华为SecoManager安全控制器

面对差异化的租户业务和频繁的业务变更场景，如何实现安全业务的自动化分析、可视及可管，安全策略调优以及合规性分析，是迫切需要解决的问题。传统依赖人工管理及配置安全业务，运维比较低效。安全策略合规性检查需要投入专人分析，往往审批不够及时，也可能疏漏风险策略。安全策略体量越来越大，致使安全运维人员难以聚焦在关键的风险策略上。业界急需基于智能化、自动化的围绕安全策略全生命周期的安全策略管理方式，可以帮助用户快速、高效完成策略变更的同时，确保策略下发安全和准确，从而有效提升运维效率、降低运维成本。

SecoManager安全控制器是华为针对数据中心、园区、海量分支等不同场景推出的统一安全控制器，提供安全网元/策略统一管理、安全策略编排、日志管理和AntiDDoS管理等功能，支持安全功能服务化、可视化，协同网络、安全设备和大数据智能分析系统形成全面威胁感知、分析和响应的整网主动安全防护体系。

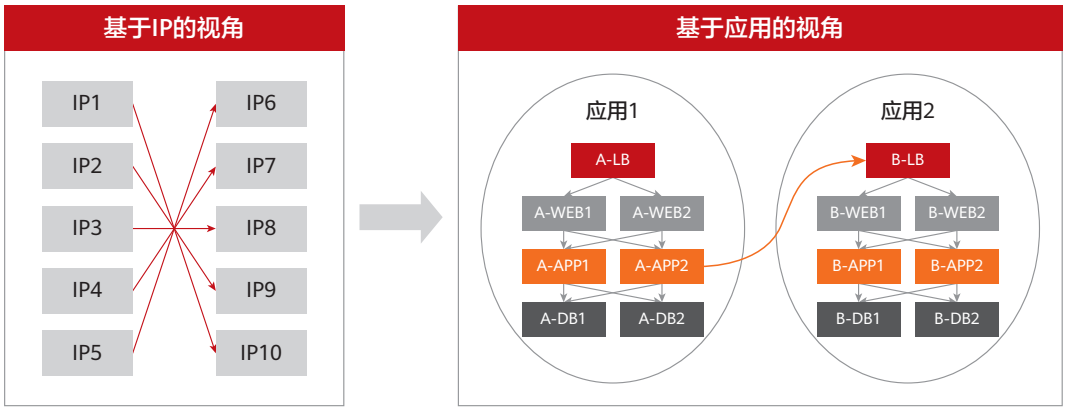
产品图

HUAWEI

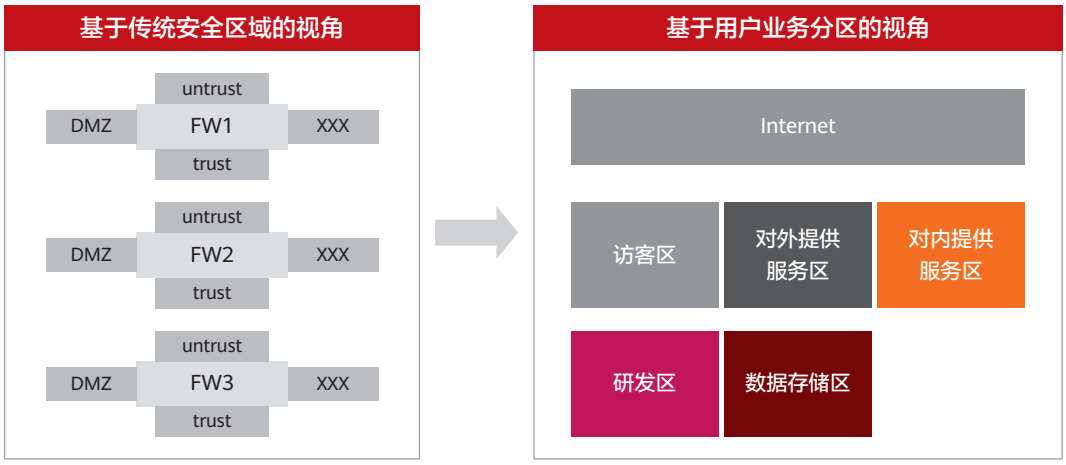
产品特点

策略多维自动化编排，安全业务分钟级部署

- **应用互访关系映射与基于应用的策略管理：**从基于IP到IP的策略管理视角过渡到基于应用互访关系的策略管理视角。以应用为核心，抽象出网络中应用的互访关系，使得用户业务变得可视，帮助用户“0距离”贴近现网中的应用服务，有效降低安全策略数量。旨在通过模型化的应用策略模型，简化用户配置工作量，从而帮助用户的全网策略管理工作化繁为简。



