供电企业信息系统云服务的研究与应用

倪阳旦，沈潇军，戚伟强，沈志豪，龚小刚，徐柳婧

（国网浙江省电力公司信息通信分公司，杭州　310007）

摘　要：以云计算、大数据、物联网及移动互联为代表的新一代信息技术的应用，正在催生新一轮的产业变革。供电企业云计算技术的引入，在创新业务模式、提高客户服务体验、强化自身服务效率、节省建设及使用成本的同时，其安全性一直备受关注。从云安全的角度，通过简述浙江电力公司的电力云发展过程，提出基于 SSL 加密技术和 Array APV 负载均衡技术的解决方案，并对安全电力云发展进行了展望。

关键词：互联网；云计算；安全

中图分类号：TN915.853　　**文献标志码：**B　　**文章编号：**1007-1881(2015)10-0061-05

Research and Application of Cloud Services of Information System in Power Supply Enterprises

NI Yangdan, *SHEN Xiaojun*, *QI Weiqiang*, *SHEN Zhihao*, *GONG Xiaogang*, *XU Liujing*

(Information and Telecommunication Branch of State Grid Zhejiang (Provincial) Electric Power Company, Hangzhou 310007, China)

Abstract: The application of new information technologies represented by cloud computing, big data, internet of things and mobile internet is creating a new round of industrial revolution. In power supply enterprises. The introduction of cloud computing technology brings business model innovation, enhancement of customer service experience, improvement of service efficiency and reduction of construction cost; at the same time, its security has been widely focused. This paper briefly introduces the development of power cloud in Zhejiang (Provincial) Electric Power Company in terms of cloud safety; furthermore, it proposes a solution based on SSL encryption technology and Array APV load balance technology and discusses the development prospect of power cloud safety.

Key words: internet; cloud computing; safety

0　引言

当前，以云计算、大数据、物联网及移动互联为代表的新一代信息技术的广泛应用，正在孕育和催生新一轮的产业变革。对于供电企业也是如此，伴随着信息化的发展和深化，传统的、刚性的 IT 系统架构会制约供电企业信息化的持续发展，因此急需引入基于云计算技术的电力云平台，形成以按需服务、高可扩展、弹性可变为特点的应用系统及数据服务技术架构。新一代信息技术电力云的引入，有助于创新供电企业业务模式、提升客户服务体验、提高自身服务效率、节省建设及使用成本，电力云的建设已成为供电企业今后一段时间信息化建设的方向。

与此同时，基于云计算技术的云平台安全性也一直备受关注，调查数据显示，用户对云平台安全的关注远高于其他方面(见图 1)。由于提供服务的系统和数据被转移部署到用户可掌控的范围之外，云服务的数据安全、身份认证、隐私保护等成为用户最为担忧的问题，特别是信息数据在云平台运行过程中的安全性，成为云计算平台即电力云能否在供电企业核心信息系统中应用的关键。

本文将从云安全的角度出发，阐述电力云建立过程采用的关键技术，介绍浙江省电力公司电力营销系统在云平台的实施过程，提出基于 SSL 云交付加密技术和 Array APV 服务器负载均衡技术的解决方案，并对安全电力云发展进行展望。

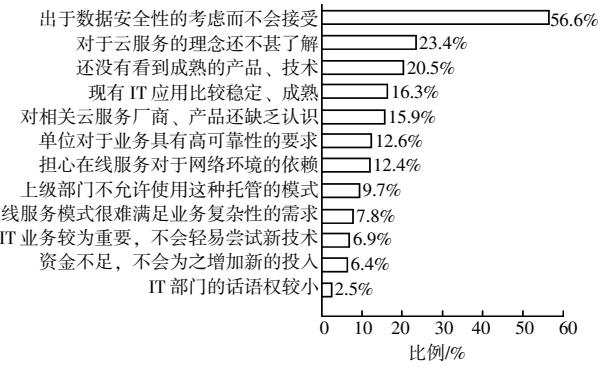

图 1 用户对云平台安全的关注

1 实现“安全电力云”的关键技术

云计算就是利用虚拟化技术建立统一的基础设施、服务、信息及应用的资源池，以分布式技术对各种基础设施资源进行有效组织和运用的运行模式。云计算使得客户获得低成本、高性能、快速配置和海量化的计算服务成为可能，然而云计算所具有的虚拟化、资源共享、分布式等技术特点，也决定了其在安全性上存在隐患。例如当系统、数据、信息存储在物理位置不确定的“云端”，服务安全、数据安全与隐私安全如何保障？在安全电力云建设过程中，建议使用基于 SSL 协议的技术，解决信息系统虚拟化、分布式后的信息系统安全交付问题。

