基于零信任理念的企业端到端安全解决方案研究

Research on End-to-End Zero Trust Security Solutions for Enterprises

蔺　旋[1]，李长连[1]，徐宝辰[1]，贺译册[2]，余思阳[2]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联通智网创新中心，北京 100046）

Lin Xuan[1], Li Changlian[1], Xu Baochen[1], He Yice[2], Yu Siyang[2]（1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 2. Intelligent Network & Innovation Center of China Unicom, Beijing 100046, China）

摘　要：

随着数字化转型和业务上云的发展需求日益增长，企业在云原生背景下的防护能力成为其安全建设的重点，传统的网络安全架构无法满足技术架构和业务模式变革下的安全需求。通过整合零信任核心技术，提出了一种满足企业端到端的零信任安全解决方案。首先介绍了企业IT架构变化下的安全需求及零信任理念和其核心技术，并在此基础上设计了企业端到端零信任安全解决方案。随后对零信任安全解决方案和传统的安全方案进行了对比分析，最后展望了零信任安全在云原生环境下的应用前景。

关键词：

零信任；虚拟安全域；SDP；MSG

doi：10.12045/j.issn.1007-3043.2023.08.004

文章编号：1007-3043（2023）08-0014-05

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the growing demand for Digital transformation and cloud based business development, the protection capability of enterprises in the cloud native background has become the focus of their security construction. The traditional network security architecture can not meet the security needs under the technical architecture and business model change. A zero trust security solution that meets the end-to-end needs of enterprises has been proposed by integrating zero trust core technologies. It first introduces the enterprise security requirements under the changes in enterprise IT architecture, as well as the zero trust concept and its core technologies. Based on this, an end-to-end zero trust security solution for enterprises is designed. Subsequently, it compares and analyzes zero trust security solutions with traditional security solutions, and finally looks forward to the application prospects of zero trust security in cloud native environments.

Keywords：

Zero trust; VSA; SDP; MSG

引用格式：蔺旋，李长连，徐宝辰，等. 基于零信任理念的企业端到端安全解决方案研究[J]. 邮电设计技术，2023（8）：14-18.

1 企业防护架构变化

信息化技术普及后，企业面临着信息安全防护的考验和压力。为确保信息安全，企业在防范来自互联网的入侵和攻击的同时，更应重视来自企业内部网的入侵和攻击。在不改变现有架构的前提下，要以有限的资源加强内部网络的通信安全，考虑到构建方便与可用性高等因素，采用以VPN结合防火墙的安全控管，为企业提供一种增强内部网络通信安全的方法。

传统IT架构设计部署方式为：办公终端为企业资产，可进行操作系统级的安全管控，包括杀毒、桌管、DLP等，还可以使用云桌面实现更强数据保护；使用企业级SSL VPN实现安全远程接入和数据安全传输；互联网边界部署多重安全机制，控制来自互联网的安全风险；通过二层VLAN和三层路由实现内部网络区域的隔离和互通；企业关键应用和数据资产集中在企业内网环境[1]。企业传统IT系统架构如图1所示。

