第 5 章 云安全技术及应用

本章结构

5.1 云计算的安全问题
5.2 云计算的安全属性
5.3 云计算的安全架构
5.4 云计算安全的标准化
5.5 云计算和服务保险
5.6 云计算安全实施步骤
5.7 阿里云安全策略与方法

5.1 云计算的安全问题

云计算使公司可以把计算处理工作的一部分外包出去，公司可以通过互联网来访问计算基础设施。但同时，数据却是一个公司最重要的财富，云计算中的数据对于数据所有者以外的其他用户是保密的，但是对于提供云计算的商业机构而言确实毫无秘密。随着基于云计算的服务日益发展，云计算服务存在由多家服务商共同承担的现象。这样一来，公司的机密文件将经过层层传递，安全风险巨大。作为一项可以大幅降低成本的新兴技术，云计算正在受到众多企业的追捧。然而，云计算所带来的安全问题也应该引起足够重视。

总的说来，由云计算带来的信息安全问题有以下几个方面：

(1) 特权用户的接入。在公司外的场所处理敏感信息可能会带来风险，因为这将绕过企业 IT 部门对这些信息“物理、逻辑和人工的控制”。

(2) 可审查性。用户对自己数据的完整性和安全性负有最终的责任。传统服务提供商需要通过外部审计和安全认证，但一些云计算提供商却拒绝接受这样的审查。

(3) 数据位置。在使用云计算服务时，用户并不清楚自己的数据存储在哪里，用户甚至都不知道数据位于哪个国家。用户应当询问服务提供商数据是否存储在专门管辖的位置，以及他们是否遵循当地的隐私协议。

(4) 数据隔离。用户应当了解云计算提供商是否将一些数据与另一些隔离开，以及加密服务是否是由专家设计并测试的。如果加密系统出现问题，那么所有数据都将不能

再使用。

(5) 数据恢复。就算用户不知道数据存储的位置,云计算提供商也应当告诉用户在发生灾难时,用户数据和服务将会面临什么样的情况。任何没有经过备份的数据和应用程序都将出现问题。用户需要询问服务提供商是否有能力恢复数据,以及需要多长时间。

5.2 云计算的安全属性

5.2.1 可靠性

可靠性是指系统能够安全可靠运行的一种特性,即系统在接收、处理、存储和使用信息的过程中,当受到自然和人为危害时所受到的影响。系统的高可靠性是云计算系统设计时的基本要求。Google 公司的电子邮件服务中断、微软公司的云计算平台 Windows Azure 运作中断、亚马逊公司"简单存储服务"(Simple Storage Service,S3)中断等问题都可归结为是由于云计算系统可靠性设计的不足而发生的。下文从环境、设备、介质三个方面来研究如何提高云计算系统的可靠性。

(1) 环境可靠性措施。在设计云系统时,机房要避开各种高危(地震、磁场、闪电、火灾等)区域,当系统遭到危害时,其应具备相应的预报、告警、自动排除危害机制,系统不仅要有完善的容错措施和单点故障修复措施,还要有大景的支撑设备(UPS、备用服务器等),为防止电磁泄漏,系统内部设备应采用屏蔽、抗干扰等技术。

(2) 设备可靠性措施。为提高云系统设备的可靠性,我们应运用电源、静电保护技术,防病毒、防电磁、防短路、断路技术等,设备的操作人员应受到相应的教育、培养、训练和管理,并要有合理的人机互通机制,这样可很大程度上避免设备非正常工作并提高设备的效率和寿命。

(3) 介质可靠性措施。在考虑云系统的传输介质时,应尽量使用光纤,也可采用美国电话系统开发的加压电缆,它密封于塑料中,置于地下并在线的两端加压,具有带报警的监视器来测试压力,可防止断路、短路和并联窃听等。

5.2.2 可用性

可用性指授权个体可访问并使用其有权使用的信息的特性。安全的云计算系统应允许授权用户使用云计算服务,并在系统部分受损或需要降级使用时,仍能为授权用户提供有效服务。

为保证系统对可用性的需求,云计算系统应引入以下机制:

(1) 标识与认证是进行身份识别的重要技术,标识指用户表明身份以确保用户在系统中的可识别性和唯一性。认证指系统对用户身份真实性进行鉴别。传统的认证技术有安全口令、令牌口令、数字签名、单点登录认证、资源认证等,可使用 Kerberos、DCE 和 Secure Shell 等目前比较成熟的分布式安全技术。

(2) 访问控制分为自主访问控制(DAC)和强制访问控制(MAC),其特点是系统能够将权限授予系统人员和用户,限制或拒绝非授权的访问。在云系统中,可参考 Bell.