- **基于客户业务分区的策略管理：**从基于安全区域的策略管理视角过渡到基于用户业务分区的策略管理视角。传统的网络分区以安全区域为单位，比如trust、untrust、dmz、local等，面对安全设备数量较多、网络规模庞大的场景，对于用户来说安全区域、设备、策略、业务上线、业务变更等要素交织在一起，很难清晰的还原出客户业务的脉络，从而不能有效的指导安全策略的设计。然而，站在客户业务分区的视角管理、控制、维护安全策略，用户不需要关注安全区域、设备以及业务的映射关系，仅需要关注业务分区和安全服务，有效降低了安全策略设计的复杂度。



- **保护网段圈定设备与策略的管理范围，策略编排有章可循：**保护网段是安全业务编排的基础模型，可以理解为一台防火墙所保护的用户网段范围，配置方式支持手工或网络拓扑学习。通过感知用户业务IP与防火墙的对应关系，在策略自动化编排时，基于策略的源地址和目的地址即可自动找到承载该策略的防火墙设备。

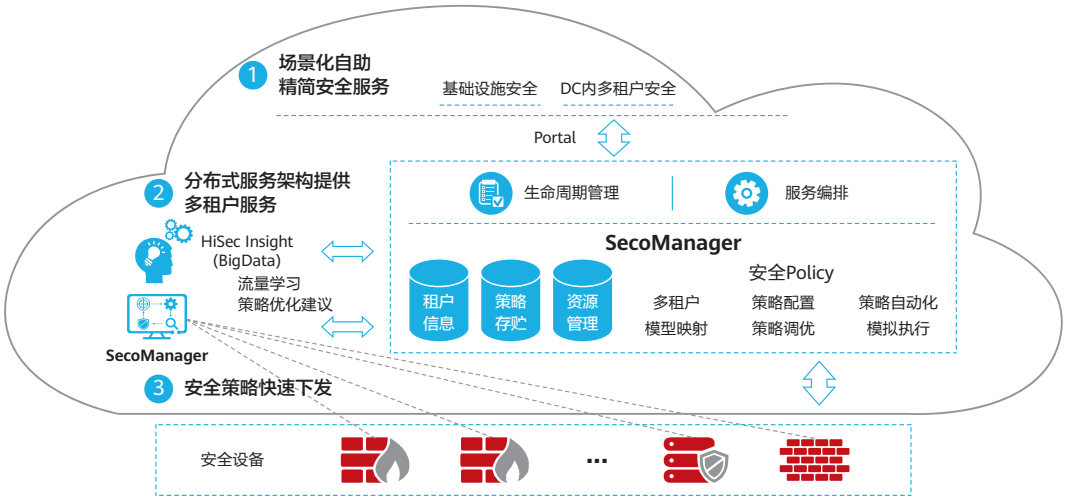
- **安全业务自动化部署：**丰富的安全服务为数据中心运营带来了安全保障。借助保护网段、策略自动编排以及基于业务链的自动化引流等技术使得实现差异化的租户安全策略成为可能。通过策略自动分层，策略的可拆分、可合并，帮助用户在变更策略时，了然于心。

策略智能运维，降低运维成本80%

- **策略合规性检查：**安全策略合规性审视需要由安全审批责任人确认，平均每天需要处理的待审批策略从几条到数百条不等。由于工具对规则支撑不全，需要人工逐条分析，每天投入多个小时进行专人分析，审批工作量大。通过定义白名单、风险规则、混合规则等检查方式，待策略提交后，匹配定义好的检查规则，及时反馈检查结果、安全等级等信息至安全审批责任人。低风险策略自动审批，致使安全审批人员仅需关注不合规的策略条目，从而提高策略审批效率，避免了审批不及时以及疏漏风险策略的事情发生。
- **策略冗余分析：**策略部署后，针对整网策略进行冗余和命中分析，结合策略优化算法，实现策略冗余分析，从而帮助用户聚焦与业务强相关的策略。

