实验与研究 Experiments and Research

# 基于私有云数据中心网络安全的应用探讨

## Based on the Private Cloud Data Center Network Security Application Discussion

张尧

Yao Zhang

天津航天长征火箭制造有限公司
中国·天津 300462
Tianjin Long March Launch Vehicle
Manufacturing Co.,Ltd.,
Tianjin, 300462, China

【摘　要】随着信息技术的快速进步，中国现迈入大数据时代。目前，单位的数据储备已越发重要，其先进技术也都体现在数据上。但是，数据信息是十分庞大的，无法只由单位自己去存储，因此，基于私有云数据中心网络安全的应用开始被各大单位关注。

【Abstract】With the rapid progress of information technology, China is now entering the era of big data. At present, the data reserve of the unit has become more and more important, and its advanced technology is also reflected in the data. However, the data information is very large, can not only be stored by the organization, so, based on the private cloud data center network security applications began to be concerned by the major organizations.

【关键词】私有云；数据中心；网络安全；应用

【Keywords】private cloud; data center; network security; application

【DOI】10.36012/etr.v1i4.717

## 1 引言

私有云数据中心网络有效避免了单位无法存储庞大数据的难题，特别是在航天长征火箭制造类的单位中，数据更是烦琐复杂且庞大。但是，以前的私有云数据中心结构复杂、传输效率低、不够安全等情况经常出现，为有效解决上述问题，论文分析了私有云数据中心网络的弹性结构，让网络不再复杂的同时，也能加快数据传输，更好地完善信息安全技术体系。论文由此介绍私有云数据中心网络的结构，并研究如何增强其安全性能。

## 2 云数据中心网络设计

### 2.1 网络弹性架构

因为私有云数据中心网络的出现，现在不少电商单位在搭建云数据中心网络时都是通过网络弹性架构。而之前的私有云数据中心网络设计是通过以 SDH 为基础的多业务传送平台组织架构，传输数据时，接入交换机和汇聚交换机时需要 SDH 的多业务传送平台协议，处理很烦琐，传输效率也很低。论文先以某单位的 IRF 技术详细说明，分析弹性架构相对于传统架构的优势所在[1]。传统架构的接入层为 MSTP+VRRP，服务器利用双网卡接入双交换机，通过双归属三角形拓扑接入到汇聚交换机，此时需要 MSTP 协议，维护相对烦琐。而云数据中心的接入与汇聚交换机均通过 IRF 架构后，每两台接入与汇聚交换机分别配置 IRF 堆叠组，使得相互之间有多条链路捆绑连接。此时，堆叠组作为设备，接入与汇聚交换机间没有二层环路，能够防止被 MSTP 配置管理，使得网络设计更加简便。

### 2.2 网络“扁平化”

网络“扁平化”设计，指的是核心层直接下连接入层，不需要在中间汇聚。“扁平化”组网的扩展性与密度都更符合条件，因此，备受云数据中心服务器的青睐。“扁平化”二层架构能够让 VLAN 的大二层互通，实现部署与迁移虚拟机，和之前的三层架构相比，其能够更好地运维管理网络[2]。以前，私有云数据中心网络有着三层架构，分别为核心层、汇聚层、接入层。而通过弹性架构，私有云网络中心实现了“扁平化”设计网络架构，能够快速连接私有云数据中心网络服务器，完成虚拟局域网的二层网络支撑。

### 2.3 大二层网络

在云数据中心内虚拟化服务器并迁移是趋势，也是必然，现在的虚拟化软件如果想实现热迁移就需要二层网络，因此，二层网络的规模也在扩张，有的还可以跨数据中心部署。利用虚拟化技术，两台或多台同一层物理交换机虚拟为逻辑设备，跨设备捆绑后，让核心与接入点互联，避免环路。如此一来，不仅有效防止网络中部署 STP，也防止大二层网络中的“生成树”协议。

### 2.4 虚拟机交换网络

服务器的虚拟化技术让计算服务可以不基于主机，而是以虚拟机为单位。为让同一物理服务器内虚拟机之间能够交换数据，单位引进了虚拟交换机，其能够对接虚拟服务器，让

虚拟服务器和外部网络互联，并完成虚拟机和外部网络之间的通讯。

## 3 信息安全技术体系的应用研究

通过上文可知，私有云数据中心网络不仅可以带来便利，也很容易带来麻烦。单位把数据都存储在私有云网络服务器中，一旦服务器被黑客恶意攻击并非法窃取，将给单位带来无法预估的损失。所以，数据存储到私有云网络服务器上也是有一定风险的，需要不断完善信息安全技术体系，下文将具体阐述主要的技术手段。

