基于零信任理念的私有云安全方案研究

Research on Private Cloud Security Scheme Based on Zero Trust Concept

蔺　旋[1]，王宏鼎[2]，徐宝辰[1]（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 100048）
Lin Xuan[1]，Wang Hongding[2]，Xu Baochen[1]（1. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China；2. Intelligent Network & Innovation Center of China Unicom，Beijing 100048，China）

摘　要：
首先介绍了私有云技术及面临的安全风险，然后介绍了零信任技术架构及零信任体系中的软件定义边界（Software Defined Perimeter，SDP）和微隔离（Micro Segmentation，MSG），在此基础上设计了基于零信任理念的私有云优化安全解决方案，接着针对优化方案与传统安全方案进行对比总结，最后展望了零信任技术在云环境中的发展和应用前景。

关键词：
私有云；零信任；SDP；MSG
doi：10.12045/j.issn.1007-3043.2022.09.012
文章编号：1007-3043（2022）09-0055-04
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：
It first introduces the private cloud technology and the security risks it faces，and then introduces the zero-trust technology architecture，software defined perimeter（SDP）and micro segmentation（MSG）in the zero-trust system. On this basis，it designs a private cloud optimization security solutions based on the concept of zero trust，then it compares and summarizes the optimized solutions and traditional security solutions，and finally looks forward to the development and application prospects of zero-trust technology in the cloud environment.

Keywords：
Private cloud；Zero trust；SDP；MSG

引用格式：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.

1 概述

私有云是为一个客户单独使用而构建的云计算平台，一般部署在客户自有网络、计算基础设施之中，也可通过“托管式专用”的委托管理模式，由云计算服务供应商提供建设、维护和管理服务[1]。

私有云为企业数据安全和资源利用效率做出了巨大贡献，但是由于云计算技术的复杂性、用户动态性等特点，私有云本身仍存在一些安全风险，包括访问权限风险、边界风险、内部流量不可视、数据隔离风险等（见图1）。

企业用户使用互联网或专用网络访问私有云业务时，无法保障数据的安全性和访问行为的合规性、合法性。私有云内部流量交互不可视，无法发现内部的流量变动和安全威胁，更无法实现对威胁的控制[2]，黑客一旦攻入私有云内部，这种开放性为攻击的横向拓展提供了便利[3]。而传统安全防护方式无法有效解决上述的私有云安全风险，因此需要设计一套更理想的安全解决方案。

2 零信任理念及核心技术

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]。零信任架构中的SDP和MSG分别作为解决南北向和东西向流量控制问题的理想方案。

2.1 软件定义边界SDP

收稿日期：2022-07-11

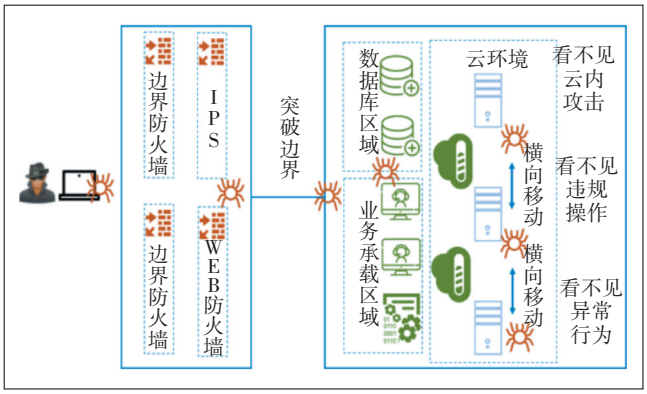

图1　私有云安全风险

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2所示。

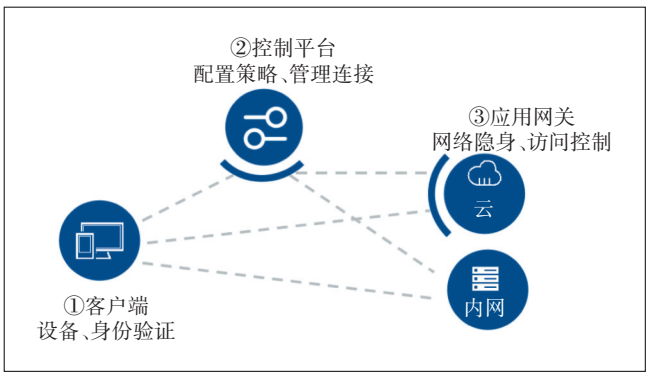

图2　SDP技术架构

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，是解决南北向流量安全防护问题的有效途径[5]。

2.2 微隔离MSG

微隔离技术是细粒度更小的网络隔离技术，能够应对传统环境、虚拟化环境、混合云环境、容器环境下对于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。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的更迭及应用带来的多变用户业务环境，技术架构如图3所示。