协同网络与安全联动，威胁分钟级闭环处置

- **与网络协同处置：**在传统的数据中心里，应用程序部署往往会经历一个漫长的过程。应用业务团队要依赖网络团队进行网络部署，网络团队需要了解应用业务团队的诉求，才能部署一套适合应用业务团队需要的网络。结合网络拓扑学习业务策略与安全策略的映射关系，通过与数据中心SDN管理与控制系统（iMaster NCE-Fabric）协同，基于业务链按需调度将租户流量引流至对应的安全设备。通过自动同步网络SDN管理与控制系统的租户、VPC、网络拓扑（包括逻辑路由器、逻辑交换机、逻辑防火墙、子网）、EPG、业务链等信息，结合学习到的应用业务互访关系，自动编排下发安全策略，从而实现与网络的协同。



- **与安全协同：**高级威胁攻击威胁国计民生的基础设施，例如金融、能源、政府等，攻击的实施者会经过大量精心的准备和等待，利用0-Day漏洞、高级逃逸技术、蠕虫+勒索等多种攻击手法。大数据安全产品HiSec Insight基于网络行为分析与关联分析技术，可有效识别未知威胁。根据威胁的严重等级来判断处置方式是隔离还是阻断，如果是南北向的威胁则通过SecoManager安全控制器下发五元组阻断策略至安全设备，如果是东西向威胁则通过下发隔离请求至网络SDN管理与控制系统，控制交换机/路由器隔离受威胁的主机。

百万级会话日志采集存储性能，NAT溯源轻松调查取证

- 百万级的会话日志采集、处理与审计性能，满足国家级网络出口带宽的会话日志审计性能需求，可为大规模、超大规模网络提供高性能的日志采集、存储、审计功能。
- 对NAT设备的会话日志进行采集和分析，获取NAT信息（包括目的IP地址、目的端口、NAT前源IP地址和协议等），从而满足安全审计和取证的需要。

威胁日志报表呈现，威胁信息了如指掌

- 提供威胁日志查询功能，通过配置威胁日志查询方式和查询条件可获取威胁日志查询结果，通过分析具体威胁日志信息，用户可了解设备受威胁状况。
- 用户可自定义威胁日志报表，例如选择报表维度、设置筛选条件等。图形化的报表呈现可使用户可从不同的维度查看、对比威胁日志数据，了解外部网络中病毒事件和攻击行为，从而制定相应的安全防护策略。

AntiDDoS管理，全局监控防御DDoS攻击

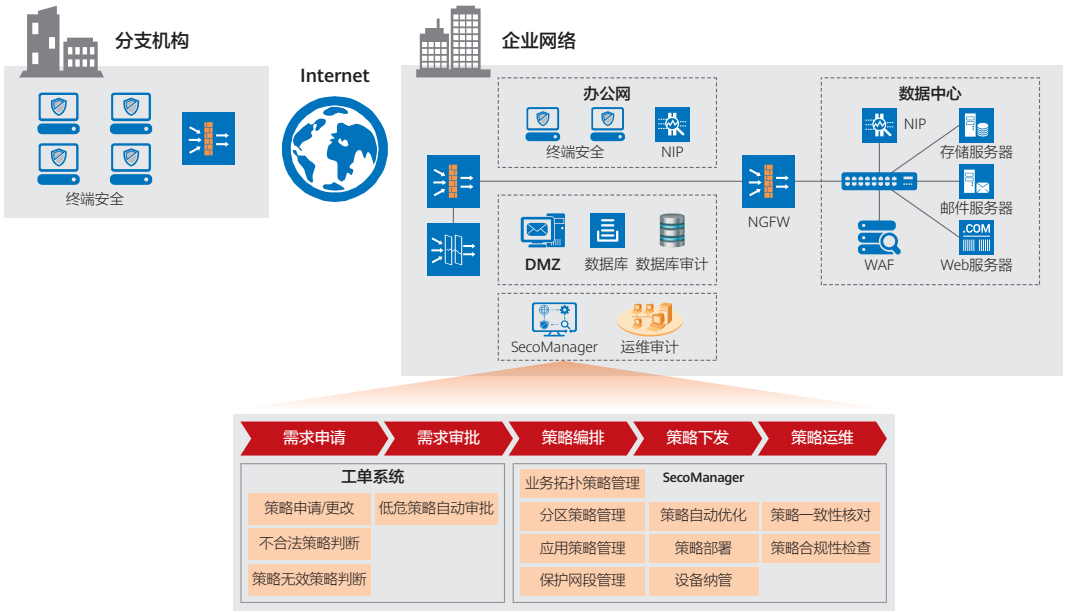
- SecoManager作为管理中心，负责检测中心和清洗中心的统一管理，提供设备管理、策略管理、性能管理、告警管理、报表管理等功能。检测中心负责对流量进行检测，发现异常后上报SecoManager，由SecoManager下发引流策略至清洗中心进行引流清洗。清洗中心主要根据SecoManager下发的策略进行引流、清洗，并把清洗后的正常流量回注。
- 全局监控DDoS攻击，用户可在监控界面实时查看攻击告警实时监控、设备流量对比、防护对象流量对比、目的IP流量对比、IP流量Top 10、连接数Top 5、设备CPU利用率和动态黑洞等信息，快速闭环DDoS攻击事件处置。
- 提供流量分析、异常/攻击分析专项报表，分析网络流量和攻击日志信息，报表可长期储存，方便用户实时并全面掌握威胁数据。