1.1 SSL 基本概念

SSL(加密套接字协议)是被设计用来保证信息安全的一个协议，它依赖于可靠的 TCP 协议来传输数据。SSL 的特点之一是独立于上层的应用层协议(如 HTTP, FTP, TELNET 等)，这些应用层协议可以透明地使用 SSL。SSL 可以协商一个对称加密算法和会话密钥，同时可以在通信之前认证服务器的合法性。因此，将机密资料数据设定为采用加密的传输模式，即可避免资料在网络上传输时被他人窃听。形象地说，SSL 提供了一种“管道式安全”，它具有 3 个特征：管道是保密的，其保密性通过使用加密技术来保证，在通过简单的握手过程之后获得一个共同的密钥，作为对称加密算法的密钥；管道是经过认证的，服务器端需要把自己的证书递交给客户端，以便客户端对服务器进行认证，而服务器可以选择是否需要客户端递交证书；管道是可靠的，消息的传输包含了消息完整性检查。

1.2 基于 SSL 的超文本传输安全协议

超文本传输安全协议是 HTTPS(超文本传输协议)和 SSL/TLS(安全传输层协议)的组合，用以提供加密通信及对网络服务器身份的鉴定。HTTPS 连接常用于万维网上的交易支付和企业信息系统中敏感信息的传输。

HTTPS 的主要思想是在不安全的网络上创建一个安全信道，并可在使用适当的加密包和服务器证书可被验证且可被信任时，对窃听和中间人攻击提供合理的保护。HTTPS 的信任继承基于预先安装在浏览器中的证书颁发机构(如 VeriSign, Microsoft 等)。

1.3 基于 SSL 的安全数据传输技术

SSL VPN(安全数据传输技术)即指采用 SSL 协议来实现远程接入的一种新型 VPN 技术。SSL VPN 的出现是为了解决 IPSec VPN 的固有缺点，它继承了 IPSec VPN 的远程使用与内网使用体验一致、与应用无关的优点，又避免了因有客户端而导致的各种问题。同时 SSL VPN 采用了 SSL 协议，可以在HTTP 层及 TCP 层之间灵活地调整解决方案，因此已成为当今使用最方便、使用场景最丰富的安全数据传输技术。

通过 SSL VPN，客户可以安全地访问企业内部的应用，而不是企业的整个网络。这就带来非常灵活的资源交付安全管理手段，而非基于传统的网络层面进行抽象的访问控制。

1.4 面向移动终端的安全管理

随着移动化办公的普及，越来越多的用户关注到其安全的问题。在内网使用 WIFI，或通过移动网络使用 3G 的方式对基于 Web 的应用进行访问时，可以通过基于 SSL 加密的技术解决账号信息和敏感数据在传输过程中泄露的问题。但另一方面，企业开发的基于 C/S 架构的 APP 可能无法受到 SSL 技术的保护。如何在移动化云接入的场景中对移动终端进行认证，如何为 APP 提供基于 SSL 的安全接入平台，如何对接入的用户进行认证，如何对移动终端数据进行加密，这些问题都变得尤为重要。

建议采用 Array SPX 系列的 Array SLL VPN 设备，该设备提供了使用便捷、部署轻松的无客户端、基于 Web 的接入以及对基于身份的应用

和资源访问的先进认证、授权和审计机制，能有效解决移动应用的安全接入。

1.5　基于硬件的负载均衡服务

SLB(负载均衡服务)有软件实现和硬件实现 2 种方案。软件负载均衡解决方案是指在 1 台或多台服务器相应的操作系统上安装 1 个或多个附加软件来实现负载均衡，它的优点是基于特定环境，配置简单，成本低廉，可以满足一般的负载均衡需求。缺点是每台服务器因安装额外的软件而占用系统不定量的资源，越是功能强大的模块，占用得越多，所以当连接请求特别大的时候，软件本身会成为服务器工作成败的关键。硬件负载均衡解决方案是直接在服务器和外部网络间安装负载均衡设备，这种设备通常称为负载均衡器，由于由专门的设备完成专门的任务，独立于操作系统，整体性能得到大幅提高，加上多样化的负载均衡策略，智能化的流量管理，可达到最佳的负载均衡效果。

经比较，硬件负载均衡在性能上优于软件方式，但成本昂贵。综合考虑后，浙江省电力公司在安全电力云实施过程中，采用了硬件负载均衡解决方案，选用了 Array APV 负载均衡服务器。