微隔离通过细粒度的策略控制及可视技术，让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[6]。

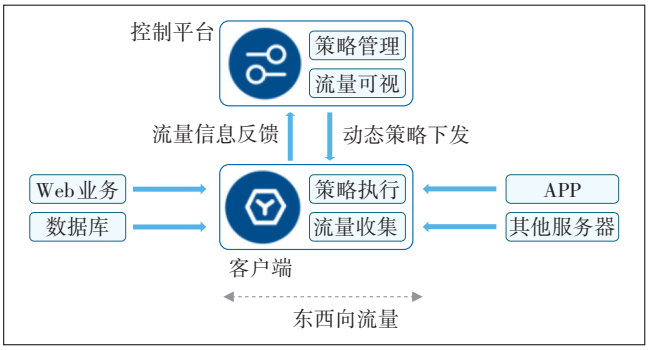

图3　代理模式微隔离架构

3 私有云安全解决方案

3.1 零信任安全方案

针对私有云存在的安全风险，传统的基于边界的安全解决方案在私有云外侧部署防火墙、IPS、IDS、WAF等安全能力，构建私有云的安全防线，抵御来自外部的网络攻击，但传统安全能力可能存在安全策略冗余、防护效率低等问题。私有云内部使用VPC、VLAN等机制隔离内部资源，但私有云内部仍存在可视化缺乏、运维难度大、隔离策略过于精细化等问题。针对采用VPN访问私有云内网资源的方式在准入权限控制方面过于粗放的安全隐患[7]，基于传统的私有云安全解决方案，引入SDP和MSG技术，对原有方案进行升级和优化。

图4展示了引入零信任理念及核心技术的私有云安全解决方案，基于传统的安全解决方案，仍在私有云入口防火墙外部署安全防护能力栈，用于防护来自互联网的攻击；零信任方案在防火墙外部署SDP软件，用于内部人员的访问需求；而在防火墙内的物理机、虚拟机、容器等服务资源部署MSG Agnet，实现云内东西向流量的可视和管控。SDP、安全能力栈和

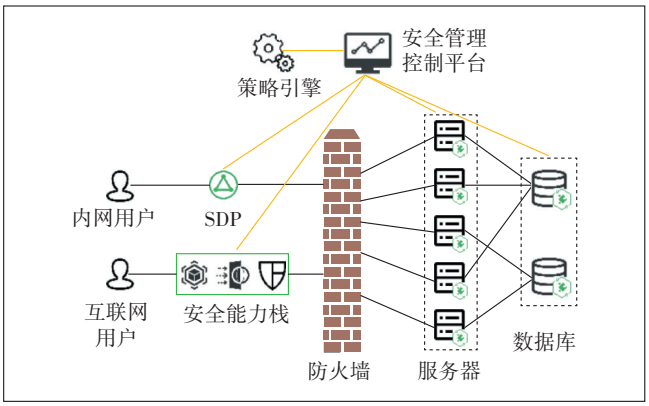

图4　零信任安全防护方案

MSG在统一管控平台的管理之下，实现对私有云南北向和东西向流量的安全防护。

3.1.1 针对南北向的防护

私有云的南北向访问可分为内网用户接入访问、外网访问2个场景，而私有云的第1道防护部署在访问者和云防护墙之间，其中内网用户通过SDP实现资源接入，SDP相较于传统的VPN更加安全，核心技术包括SPA单包认证和动态防火墙等，具体的访问过程如下（见图5）。

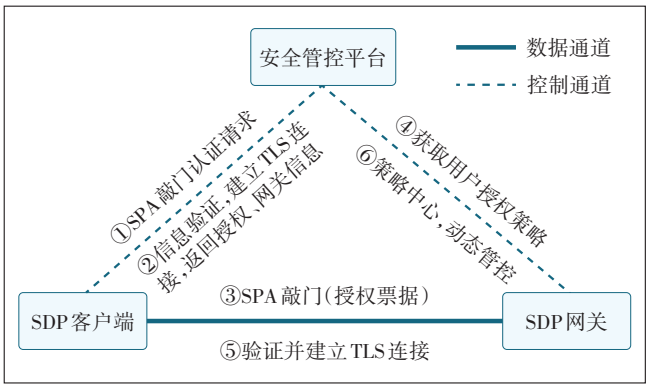

图5　私有云内网资源访问过程

a）内网用户使用SDP客户端先发送包含用户身份和设备信息的SPA认证包。

b）安全管控平台捕获认证包对内部信息进行认证，不通过即不回复，认证通过后则反向与客户端建立TLS加密隧道，并返回用户授权信息和网关信息，此过程结合动态防火墙技术实现了安全管控平台的网络隐身。