1aPadula 模型和 Biba 模型来设计适用于云系统的访问机制。

(3) 数据流控制为防止数据流量过度集中而引起网络阻塞，云计算系统要能够分析服务器的负荷程度，并根据负荷程度对用户的请求进行正确的引导，控制机制应从结构控制、位移寄存器控制、变量控制等方面来解决数据流问题，并能自动选择那些稳定可靠的网络，在服务器之间实现负载均衡。

(4) 审计是支持系统安全运行的重要工具，它可准确反映系统运行中与安全相关的事件。审计渗透于系统的每一过程，包括 OS、DBMS 和网络设备等。在云计算系统中，安全审计要能够在检测到侵害事件时自动响应，记录事件的情况并确定审计的级别。日志审计内容应包括时间、事件类型、事件主体和事件结果等重要通信数据和行为。为了便于对大量同志进行有效审计，日志审计系统要具有自己专用的日志格式，审计管理员要定时对日志进行分析。为了有效表示不同日志信息的重要程度，日志审计系统应按照一定的规则进行排序，如按照时间、事件的敏感程度等。

5.2.3　保密性

保密性要求信息不被泄露给非授权的用户、实体或供其利用。为保证云计算系统中数据的安全，首先要加强对相关人员的管理；其次，利用密码技术对数据进行处理是保证云系统中数据安全最简单、有效的方法，常见的密码技术有分组密码系统 DES、公钥密码系统 RSA、椭圆曲线密码系统 ECC 和背包公钥密码系统等；此外，云系统设施要能够防侦收(使外界侦收不到有用的信息)、防辐射(防止有用信息以各种途径辐射出去)，并要利用限制、隔离、掩蔽、控制等物理措施保护数据不被泄露。我们可以使用防火墙技术、NAT 技术、SSL、PPTP 或 VPN 等不同的方式来对云系统中传输的信息进行保护。建立“私有云”是人们针对保密性问题所提出的一个解决方法。私有云是居于用户防火墙内的一种更加安全稳定的云计算环境，为内部用户或者外部客户提供云计算服务，用户拥有云计算环境的自主权；“公共云”则是通过云计算提供商自己的基础架构直接向公众用户提供服务的云环境，用户通过互联网访问服务。其中的透明加密技术可以帮助用户强制执行安全策略，保证存储在云里的数据只能是以密文的形式存在，用户自主控制数据安全性，不再被动依赖服务提供商的安全保障措施。采用私有云/公共云机制可让用户自主选择对敏感数据的处理，这也极大地减少了数据泄露的风险。

5.2.4　完整性

完整性指信息在存储或传输过程中不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等以造成破坏和丢失的特性。保护数据完整性的两种技术是预防与恢复。为保证存储、传输、处理数据的完整性，经常采用分级存储、密码校验、纠错编码(奇偶校验)、协议、镜像、公证等方法。在设计云系统时，由于其复杂性，目前可采用的主要技术有两阶段提交技术和复制服务器技术。

5.2.5　不可抵赖性

不可抵赖性也称为不可否认性，指在信息交互过程中，明确厂商及用户的真实同一

性，任何人都能否认或抵赖曾经完成的操作和承诺。由于云计算制度的不完善，云提供厂商和用户之间可能会在非技术层面产生各种纠纷，对此，云计算系统可以增加可信任的第三方机构来办理和协调提供商和用户之间的业务，并可利用信息源证据/递交接收证据来防止发送方/接收方事后否认已发送/接收的信息。

5.2.6 可控性

可控性指系统对其数据应具有控制能力。在云计算系统中，我们可以建立从节点到主干的树状控制体系，使系统可以对数据传播的内容、速率、范围、方式等进行有效控制，这样可以增加系统的扩展、有效性和自动容错能力，有效控制数据的传播，并降低数据系统出现故障时的修复难度。

