省级气象通信网络安全改造探讨①

黄 志，高钰杰，林 晖

(广西区气象信息中心，南宁 530022)

摘 要：互联网技术的不断发展，随之而来的网络安全问题也变得越来越突出。广西气象局网络虽已运行多年，但在网络安全方面一直缺少系统的防御和管理；因此，进行网络安全的规划设计与升级就显得十分迫切。分析了广西气象局网络现状结构，依照现行网络全设计的总体规划，结合目前网络安全的主流手段和设计思路，设计了一个较完整的、多层次的本局网络安全升级改造方案。

关键词：网络安全；应用控制网关；防火墙；入侵检测；终端准入；安全管理

Improving Provincial Meteorological Telecommunication Network

HUANG Zhi, GAO Yu-Jie, LIN Hui

(Guangxi Zhuang Meteorological Information Center, Nanning 530022, China)

Abstract: With the development of Internet, the security of network is more and more concerned. Guangxi weather bureau has lacked network system defence and management for years. Therefore, it is essential and urgent to reprogram network and upgrade the ability of defence system. This article analyzes the structure of the Guangxi weather bureau internet, in accordance with the current overall planning of the network design, which integrates with the General technology of the network security and way of design. It is available to build a more complete and Multi-level project to reform and upgrade the network security.

Key words: network security; application controling gateway; firewall; intrusion detection; terminal access; security management

1 网络现状分析

广西气象局在 2005 年对其网络宽带改造升级设计之初，只考虑了其上到国家局与下至地市的相互兼容互通，并没有考虑随之而来的一系列安全问题 ；随着互联网、本局数据传输业务与视频会议等网络多媒体业务迅速发展，网络病毒泛滥、黑客攻击等事情日益增多，网络安全形势越来越严峻。网络信息化发展催生出很多的应用，如 BT、迅雷、网络电视等应用，这些应用不仅降低了办公效率，同时也浪费了网络带宽。所谓“病从口入”，网络的安全需要对各个“口”进行安全防护，常见的“口”包括终 Internet 出口、端 PC、广域网出口等，通过对当前网络结构的分析，存在以下问题待解决。下图 1 显示了广西气象局当前的网络结构。

1.1 外网 Internet 出口

由于当前物理设备无法做到对基于 internet 多种应用进行带宽规划与管理，使得用户时常感到访问网络速率较慢；面向 Internet 的门户网站与 WEB 服务器仍然部署在内网的 DMZ 域中（详见下图），所有访问 WEB 服务器的请求都会直接进入内网，而 WEB 服务器是黑客常见的攻击对象，无形中加剧了内网的安全隐患；当前出口只部署了防火墙，而防火墙的防御能力只定位在 OSI 七层架构中的 2-4 层的基础病毒和攻击，而 4-7 层的病毒和攻击却无能为力，如常见的网页篡改、病毒、七层 DDoS 攻击等。一旦攻击穿透防火墙，内网将直接承受安全压力。

