云数据中心信息安全建设方案分析

刘　宇
（合肥城市云数据中心股份有限公司　合肥　230000）

摘　要　云数据中心是现代网络技术发展的重要成果，其达成了网络虚拟化的最终目标。传统视角下的安全防护策略整体较为固定，主要包括固定IP、静态网络等，面对云数据中心的崛起，各项安全防护策略难以满足实践发展需求。文中以此为切入点，从安全服务需求的角度详尽分析了其架构思路，探讨了云数据中心网络安全服务建设的具体方案。

关键词： 云数据中心；信息安全；防护挑战；解决方案
中图分类号　TN915.08

Analysis of the Information Security Construction Scheme of the Cloud Data Center

LIU Yu
（Hefei City Cloud Data Center Co.,Ltd.,Hefei 230000,China）

Abstract　Cloud data center is an important achievement of the development of modern network technology, which has achieved the ultimate goal of network virtualization. The security protection strategy from the traditional perspective is relatively fixed as a whole, mainly including fixed IP, static network, etc. Faced with the rise of cloud data center, various security protection strategies are difficult to meet the practical development needs. Taking this as the starting point, this paper analyzes its architecture ideas in detail from the perspective of security service requirements, and discusses the specific scheme of cloud data center networking security service construction.

Key words　Cloud data center,Information security,Protection challenges,Solution

0　引言

网络技术与生产生活的融合，让社会变得更加便捷，各项通信技术让信息的交互变得更加简单、方便，同时构建了越发丰富的管理平台功能，为信息的管理提供了良好支持。云数据中心建立在各项技术管理手段的基础之上，围绕着客户需求完成自动化技术，为数据传递的高效性和服务的敏捷性提供了良好的保障。但受到客观社会实践的影响，传统物理网络中储存的数据的转移，往往会面临更大的安全性挑战，这进一步加剧了用户的不安。随着时代的发展与进步，传统物理网络储存数据使用的设备已经不符合现阶段的发展需求，原因在于该方案难以保障数据的安全性。为改变这一现状，必须加大技术研究力度，明确数据中心虚拟化的整体思路，并联合其他技术，更好地服务于数据中心，为其提供完善的服务。

1　云数据中心概述

云计算的本质是一种计算方式，其建立在互联网技术的基础之上，通过云计算网络，能实现信息和资源的共建共享，充分满足用户的多样化需求。随着现代技术的不断发展，数据中心的建设更加完善，云计算的出现让其功能更加强大。传统仅提供储存设备租用的服务方式并不能满足现阶段的发展需求，因此其必须朝着按需分配的资源虚拟云数据中心进一步转型。云数据中心的各项操作通过虚拟技术实现，用户能在其中完成数据资源的交互，且交互行为更加灵活多变[1]。

2　云数据中心的安全防护目标

2.1　数据的机密性

安全防护的目的是保障数据的安全性，解除用户的安全忧虑。因此，安全防护工作的开展，必须保证数据的机密，不能出现数据泄露问题，否则只会造成更大的隐患。从云数据中心的角度来看，其数据具备机密性，为做好安全防护工作，需从以下几个角度进行思考。(1)加大人才队伍建设，打造专业水平高、综合素质强的安全防护管理队伍。除传统的培训工作之外，还可根据云数据中心防护需求引进相应的人才[2]。(2)应用数据加密技术。数据加密在安全防护实践中的应用十分广泛，包括云数据中心用户授权管理技术等，该技术能避免数据被窃取，最大程度地保障数据安全。值得注意的是，数据加密技术在实践中的应用同样会面临很多挑战，如服务器

作者简介：刘宇（1983—），本科，高级工程师，研究方向为计算机科学与技术。

内部攻击，因此在加密数据时，需要与数据储存服务之间保留一定的分离性，避免出现数据被窃取的情况。可以采用DES系统、ECC系统、RSA系统等来强化数据加密效果，使云数据中心客户端单独完成加密工作，第三方机构则可负责管理用户的不对称密钥。现阶段，云数据中心用户授权具有粗粒度特征。但安全问题是客观存在的，若想保证数据的加密效果，则必须优化访问管理技术和身份认证技术。