5.3 云计算的安全架构

通过对目前 IaaS、PaaS、SaaS 三种云计算服务模式中的安全问题的分析，云计算的安全框架如图 5.1 所示。

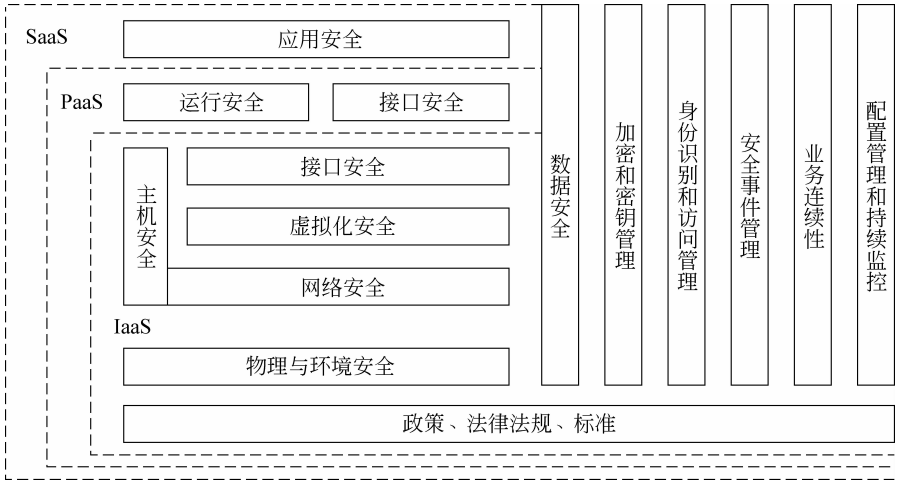

图 5.1 云计算的安全框架

由图 5.1 可知，云计算的安全框架针对云计算各个层次均设置了相应的安全技术来保障其安全特性。

5.3.1 用户认证与授权

身份认证是整个信息安全体系最基础的环节，身份安全是信息安全的基础。

相信大家都还记得一个经典的漫画，一条狗在计算机面前一边打字，一边对另一条狗说："在互联网上，没有人知道你是一个人还是一条狗！"这个漫画说明了在互联网上很难识别身份。身份认证是指计算机及网络系统确认操作者身份的过程。计算机系统和计算机网络是一个虚拟的数字世界。在这个数字世界中，一切信息包括用户的身份信息都是

用一组特定的数据来表示的，计算机只能识别用户的数字身份，所有对用户的授权也是针对用户数字身份的授权。而我们生活的现实世界是一个真实的物理世界，每个人都拥有独一无二的物理身份。如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者，也就是说保证操作者的物理身份与数字身份相对应，就成为一个很重要的问题。身份认证技术的诞生就是为了解决这个问题。

在真实世界中，验证一个人的身份主要通过三种方式判定，一是根据你所知道的信息来证明你的身份(what you know)，假设某些信息只有某个人知道，如暗号等，通过询问这个信息就可以确认这个人的身份；二是根据你所拥有的东西来证明你的身份(what you have)，假设某一个东西只有某个人有，如印章等，通过出示这个东西也可以确认这个人的身份；三是直接根据你独一无二的身体特征来证明你的身份(who you are)，如指纹、面貌等。

信息系统中，对用户的身份认证手段也大体可以分为这三种，仅通过一个条件的符合来证明一个人的身份称之为单因子认证，由于仅使用一种条件判断用户的身份容易被仿冒，可以通过组合两种不同条件来证明一个人的身份，称之为双因子认证。身份认证技术从是否使用硬件可以分为软件认证和硬件认证；从认证需要验证的条件来看，可以分为单因子认证和双因子认证；从认证信息来看，可以分为静态认证和动态认证。身份认证技术的发展，经历了从软件认证到硬件认证，从单因子认证到双因子认证，从静态认证到动态认证的过程。现在计算机及网络系统中常用的身份认证方式主要有以下几种。