### 3.1 身份认证技术

作为信息安全体系对私有云数据中心网络的第 1 项保护措施，身份认证技术需要核查访问数据库人员的身份，只允许单位内部人员进入私有云数据中心网络，一旦访问人员有着非法的身份信息，系统会及时报警并记录 IP 地址。如果发现是黑客入侵，就能最快时间联系网警。为避免外部人员窃取单位内部人员账号并冒充访问，身份认证技术还有很多高科技身份识别手段，比如，面部识别、指纹识别、虹膜识别等。

### 3.2 访问控制技术

身份认证技术主要针对单位外部人员，而访问控制技术则是针对单位内部成员的第 2 道防护措施。为避免单位内部人员因为收受贿赂而监守自盗，访问控制技术根据不同级别的员工有着不同的访问权限，不可以越级访问。在工作过程中，访问控制技术不仅不会妨碍员工的正常工作使用，还能给单位的私有云数据中心网络带来安全保障。

### 3.3 内容安全技术

内容安全技术作为信息安全体系中的第 3 道防线，主要用来应对私有云数据中心网络被非法入侵之后的数据保护。系统一旦被侵入，其可能造成的连锁破坏是无法预估的，所以，内容安全系统综合了各种不同的安全防御手段，便于全面针对非法入侵之后带来的各种严重破坏。单位可通过页面锁定技术避免非法入侵者随意篡改访问页面，妨碍单位内部人员的正常工作使用。此外，单位还可以通过流量清洗、入侵防御等技术手段避免非法入侵者恶意攻击服务器，不仅有利于安全传输网络数据，还可以通过文件加密技术手段确保终端数据安全可靠。

### 3.4 监控审计技术

上面提到的 3 项技术都是针对非法入侵的防御性技术，而监控审计技术还能够帮助信息安全体系的自我检测与自我完善。监控审计技术能够实时监控并分析私有云数据中心网络的访问情况、信息数据及安全状态。利用分析访问记录数据，能够获取私有云数据中心网络的起始点、访问路径、访问手段等数据，有利于分析其中暗藏的安全隐患。利用该技术不仅能够实时监督私有云数据中心的网络安全，还能找出安全风险，不断完善升级系统信息的安全技术体系。

### 3.5 备份恢复技术

备份恢复技术的使用也很关键，包括备份与恢复两个环节。单位应该经常备份私有云数据中心的数据，同时，详细记录备份时间。如果数据被恶意攻击或由于人员操作失误等情况出现损坏，单位就可以即刻恢复到上一次备份时的数据状况。

### 3.6 安全区域模块化

数据中心网络要想安全设计主体到客体的安全访问，首先应该把安全区域模块化，明确定义网络安全边界；其次，利用访问控制，进行深层安全防护、网络监控及审计分析，确保数据中心的网络安全。数据中心防范网络安全需要把网络根据不同的应用或安全信任级别，划分为不同的安全区域。如果这些安全区域之间需要互相访问，应该通过不同的安全控制手段，遵循有限互通原则，不能未经安全访问控制，就让不同区域直接联通。同时，数据中心分区设计了由核心到边缘的模式，各区域利用汇聚层设备连接核心层并作为该区域的网络安全边界，在汇聚层通过安全访问控制技术进行控制。

### 3.7 虚拟机流量监控

引进虚拟交换机给运作云数据中心带来的问题如下：首先，网络界面不清。在服务器内部虚拟机之间实行数据交换，外部网络是看不见的，不管是流量监管、策略控制还是安全等级都不能一味依靠外部硬件，否则，数据交换界面进入主机后，由于虚拟交换机的功能、性能与管理弱化，毫无高级网络的特性和服务。其次，虚拟机的不可感知性。物理服务器连接网络需要利用链路状态，但服务器被虚拟化后，主机需要同时运行大量虚拟机，之前的网络不能感知运行状态，也不能实时定位虚拟机。

## 4 结语

私有云数据中心网络的弹性架构与“扁平化”设计，极大地加快了系统传输。同时，信息安全技术体系可以全方位确保私有云数据中心的安全可靠。全新的私有云数据中心网络将更好地应用在单位中，方便单位存储海量数据，推动航天长征火箭制造单位的长远发展。

**参考文献**

[1]王金波.虚拟化与云计算[M].北京:电子工业出版社,2019.

[2]黄大川.云计算数据中心网络的关键技术[J].邮电设计技术,2017(10):14-18.