论计算机网络的安全性设计

摘要:

我在中央银行某省分行信息技术部门工作，我单位与 1998 年建成与总行和县支行的连接的网络，并先后在内部网络上建设了 OA 系统，个人征信系统，2003 年建设支付结算等重要的资金类业务系统。这些系统均以网络为支撑，采取多类型客户机/服务器模式运行，并且各系统对于安全性要求不同，安全可靠性不同的应用运行在统一个网上，给黑客、病毒攻击提供了方面之门,给我单位的网络造成了极大的威胁。作为信息技术中心网络部的负责人，我在经过各方面的协调下，在得到领导的大力支持下，并获得了一定额度的资金的前提条件下，充分利用成熟技术，对我单位及其我省的网络进行了全方面细致的规划，使得改造后的网络大大提高的它的安全性。本文将阐述就我在网络安全方面采取的方法和策略。主要有网络边界防火墙技术、入侵检测技术、防病毒技术、交换机技术、集中网络管理。由于资金投入不足，我的单位的网络还存在一些问题和不足，并且提出改进的办法。

正文

我在中央银行某省分行信息技术中心工作，我单位与 1998 年建成向上连接到总行，向下连接到各市县的县级支行的网络。随着信息技术的不断发展，我单位的信息化建设程度不断提高，建设以办公自动化系统（OA）为中心，附带电子邮件、即时消息系统、公文传输、门户网站等办公系统，同时我单位又是央行的基层单位，负责解决本省各家金融机构跨行资金清算实时清算的问题，建设一套加快资金运转的系统—同城清算系统，还有总行推行的全国支付清算系统，是为全国跨省、跨行进行资金实时清算的系统。随着业务需求的不断增加，银行信息系统对网络的依赖程度越来越高，网络的安全问题不断的暴露出来。网络安全遵循与木桶原则，也就是网络的安全性决定于最低的那块木板。不同的业务系统运行在同一个网络上，网络安全程度就可想而知了，这就会为黑客、病毒攻击提供了方便之门。

我作为网络部的负责人，系统安全一致是困扰我的一个话题。特别是随着办公自动化系统，同城清算系统，大、小额支付系统、个人征信系统、企业征信系统的上线，网络安全问

题显得尤为突出，到了非解决不可的时候。与 2005 年我与相关部门沟通、交流，并且得到了领导的理解和大力的支持。在一定的资金支持下，我在网络安全可以容忍的程度上和建设成本上之间作出了取舍。充分使用现有的成熟的技术，并且极大的发挥管理的功效，提高了我省网络的安全，为业务系统的安全、稳定运行保驾护航。我采用了以下技术和策略提高网络的安全性。一、利用交换机技术的 vlan 技术依据业务需求划分的办公虚拟子网、清算系统虚拟子网、征信虚拟子网等。二、在边界架设防火墙，进行访问控制、端口限制。三、多角度的防止病毒入侵。四、制定网络安全管理办法，建立集中网络安全管理。

一、网络安全隔离

为了达到各业务系统不互相干扰，最好的办法是对网络进行隔离，隔离有两种方式，一种是物理隔离，一种是逻辑隔离。物理隔离是最安全的网络隔离方式，但是他的建设成本非常大，不仅要在网络设备、终端设备上进行重复投资，而且还要在网络线路上花费较大的投资。而逻辑隔离可以减少成本投入，但是它的安全级别就会降低。所以综合考虑我采用逻辑隔离的方式进行网络隔离，正对不同业务的不同需求和各业务的性质，划分不同的虚拟子网。我在分行的机关的局域网部署了两台 cisco6509 交换机作为局域网的核心设备，并利用交换机技术-VLAN 技术，根据目前的业务系统的需求，划分了不同的虚拟子网进行网络隔离。为 OA 系统的服务器及其所以的客户端划分了 OA 虚拟子网，由于客户端的数量较多，我设置了两个 OA 虚拟子网，使用了两个 C 类的地址；为征信类系统的及其客户端划分 zhengxin 虚拟子网，因使用该系统的人数较少，使用了一个 C 类地址的前 60 个地址；为资金类业务系统划分了 zijin 虚拟子网。并且利用交换机的访问控制技术严格控制访问的权限。最终这几个虚拟子网不能相互访问，达到提高网络安全性，保护重要业务系统。