1. 用户名/密码方式

用户名/密码是最简单也是最常用的身份认证方法，它是基于 what you know 的验证手段。每个用户的密码是由这个用户自己设定的，只有他自己才知道，因此只要能够正确输入密码，计算机就认为他就是这个用户。然而实际上，由于许多用户为了防止忘记密码，经常采用诸如自己或家人的生日、电话号码等容易被他人猜测到的有意义的字符串作为密码，或者把密码抄在一个自己认为安全的地方，这都存在着许多安全隐患，极易造成密码泄露。即使能保证用户密码不被泄露，由于密码是静态的数据，并且在验证过程中需要在计算机内存中和网络中传输，而每次验证过程使用的验证信息都是相同的，很容易驻留在计算机内存中的木马程序或网络中的监听设备截获。因此用户名/密码方式一种是极不安全的身份认证方式。

2. IC 卡认证

IC 卡是一种内置集成电路的卡片，卡片中存有与用户身份相关的数据，IC 卡由专门的厂商通过专门的设备生产，可以认为是不可复制的硬件。IC 卡由合法用户随身携带，登录时必须将 IC 卡插入专用的读卡器读取其中的信息，以验证用户的身份。IC 卡认证是基于 what you have 的手段，通过 IC 卡硬件不可复制来保证用户身份不会被仿冒。然而由于每次从 IC 卡中读取的数据还是静态的，通过内存扫描或网络监听等技术还是很容易截取到用户的身份验证信息。因此，静态验证的方式还是存在一定的安全隐患。

3. 动态口令

动态口令技术是一种让用户的密码按照时间或使用次数不断动态变化，每个密码只使用一次的技术。它采用一种称之为动态令牌的专用硬件，内置电源、密码生成芯片和显

示屏，密码生成芯片运行专门的密码算法，根据当前时间或使用次数生成当前密码并显示在显示屏上。认证服务器采用相同的算法计算当前的有效密码。用户使用时只需要将动态令牌上显示的当前密码输入客户端计算机，即可实现身份的确认。由于每次使用的密码必须由动态令牌来产生，只有合法用户才持有该硬件，所以只要密码验证通过就可以认为该用户的身份是可靠的。而用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒合法用户的身份。

动态口令技术采用一次一密的方法，有效地保证了用户身份的安全性。但是如果客户端硬件与服务器端程序的时间或次数不能保持良好的同步，就可能发生合法用户无法登录的问题。并且用户每次登录时还需要通过键盘输入一长串无规律的密码，一旦看错或输错就要重新来过，用户的使用不方便。

4. 生物特征认证

生物特征认证是指采用每个人独一无二的生物特征来验证用户身份的技术。常见的有指纹识别、虹膜识别等。从理论上说，生物特征认证是最可靠的身份认证方式，因为它直接使用人的物理特征来表示每一个人的数字身份，不同的人具有相同生物特征的可能性可以忽略不计，因此几乎不可能被仿冒。

生物特征认证基于生物特征识别技术，受到现在的生物特征识别技术成熟度的影响，采用生物特征认证还具有较大的局限性。首先，生物特征识别的准确性和稳定性还有待提高，特别是如果用户身体受到伤病或污渍的影响，往往导致无法正常识别，造成合法用户无法登录的情况。其次，由于研发投入较大和产量较小的原因，生物特征认证系统的成本非常高，目前只适合于一些安全性要求非常高的场合如银行、部队等使用，还无法做到大面积推广。

5. USB Key 认证

基于 USB Key 的身份认证方式是近几年发展起来的一种方便、安全、经济的身份认证技术，它采用软硬件相结合一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USB Key 内置的密码学算法实现对用户身份的认证。基于 USB Key 身份认证系统主要有两种应用模式：一是基于冲击/相应的认证模式，二是基于 PKI 体系的认证模式。由于 USB Key 具有安全可靠，便于携带、使用方便、成本低廉的优点，加上 PKI 体系完善的数据保护机制，使用 USB Key 存储数字证书的认证方式已经成为目前以及未来最具有前景的主要认证模式。

现在信息安全越来越受到人们的重视。建立信息安全体系的目的就是要保证存储在计算机及网络系统中的数据只能够被有权操作的人访问，所有未被授权的人无法访问到这些数据。这里说的是对“人”的权限的控制，即对操作者物理身份的权限控制。不论安全性要求多高的数据，它存在就必然要有相对应的授权人可以访问它，否则，保存一个任何人都无权访问的数据有什么意义？然而，如果没有有效的身份认证手段，这个有权访问者的身份就很容易被伪造，那么，不论投入再大的资金，建立的再坚固安全防范体系都形同虚设。就好像我们建造了一座非常结实的保险库，安装了非常坚固的大门，却没有安装门锁一样。所以身份认证是整个信息安全体系的基础，是信息安全的第一道关隘。

而防火墙、入侵检测、VPN、安全网关、安全目录与身份认证系统有什么区别和联系呢?