云原生环境下的企业IT计算资源全面云化，部分

收稿日期：2023-06-16

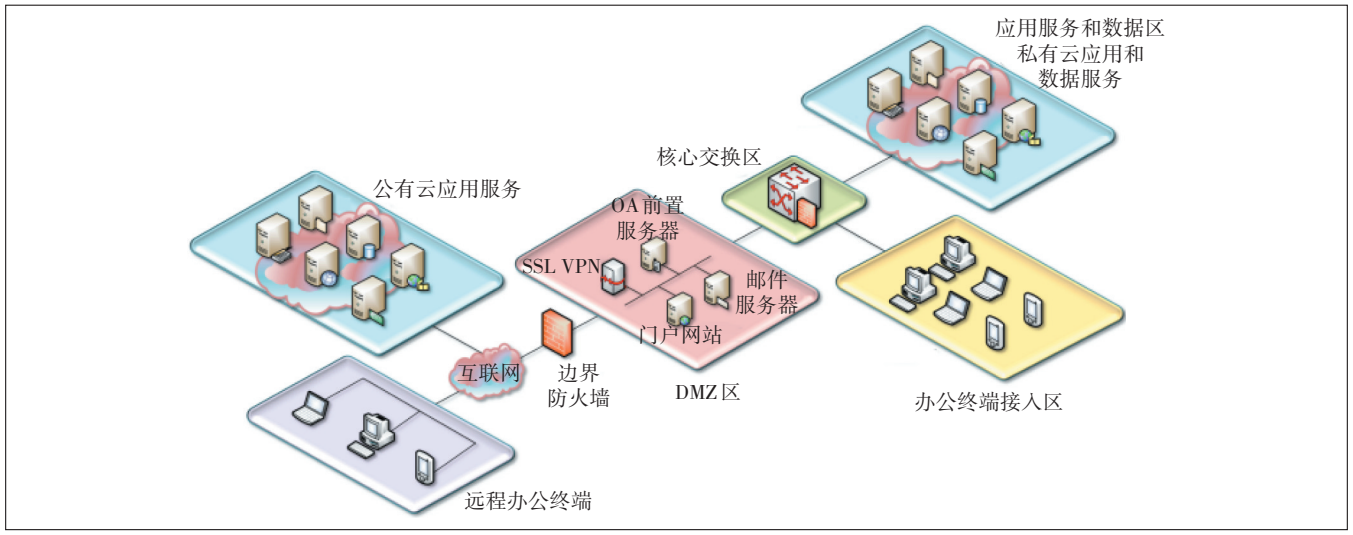

图1　企业传统IT系统架构

关键应用和数据迁移出私有数据中心，部署在公有云上，或直接使用公有云SaaS服务；业务移动化推动多种角色（员工外包方、合作伙伴）使用多样化BYOD终端（PC、笔记本电脑、移动终端）从内、外网访问私有云/公有云中企业关键应用服务和数据；以网络边界为中心，严防外部安全威胁，保护内部服务和数据资产的安全保障思路遭遇挑战。

业务云化也带了很多应用局限性。更多的第三方终端设备进入默认信任程度更高的企业内网环境，若缺乏有效管控，则易增加内网恶意代码爆发、恶意人为攻击、数据泄露等安全风险；更多的BYOD终端从内、外网访问企业关键业务应用，若无法进行设备级安全管控，则易发生业务数据在终端侧的泄露；更多的互联网服务端口暴露，存在安全漏洞，发生入侵攻击的可能性增加；在默认信任级别更高的内网环境中，网络访问控制机制不够严格，给恶意攻击者在内网的横向移动提供了可乘之机；安全通信机制缺失易发生网络流量劫持，导致账户、权限、敏感数据泄露[2]。

零信任理念及其核心技术可以针对性地解决云化所带来的企业安全应用问题，本文提出了一种基于零信任理念的企业端到端安全解决方案。

2 企业现代化安全需求

上文介绍了云原生环境下的企业IT架构变化后所面临的安全风险，通过安全需求分析，现代企业的安全建设普遍存在收敛暴露面、可信访问控制、数据链路安全等需求。

企业IT资源的全面云化，其核心应用及数据迁移至公有云，企业系统的互联网暴露面增加，且由于企业的多分支结构和混合云环境的复杂性，难以进行暴露面的有效收敛，企业迫切需要将关键应用服务从互联网隐身，最大限度收敛互联网资产暴露面，从而缩减攻击面，降低被恶意攻击和入侵的风险。

针对分布在混合云环境中的企业业务系统和数据中心，资源的统一管理和接入控制成为企业进行接入管理的重要保障，而传统接入方式无法针对访问用户接入要素进行校验和权限控制。企业需要建立以身份验证为中心，消除隐形信任，全面实现各类主体对应用服务/数据资源的细粒度可信访问控制。

企业搭建基于混合云架构的IT系统及相应安全防护能力，最重要的就是保障其核心业务开展和业务数据安全。传统方式通常在终端侧至资源侧使用SSL VPN或IPSec VPN解决传输阶段的数据安全问题，但是终端展示环节无防护措施，使终端侧成为数据保障的脆弱环节。企业在现有场景下需要对应用数据流转的全链路进行有效管控，降低敏感应用数据在通信传输、终端展示和存储环节发生泄露的风险[3]。

