刘家玉,荀广连,曹　萌,等. 基于安全域的省级农业科研单位网络安全建设研究[J]. 江苏农业科学,2018,46(6):346 - 348.
doi:10.15889/j.issn.1002 - 1302.2018.06.086

基于安全域的省级农业科研单位网络安全建设研究

刘家玉, 荀广连, 曹　萌, 刘家祥, 戴　秀, 施　奎, 高晓辉, 陈　磊
(江苏省农业科学院信息服务中心,江苏南京 210014)

摘要:互联网与 IT 技术的发展,提升了农业科研单位对外交流、科研管理及科研数据的存储与利用,网络与信息安全愈显重要。分析了江苏省农业科学院的网络安全现状,根据农业科研的业务需要及信息承载,提出了基于安全域构建局域网安全防护架构的思路,为兄弟农科院的网络信息安全提供参考。

关键词:农业科研单位;信息安全;安全域;划分原则;划分方法;现状分析;建设方案
中图分类号: TP309.2　　**文献标志码**: A　　**文章编号**:1002 - 1302(2018)06 - 0346 - 03

近年来,随着互联网与 IT 技术的发展,信息化已经成为当前科技、经济与社会发展的重要趋势。信息技术在社会各领域的广泛渗透,开创了经济发展的新时代,在推动人类社会生产力的同时,各种形式的网络安全问题也频频发生,给国家安全和社会稳定带来了极大的威胁。根据国家互联网应急中心(CNCERT)发布的《2016 年中国互联网网络安全报告》[1]显示,2016 年,我国捕获的移动互联网恶意程序数量 205 万余个,国家信息安全漏洞共享平台(CNVD)共收录通用软硬件漏洞 10 822 个,约 4 万个 IP 地址对我国境内 8 万余个网站植入后门,等等。网络安全问题已经引起了我国政府的高度重视。全国人大常委会于 2016 年 11 月发布《中华人民共和国网络安全法》[2],规定了网络安全建设监督条例,并对包括农业科研机构在内的各级单位的网络安全建设提出了更高的要求。如何建设安全可靠的农业科研局域网,如何合理、安全、有效地管理、保护农业科研信息资源,安全利用农业科研大数据,已经成为省级农业科研单位必须面对的重要问题。

1　网络安全建设现状

省级农业科研单位组织架构及局域网建设情况比较类似,以江苏省农业科学院为例,除管理服务部门外,还有 10 多个专业研究所或投资企业,在职人数超过 1 000 人,终端类型多、数量大。局域网建设之初是为了方便科研和管理人员对外联系、与国内外同行交流,采用与因特网逻辑隔离的技术架构,网络拓朴为典型的三层结构,包括核心层、汇聚层和接入层,核心交换进行热备冗余部署,保证网络的稳定,同时建设单位门户网站,对外宣传和展示,为三农提供技术支持和服务。随着 IT 技术应用的发展,局域网逐步建设了支撑单位管理和科研业务的办公自动化(OA)、科研项目管理、积分制绩效考核、财务管理、档案管理等多个信息管理系统。在与 Internet 连接的局域网出口处部署了网络防火墙和上网行为管理系统,将面向互联网服务的应用集中部署到 DMZ 区,并前置专用的 Web 应用防火墙进行多层安全防护,分支机构和出差职工可通过 VPN 接入访问内部系统。

该局域网从安全配置上具备一定的安全防护能力,也有一定的防御外部网路攻击的安全措施,但与当前的网络安全形势及相关职能部门的要求相比,仍然存在一定的安全隐患:如科研人员更强调便利,信息安全意识不足;科研单位经费管理分散,电脑购置经费来源多样,个人使用维护,难以实现终端统一安全管理;内网应用服务器与办公区、生活区同属 1 个子网,容易受到来自内部终端的攻击;网络结构边界不清晰,不利于精细化的安全防护;投入不足,网络安全设备无法满足性能要求等。

随着信息化建设的不断推进,日常办公的公文流转、科研信息的数字化保存与未来大数据的分析利用对 IT 系统的依赖日趋升高,局域网信息资产的安全防护更趋重要,如何利用有限的资金,在保护原有投资的前提下进行网络安全改造,实现网络安全性能提升的平滑过渡,满足信息化对管理和科研活动的支撑,是当前工作亟待解决的问题。