从云安全角度看，采用基于硬件的 Array APV 负载均衡服器，还有以下优势：由于采取了 SSL 加密传输的信息安全协议，而 SSL 协议是对 HTTP 请求的敏感数据加密的技术，一般握手、加密和解密过程由 Web 服务器处理，由 Web 服务器提供传统的软件 SSL 加速方式将占用 Web 服务器资源并严重降低其性能，而像 Array APV 这样的硬件负载均衡服务器提供了称为“SSL 加速器”的硬件，用于截获加密的通信并执行 SSL 处理(握手、加密和解密)，加速器与 Web 服务器之间的通信通常以明文形式进行，因此，这种通过专用硬件来执行 SSL 处理将可以获得更好的性能。

2　“安全电力云”在浙江电力的部署

近年来，浙江省电力公司在由自身传统的网格式渠道发展模型向安全电力云服务转型的过程中不断摸索，取得了阶段性成果。

在“安全电力云”的建设过程中，浙江省电力公司结合自身业务发展模式和企业向云服务战略转型的计划，选择电力营销系统作为试点，采用了 Array 负载均衡设备的应用安全交付解决方案，不仅解决了基于软件的集群技术在交付性能、扩展性以及部署层面的问题，实现该业务系统的“云化”，而且在解决云计算安全性问题上进行了有益的探索。该解决方案的架构示意见图 2。

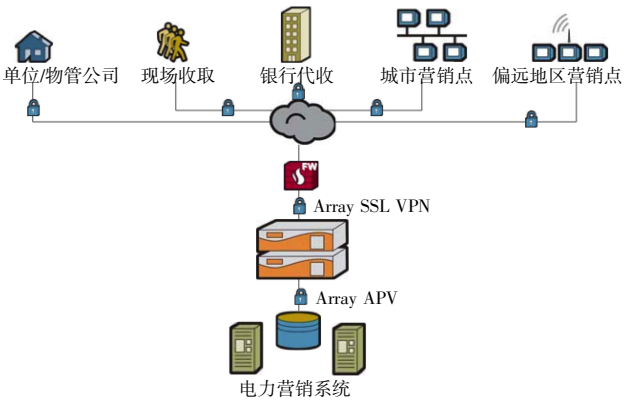

图 2　Array 解决方案在浙江电力的应用

营销业务系统的云服务转型分为系统的“云化”和“安全电力云”2 个阶段。第一阶段的“云化”，将使业务系统整体的健壮性、灵活性以及容灾能力得到提升，充分享受“云计算”模型带来的高端业务体验。第二阶段通过应用 SSL 加密交付，实现营销业务的安全应用交付。

2.1　采用 Array 解决方案实现营销业务系统的“云化”

在“云化”过程中，Array APV 提供的SLB，打破了基于传统软件集群技术的解决方案的种种限制，通过唯一的服务 IP 和端口，隐藏了背后提供相同业务的多台服务器集群，在逻辑层面实现了业务系统的唯一接口。

Array APV 提供的服务器负载均衡技术，通过面向不同协议的负载平衡算法来实现合理的流量分配，使每台服务器的处理能力都得到充分发挥。配合 APV 自身针对不同业务的安全检查机制，可以动态检测后台服务器的健康状态，自动屏蔽不能提供服务的后台服务器，使前段用户无感知，最终实现了营销业务系统的“云化”。

Array APV 的服务器负载均衡工作模式如图 3 所示。

实践表明，在营销业务系统的各后台服务器组均能够正常提供服务时，客户端仅需向 APV 上特定的对外提供服务的 IP 地址(VIP)和端口发

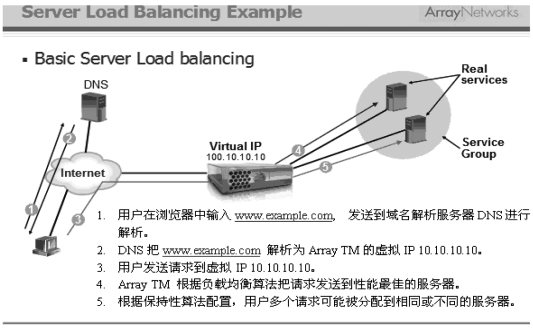

图 3 Array 服务器负载均衡实现应用云交付

起访问请求，即可实现所有应用功能。后台真实提供服务的 IP 地址和端口将被 APV 隐藏起来。在进行服务器负载均衡时(4 层负载均衡功能、7 层负载均衡功能)，APV 提供了多种策略和算法以满足不同应用系统的特定需求。

在浙江电力营销业务系统试点应用中，SLB 体现了如下优点：真正面向营销业务应用的 WWW 代理服务；无需改动浙江电力现有网络结构即可实现功能；支持路由功能，根据实际响应时间的负载平衡算法来实现真正合理的流量分配；使用特有的连接复用技术和连接池技术，有效减少后台服务器的负载，保护投资成本。

