城轨云建设下网络安全资源池建设模式的讨论

蒋丽洁
武汉科铁人才发展有限公司　湖北　武汉　430000

摘　要：随着城轨云在城市轨道交通逐渐推广应用，越来越多的城市经历着从传统向云化转型的阵痛。城轨云平台不仅对传统硬件架构带来了颠覆性的革命，还给网络安全建设和运维模式、组织架构带来了翻天覆地的变化。本研究通过分析国内各城市轨道交通云平台发展现状，结合各城市在城轨云的推广应用情况，提出城轨云安全资源池的解决方案，为云平台内业务系统的有序、健康发展奠定基础。

关键词：城轨云、网络安全、安全资源池

1 研究背景及意义

目前国外尚无轨道交通业务系统部署在城轨云平台的典型案例，国内轨道交通城轨云平台正处于发展阶段。各个城市对云计算等新技术的推广进度层次不齐，然而随着各业务数据的入云程度越来越高，网络安全越来越受到国家的重视，在安全数据充分共享的情况下，充分利用云平台获取各系统的网络数据、业务数据，实现对安全威胁进行预测，从被动防御逐步转换为主动防御，并实现云平台与网络安全的紧耦合[1]。

近年云数据中心庞大的系统给各行各业带来商业和技术红利的同时，需要考虑建立动态的安全防护体系保障系统的稳定、安全运行。本次研究基于云平台系统总体环境，构建云上业务系统的网络安全防御架构，采用系统化的安全保护策略，实施基于云计算基础设施的业务应用与数据安全、访问控制与认证授权等多重保护，形成系统的纵深安全防御体系[2]。

2 城轨云安全资源池研究

安全技术支撑体系从分层、纵深防御思想出发，根据层次分为网络安全、虚拟化安全、主机安全、应用安全、数据安全、安全管理中心、云安全资源池几个层面，用来指导城轨云平台安全整体解决方案的设计[3]。

云上业务租户在利用虚拟化技术带来好处的同时，也带来新的安全风险。云租户安全是云数据中心区别于传统数据中心安全业务部署与管理的关键需求，涉及云租户应用系统的安全运行防护、云租户间安全隔离、云租户主机安全防护、云租户漏洞扫描等多个方面。为应对云租户安全，提供安全服务目录，让租户可以从云平台获得一站式安全服务功能，避免安全成为业务上云的障碍，提升租户向云平台迁移的动力[4]。建设统一的安全资源池，为租户提供服务化的安全功能。安全资源池技术对云内系统实现全方位的安全防护，安全管理平台可以对安全组件进行编排与统管，在安全风险监测、排查、处置、闭环过程中应考虑与运营中心的管理体系结合。

2.1 安全资源池部署研究

目前云内业务系统安全资源池常用架构有2种，一种为软硬一体部署方式，一种为软部署方式。软硬一体部署方式采用交换机旁路引流的旁挂安全资源池实现系统安全；软部署方式是通过云平台的虚拟机资源来承载安全能力组件和管理。两种方式对比如下表所示：

表2.1-1 安全资源池部署架构

功能架构	软硬一体部署	软部署
硬件平台	需要独立的硬件设备	可集成部署在云平台
可靠性	支持副本、快照、副本等机制，可靠性强	支持副本、快照、副本等机制，可靠性强
兼容性	可以与云管定制实现对接	可以与云管定制实现对接
稳定性	与云平台独立，稳定性强	云平台故障后，资源丢失
灵活性	可以实现跨云、多云防护，灵活性高	无法跨云、多云使用，灵活度低
可扩展性	硬件资源可横向扩展，软件性能横向叠加，扩展性弱	硬件资源可横向扩展，软件性能可纵向扩展，扩展性强
安全组件能力	支持等保组件	支持等保组件
配置复杂程度	需结合交换机配置引流，复杂	云内引流，容易

中心云平台安全资源池应考虑与SDN网络架构的融合与对接，中心云平台SDN网络架构包括border、span、leaf节点，中心云平台安全资源池部署有3种，旁路在border交换机引流，旁路在span交换机引流或旁路在leaf交换机引流，三种旁路部署方式架构图如下所示：

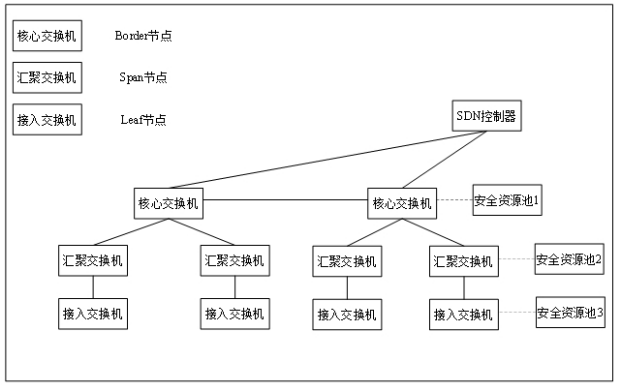

图2.2-1 安全资源池三种引流架构示意图

在border交换机进行安全资源池引流，可以实现安全生产网、内部管理网、外部服务网之间的流量过滤，网间流量通过镜像引流实现，网内流量只能实现安全威胁检测、审计，无法实现系统防护。

