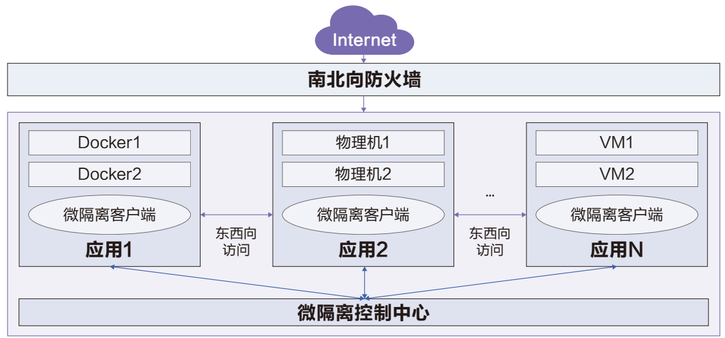
以微隔离为核心的零信任体系

传统的东西向安全场景中，随着业务上云的需求逐渐增多，云边界逐渐消失，云租户内部资源的安全隔离和访问控制需求日益复杂。新华三经过多年云安全的研究，正式发布了云安全2.0战略方针，充分将新华三原生的安全能力融入到云化变革当中，构建起完整的、与多种云计算环境全面融合的安全体系架构。其中针对于云内资源安全访问的场景推出了以微隔离为核心的零信任体系，整体分为微隔离控制中心和微隔离客户端两个部分，通过云主机之间的访问控制策略，阻断勒索病毒等安全事件在内部网络中蔓延，降低黑客的攻击面，从而实现东西向流量的可视化展示及策略的控制编排。



价值能力

东西向流量细粒度管控

识别数据流的流动方式，明确各应用之间连接和依赖性，构建清晰的可视化流量拓扑图

缩减内部攻击面

了解每个云主机的攻击面，从关键应用开始隔离，使用白名单策略，保持默认拒绝

基于业务的策略编排

不同于传统的基于网络结构创建策略，而是基于应用、角色、标签、分组来定义和编排策略

灵活划分隔离域

最小化网络分段划分，做到应用负载间的微隔离，服务进程之间的微隔离，防止横向跳板攻击、蠕虫病毒蔓延

新华三零信任解决方案应用场景

零信任远程办公接入

业务现状： 接入分支多，接入多样，信息风险高，业务系统多，种类繁杂，账号不一致

安全现状： 由于业务系统不能直接暴露在公网上，使用VPN远程接入，VPN自身爆出高危漏洞，黑客渗透进入内网

价值能力

隐身应用系统 | 集中身份管理 | 多因子认证方式 | 动态访问控制

零信任多云业务接入

业务现状： 云上用户、资源集中，资源的种类较多，登录方式各异访问人员复杂，业务系统公网可访问

安全现状： 公有云上资源与内网资源无法统一管理，云上资源安全应用等级杂乱 多云访问，无统一边界，云主机之间

价值能力

统一接入管理 | 集中身份管理 | 可视化策略拓扑 | 可跨云弹性扩展

零信任内网业务访问

业务现状： 传统的内外网划分，内网所有办公电脑和移动终端均可访问非隔离的区域，无具体权限的访问控制

安全现状： 黑客通过渗透或者社工等高级攻击方式，进入到内网，通过控制肉 鸡主机进行横向渗透，获取并破坏其他关键业务系统的数据信息

价值能力

细粒度访问控制 | 防止横向渗透 | 统一权限管控 | 可视化运维管理

新华三集团 www.h3c.com

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
杭州市滨江区长河路466号
邮编:310052

客户服务热线
400-810-0504

CN-161030-20210611-LF-HZ-V1.0

新华三零信任安全解决方案

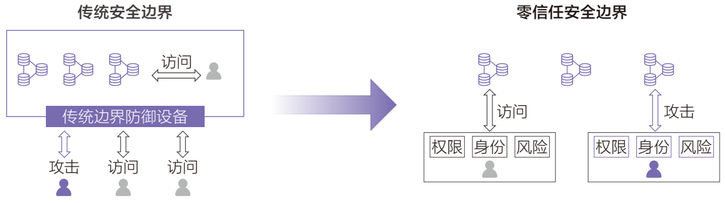
贯彻“永不信任，始终验证”原则

建立新边界，全面身份化

安全理念的转变：以身份为边界

安全挑战背景：复杂的网络架构、多样化的业务系统、交叉流动的业务数据，使得访问者与业务数据的边界逐渐模糊，从而导致了非黑即白的一次性授权、粗放的权限控制、不及时的威胁响应能力和内部数据泄露等安全风险出现。零信任架构正是在这种背景下诞生，可以有效解决传统的安全挑战。

传统安全机制受到挑战的主要原因是过度信任的问题，随着新技术的发展和混合云的大规模部署落地，基础设施和网络流量类型变得愈发复杂，企业用户无法明确网络边界。此时需要将访问人员的身份作为全新的安全边界，同时对访问人员的权限和安全风险情况进行实时综合分析，形成零信任的安全防护。根据NIST零信任安全架构，共分为南北向和东西向两大零信任安全防护的场景。



实现南北向零信任安全防护可使用身份识别与访问管理（IAM）和软件定义边界（SDP）两大技术架构。通过将原本分散的用户体系、认证体系进行整合，对用户的数字身份管理、认证、授权、审计进行集中管理，同时将控制平面和数据平面分离，遵循应用安全访问、持续信任评估和动态访问控制等核心原则，实现用户侧南北向的可信接入。