3 零信任核心能力

零信任概念最早由Forrester Research的John Kindervag所提出，其核心思想是“从不信任，始终验证”[4]。零信任的核心能力包括虚拟安全域（Virutal Security Area，VSA）、软件定义边界（Software Defined Perimeter，SDP）、微隔离（Micro Segmentation，MSG）等，

可满足云原生环境下的用户终端到资源端的安全防护需求。

3.1 VSA

VSA是基于移动操作系统底层技术，对移动应用进行完整安全控制的技术。VSA可在无需获取应用源代码、无需对操作系统进行Root或越狱的情况下，对应用进行容器化，建立一个可管理的、相对隔离的虚拟系统，作为构建在应用和系统、应用和应用之间的桥梁，从而对应用数据及用户使用行为等进行全方位的管理和保护。VSA技术如图2所示。

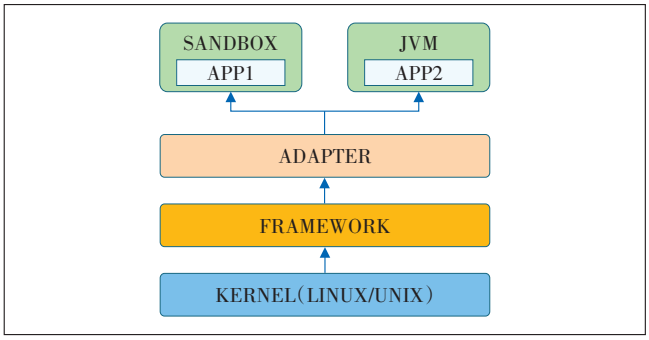

图2　VSA技术

使用VSA技术，可在BYOD的桌面终端和移动终端设备上隔离出安全工作空间，作为业务数据在终端上的安全边界，控制数据泄露，同时兼顾终端设备上个人信息的保护[5]。

3.2 SDP

SDP技术是通过软件的方式，在“移动+云”的背景下构建起虚拟边界，利用基于身份的访问控制及完备的权限认证机制提供有效的隐身保护，其技术架构如图3所示。

SDP可隐藏所有资源，非法用户无法获取资源入口，而合法用户访问流量均通过加密方式传输，其具备的持续认证、细粒度访问权限控制等主动防御理念可有效解决企业业务拓展中的安全问题[6]。

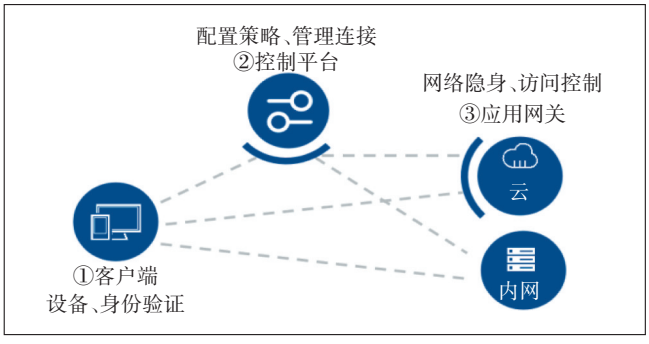

图3　SDP技术架构

3.3 MSG

MSG是更细粒度的网络隔离技术，能够满足传统环境、虚拟化环境、混合云环境、容器环境下对东西向流量隔离的需求，旨在为企业提供流量的可见性和监控能力[6]。微隔离有多种技术路线，主机代理路线的微隔离更加适应新兴技术更迭及应用带来的多变的用户业务环境，其技术架构如图4所示。