c）客户端获得授权票据信息和网关信息之后向网关发送，进行单包敲门认证，网关从管控平台获取用户身份和授权信息后与客户端建立加密传输通道，实现先认证再连接，并对用户访问进行策略控制。

私有云的互联网用户接入访问过程与传统方案类似，用户流量通过互联网链路到达私有云前端的安全防护能力栈，其中DDoS、IPS、WAF等传统安全能力在统一安全管理平台的协调之下，针对来自互联网的网络层、应用层攻击进行流量过滤，此后用户流量经过防火墙可进入私有云内部。

3.1.2 针对于东西向的防护

用户访问流量通过私有云前端的第1道安全防线后进入私有云内部，无论是内网用户还是互联网用户，其流量均可在内部资源间进行横向扩展。虽然SDP可对内网用户身份、资源、行为进行安全保障，但无法杜绝社会学攻击；而安全能力栈可过滤绝大部分的网络攻击威胁，但是对0day等漏洞的攻击则束手无策。而私有云内部的MSG则搭建了第2道防线，其防护过程如下（见图6）。

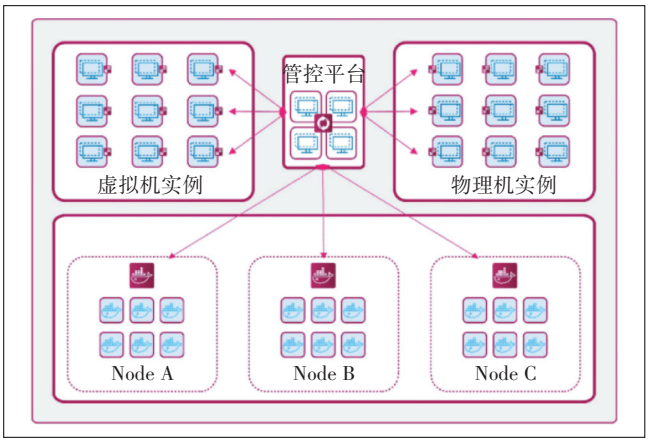

图6　私有云内部防护过程

a）云内虚拟机实例、物理机实例、容器节点部署的MSG Agent收集机器流量数据信息，并上传到管控平台，管控平台的可视化模块将私有云内部的资源、流量信息绘制业务拓扑图，对云内流量进行监控。

b）安全管控平台通过一段时间的资源间流量监控和学习，制定了资源（IP、端口、访问时间、访问频率）的安全基线，并自动生成资源的安全访问策略下发至各个资源实例Agent。

c）各个资源实例根据下发的安全访问策略控制出入方向的流量，防止进入私有云内部的攻击流量横向扩展。

3.2 方案对比分析

基于边界的私有云传统安全解决方案通过使用VPN、防火墙、IPS等安全能力和VPC等网络方案实现私有云初步安全防护，而引入零信任理念的私有云安全解决方案则基于身份概念和软件定义安全等技术进一步保障私有云数据安全，针对传统方案无法解决的风险进行安全措施优化和加固。

3.2.1 访问行为可信

传统的私有云内网资源访问接入采用VPN，在实现用户与资源间打通网络的同时无法实现用户访问的最小化权限控制，对私有云的数据安全带来较大威胁。

零信任方案中的SDP利用基于用户身份的权限控制保障了用户访问资源的合法性，用户只能访问权限列表内的资源，无权限外资源的访问入口，尝试进

行端口扫描和探测会被视为越权访问和攻击行为，保障了用户认证接入后访问行为的可信合规。

3.2.2 网络资源隐身

传统安全解决方案的VPN等工具提供内网资源服务访问入口，私有云存在公网暴露面，无法应对0day漏洞等安全威胁，使得私有云针对内网接入工具也需要进行持续的网络安全加固，并始终处于被动防御状态。

零信任解决方案的SDP基于主动防护理念，通过使用SPA单包认证和动态防火墙技术实现私有云访问入口的隐藏（见图7），私有云业务服务器只对授权的SDP客户端可见，对其他工具完全不可见，缩减了公网暴露面，是企业应对护网等场景的有效防护手段[8]。

