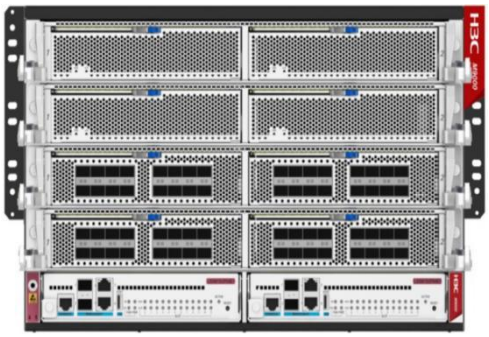
H3C SecPath M9000-AI-E 系列多业务安全网关

产品概述

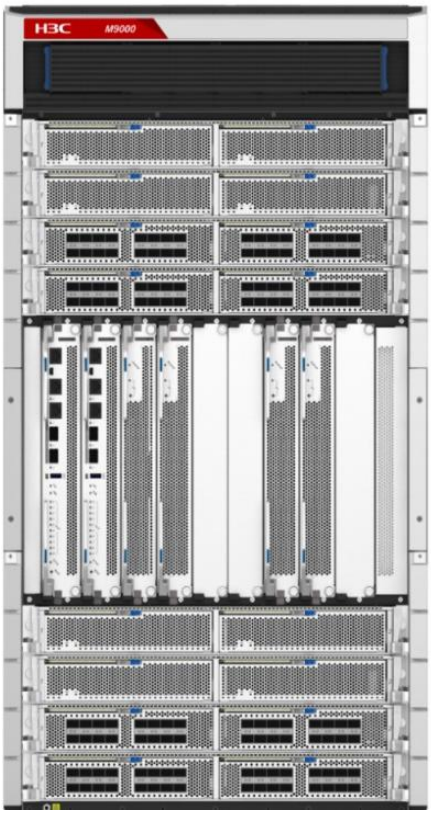
H3C SecPath M9000-AI-E 系列多业务安全网关是新华三技术有限公司（以下简称 H3C 公司）结合云计算、5G、物联网、IPv6、大数据及高性能计算的发展趋势，针对云计算数据中心、运营商 CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。

H3C SecPath M9000-AI-E 系列支持双 GPU+双 CPU+AI 芯片的芯架构、以及 AI 算法加持的全新计算模块，全面支持攻击防范、异常流量清洗、未知威胁检测、服务器异常外联检测、敏感数据保护、web 应用安全防护、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；深度业务安全检测可更细致的为 web 服务器提供保护。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 SecPath M9000-AI-E 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，模块分离可拔插式设计，便于灵活组网和扩容。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。



M9000-AI-E8



M9000-AI-E16

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

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 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

深入的 WEB 安全防护 不局限于常规的 IPS/AV 防护，针对内网服务器，提供细致化的 web 应用防护，对于服务器最为头疼的 C C 攻击，异常外联，SQL 注入、HTTP 慢速攻击、跨站脚本等常见攻击行为，对来自 Web 应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。

未知威胁检测 单靠特征分析已不足以应对复杂的网络环境，面对典型的 APT（Advanced Persistent Threat，高级持续性威胁）攻击沙箱技术是防御 APT 攻击最有效的方法之一，它用于构造隔离的威胁检测环境。H3C 安全网关通过将网络流量送入沙箱进行隔离分析，由沙箱给出是否存在威胁的结论。检测到某流量为恶意流量，设备将对流量实施阻断等处理。

终端识别，共享管理 终端识别是建立物联网安全连接的重要前提，用于识别物联网中的终端，。当终端流量流经设备时，H3C 安全网关可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时（比如将原厂商的摄像头换为其他厂商的摄像头）向用户发送日志，提示用户。同时采用应用检测方式和 IPID 检测方式对通过 NAT 技术或代理技术进行共享上网的行为进行识别和管理。

服务器异常外联检测 服务器外联防护是一种针对内网服务器的保护机制，可以有效识别服务器的主动外联行为，制定相应的外联防护策略来识别异常报文，并输出告警信息，以便管理员进行进一步的处理。为管理员检查服务器提供依据，进而防止服务器成为僵尸网络的一部分，对外发动攻击或对内进行渗透。

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。

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

自检运维，策略风险调优 通过对安全策略的冗余及命中分析，识别出冗余和未命中的安全策略，以帮助管理员对设备上的安全策略进行深度分析和处理。同时通过应用层检测引擎智能地分析安全策略允许通过的流量中存在的潜在风险，为设备中所有安全策略的安全系数进行总体评估。

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

支持基于接口及 IP 的报文捕获 将捕获到的报文生成 Wireshark（一种网络封包分析软件）可识别的.cap 后缀文件，保存到本地或外部服务器，供用户分析诊断出入设备的流量。

支持丢包统计功能 用与分析和记录设备的转发流程和安全业务模块（如：攻击防范、会话管理和连接数限制等）丢弃报文的详细原因

支持网页诊断功能 当内网用户访问网页出现故障时，对网络进行基本的诊断，并给出故障原因。

支持报文示踪功能 支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和连接数限制等）对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。