防火墙保证了未经授权的用户无法访问相应的端口或使用相应的协议;入侵检测系统能够发现未经授权用户攻击系统的企图;VPN在公共网络上建立一个经过加密的虚拟的专用通道供经过授权的用户使用;安全网关保证了用户无法进入未经授权的网段,安全目录保证了授权用户能够对存储在系统中的资源迅速定位和访问。这些安全产品实际上都是针对用户数字身份的权限管理,它们解决了哪个数字身份对应能干什么的问题。而身份认证解决了用户的物理身份和数字身份相对应的问题,提供了权限管理的客观依据。

5.3.2　数据隔离

对于IT软件服务商来说,他们所提供的传统企业软件系统大多基于多实例架构,即对于每一个客户组织,都有一个单独的软件系统实例为其服务,而搭建于云计算平台的软件系统则广泛地采用了多租户(Multi-tenancy)架构,即单个软件系统实例服务于多个客户组织。在Multi-instance架构下,由于每个客户拥有自己的软件实例,故不存在数据隔离的问题,但是在Multi-tenancy架构下,由于所有客户数据将被共同保存在唯一一个软件系统实例内,因此需要开发额外的数据隔离机制来保证各个客户之间的数据不可见性并提供相应的灾备方案。

随着云计算技术的成熟,Multi-tenancy也已不再是新鲜的概念,目前已经有几种相当成熟的架构用来帮助系统实现数据隔离:Shared schema multi-tenancy(下文简称为共享表架构),Shared database,Separated schema(下文简称为分离表架构)以及Separated database(下文简称为分离数据库架构)。

1. 共享表架构

即所有的软件系统客户共享使用相同的数据库实例以及相同的数据库表。因为共享表架构最大化地利用了单个数据库实例的存储能力,所以这种架构的硬件成本非常低廉,但是其程序开发者来说,却增加了额外的复杂度,由于多个客户的数据共存于相同的数据库表内,因此需要额外的业务逻辑来隔离各个客户的数据。此外,这种架构实现灾难备份的成本也十分高昂,不但需要专门编写代码实现数据备份,而且在恢复数据时,需要对数据库表进行大量的删除和插入操作,一旦数据库表包含大量其他客户的数据,势必对系统性能和其他客户的体验带来巨大的影响。

2. 分离数据库架构

即每个软件系统客户单独拥有自己的数据库实例。相比于共享表架构,由于每个客户拥有单独的数据库实例,这种架构可以非常高效便捷地实现数据安全性和灾难备份,但是随之而来的缺点便是其硬件成本非常高昂。

3. 分离表架构

即软件系统客户共享相同的数据实例,但是每个客户单独拥有自己的由一系列数据库表组成的schema。分离表架构是一种折中的Multi-tenancy方案,在这种架构下,实现数据分离和灾难备份相对共享表架构更加容易一些,另一方面,它的硬件成本也较分离数

据库架构为低。

无论是分离数据库还是分离表，抑或是共享表，每种架构都有它的优点和不足，在设计云端系统时，系统架构师需要进行全面的分析和考量，综合各方面的因素以选择合适的Multi-tenancy架构。一般说来，系统服务的客户数量越多，则越适合使用共享表的架构，对数据隔离性和安全性要求越高，则越适合使用分离数据库的架构。在超大型的云系统中，一般都会采用复合型的Multi-tenancy架构，以平衡系统成本和性能，这其中Salesforce便是一个典型的案例。Salesforce.com最初搭建于共享表架构，但是随着新客户的不断签入，单纯的共享表架构已经很难满足日益增长的性能要求，Salesforce逐步开始在不同的物理区域搭建分布式系统。在全局上，Salesforce.com以类似于分离数据库的架构运行，在单个区域内，系统仍然按照共享表架构运行。