产品部署模式

- **独立部署：**SecoManager安全控制器以独立软件的形式部署在服务器或虚拟机
- **合一部署：**SecoManager安全控制器与网络SDN管理与控制系统部署在同一物理服务器的同一虚拟机

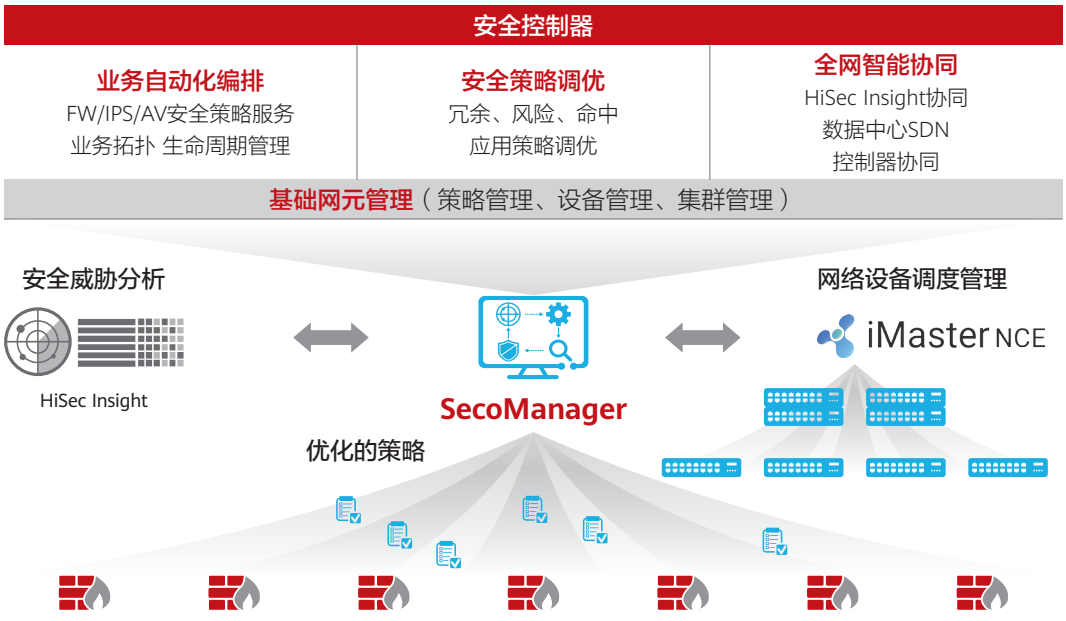
典型应用

传统网络：全网安全策略统一管理



- 分支机构数量众多，比如大型商贸连锁、大型物流企业、金融营业网点等，安全网元数量庞大，集中纳管安全网元；
- 对接企业工单系统，策略合规性检查、策略编排以及策略下发，处理流程自动化；
- 策略合规检查、策略冗余分析以及策略一致性对比等方式，分析已部署策略的合理性，提高运维效率。