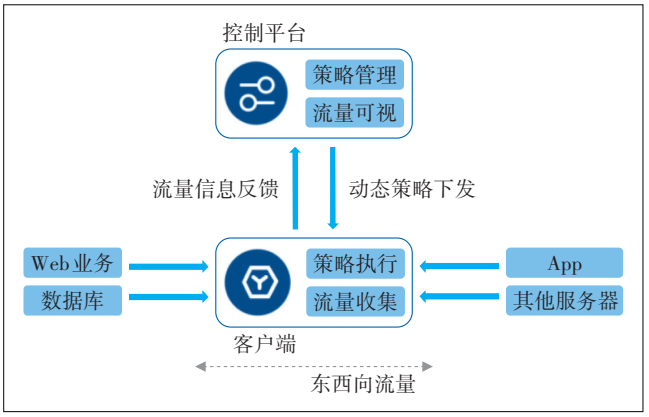

图4　代理模式微隔离架构

4 端到端零信任安全解决方案

企业在传统IT架构的基础上，通常采用防火墙、VPN、安全能力结合的方式实现现有系统的整体防护效果。安全能力包括出向的上网行为管理和安全审计，入向的IPS、IDS、防病毒等能力，可实现针对互联网访问和服务的安全防护[7]。

随着企业IT架构的调整，业务系统云化导致了网络边界模糊化，无法以边界为中心进行安全架构及能力建设，而且传统方案在数据加密、权限管理、暴露面隐藏等方面仍存在较多不足，需要引入零信任理念及能力，搭建适配云原生背景下的企业安全解决方案。端到端零信任安全解决方案如图5所示。

本方案集成了终端VSA、SDP、MSG等零信任安全能力，实现用户终端侧、终端至企业接入网关间、企业内部负载侧的全链路安全防护，保障企业端到端的数据安全、接入安全和负载安全。零信任能力分析如图6所示。

4.1 方案应用效果

4.1.1 收敛暴露面

在零信任安全解决方案中引入SDP能力，将所有企业资源进行统一入口管理，员工通过统一接入门户

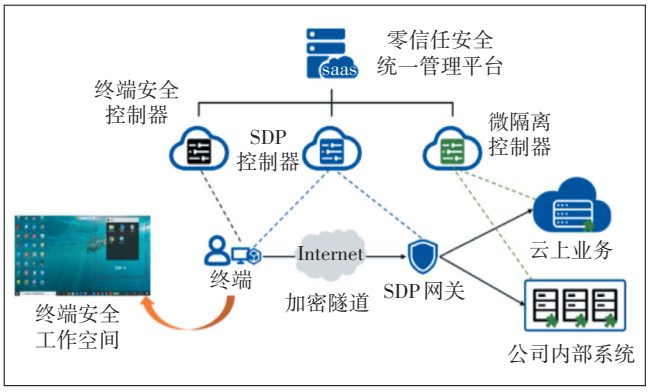

图5　端到端零信任安全解决方案

进行企业资源的访问。SDP的部署架构决定了需要在所有的资源接入节点部署专用的SDP网关设备，该网关设备在实现接入代理访问的同时，实现了资源节点的隐藏。因此，本方案可实现企业互联网暴露面收敛90%以上，仅保留面向公众开放的互联网服务，提高企业信息系统的防护水平。

4.1.2　可信访问控制

企业内网与互联网资源的接入要求随着面向用户群体、资源类型、重要性的不同具有不同的管理控制特点，面向内网应用的访问控制能力是企业进行可信访问控制的重中之重。本方案通过建设基于身份