图形化界面，提供简单易用的 Web 管理

通过 H3C SSM 管理系统，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

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

产品规格

属性	M9000-AI-E8	M9000-AI-E16
主控板槽位数	2	2
业务板槽位数	8	16

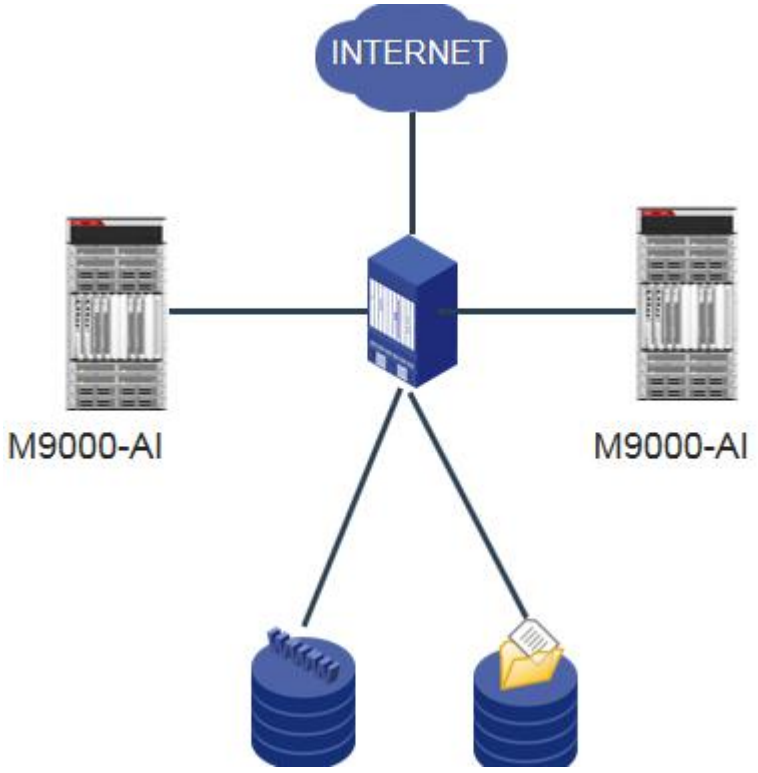
属性	M9000-AI-E8	M9000-AI-E16
交换网板槽位数	4	4
冗余设计	主控、交换网板、电源、风扇	主控、交换网板、电源、风扇
尺寸（W X H X D）	440mm×264mm×857mm（6RU）	440mm×841.7mm×640mm （19RU）
重量（kg）	< 140kg	<220kg
总功耗(W)	<2252W	<3360W
环境温度	工作：0～45℃ 非工作：-40～70℃	
运行模式	路由模式、透明模式、网桥模式	
AAA 服务	Portal 认证、RADIUS 认证、HWTACACS 认证、PKI /CA（X.509 格式）认证、 域认证 支持手动密钥、IKEv2、冗余 VPN 网关、EAP 认证、IKEv2 重定向	
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 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 ICMPv6、DHCPv6 支持 802.1q VLAN 透传 MPLS L3VPN、MLD、ND	
安全策略	基于域名（域名组）、服务、用户、应用、时间段等访问控制列表，可将基于端口的安全策略转换为基于应用的安全策略 支持策略风险等级划分，可根据风险等级进行策略调优 策略可模糊查询，可检索冗余和无命中策略，且支持与第三方系统对接，以实现策略优化，便于分析冗余和无命中的策略 支持策略分组，支持策略规则标签管理，可通过 NETCONF 接口与第三方平台对接，以对策略进行新建、删除、修改、移动、锁定、解锁等动作 基于状态合法性的安全监测 支持基于黑白名单的访问控制，支持根据告警一键设置黑白名单 安全策略可识别并管理网络中应用间的互访关系	
路由功能	支持静态路由 支持动态路由：RIP、OSPF、BGP、ISIS 等路由协议 支持基于源/目的 IP，源/目的端口、服务，基于应用类型和用户及用户组，基于出/入接口，链路状态、DSCP 优先级等的策略路由	
病毒防护	支持基于 IPV4 与 IPV6 双栈的病毒特征检测和防护，可对邮件类病毒、web 应用类病毒、常见文件病毒、木马、蠕虫，恶意网页、压缩数据、加壳和压缩包（zip、gzip、tar）病毒的查杀 支持病毒库手动和自动升级，支持手动导入特征库	