SDN网络：全网安全策略统一管理，多维威胁防护



- 与网络SDN管理与控制系统协同，感知网络拓扑变化，实现基于租户的安全服务自动化部署；
- 阻断南北向威胁，隔离东西向威胁，基于业务链引流实现SDN网络精细化安全管控；
- 与云平台联动，通过云平台对接，实现业务策略到安全策略的自动转化。

产品规格

主要功能		
大类	**子类**	**描述**
基础网元管理	设备管理	设备发现、设备管理（防火墙、IPS和AntiDDoS等）、设备组管理（支持3级）、虚拟系统管理、配置一致性检查、设备单点登录、双机热备组管理、自定义分权分域、系统模板、设备监控、全局监控
	资源池管理	资源池的增、删、改、查
	对象管理	地址、服务、时间段、NAT地址池、安全域、URL分类、入侵防御、反病毒、URL过滤、APT防御、应用主机、网络分区、应用、应用组
	策略管理	安全策略、NAT策略、IPSec策略、带宽策略、部署任务
策略协同	大数据安全分析系统协同	接收发自大数据安全分析系统的威胁处置请求，传递至威胁阻断设备
	网络控制器协同	感知网络拓扑、基于业务链的引流策略下发
策略编排	基于网络分区、应用互访关系、安全服务、VPC，自动化下发安全策略	
策略调优	根据冗余分析的结果进行策略调优	
日志管理	会话日志	百万级IPv4/IPv6会话日志查询以及NAT-Port Range日志、用户端口预分配日志查询 通过NAT日志中记录的转换前后IP地址和端口对应关系进行身份关联溯源，实现各类安全审计和取证
	威胁日志	支持对设备威胁日志（IPS、AV）进行采集、存储、查询，及报表呈现能力。并支持通过syslog协议外发

运行环境	
硬件要求：如果自备服务器，推荐采用2288X V5（X86）或TaiShan 2280 V2（ARM）	
业务需求	**每台服务器配置要求**
设备集中管理（除AntiDDoS）、策略智能运维	CPU：2*10CORE 内存：64G 系统盘：2*600G SAS RAID1 硬盘读写速率：20MB/s 网口：单机部署时>=2，集群部署时>=4

主要功能		
大类	子类	描述
设备集中管理（除AntiDDoS）、策略智能运维；设备日志管理（企业网场景）		CPU：2*10CORE 内存：96G 系统盘 ：2*600G SAS RAID1 数据盘：4*6T SATA RAID6 硬盘读写速率：200MB/s 网口：单机部署时>=2，集群部署时>=4
设备集中管理（含AntiDDoS，30,000 IP规模）、策略智能运维		
设备集中管理（仅AntiDDoS，100,000 IP规模）		
设备集中管理（除AntiDDoS）、策略智能运维；设备日志管理（运营商场景）		CPU：2*10CORE 内存：96G 系统盘：2*600G SAS RAID1 数据盘：12*6T SATA RAID6 硬盘读写速率：200MB/s 网口：单机部署时>=2，集群部署时>=4
软件要求		
服务器CPU架构	操作系统版本	
X86	Euler V2.9	
ARM	Euler V2.9	

订购信息

编码	描述
机架服务器	
SCM-AC-01	功能模块-SecoManager-SCM-AC-01-SecoManager交流典配01(2*10核/2.2GHz CPU，2*32GB内存，2*600GB-SAS 3.5英寸后置硬盘，4*GE+2*10GE，2*900W电源，RAID卡，滑道)
SCM-AC-02	功能模块-SecoManager-SCM-AC-02-SecoManager交流典配02(2*10核/2.2GHz CPU，2*32GB内存，2*600GB-SAS 3.5英寸后置硬盘，4*GE+2*10GE，2*900W电源，RAID卡，滑道)
SCM-AC-03	功能模块-SecoManager-SCM-AC-03-SecoManager交流典配03(2*10核/2.2GHz CPU，2*32GB内存，2*600GB-SAS 3.5英寸后置硬盘，4*GE+2*10GE，2*900W电源，RAID卡，滑道)
SCM-AC-04	功能模块-SecoManager-SCM-AC-04-SecoManager交流典配04(2*10核/2.2GHz CPU，2*32GB内存，2*600GB-SAS 3.5英寸后置硬盘，4*GE+2*10GE，2*900W电源，RAID卡，滑道)
SCM-AC-05	功能模块-SecoManager-SCM-AC-05-SecoManager交流典配05(2*10核/2.2GHz CPU，2*32GB内存，2*600GB-SAS 3.5英寸后置硬盘，4*GE+2*10GE，2*900W电源，RAID卡，滑道)