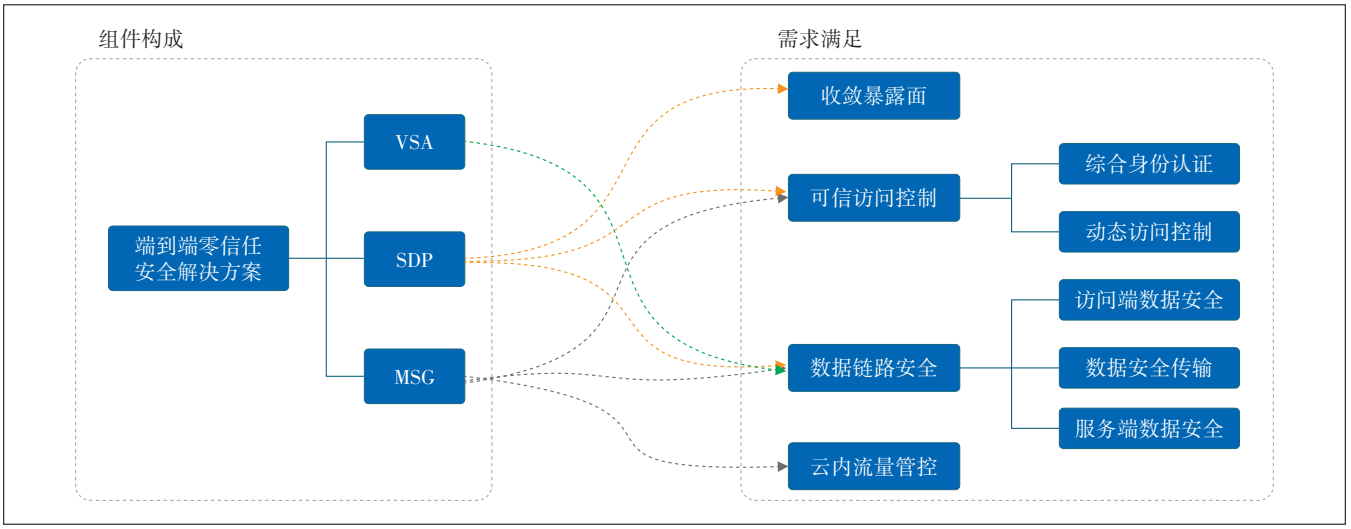

图6　零信任能力分析

的可信接入、基于行为的访问管理和实时动态的信任评估，实现了全流程的可信访问控制。

SDP的加强身份认证通过引入多因素认证（短信认证、邮箱认证、动态码认证、第三方扫码认证等）和基于终端和环境的接入因素评估等能力，保障了企业员工在接入阶段的身份可信、终端可信及环境可信。SDP的细粒度权限管控能力则可以针对用户身份分配不同的资源访问权限，实现内网系统接入的“最小化原则”，充分保障企业信息系统的安全，最大程度避免了系统的社会学攻击风险，细化程度可达到端口级和页面级，保障了访问行为的合规性。此外，SDP的动态信任度评估机制可以对用户访问行为进行实时监控，并基于行为监控分析结果调整其信任分数，通过动态修正用户访问权限和身份二次认证等方式保障用户接入访问过程的安全性。

4.1.3　数据链路安全

企业传统的信息系统通常采用IPSec VPN、SSL VPN进行内网业务系统的接入，在传输阶段可保障数据的安全加密，但在员工终端则没有任何数据安全保障措施，敏感数据在客户端终端处完全暴露，安全意识的缺失或社会学攻击会导致敏感数据或文件的泄露，因此实现覆盖传输链路、终端的数据加密能力是保障企业安全的重要一环。本方案采用SDP和VSA产品。SDP在用户终端与业务系统间搭建了一段加密链路，保障业务系统数据在互联网传输链路的安全性。与此同时，VSA能力则可开辟与个人桌面空间隔离的安全工作空间，所有的重要系统业务访问可在该空间内完成，所有的敏感数据均留存在该空间，可实现终端侧的数据保护、检测加固、行为控制、检测采集等能力。VSA应用效果如图7所示。

4.1.4　云内安全管控

传统的云内及数据中心内部的管控方式是采用

图7　VSA应用效果

有防火墙或云平台的安全组进行组合管理，细化至IP及端口级别，通过定义复杂的网络访问策略进行云内负载的管控。但是该方式无法有效、实时地掌握云内所有负载的访问关系及访问情况，同时管理复杂度高且无法有效解决内部威胁横向扩展的问题。本方案集成MSG能力，通过细粒度的策略控制及可视技术，使东西向流量可视可控，在此基础上实现业务系统内外部主机与主机的隔离，从而更加有效地防御黑客或病毒持续性大面积的渗透和破坏。

4.2 方案优势分析

基于零信任理念的企业端到端安全解决方案通过集成VSA、SDP和MSG等能力，为企业客户提供了覆盖终端数据安全、南北向安全接入、东西向安全管控等场景，提高企业的安全防护水平。IT系统防护方案对比如表1所示。