二、多角度的防病毒体系

随着技术的更新、发展，系统漏洞似乎永远也补不完全，病毒已到了无处不在， 无时不在的处境。严重影响网络安全和系统安全，小则可以毁掉一个系统，大则使得网络瘫痪、机密信息泄漏、重要业务系统不能提高正常服务，在社会中造成不良影响。因而首先经过测试、调研在我省系统内部建立一套企业版的 symantec 防病毒系统，取代单机版的防病毒软件，而且能够保证实时更新病毒代码，这就提高了网络杀毒能力。其次，防病毒软件是被动

肯定无力防范，而且不能防止针对系统漏洞的攻击。我采用了两种策略提高主动防范的能力。

1.我依靠成熟的广域网路由器上建立一个策略禁止访问常见病毒攻击端口，并且把它应用到广域网出口上，防止病毒入侵。实践证明在查看策略表时会发现有较多的被拦截的数据包。

2.在核心交换机上，依据业务数据的数据流流向建立了一系列的访问控制列表，就是把应该或必须访问的客户端对服务器的访问放开，其它客户端一概被策略拒绝访问。3 由于我省大多数计算机是 windows 系列的操作系统，所以综合考虑在网络上建设一套 landesk 补丁分发系统，解决为 windows 自动安全补丁程序的问题。进一步提高的计算机安全性，当然也提高了网络的安全性。

三、在网络边界采取安全访问控制机制

我单位作为中央银行的基层单位要通过与各家金融机构、企业、事业单位和相关政府提供金融服务，所以在建网初期使用一台 cisco3662 的路由器与各家机构互联，并且通过 NAT 进行地址转换来提供服务。但是随着个人征信系统、企业征信系统，和大、下额现代化支付等系统的正式上线，这种简单的网络构架已不能满足网络的安全性需求。此次工程中购置了两台 cisco7304 路由器和两台中软华泰 2000 型防火墙建设金融同城市网络，就是我行通过此网络为各家机构提供的金融服务。经过详细的调查研究，我行对外提供服务系统都是通过防火墙进行地址转换，转换为虚地址提供访问，同时其他机构数据通过防火墙时要进行双向地址的端口映射，也就是说只有规定的 IP 地址能够访问指定的那个 IP 地址的指定的端口，其它 IP 地址或者端口不能被访问。事实证明该策略恰当有效，保证了系统安全。

四、 集中网络安全管理

由于我省县级机构较多，而且没有统一的管理平台，所以在网络安全管理上较混乱，管理不善其本身就有增加非常多的人为安全隐患。我组织了全省的网络管理人员一起认真学习了相关的网络安全管理制度、成功的企业网络管理案例等后，仔细讨论研究拟定了适合我省的网络安全管理制度。当然，只是依靠制度，没有先进的技术是不能把网络管理起来的。所以在全省统一建立一套网络管理平台，统一监控平台。把网络系统平台由原先的被动管理转向主动管理，被动处理故障转变为主动故障预警。使得制度通过网络管理平台得以具体体现，管理平台使得制度被严格的执行起来。

总之，在工程实施完成后网络的安全性得到很大的提升，得到了各方面的认可。但是同时也发现了一些不足之处需要改进。

一、在核心交换机中部署的业务系统的访问控制列表，只是具体到了 IP 级控制，没有具体到端口，这就为合法访问的 IP 地址提供了非法攻击的可能。

二、在接入层交换机中对于重要的业务系统服务器采取 MAC 地址+IP 地址+交换机端口进行绑定。可以有效的阻止 ARP 等病毒的攻击。

三、在部署了入侵检系统后，因该考虑使用与防火墙联动起来，阻拦外部入侵。

四、在各单位的网络出口上也要部署防火墙系统，并且与入侵检测系统联动，可以有效制止来自内部的非法入侵行为。