5.3.3 数据加密及隐私保护

随着云计算技术的逐步成熟，它给IT应用带来的商业价值越来越明显地表现出来，相对于传统的软件架构，云计算运营和支持方面的成本更低廉，但同时又能够获得更快速的部署能力，近乎无限的伸缩性等收益。然而，尽管云计算带来的价值是如此巨大，但是仍然有诸多企业在云计算和传统软件架构中选择了后者，其原因很大程度上在于云计算领域中，有关企业数据的安全问题没有得到妥善的解决。一些分析机构的调查结果显示出，数据安全问题是企业应用迁移到云计算过程中的最大障碍之一。

数据安全是指通过一些技术或者非技术的方式来保证数据的访问是受到合理控制，并保证数据不被人为或者意外的损坏泄露或更改。从非技术角度上来看，可以通过法律或者一些规章制度来保证数据的安全性；从技术的角度上来看，可以通过防火墙、入侵检测、安全配置、数据加密、访问认证、权限控制、数据备份等手段来保证数据的安全性。由于传统软件和云计算在技术架构上有着非常明显的差异，这就需要我们用不同的思路来思考两种架构下有关数据安全的解决方案。下面笔者从技术角度就云计算中数据安全的某些方面和大家进行简单的探讨，希望能够起到抛砖引玉的作用。

数据隐私

对于任何一个IT系统来说，在运行生命周期过程中使用的以及生产的数据都是整个系统的核心部分，而我们一般把这些系统数据分为公有数据和私有数据两种类型。公有数据代表可以从公共资源获得的数据信息，例如股票信息公开的财务信息等，这类数据可以被任何一个IT系统获得并使用。而私有数据则代表这些数据是被IT系统所独占并无法和其他IT系统所共享的。对于公有数据，使用它们的IT系统并不需要处理安全相关的事物，然而对于私有数据特别是一些较为敏感的私有数据，在构建IT系统时是需要专门考虑如何保证数据不被盗用甚至修改。传统的IT系统通常搭建在客户自身的数据中心内，数据中心的内部防火墙保证了系统数据的安全性。和传统软件相比较，云计算在数据方面的最大不同便是所有的数据将由第三方而非第一方来负责维护，并且由于云计算架构的特点，这些数据可能被存储在非常分散的地方，并且都按照明文的方式进行存储，尽管防火墙能够对恶意的外来攻击提供一定程度的保护，但是这种架构使得一些关键性的数据可以被泄露，无论是偶然还是恶意(例如，由于开发和维护的需要，软件提供商的

员工一般都能够访问存储在云平台上的数据，一旦这些员工信息被非法获得，那么黑客便可以在万维网上访问部署在云平台上的程序或者得到关键性的数据）。这对于对安全性有较高要求的企业应用来说是完全不可以接受的。

尽管目前在公有云平台还没有很好的数据隐私解决方案，但是企业仍然可以选择构建私有云或者混合云来实现弹性计算和数据隐私的均衡，同时也为未来在公有云平台上的实施积累经验。从弹性计算的角度来看，私有云和公有云并无太大差别，都是通过自动化的管理虚拟化的IT资源来实现弹性计算的目的。然而，由于现有的企业应用基本上都基于传统的IT基础架构搭建，几乎所有的IT资源都要求IT工程师花费大量的时间和精力来手动管理，并没有办法实现敏捷高效的自动化管理，因次无法满足云计算的要求。实施私有云计算的第一步也是最重要的一步便是重新搭建IT基础架构：将现有的处理器、存储、网络等IT资源高度虚拟化并重新组织整合，构建高度扩展性的IT集群架构，辅以强大的管理软件来实现高效自动化的IT资源管理。整个IT架构可以搭建在企业内或者是第三方的数据中心内，但是无论私有云部署在什么地理位置，企业都拥有完全的IT资源控制能力。通过网络控制和独享的防火墙保护，私有云上的企业数据能够得到和传统IT架构下企业数据相同级别的安全保障。

