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。安全策略下发对业务的影响不可预见，不能在策略部署前评估策略对用户业务的影响。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、广域、物联网等不同场景推出的统一安全控制器，提供安全业务编排和策略统一管理，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。

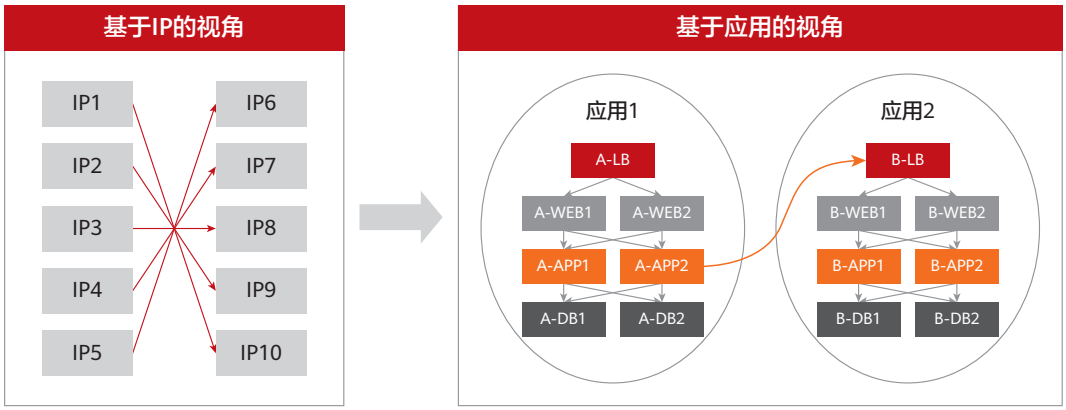
产品图

HUAWEI

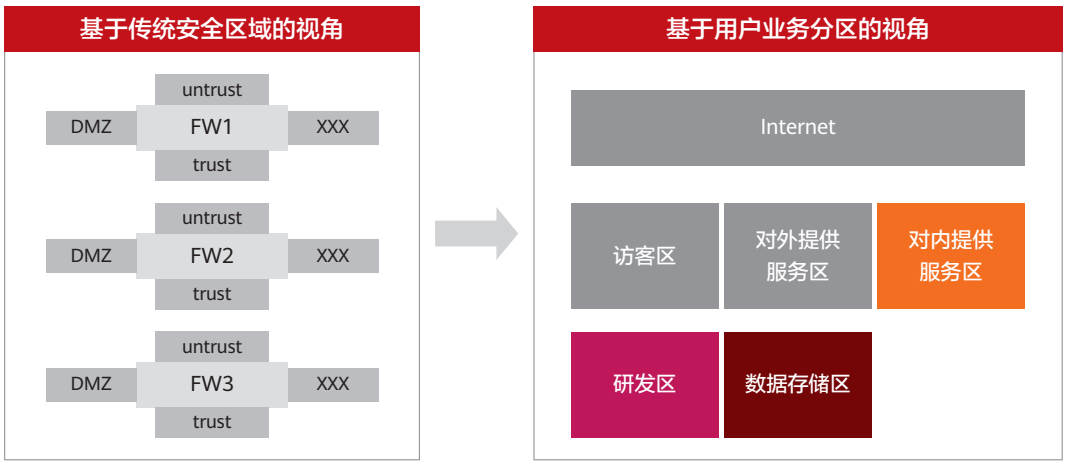
产品特点

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。



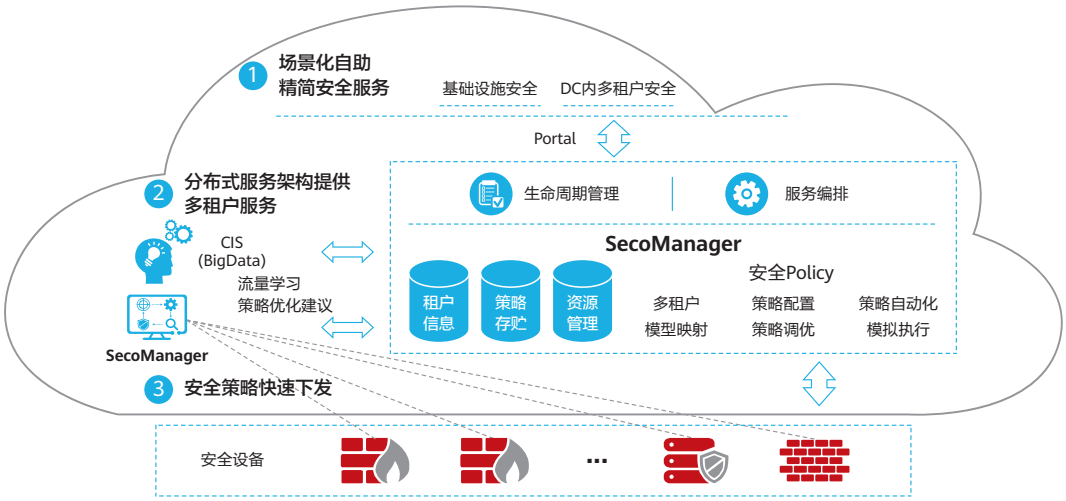
- **保护网段圈定设备与策略的管理范围，策略编排有章可循：**保护网段是安全业务编排的基础模型，可以理解为一台防火墙所保护的用户网段范围，配置方式支持手工或网络拓扑学习。通过感知用户业务IP与防火墙的对应关系，在策略自动化编排时，基于策略的源地址和目的地址即可自动找到承载该策略的防火墙设备。
- **安全业务自动化部署：**丰富的安全服务为数据中心运营带来了安全保障。借助保护网段、策略自动编排以及基于业务链的自动化引流等技术使得实现差异化的租户安全策略成为可能。通过策略自动分层，策略的可拆分、可合并，帮助用户在变更策略时，了然于心。