2　网络安全建设方案

1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》(国务院令第 147 号)[3]规定了计算机信息系统应实行安全等级保护。国家保密局 2000 年 1 月 1 日起颁布实施的《计算机信息系统国际联网保密管理规定》[4]规定“涉及国家秘密的计算机信息系统,不得直接或间接地与国际互联网或其它公共信息网络相连接,必须实行物理隔离”。农业科研单位的网络承载的多是与科研业务相关的科研、财务、管理等信息,不涉及国家秘密,因此应按照等级保护的相关安全要求进行网络建设。

2.1　安全域的划分

大型网络及信息系统进行等级保护,不是对整个网络或系统进行同一等级的保护,而是针对系统内部不同的业务区域或业务子网进行不同等级的保护,以达到安全策略统一、资源调配合理、业务交互便捷可靠的目标。安全域划分是进行

收稿日期:2017 - 11 - 08
基金项目:江苏省农业科学院基本科研业务专项[编号:ZX(17)4038]。
作者简介:刘家玉(1968—),男,江苏徐州人,副研究员,主要从事网络信息安全和信息化建设与管理研究。Tel:(025)84392779;E - mail:liu@jaas.ac.cn。
通信作者:荀广连,助理研究员,主要从事农业信息安全研究与系统研发。E - mail:xun@jaas.ac.cn。

信息安全等级保护的首要步骤[5-6]，安全域是指同一环境内有相同的安全保护需求、相互信任、并具有相同的安全访问控制和边界控制策略的网络或系统，将网络划分为不同的区域或逻辑子网，对每个区域进行层次化、有重点的保护。通过安全域的划分，可以把复杂的大型网络系统安全问题转化为较小区域与业务板块更为统一的安全保护问题，从而更好地控制网络安全风险，将有限的安全防控资源分配给最需要保护的资产，提高网络整体安全性与安全防护的经济性。

2.2　安全域划分原则

进行安全域的划分时，应考虑到网络系统规划设计、部署、维护管理到运营全过程中的所有因素。安全域划分的基本原则包括以下几条：(1)业务保障原则。安全域方法的根本目标是能够更好地保障网络上承载的业务。在保证安全的同时，还要保障日常办公和科研业务的正常运行和运行效率。(2)结构简化原则。安全域划分的直接目的和效果是要将整个网络变得更加简单，简单的网络结构便于设计防护体系。比如，安全域划分并不是粒度越细越好，安全域数量过多过杂可能导致安全域的管理过于复杂和困难。(3)等级保护原则。安全域的划分要做到每个安全域的信息资产价值相近，具有相同或相近的安全等级、安全环境、安全策略等。(4)生命周期原则。对于安全域的划分和布防不仅仅要考虑静态设计，还要考虑动态、不断变化调整的工作。

2.3　安全域划分方法

目前国内比较常用的网络安全域划分有以下几种基本方法：(1)按照业务系统等级划分。这种方法依据业务系统的分类来区分支持不同业务系统的网络区域，从而把网络划分成不同的网络安全域。(2)按照防护等级划分。这种方法依据网络中信息资产的价值划分不同的防护等级，相同等级构成相同的网络安全域。不同等级的安全域采用不同的安全手段，有效地减少了重复投资，同时也体现了安全纵深防御的思想。(3)按照系统行为等级划分。这种方法按照信息系统的不同行为和需求来划分相应网络安全域，并根据信息系统的等级和特点选择相应的防护手段。

2.4　安全域划分

由于每个单位的网络情况和业务需求都有所不同，因此进行安全域划分时必须兼顾网络的管理和业务属性，既要保证现有业务的正常运行，也要考虑划分方案是否可行。遵循任何单一的安全域划分方法都无法实现网络安全域的合理划分，因此，应当从网络承载的业务和管理需求，基于安全域划分的 4 个原则，综合几种划分方法，有针对性地合理划分安全域。

根据江苏省农业科学院的网络结构及业务信息承载，通过调研和分析，设计出基于网络现状的基于安全域的网络安全建设方案。首先根据网络的拓朴将整个网络划分为内网和外网两部分，其目的是保障内网中的核心业务安全运行，Internet 出口位于外网区，内网和外网之间设置网络防火墙，规避了来自外网和 Internet 的威胁，实现内外网之间的安全隔离。其次，分别在内网区和外网区按照业务系统进行安全域划分。外网区为对外服务区，内网则首先划分为内网数据区、网络交换区和用户接入区，根据功能重要性分为内网核心业务数据服务器区、内网非核心业务数据服务器区、生活小区、办公用户接入区和智慧园区等子区域，最终得出安全域划分(图 1)。