表1　IT系统防护方案对比

	传统安全方案	零信任安全方案
数据防泄漏	数据传输链路采用SSL VPN、IPSec VPN等搭建加密隧道，保障数据传输安全；终端侧无保障	SDP可建立TLS加密隧道并实现国密算法替换，保障数据传输加密和安全合规要求；VSA在终端侧可实现数据保护、检测加固、行为控制、检测采集，保障终端数据防泄漏能力
收敛暴露面	使用VPN接入，无法收敛系统本身的暴露面，存在安全风险和攻击入口	SDP可实现自身系统和防护资源的网络隐身，可最大限度缩减公网暴露面
多因素认证	依靠应用自身认证功能，认证方式单一；一次认证，始终访问	SDP集成IAM模块并实现多因素认证，此外可对接企业现有的4A系统
访问权限管控	一般基于网段进行授权控制，权限控制颗粒度粗	SDP根据客户需求动态设置资源颗粒度与访问权限，可基于URL、应用进行访问控制
业务流量管控	通过防火墙、安全组等方式进行规则定义和管理，无可视化监控能力	MSG提供了所有负载设备的流量可视化能力，同时可实现基于业务的流量策略定义，防止虚机漂移和威胁横向扩展等问题

5 结束语

自零信任理念落地以来，SDP、VSA等技术产品逐渐成熟化，MSG等技术也完成产品化和应用，零信任安全为企业客户在数字化、云化背景下的IT系统防护提供了新的思路和优化解决方案。

本文通过将企业安全需求进行细化分析，引入零信任核心技术VSA、SDP和MSG，设计搭建了面向企业客户的端到端零信任安全解决方案，满足了企业在收敛暴露面、可信访问控制、数据链路安全、云内流量管控等方面的需求。SDP具备网络隐身能力，可实现企业的暴露面收口，并保障数据传输链路安全，同时，其加强身份管理和业务策略等模块可实现对企业用户接入安全和访问权限的管控等。VSA利用其数据隔离技术可实现企业员工在终端侧的数据安全防护。MSG则实现流量可视化、流量态势实时监控、自适应策略管理等，降低云内部的运维成本，防止攻击流量在云内肆意横向拓展。零信任安全方案为企业客户提供了覆盖员工终端、数据传输链路、资源负载侧的全方位防护和管控能力。对比传统方案，该方案在降低应用成本、防护效果上均有明显的提升，将成为现代企业IT系统防护重要选择。

参考文献：

[1] 刘建伟. 基于防火墙与VPN技术的企业网络安全架构研究[D]. 青岛：中国石油大学，2010.
[2] 周岳亮. 基于零信任安全模型的数据中心安全防护研究[J]. 网络安全技术与应用，2020(10)：88-89.
[3] 张伟宏，黄麟，陈媛. 企业网络安全需求与网络安全方案研究[J]. 电子测试，2020(12)：107-108.
[4] 李欢欢，徐小云，王红蕾. 基于零信任的网络安全模型架构与应用研究[J]. 科技资讯，2021，19(17)：7-9.
[5] 李晨，涂碧波，孟丹，等. 基于多安全机制的Linux应用沙箱的设计与实现[J]. 集成技术，2014，3(4)：31-37.
[6] 蔺旋，王宏鼎，徐宝辰. 基于零信任理念的私有云安全方案研究[J]. 邮电设计技术，2022(9)：55-58.
[7] 张蓓，冯梅，靖小伟，等. 基于安全域的企业网络安全防护体系研究[J]. 计算机安全，2010(4)：36-38.

作者简介：
蔺旋，毕业于西安交通大学，硕士，主要从事网络安全技术的研究工作；李长连，毕业于西北工业大学，高级工程师，主要从事网络安全技术方向的研究工作；徐宝辰，毕业于西安电子科技大学，学士，主要从事网络安全产品的研发工作；贺译册，毕业于北京交通大学，学士，主要从事网络安全产品研究、网络安全产品规划设计工作；余思阳，毕业于北京邮电大学，工程师，硕士，从事网络安全体系规划及产品研究工作。