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。
- **策略仿真：**通过学习业务互访关系，对比待部署策略，以模拟部署的方式，在策略部署前评估策略对业务的影响，有效降低策略部署后对业务带来的风险。
- **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控制器（Agile Controller-DCN）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控制器的租户、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。



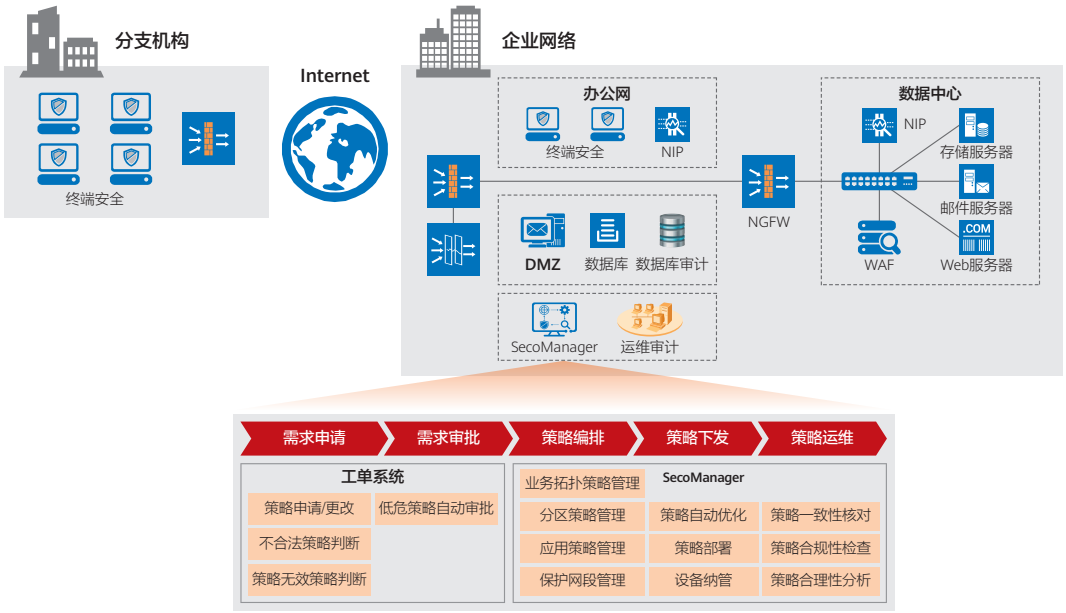
- **与安全协同：**高级威胁攻击威胁国计民生的基础设施，例如金融、能源、政府等，攻击的实施者会经过大量精心的准备和等待，利用0-Day漏洞、高级逃逸技术、蠕虫+勒索等多种攻击手法。大数据安全产品CIS基于网络行为分析与关联分析技术，可有效识别未知威胁。根据威胁的严重等级来判断处置方式是隔离还是阻断，如果是南北向的威胁则通过SecoManager安全控制器下发五元组阻断策略至安全设备，如果是东西向威胁则通过下发隔离请求至网络SDN控制器，控制交换机/路由器隔离受威胁的主机。