通过部署 Array APV 解决方案，浙江电力一方面实现了对营销业务系统内多台服务器节点的整合，利用负载均衡算法实现了硬件处理性能的累加，另一方面实现了对营销业务系统内不同业务节点的动态监控，利用其健康检查机制实现了节点的互相备份，实现了营销业务系统的“云化”。同时利用自身基于硬件的产品架构，确保营销业务系统未来的线性扩展，为接下来更大范围的推广提供基础。

2.2 采用 Array 解决方案实现营销业务系统的“安全云交付”

在 SSL 处理过程中，所有的传输内容均采用加密算法处理，其中最重要的 2 个部分是 SSL 握手时交换秘钥的非对称加密和数据传输时的对称加密。

随着 2013 年基于 1024 位的密钥被互联网全面淘汰，非对称加密必须采用至少 2048 位的密钥进行加/解密，对称加密也开始从 128 位向 256 位过渡，因此在服务器上完成 SSL 的加/解密，对服务器的 CPU 占用率非常高，用户数一多就无法保证服务。因此，对已实现全省集中信息系统部署的供电企业来说，采用 SSL 加速(卸载)设备来进行处理是必然选择。

Array 负载均衡设备可以实现全硬件处理 SSL 非对称加密和对称加密流量，具备业内最佳的处理性能。因此在“云服务的加密交付”阶段，仅需要在现有的 Array APV 设备上开启相应的功能并导入证书，即可实现针对营销业务系统的全方位应用交付加密，轻松完成云服务的加密交付。

在解决方案中，位于 Array APV 前端的 Array SSL VPN 设备建立的虚拟专用网络为采用移动设备工作的人员远程接入提供了安全的接入手段，使其可随时随地访问信息资源；可实现对受管理和未受管理的移动设备的接入管理控制，包括台式机、笔记本电脑、平板电脑和智能手机；提供了一系列接入方法，如 Web，Layer-3 和特定客户端-服务器端和瘦客户端应用。通过与 Array APV 的结合，实现了各种信息设备的统一接入，大大方便了信息系统的开发与维护。

3 应用效果及发展展望

浙江省电力公司通过“安全电力云”在营销系统的试点应用，证明了将电力核心信息系统迁移至云计算服务平台，在技术上是安全可行的。试点应用取得了以下成效：

(1)实现了营销系统由传统结构向云平台的平稳迁移，初步实现了营销系统的“云化”。

(2)通过 Array APV 实现了营销系统在云平台的负载均衡，平台服务更为可靠、灵活，为客户提供更为优良的信息服务。

(3)通过 Array APV 提供的唯一的服务 IP 和端口，在逻辑层面实现了业务系统的唯一接口。

(4)通过 Array APV 实现了基于 SSL 协议的应用安全交付，保障了营销系统的应用安全。

(5)通过 Array APV 提供的 SSL VPN 服务实现了智能移动终端设备的统一接入。

应该看到，利用 Array APV 实施的云的 SSL 加密安全交付，只是提供了一个经加密认证的安全通道，也仅是“安全电力云”交付的第一步，要实现信息系统在云平台的安全，其后还有云服务数据本身的加密传输以及云服务数据在云终端本地的加密存储等安全问题需要解决。当然，云服

务引发的安全问题除了包括系统防护、数据加密、用户访问控制、Dos 攻击等传统网络与信息安全问题外，还包括由集中服务模式及云计算所引发的诸如虚拟机隔离、多租户数据隔离、残余数据擦除以及多 SaaS 应用统一身份认证等问题，因此保障云计算平台的安全依然任重道远。

大力推进云计算、大数据、物联网及移动互联为代表的新一代信息技术是电力行业的战略决策，下一步将在试点经验基础上，有计划地扩大云平台的应用，将其他信息系统逐步迁移至云平台，努力实现“安全电力云”的建设目标。

4　结语

浙江省电力公司以电力营销系统为试点，实现了系统的“云化”，而且在云安全方面作了有益尝试，为供电企业全面实施云计算战略积累了经验，具有借鉴意义。

参考文献：

[1] RONALD L KRUTZ,RUSSELL DEAN VINES.云计算安全指南[M].北京：人民邮电出版社,2013.

[2] GARTNER.基于云计算的安全服务启程[EB/OL].http://www.gartner.com,2013.

[3] 冯登国,张敏,张妍,等.云计算安全研究[J].软件学报,2011,22(1):71-83.

[4] 张云勇,陈清金,潘松柏,等.云计算安全关键技术分析[J].电信科学,2010(9):64-69.

收稿日期：2015-08-05

作者简介：倪阳旦(1986)，男，工程师，从事电力信息系统安全、数据库运维等工作。

（本文编辑：方明霞）