属性	M9000-AI-E8	M9000-AI-E16
	支持云端病毒库 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	
web 安全防护	支持 web 安全检测 支持 CC 攻击防护 支持服务器异常外联检测 支持网页挂马、木马、等攻击防护 支持对常见 web 服务（包括 HTTP、FTP、SSH、SMTP、IMAP 等）、常见数据库软件（MySQL、Oracle、MSSQL）的密码和口令暴力破解检测和防护，可自定义防护阈值	
深度安全防护	支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，可根据不同场景，细分策略，制定入侵防御的模板 支持应用层（HTTP、HTTPS、DNS、FTP、SIP 等）Flood 攻击，可通过机器自学习，设定学习时间和阈值，自动根据结果生成 DDoS 防范策略 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） 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 支持 URL 识别，支持恶意 URL 阻断，可与云端或本地的 URL 服务器对接，以扩容 URL 地址库数量 支持基于域名的安全防护与审计功能，可防护恶意域名及黑名单服务器地址，并且支持定期从云端同步 对于未知威胁攻击，支持本地和云端沙箱对接，实时检测 APT 类攻击 支持与统一安全管理平台对接和纳管，便于全网安全态势防护	
加密流量防护	支持 HTTPS 代理、ssl 卸载，可对解密后的 HTTPS，POP3S，SMTPS,IMAPS 等加密流量进行内容检测与过滤、审计和攻击防护。 可对 URL 进行精细化分类和解密，提高防护效果 可将解密后流量镜像给其他系统，便于审计	
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	

属性	M9000-AI-E8	M9000-AI-E16
智能带宽控制	支持基于用户、IP、接口、服务的带宽保证，支持流量整形，支持每 IP、每用户的最大/最小流量和连接数限速管理 可支持基于应用层协议设置流控策略，可设置最大/最小带宽、保证带宽、协议流量优先级等，支持八级管控	
负载均衡	支持基于 HTTP 和 HTTPS 的应用层链路负载均衡 支持 DNS 透明代理，支持 DNS 过滤，支持智能 DNS 支持服务器负载均衡 支持全局负载 支持链路健康状态检测 支持智能链路选择	
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 支持端口复用技术，可增加 NAT 转换上限 支持源地址和目的地址同时转换，当源 NAT 地址池使用率超限时实时告警 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 支持 NAT44(4)、NAT64、PCP、溯源方案	
VPN	L2TP VPN、IPSec VPN、GRE VPN、MPLS VPN、SSL VPN 支持 IPv6 over IPv4 GRE 隧道	
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 支持不间断升级 ISSU 支持热补丁技术，可平滑升级，支持对不同版本的软件实现双机热备 支持 BFD 链路检测 支持 BFD 与 VRRP 联动实现双机快速切换	

属性	M9000-AI-E8	M9000-AI-E16
	支持 BFD 与 OSPF 联动实现双机快速切换	
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 支持通过通过模拟部署的方式，可根据业务互访关系学习结果，对比待部署策略，便于运维人员管理安全策略，同时支持对黑白名单、应用类型、策略风险、安全规则、混合规则等方式对安全策略进行合规性检查 支持安全策略日志、NAT 日志、安全防护日志、URL 日志，可同时包含以上类型的日志字段，NAT 日志可支持端口段分配，设备日志可轮询发送	
环保与认证	支持欧洲严格的 RoHS 环保认证	

典型组网



H3C SecPath M9000 与企业组网

双机状态热备技术，高可靠网络设计

强劲的业务处理能力

卓越的 VPN 加密处理能力

优异的防攻击能力，有效防止单包、Flood 等攻击

丰富路由协议，实现安全与网络融合

选配信息

主机选购一览表

主机	描述	备注
H3C SecPath M9000-AI-E8	H3C SecPath M9000-AI-E8 主机框	必配
H3C SecPath M9000-AI-E16	H3C SecPath M9000-AI-E16 主机框	必配
主控制引擎模块	H3C SecPath M9000-AI-E 系列主控引擎	必配，1+1 冗余

安全业务引擎选购一览表

安全业务模块	描述	备注
SecBlade V 下一代防火墙 A 模块	SecBlade 安全业务板	选配

接口单元选购一览表

接口模块	描述	备注
接口交换 A 模块(SH)		选配
2 端口 100G 以太网光接口(QSFP28)+16 端口万兆以太网光接口模块(SFP+)		选配
4 端口 40G 以太网光接口(QSFP+)+16 端口万兆		选配
24 端口万兆以太网光接口模块(SFP+)		选配
6 端口 100G 以太网光接口模块(QSFP28)		选配

交换引擎

交换引擎		备注
H3C SecPath M9000-AI-E8 交换网板,A 类		必配
H3C SecPath M9000-AI-E16 交换网板,A 类		必配

电源模块选购一览表

电源模块	备注
2400W 交流电源模块	必配
2400W 直流电源模块	必配
3000W 交流电源模块	必配
3000W 交流&240V-380V 高压直流电源模块	必配

风扇模块选购一览表

风扇模块	备注

风扇模块	备注
H3C 风扇框模块	必配

杭州华三通信技术有限公司

http://www.h3c.com.cn

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
版本：20120316-V1.0

北京分部
北京市宣武门外大街 10 号庄胜广场中
央办公楼南翼 16 层
邮编：100052
电话：010-63108666
传真：010-63108777

客户服务热线
400-810-0504
800-810-0504