在主流的私有云架构之外，Amazon公司的Virtual Private Cloud提供了一套全新的企业级私有云构建方案。主流的私有云解决方案都致力于IT资源的虚拟化以及自动化管理，而Amazon VPC则将重点放在了如何构建专门针对单个企业的虚拟网络并与企业现有的IT架构安全无缝地连接起来。企业可以在Amazon公司的公有云平台上创建VPC虚拟网络，并通过企业自身的加密VPN将VPC虚拟网络与企业局域网连接起来，并将整个VPC虚拟网络加入到企业现有的安全架构下。在申请创建EC2实例时，可以将其指定与相应的VPC网络绑定，在EC2实例启动之后，该实例也就相当于运行在整个大的企业局域网之内了。虽然VPC网络中所有的EC2实例仍然位于公有云平台上，但是在这种IT架构下，企业内的防火墙能够保证这些公有云上的数据安全。

采用Amazon VPC的私有云解决方案无须对企业现有IT架构做出大规模的调整，因此无法减少IT运营成本，但是相比主流的私有云解决方案，实施成本和风险则减少了很多。混合云则将云平台与in-house系统或者是私有云结合起来，将部分子系统搭建在企业内部的数据中心（通常这些子系统中的数据对安全性有非常严格的要求，或是一些legacy系统），而把系统的其他部分构建于云计算平台之上（通常这类子系统不带有数据安全性的问题），通过Service Bus将in-house系统（私有云）与公有云端系统连接起来。

5.3.4　分级安全控制与网络隔离

1. 网络隔离技术

面对新型网络攻击手段的出现和高安全度网络对安全的特殊需求，全新安全防护防范理念的网络安全技术——“网络隔离技术”应运而生。网络隔离技术的目标是确保隔离有害的攻击，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。网络隔离技术是在原有安全技术的基础上发展起来的，它弥补了原有安全技术的不足，突出了自己的优势。

2. 隔离技术的发展历程

网络隔离，英文名为 Network Isolation，主要是指把两个或两个以上可路由的网络（如 TCP/IP）通过不可路由的协议（如 IPX/SPX、NetBEUI 等）进行数据交换而达到隔离目的。由于其原理主要是采用了不同的协议所以通常也称为协议隔离（Protocol Isolation）。1997 年，信息安全专家 Mark Joseph Edwards 在他编写的 *Understanding Network Security* 一书中，对协议隔离进行了归类。在书中他明确地指出了协议隔离和防火墙不属于同类产品。隔离概念是在为了保护高安全度网络环境的情况下产生的；隔离产品的大量出现，也是经历了五代隔离技术不断的实践和理论相结合后得来的。

第一代隔离技术——完全的隔离。此方法使得网络处于信息孤岛状态，做到了完全的物理隔离，需要至少两套网络和系统，更重要的是信息交流的不便和成本的提高，这样给维护和使用带来了极大的不便。

第二代隔离技术——硬件卡隔离。在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时，同时选择了该卡上不同的网络接口，连接到不同的网络。但是，这种隔离产品有的仍然需要网络布线为双网线结构，产品存在着较大的安全隐患。

第三代隔离技术——数据转播隔离。利用转播系统分时复制文件的途径来实现隔离，切换时间非常之久，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

第四代隔离技术——空气开关隔离。它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换的，但在安全和性能上存在有许多问题。

第五代隔离技术——安全通道隔离。此技术通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。第五代隔离技术的实现原理是通过专用通信设备、专有安全协议和加密验证机制及应用层数据提取和鉴别认证技术，进行不同安全级别网络之间的数据交换，彻底阻断了网络间的直接 TCP/IP 连接，同时对网间通信的双方、内容、过程施以严格的身份认证、内容过滤、安全审计等多种安全防护机制，从而保证了网间数据交换的安全、可控，杜绝了由于操作系统和网络协议自身漏洞带来的安全风险。

3. 隔离技术需具备的安全要点

1）要具有高度的自身安全性

隔离产品要保证自身具有高度的安全性，至少在理论和实践上要比防火墙高一个安全级别。从技术实现上，除了和防火墙一样对操作系统进行加固优化或采用安全操作系统外，关键在于要把外网接口和内网接口从一套操作系统中分离出来。也就是说至少要由两套主机系统组成，一套控制外网接口，另一套控制内网接口，然后在两套主机系统之间通过不可路由的协议进行数据交换，如此，即便黑客攻破了外网系统，仍然无法控制内网系统，就达到了更高的安全级别。

2）要确保网络之间是隔离的

保证网间隔离的关键是网络包不可路由到对方网络，无论中间采用了什么转换方法，