在span交换机进行安全资源池引流，可以实现三网间、线路与线路之间的流量过滤，三网间流量通过镜像引流实现，线路与线路内流量通过策略路由实现，系统与系统间流量只能安全威胁检测、审计，无法实现系统防护。

在leaf交换机进行安全资源池引流，可以实现三网间、线路与线路之间、系统与系统之间的流量过滤，网络间的流量通过镜像引流实现，线路与线路之间、系统与系统之间流量通过策略路由实现，单个系统内部流量通过，无法实现系统防护。

三网间、线路与线路之间、系统与系统之间均可以通过安全资源池实现安全流量编排，灵活定义安全防护能力，单个系统内部依托于安全资源池的云工作负载安全组件实现系统内部东西向流量防护。

2.2 安全资源池选型研究

若采用软部署方式部署安全资源池，则软件平台应具备安全组件的生命周期管理、资源统一调配管理、性能监控管理、等保组件编排功能。软件平台为系统自身提供安全防护能力。

参考主流安全资源池设计方案，统计三级等保基础组件需提供安全组件7个：防火墙、主机安全、堡垒机、数据库审计、日志审计、Web应用防火墙、安全态势感知。三级等保基础组件参考《城市轨道交通信息化工程设计规范》研究成果，其资源配置表如下：

表2.2-1 三级等保安全资源池资源配置表

安全组件	资源配置			
业务吞吐量（byte）	100M	200M	500M	1G
资源配置	16VCPU，32G内存，2T硬盘	24VCPU，48G内存，2T硬盘	32VCPU，64G内存，3T硬盘	48VCPU，96G内存，4T硬盘
资产数量（资产）	50	100	200	300
资产管理部分	16VCPU，32G内存，4T硬盘	16VCPU，32G内存，4T硬盘	24VCPU，48G内存，4T硬盘	32VCPU，64G内存，4T硬盘

安全资源池中三级等保组件（7个）需要算力至少为16vCPU × 7 = 112vCPU，需要内存至少为32G × 7 = 224G，需要硬盘空间4T × 7 = 28T。安全资源池管理平台与底层虚拟化技术需要额外消耗约16vCPU，32G内存，满足三级等保组件资源至少需要128vCPU，256G内存，28T存储空间。

参考主流安全资源池设计方案，统计二级等保基础组件需提供安全组件7个：防火墙、主机安全、堡垒机、数据库审计、日志审计。二级等保基础组件参考《城市轨道交通信息化工程设计规范》研究成果，其资源配置表如下：

表2.2-2 三级等保安全资源池资源配置表

安全组件	资源配置			
业务吞吐量（byte）	100M	200M	500M	1G
资源配置	8VCPU，16G内存，500G硬盘	12VCPU，24G内存，500G硬盘	16VCPU，32G内存，1T硬盘	32VCPU，64G内存，1T硬盘
资产数量（资产）	50	100	200	300
资产管理部分	4VCPU，8G内存，2T硬盘	4VCPU8G内存，2T硬盘	8VCPU，16G内存，4T硬盘	8VCPU，16G内存，4T硬盘

安全资源池中二级等保组件（5个）需要算力至少为8vCPU × 5 = 40vCPU，需要内存至少为16G × 5 = 80G，需要硬盘空间2T × 5 = 10T。安全资源池管理平台与底层虚拟化技术需要额外消耗约16vCPU，32G内存，满足二级等保组件资源至少需要56vCPU，112G内存，10T存储空间。

3 结语

根据《智慧城市轨道交通信息技术架构及网络安全规范》、《城市轨道交通云平台网络安全技术规范》和《城市轨道交通信息化工程设计规范》中的要求，尝试研究安全资源池在网络安全中针对业务系统自身防护的实践性，同时也为后续云平台项目系统自保的落地提供了依据，逐步明确安全资源池的技术路线，安全资源池应在安全生产网、内部管理网、外部服务网中分别部署，可自行选择安全组件采用X86服务器、虚拟机或软硬件一体形态部署。安全资源池需保证连通云上业务系统，提供安全服务，每个安全资源池内的安全组件基于云上专业系统的定级分为网络安全等级保护（简称“等保”）二级安全组件和等保三级安全组件。

参考文献

[1]《中国城市轨道交通 智慧城轨发展纲要》

[2]T/CAMET 11001.1-2019《智慧城市轨道交通信息技术架构及网络安全规范 第一部分：总体需求》

[3]T/CAMET 11001.3-2019《智慧城市轨道交通信息技术架构及网络安全规范 第三部分：网络安全》

[4]T/CAMET 11005-2020《城市轨道交通云平台网络安全技术规范》