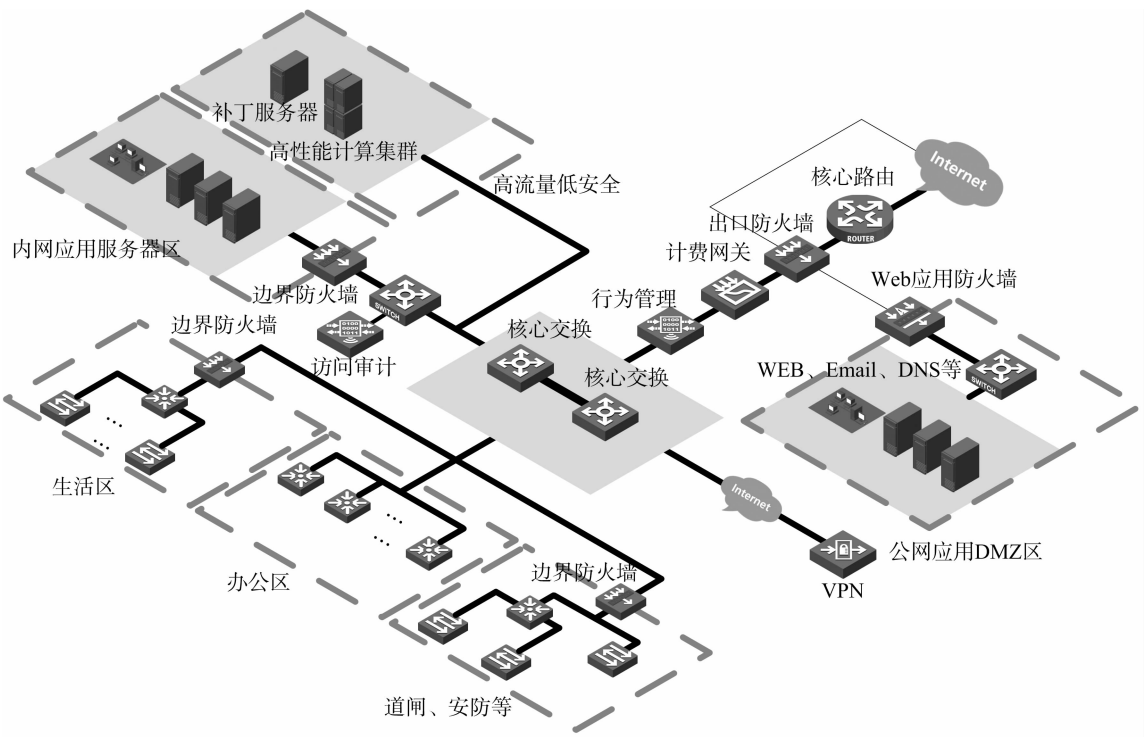

图1　院局域网安全域划分拓扑

对外服务区,即 DMZ 区,主要部署对互联网开放的信息系统和服务,如门户网站、邮件服务器等;内网核心业务数据服务器区主要部署提供院内服务的业务系统,安全性要求比较高,如 OA、科研管理、积分考核、财务系统等;内部大流量应用服务器区面向内部提供服务,主要为上传下载的高流量、安全性要求不高的服务与应用,如高性能计算、补丁服务器等;网络交换区主要包含保障网络畅通的各类网络通信设备;生活区接入单位局域网的生活小区网络,用户群体类型比较丰富;办公区,即单位办公区域的网络,用户群体主要为单位职工;智慧园区主要包含车辆进出的道闸管理系统、视频安防监控、智慧一卡通等与日常办公关系不密切,有一定安全需求同时没有大量访问需求的应用和业务系统。