编码	描述
SCM-LRGLOG-01	功能模块-SecoManager-SCM-LRGLOG-01-策略集中管理|海量日志服务器01(2*10核/2.2GHz CPU，3*32GB内存，12*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-LRGLOG-02	功能模块-SecoManager-SCM-LRGLOG-02-策略集中管理|海量日志服务器02(2*10核/2.2GHz CPU，3*32GB内存，12*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-LRGLOG-03	功能模块-SecoManager-SCM-LRGLOG-03-策略集中管理|海量日志服务器03(2*10核/2.2GHz CPU，3*32GB内存，12*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-LRGLOG-04	功能模块-SecoManager-SCM-LRGLOG-04-策略集中管理|海量日志服务器04(2*10核/2.2GHz CPU，3*32GB内存，12*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-LRGLOG-05	功能模块-SecoManager-SCM-LRGLOG-05-策略集中管理|海量日志服务器05(2*10核/2.2GHz CPU，3*32GB内存，12*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-01	功能模块-SecoManager-SCM-MDMLOG-01-策略集中管理|轻量日志|AntiDDoS防护服务器01(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-02	功能模块-SecoManager-SCM-MDMLOG-02-策略集中管理|轻量日志|AntiDDoS防护服务器02(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-03	功能模块-SecoManager-SCM-MDMLOG-03-策略集中管理|轻量日志|AntiDDoS防护服务器03(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-04	功能模块-SecoManager-SCM-MDMLOG-04-策略集中管理|轻量日志|AntiDDoS防护服务器04(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-05	功能模块-SecoManager-SCM-MDMLOG-05-策略集中管理|轻量日志|AntiDDoS防护服务器05(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-01	功能模块-SecoManager-SCM-MDMLOG-01-策略集中管理|轻量日志|AntiDDoS防护服务器01(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-02	功能模块-SecoManager-SCM-MDMLOG-02-策略集中管理|轻量日志|AntiDDoS防护服务器02(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-03	功能模块-SecoManager-SCM-MDMLOG-03-策略集中管理|轻量日志|AntiDDoS防护服务器03(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)
SCM-MDMLOG-04	功能模块-SecoManager-SCM-MDMLOG-04-策略集中管理|轻量日志|AntiDDoS防护服务器04(2*10核/2.2GHz CPU，3*32GB内存，4*6000GB-SATA 3.5前置+2*600GB-SAS 3.5后置，2*4GE电口+2*10GE光口，2*900W电源，RAID卡，滑道)

编码	描述
软件	
SCMPLF01	软件费用-SecoManager-SCMPLF01-SecoManager软件平台-Electronic
SCMDM	软件费用-SecoManager-SCMDM-SCM防火墙基础网元管理每节点-Electronic
SCMPO	软件费用-SecoManager-SCMPO-SCM防火墙安全业务编排每节点-Electronic
SCMDMVAS	软件费用-SecoManager-SCMDMVAS-SCM防火墙基础网元管理，每VAS-Electronic
SCMPOVAS05	软件费用-SecoManager-SCMPOVAS05-SCM防火墙安全业务编排管理，每5VAS-Electronic
SCMPOVAS10	软件费用-SecoManager-SCMPOVAS10-SCM防火墙安全业务编排管理，每10VAS-Electronic
SCMPOVAS50	软件费用-SecoManager-SCMPOVAS50-SCM防火墙安全业务编排管理，每50VAS-Electronic
SCMPOVAS100	软件费用-SecoManager-SCMPOVAS100-SCM防火墙安全业务编排管理，每100VAS-Electronic
SCMPOVAS500	软件费用-SecoManager-SCMPOVAS500-SCM防火墙安全业务编排管理，每500VAS-Electronic
SCMPOVAS1000	软件费用-SecoManager-SCMPOVAS1000-SCM防火墙安全业务编排管理，每1000VAS-Electronic
SCMADAT	软件费用-SecoManager-SCMADAT-SCM，第三方平台适配许可-Electronic
SCMDLMSMLNAT	软件费用-SecoManager-SCMDLMSMLNAT-小规模NAT溯源日志License(每秒1250条日志)-Electronic
SCMDLMMDMNAT	软件费用-SecoManager-SCMDLMMDMNAT-中规模NAT溯源日志License(每秒5000条日志)-Electronic
SCMDLMLRGNAT	软件费用-SecoManager-SCMDLMLRGNAT-大规模NAT溯源日志License(每秒12500条日志)-Electronic
SCMDLMSMLNSL	软件费用-SecoManager-SCMDLMSMLNSL-小规模网络安全业务日志License(每秒250条日志)-Electronic
SCMDLMMDMNSL	软件费用-SecoManager-SCMDLMMDMNSL-中规模网络安全业务日志License(每秒1000条日志)-Electronic
SCMDLMLRGNSL	软件费用-SecoManager-SCMDLMLRGNSL-大规模网络安全业务日志License(每秒2500条日志)-Electronic
SCMPLFSNS01	软件年费-SecoManager-SCMPLFSNS 01-SCM软件平台订阅与保障年费，1年-Electronic
SCMDMSNS1Y	软件年费-SecoManager-SCMDMSNS1Y-SCM防火墙基础网元管理，1年订阅与保障年费，每节点-Electronic
SCMPOSNS1Y	软件年费-SecoManager-SCMPOSNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每节点-Electronic
SCMDMVASSNS1Y	软件年费-SecoManager-SCMDMVASSNS1Y-SCM防火墙基础网元管理，1年订阅与保障年费，每VAS-Electronic