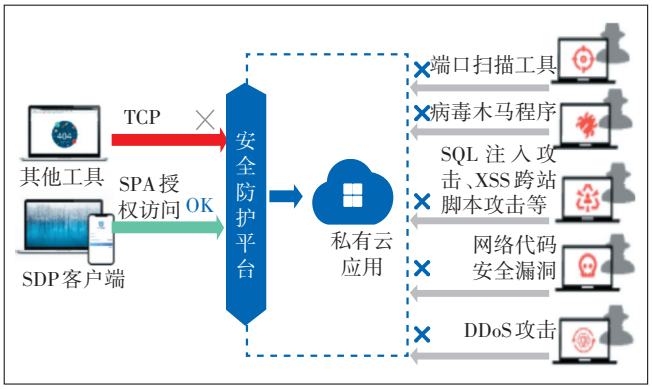

图7　网络资源隐身

3.2.3 流量态势监控

传统安全解决方案通过防火墙、VLAN等措施对私有云内部的机器进行管理，运维人员只能通过服务器、IP、端口等进行安全策略的定制和确认，无法进行云内流量的监控，从流量全局判断云内流量态势。

零信任方案通过部署MSG可以实现流量的深度可视，进行流量态势的展示和运维，针对异常流量进行监控、发现、告警，为运维人员提供了流量全局视角，提高了私有云安全运维的灵活性和安全性[9]。

3.2.4 智能化策略配置

传统安全解决方案需要在各个VPC之间配置复杂的防火墙策略，如果云内机器、容器等资源众多且相互之间存在复杂的隔离和控制逻辑，将导致私有云内的配置运维工作复杂且策略灵活性差。

零信任方案中微隔离MSG的自适应策略特性可自动生成云内各个机器资源的策略安全基线，减少传统方案中防火墙90%以上的安全策略，提高了隔离策略的灵活性。微隔离的自动化策略搭配运维人员定制的安全策略，实现私有云内东西向流量的安全管控[10]。

4 结束语

随着零信任等创新安全技术的诞生和发展，传统的网络安全方案也得到提升和加固。本文通过将SDP、MSG引入私有云安全解决方案，与传统的防护方式相结合，升级了其安全防护方案。在私有云外部对内网用户接入进行“先认证再接入”，并实现了网络暴露面的收缩，而外网用户的访问流量仍采用传统的安全能力过滤再进入私有云内部。在私有云内部则部署MSG和EDR的Agent，对云内流量进行拓扑绘制，实现流量态势的实时监控，还可自动生成内部流量的流转安全基线和策略，降低了私有云内部的运维成本，也防止攻击流量在云内肆意横向拓展。未来可将SDP、安全能力栈、EDR、MSG的安全信息实现标准化、通用化，打通多个安全能力的情报池，实现各个产品之间的策略联动。

参考文献：

[1] 刘淑艳，史迎春，母俐丽. 面向企业私有云计算平台的安全框架研究[J]. 无线互联科技，2019，16(21)：120-121.
[2] 李富宇. 基于分布式微隔离的云计算安全研究[J]. 辽宁大学学报(自然科学版)，2018，45(1)：19-22.
[3] 李飞. 电力企业私有云应用安全研究[J]. 电信科学，2010，26(S3)：4.
[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] 夏树. 零信任安全网络安全体系建设的新趋势[J]. 数据，2021(Z1)：16-17.
[6] 管纪伟，朱凌君，张文勇. 基于零信任的公有云微隔离安全研究[J]. 电信工程技术与标准化，2021，34(12)：46-50，56.
[7] 庞浩，何渊文. 基于零信任的网络安全架构研究与应用[J]. 广东通信技术，2022，42(2)：63-67.
[8] 潘吴斌，任国强. 软件定义边界SDP：概念、技术及应用研究综述[J]. 数字通信世界，2021(3)：192-195.
[9] 游益锋. 面向虚拟化环境的微隔离技术的研究[D]. 成都：电子科技大学，2019.
[10] 钟国新，刘璐豪，王辉鹏，等. 自适应主机微隔离安全策略自动生成方法研究[J]. 自动化技术与应用，2021，40(12)：54-57.

作者简介：
蔺旋，硕士，主要从事网络安全技术研究工作；王宏鼎，高级工程师，博士，主要从事网络SDN、云网产品、网络安全产品研发等方面的工作；徐宝辰，主要从事网络安全产品的研发工作。