2.5　安全防护策略

基于安全域的安全防护策略主要通过在安全域之间边界适当部署安全访问控制措施实现,而安全域的防护载体一般为逻辑结构边界上部署交换机、防火墙等防护设备[7]。

对外服务区边界在原有防火墙、上网行为管理设备及访问控制策略的基础上增添部署网页防篡改、IPS 等设备,满足对应的等级保护要求,增强安全防护功能。内网核心业务数据服务区边界部署防火墙及 IPS 并根据业务需求设定防护策略,同时在边界交换机上旁路接入访问审计设备,实现对内网应用访问的记录,便于安全审查。网络交换区的主要安全防护措施包括采用“https”或“ssh”等安全方式对网络设备进行管理,避免管理帐号信息被非法窃取。定期对相关网络设备进行周期性安全漏洞检查和安全配置检查和修补,防止利用漏洞的攻击。实施冗余部署,避免单点故障。生活区边界部署防火墙,结合 VLAN 划分实施访问控制策略,生活区对内网其他逻辑区域不可访问,最大程度地将生活区从办公网络中隔离。智慧园区边界部署防火墙,设置此区域终端设备只可访问内网核心业务服务区与业务相关的指定服务器,拒绝外部其他接入区域的访问,将此区域与其他区域隔离。内部大流量应用服务器区和生活区这 2 个区域,因为其业务特性和较大的用户数量,信息敏感度不高且对网速和带宽有很高的要求,高性能的安全防护设备价格昂贵,暂未考虑对此区域增加专用设备防护。通过对内网其他区域安全策略的设置,自然形成这 2 个分区的保护,以后如果需要更高防护,只需将此区域中有特别需求的 VLAN 划成单独的安全域部署实施相关的安全防护策略即可。终端管理在内网安全管理中难度最大,采用网络准入既需要科研人员配合,又需要所有设备都支持 802.1x 协议,实施推广较难。用户终端安全可以通过微软的 WSUS 或者 SCCM 方案在局域网中部署补丁服务器,及时升级防止系统漏洞,或使用 360 安全卫士等第三方客户端进行补丁升级。

通过安全域划分及安全策略部署,可以清晰地标识出整个网络的子网边界,确定网络防护的对象和范围,从而将复杂的网络安全问题化解为多个相对简单的问题,便于按照纵深防护的思想进行相关部署。同时,部署运维堡垒机,采用协议代理的方式,接管终端计算机对网络和服务器的访问,通过切断终端计算机对网络和服务器资源的直接访问,实现核心系统运维和安全审计管控的功能,既能拦截非法访问和恶意攻击,对不合法命令进行命令阻断,过滤掉所有对目标设备的非法访问行为,又能对内部人员误操作和非法操作进行审计监控,以便事后责任追踪。

从实施结果看,防护效果显著,一方面能实时发现服务器存在的配置漏洞、弱密码漏洞、系统漏洞,并及时对网络和服务器系统存在的漏洞进行防护,特别是近 2 年常见的 Struts2 高危漏洞,可以根据日志及时地制定防护策略;另一方面,发现用户终端的威胁,及时给予提醒和处理。

3　总结

本文提出的基于安全域的农业科研单位网络安全建设方案,在现有网络的基础上进行了安全升级,改造成本低,对网络和业务影响小,有效减少来自互联网和内部网络的安全威胁,整体提高了局域网的安全防护能力。但网络安全涉及技术和管理等许多方面,技术是手段,关键看管理,只有制定一系列的安全管理制度,并将其切实贯彻执行,才能确保网络安全。

参考文献:

[1]2016 年中国互联网网络安全报告[EB/OL]. [2017 - 11 - 01]. http://www. cert. org. cn/publish/main/46/2017/2017052715122890 8822757/ 20170527151228908822757_. html.

[2]《中华人民共和国网络安全法》[EB/OL]. [2017 - 11 - 01]. http://www. npc. gov. cn/npc/xinwen/2016 - 11/07/content _ 2001605. htm.

[3]《中华人民共和国计算机信息系统安全保护条例》[EB/OL]. [2017 - 11 - 01]. http://www. gov. cn/gongbao/content/2011/content_1860849. htm.

[4]《计算机信息系统国际联网保密管理规定》[EB/OL]. [2017 - 11 - 01]. http://cpc. people. com. cn/n/2013/0316/c359051 - 20812039. html.

[5]信息安全技术. 信息系统安全等级保护体系框架:GA/T 708—2007[S]. 北京:公安部信息系统安全标准化技术委员会,2007.

[6]于慧龙. 如何进行大型信息系统的安全域划分和等级保护建设[J]. 网络安全技术与应用,2006(6):12 - 12.

[7]郭　睿,陈　涛. 安全域划分在企业中的实际应用研究[J]. 信息网络安全,2016(增刊 1):158 - 163.