编码	描述
SCMPOVAS05SNS1Y	软件年费-SecoManager-SCMPOVAS05SNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每5VAS-Electronic
SCMPOVAS10SNS1Y	软件年费-SecoManager-SCMPOVAS10SNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每10VAS-Electronic
SCMPOVAS50SNS1Y	软件年费-SecoManager-SCMPOVAS50SNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每50VAS-Electronic
SCMPOVAS100SNS1Y	软件年费-SecoManager-SCMPOVAS100SNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每100VAS-Electronic
SCMPOVAS500SNS1Y	软件年费-SecoManager-SCMPOVAS500SNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每500VAS-Electronic
SCMPOVAS1000SNS1Y	软件年费-SecoManager-SCMPOVAS1000SNS1Y-SCM防火墙安全业务编排，1年订阅与保障年费，每1000VAS-Electronic
SCMPLFSNS02	软件年费-SecoManager-SCMPLFSNS 02-SCM软件平台订阅与保障年费，3年-Electronic
SCMDMSNS3Y	软件年费-SecoManager-SCMDMSNS3Y-SCM防火墙基础网元管理3年订阅与保障年费每节点-Electronic
SCMPOSNS3Y	软件年费-SecoManager-SCMPOSNS3Y-SCM防火墙安全业务编排3年订阅与保障年费每节点-Electronic
SCMDMVASSNS3Y	软件年费-SecoManager-SCMDMVASSNS3Y-SCM防火墙基础网元管理，3年订阅与保障年费，每VAS-Electronic
SCMPOVAS5SNS3Y	软件年费-SecoManager-SCMPOVAS5SNS3Y-SCM防火墙安全业务编排，3年订阅与保障年费，每5VAS-Electronic
SCMPOVAS10SNS3Y	软件年费-SecoManager-SCMPOVAS10SNS3Y-SCM防火墙安全业务编排，3年订阅与保障年费，每10VAS-Electronic
SCMPOVAS50SNS3Y	软件年费-SecoManager-SCMPOVAS50SNS3Y-SCM防火墙安全业务编排，3年订阅与保障年费，每50VAS-Electronic
SCMPOVAS100SNS3Y	软件年费-SecoManager-SCMPOVAS100SNS3Y-SCM防火墙安全业务编排，3年订阅与保障年费，每100VAS-Electronic
SCMPOVAS500SNS3Y	软件年费-SecoManager-SCMPOVAS500SNS3Y-SCM防火墙安全业务编排，3年订阅与保障年费，每500VAS-Electronic
SCMPOVAS1000SNS3Y	软件年费-SecoManager-SCMPOVAS1000SNS3Y-SCM防火墙安全业务编排，3年订阅与保障年费，每1000VAS-Electronic

注：订购清单仅供参考，具体产品订购请咨询华为工程师。