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控制器部署在同一物理服务器的同一虚拟机

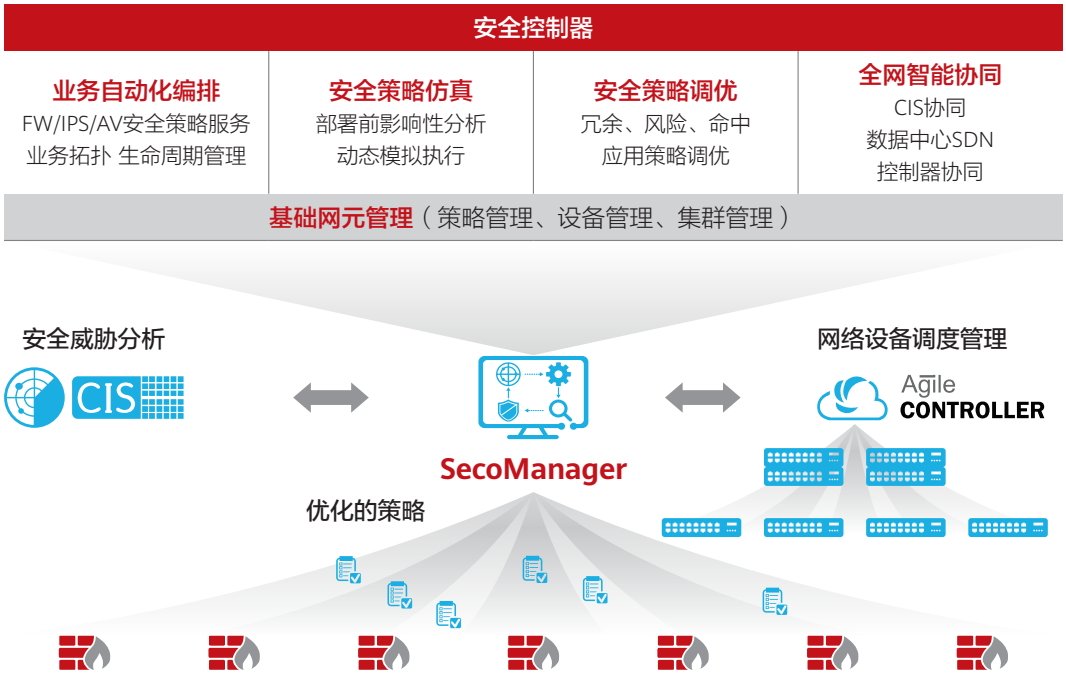
典型应用

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控制器协同，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		
基础网元管理	设备管理	设备发现、设备管理、设备组管理、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
	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、入侵防御、反病毒、URL过滤、APT防御、应用主机、网络分区、预定义应用
	策略管理	安全策略、NAT策略、VPC策略、安全服务、部署任务
策略协同	大数据安全协同	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
	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	
策略仿真	根据仿真结果分析变更策略对应用业务的事前影响	
运行环境		
硬件要求	• CPU：2.4GHz，16-core • 内存：64G • 硬盘：2*600G RAID1 • 网络：6*GE	
软件要求	操作系统（如自备操作系统，需满足如下条件） • Novell SUSE Linux Enterprise Server-企业版-12.0 SP4 • CentOS 7.4/7.5/7.6 • 虚拟化软件（SecoManager安全控制器部署在虚拟机上需自备） • FusionCompute KVM 6.3/6.5 • FusionSphere 6.5	

订购信息

编码	描述
机架服务器	
SCM-CLU-AC-03	功能模块-SecoManager-SCM-CLU-AC-03-安全控制器SecoManager单机交流高配(2*550W交流，滑轨)
软件	
SCMPLF01	软件费用-SecoManager-SCMPLF01-SecoManager软件平台-Electronic

编码	描述
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
SCMPLFSNS02	软件年费-SecoManager-SCMPLFSNS02-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
SCMPLFSNS01	软件年费-SecoManager-SCMPLFSNS01-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
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

编码	描述
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
外购件	
06040183	KVM-KVM 4 in 1 Control Module-1U高-17" LED-8路KVM接口-带国标电源线-八根USB直头线缆/带机架安装配件-英文资料-100~240V AC-黑色-满足

注：订购清单仅供参考，具体产品订购请咨询华为工程师。