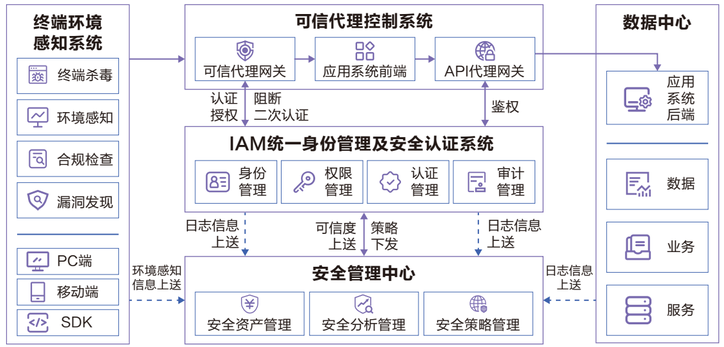
实现东西向零信任安全防护可使用微隔离（MSG）技术架构。通过将数据中心的资源按不同的工作负载角色在逻辑上细分为不同的安全段，再配置相关安全设备为这些安全段定义访问控制策略，实现租户内云主机的访问控制。

新华三基于对零信任网络安全解决方案的研究，贯彻“永不信任，始终验证”的原则，通过对身份进行统一管理，实现了设备、用户、应用等实体的全面身份化，建立全新的身份边界。通过在各个安全场景下的实践，陆续发布了基于南北向和东西向的零信任安全防护解决方案。

以身份管理为核心的零信任解决方案

在南北向安全防护场景中，新华三将零信任的理念融入到各个阶段的安全建设中，通过对访问者身份的管理，接入行为的持续性分析，根据分析结果来动态的控制访问权限，从而形成闭环的零信任安全架构。

零信任的核心本质即是身份管理，新华三以深度解耦、异构兼容为设计理念，贴合用户“安全、合规、可信”的需求，通过安全管理中心、可信代理控制系统、IAM统一身份管理及安全认证系统和终端环境感知系统的建设，将控制平面与数据平面分离，从而实现细粒度授权、动态环境感知、全流程审计、最小化原则的零信任安全理念。



价值能力

实时度量的终端可信感知

实时感知用户终端的关键信息，包括安全、进程、运行软件等信息，为持续动态的访问控制和整体的安全分析提供数据支撑

持续动态的访问控制

代理网关根据访问者实时变化的安全信息和身份信息，动态的调整访问控制策略。当发现安全风险和行为异常时，终止用户访问或者进行二次认证

细粒度的权限管控

对访问请求按照用户、应用、API接口、功能、数据进行多级的细粒度权限控制，限制访问者的权限，充分保护后端资源的安全访问

严格的多因素身份认证

对接主流的账号密码、物理、生物等身份认证系统，并对不同密级的应用资源编排认证链，进行二次及多次的认证，提高访问者身份的可靠性

自动化的安全威胁处置

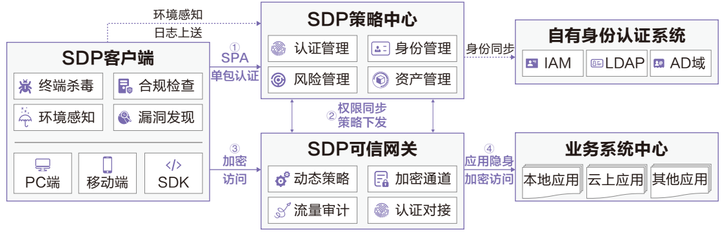
安全管理中心会综合用户及设备的异常访问信息，身份识别信息和攻击告警信息，结合AI分析引擎进行智能化的分析，从而实现自动化的安全处置

统一应用导航平台

用户统一登录入口，仅能查看有权限的应用列表，有效减少重复登录的交互过程，同时也在实时进行身份认证和访问控制，给用户既安全又无感知的访问

以安全接入为核心的零信任解决方案

新华三整合了一体化电信级可信网关、安全准入终端和安全态势分析引擎的核心优势能力，打造了以安全接入为核心的SDP零信任解决方案。方案主要由SDP客户端、SDP可信网关、SDP控制器组成，结合对零信任的研究及实践，通过对用户的统一安全接入及动态权限管理，实现了身份、终端、应用系统的安全可信。



价值能力

动态权限管控

通过收集用户风险、终端风险、UEBA等信息，同时利用动态防火墙技术快速建立安全防护策略、准入策略，从而动态地调整安全访问控制策略

应用服务隐藏

可信网关默认关闭所有端口，攻击方端口嗅探和漏洞扫描等信息探测手段不会得到任何响应， 可屏蔽所有后端业务系统遭受安全攻击

细粒度访问控制

可支持基于应用、功能、 身份、接口等，最小化原则 进行访问控制授权，即使 获取了某台服务器的权 限，也无法对其他服务器 进行横向渗透

一体化可信网关

全系列电信级可信网关设备，提供稳定性和高可用性能力，动态的访问控制，同时具备深度DPI检测能力，并搭载应用交付算法，最精准的满足访问资源负载分担

威胁协同处置

深度融合全网的身份管理、资产管理、权限管理、威胁管理数据，根据用户实时的安全风险和行为风险情况，自动化编排协同，形成安全闭环处置