2.2 数据的完整性

安全防护工作的目的是保障数据的安全性，避免数据被蓄意破坏、修改等。为达到良好的保护效果，必须保证数据的完整性，以提高云数据中心的安全防护效果。很多因素都会影响数据的完整性，如果不能保障数据的完整性，则会产生很大的安全隐患，因此必须严格控制各种不确定因素，如设备故障。在开展防护工作时，可以从防止数据丢失、恢复数据两个角度入手。在数据的处理、传输等过程中，为保证其完整性，管理人员必须科学应用分级处理、分级储存等技术。但在实践过程中，IaaS的储存方式会面临更高的数据迁移成本，且动态化的数据特征，也让传统数据的完整性检验机制面临更多挑战。为保证数据的完整性，工作者必须充分的了解云计算环境，掌握其技术特征，并选择相应的技术措施，以保证云数据中心的数据完整性[3]。

3 云数据中心网络信息安全建设方案分析

3.1 云数据中心的总体架构

作为对外运行的基础硬件设备，物理基础架构负责数据中心的支撑工作，其中包含网络资源、计算资源等。资源采用统一管理方法，资源管理平台获取信息之后，可以根据实际情况对其进行合理分配，弹性拓展上层业务。随着现代技术的不断进步，云数据中心表现出了更明显的优势。(1)该技术可以提供差异化的云计算服务。例如，随着网民规模的不断扩大，用户的需求呈现出个性化特点，为了灵活配置各项资源，最大程度地满足用户需求，云主机则担当了这一工作。增值服务就是在云主机功能的基础之上进行拓展，以满足软硬件运行需求的一种有效方式。(2)云数据中心在运算时，会将资源池化的管理模式引入其中，极大地提高硬件资源的利用效率。资源池化在实践中的应用能充分整合各项资源，然后根据用户需求进行合理分配，这种方式不仅能满足用户需求，也能避免不必要的资源浪费。由此可知，云数据中心的弹性拓展能力得到了明显提高，同时也使系统设备形成了良好的可伸缩性。

3.2 网络总体架构设计

网络总体架构设计师首先需要明确数据中心具备网络分层和功能分析的能力。随着现代技术的不断进步，用户需求的多样化特点对网络总体组织架构设计提出了更高的要求，必须不断细化其层次性和功能性，以合理划分各项功能。为强化数据中心的管理效果，可以从管理、储存、业务等3个网络平面形成网络架构。在完成网络分层设计时，需要科学应用虚拟化技术，以提高整体的使用性能。从实践应用的角度来看，核心层网络架构管理具有扁平化的特点，可以通过各项信息技术加大资源的共享力度，同时满足整体的信息交换需求。接入层采用堆叠技术，能极大提高设备的交换能力，实现信息的沟通和共享。网络平面设计可以将其划分为不同的部分，高效完成用户端的数据流量承载，满足设备设施的运行需求[4]。

3.3 网络核心层的设计

在大多数情况下，为满足网络核心层的设计需求，通常需要使用两台核心交换机。在具体运行时，首先需要完成两台设备的虚拟化合成，将其合为一台交换机，增大设备容量，以高效处理核心流量。通过网络核心层的设计，能营造出更加可靠的网络环境，满足稳定性需求。接入层的交换机设计同样采用堆叠技术，使其运行能力和性能实现最大化。在连接核心交换机和接入交换机时，可以根据需求采用链路连接的方法。该方法不仅能保证数据传输的稳定性和高效率，也为网络的安全性和稳定性提供了良好的保障。由于网络的复杂程度较高，在实际运营时，可以采用扁平化的构架方法，提高网络的整体性能和管理效率。

3.4 网络功能区的设计

网络功能区的设计关系着互联网的门户，其是对外开放的窗口。设备设施的运行不仅存在内部通信，同时也存在外部互联网通信需求，因此需保证整体的安全性。此外，作为关键区域的网络服务区，同样也对整体设计有着非常深远的影响，需要部署防火墙等，满足系统的运行需求。

4 数据中心网络安全服务

4.1 现有网络安全服务的实现

网络技术的全面进步让数据安全服务变得更加重要[5]。虚拟化网络安全设备能充分考量多样化的服务需求，且能最大程度地满足数据中心的各项要求，因此虚拟化网络安全设备不可或缺。但虚拟化网络安全设备同样存在极大不足，如果不能有效化解业务跟随方面的问题，则会影响设备设施的整体运行情况。该设备在虚拟网络边界的服务范围较小，服务种类的支撑情况不多。用户需求处在不断的变化之中，如果不能有效克服这一问题，则难以配置各项资源。尤其是在迁移位置时，早期安全设备与新设备无法直接连接，若不能解决这一问题，便会导致业务中断。虚拟安全设备的特性决定了其能为安全转移和拓展提供良好的保障，但在面对不同的环境时，数据中心的可伸缩性和可扩展性也会受到不同程度的影响。

4.2 分布式网络安全虚拟化架构

(1)控制平面和数据平面分离，其在安全服务设计中扮演着重要角色。两者的职能分别是制定控制安全策略、负责数据的处理和转发。两者之间的相互分离，极大地提高了安全策略的灵活性。

(2)采用虚拟化架构。数据中心的基本架构被分为不

同的部分，需完成安全服务的控制平面、服务平面和引流平面的部署。通过控制平面和数据中心管理平台，可以在信息交互的基础上实现信息共享，同时配置相应的服务平台功能。在各个物理机上，安全服务的功能均有分布，不同模块之间可以高效协同，进一步满足通信业务的需求。

(3)安全服务设计。数据中心环境会随着时间的推移处在动态变化中，且整体的复杂性较高。若想满足用户的需求，则首先需要了解用户需求，并提高自适应能力，根据实践状况对其进行优化，创建更加安全的环境，使其稳定运行。

5 系统架构可提供的服务

5.1 流量可视化

安全服务的虚拟机能科学展现用户的虚拟机流量等数据，同时也是管理虚拟机流量的一种有效方法。对于管理人员而言，可以采用分布式的安全虚拟架构，实现细粒度控制。网络安全模块能监测任意端口的用户流量，以了解不同业务数据的变化情况，完成高质量的流量控制。一方面，该架构具有全局统一性。这意味着控制平板具备良好的监测功能，能完成不同虚拟机模块局部流量的监测工作，使细节控制和全局控制都能掌握在工作人员的手中。该方法不仅能构建安全的维护环境，也保证了数据中心的稳定运行，具有较大的实践推广价值。

5.2 微隔离功能

微隔离功能的本质是进行安全监测，相较于其他技术，该功能强调的是监测特定用户。网络安全一直是人们担心的内容，一旦出现攻击行为，就可能造成信息泄密，为避免伤害的扩大，安全管理人员可通过该技术进行特定监测，以遏制深入攻击。该方法能对虚拟网络进行隔离和安全控制，也具有降本增效的效果，在实际生活中的应用非常广泛。为更好地了解分布式网络安全架构，首先需要对现有资料进行分析。该架构能监测任何用户虚拟机，通过未隔离控制方法控制任意端口，以了解端口的安全情况，达到安全控制的效果。微隔离控制的粒度能扩散至用户虚拟机，安全策略的实施则能为虚拟网络的安全性提供良好的保障。

5.3 业务迁移

迁移是数据安全控制中的重点部分。由于虚拟网络中含有大量的数据，传统迁移技术的实施难度很大，但安全控制平面的出现，则能顺利完成安全定位，实施针对性的建议操作。业务迁移的目的是保障网络的安全性，这不仅能提高整体的保护效果，同时也可进行安全状态迁移，保持业务运行的稳定性。

5.4 全网行为分析

数据中含有大量的信息，为了解不同模块的流量数据，可以采用全网行为分析的方法，充分了解具体行为的实施和分布。在进行全网行为分析前，首先需要汇集数据，通过特定虚拟机的分析来明确目标实施的准确性。在实施分析时，可以分析单个虚拟机，也可以分析整个集群，甚至可以将其细化到某一端口。通过分析，能从全局性的视角了解数据的变化，科学分析虚拟网络业务的发展现状。该方法不仅能实现数据整合，还可识别潜在风险，尽早发现异常流量、攻击行为等问题，并结合实际情况进行防御保护。通过权行为分析，其能及时察觉异常行为，在第一时间实现响应与处理，实现网络系统的整体安全。

6 结语

现代网络技术的高度发展，让用户的需求得到了极大的满足，但如何保障网络信息安全，也是社会各界普遍关注的话题。任何信息的传递都需要保证其安全性，云数据中心的网络安全性能给人带来更多的便利，这不仅能加大安全保护效果，还可以完成信息的动态建议，促进云数据技术的全面进步。

参考文献

[1] 许鹏，张桂玉，马季春，等.云化时代运营商数据中心业务及网络演进研究[J].邮电设计技术，2021(6)：52-58.

[2] 方祥毅，张永嘉.大数据背景下软件定义安全的服务架构研究与分析[J].数码世界，2018(11)：108-109.

[3] 陈鹏州.对云数据中心网络安全服务架构的研究[J].网络安全技术与应用，2018(8)：64，74.

[4] 冼学辉，熊伟.基于超融合技术的高校数据中心设计与实现[J].中国教育信息化，2020(15)：80-82.

[5] 耿延军，王俊，周红亮.云数据中心网络纵深防御研究[J].信息安全与通信保密，2019(7)：22-29.