① 收稿时间:2011-05-16;收到修改稿时间:2011-06-08

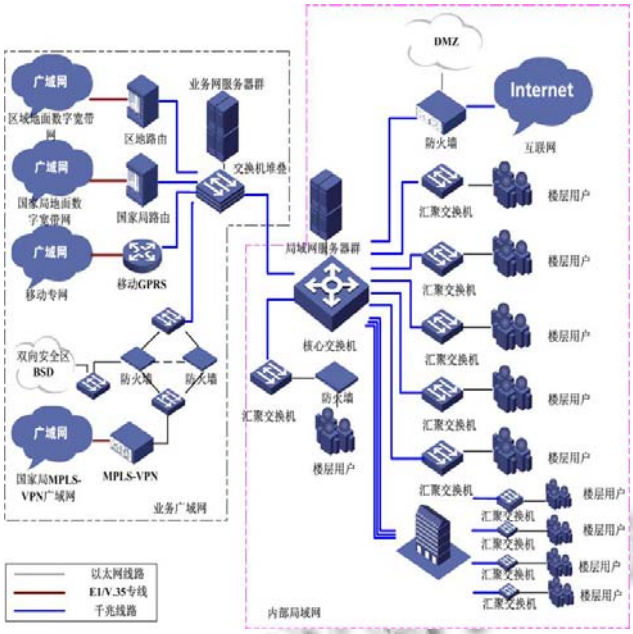

图 1　广西气象局当前的网络结构

1.2 内网 PC 终端

职工随意安装各种软件(如 BT、迅雷、网络电视等)，这些软件在上班期间使用不当不仅导致各种资源（PC、网络等）的严重浪费，同时浪费了大量的人力成本，极大影响了工作效率。与此同时，一旦出现攻击（如常见的 ARP 攻击）或病毒，网络无法有效应对病毒的攻击，且源头的定位也较为困难；给网络管理员的日常网络维护带来了极大困难，严重影响了业务的正常进行。

由于缺少系统服务器和终端杀毒管理软件，病毒日益泛滥，员工经常无意将带有病毒的 U 盘插入工作用的终端，导致病毒在内网扩散；无法排除非法设备访问内网资源。由于没有认证机制，员工可以肆意携带电脑，通过网线接入内网，从而非法访问内网资源；

1.3 广域网出口

虽然级联至国家局的 MPLS-VPN 广域网出口配备防火墙，保障 OSI 的 2-4 层的安全防护，但是对联至区内各个地市和国家局地面数字宽带网的广域网出口却无任何安全防护设备，一旦地市 PC 终端感染病毒，很容易就会穿过广域网接口扩散至区内网。

1.4 关键业务安全防护

各个地市都会访问部署在交换机堆叠的业务网络服务器群，作为关键业务，前端没有安全防护设备，特别是日益兴盛的应用层病毒和攻击；而部署在核心交换机的局域网服务器群上都是我局最关键的核心业务，其安全可靠性更是不言而喻，然而前端仍然无安全防护策略。

1.5 其他

网络平台缺乏智能化管理，无业务识别能力，不能对关键业务应用提供端到端的高质量数据传输的有效保证，通常采用的设备升级、链路带宽升级等简单方式使得网络建设、运营、管理成本大幅度上升，而网络资源的利用率却在大幅度下降；设备、业务和用户缺乏一个统一的管理平台。所有的维护工作都是逐台设备进行配置维护，工作压力很大。

2 可采取的安全控制策略

2.1 硬件安全策略

硬件安全是网络安全最重要的部分,要保证网络正常,首先要保证硬件能够正常使用。通常情况下可采取的措施主要有:减少自然灾害(如火灾、水灾、地震等)对计算机硬件及软件资源的破坏,减少外界环境(如温度、湿度、灰尘、供电系统、外界强电磁干扰等)对网络信息系统运行可靠性造成的不良影响[2]。

2.2 访问控制策略

访问控制方面的策略任务是保证网络资源不被非法使用或访问。包括入侵监测控制策略、服务器访问控制策略、防火墙控制策略等多个方面的内容。

2.2.1 防火墙控制策略

防火墙控制策略维护网络安全最重要的手段。防火墙是具有网络安全功能的路由器,对网络提供的服务和访问定义,并实现更大的安全策略。它通常用来保护内部网络不受来自外部的非法或非授权侵入的逻辑装置[1]。

2.2.2 入侵监测控制策略

入侵监测控制策略就是使用入侵监测系统对网络进行监测。入侵检测系统(Intrusion Detection Systems)专业上讲就是依照一定的安全策略,对网络、系统的运行状况进行监视,尽可能发现各种攻击企图、攻击行为或者攻击结果,以保证网络系统资源的机密性、完整性和可用性。

2.2.3 服务器访问控制策略

服务器和路由器这样的网络基础设备,避免非法入侵的有效方法是去掉不必要的网络访问,在所需要的网络访问周围建立访问控制。另外对用户和账户进

行必要的权限设置。一是要限制数据库管理员用户的数量和给用户授予其所需要的最小权限。二是取消默认账户不需要的权限选择合适的账户连接到数据库。

2.3 病毒防护策略

病毒主要由数据破坏和删除、后门攻击、拒绝服务、垃圾邮件传播几种方式的对网络进行传播和破坏,照成线路堵塞和数据丢失损毁。那么建立统一的整体网络病毒防范体系是对校园网络整体有效防护的解决办法。

2.4 不良信息的防护策略

Internet 上存在大量的不良信息,网络因为 Internet 连接,员工有可能无意中接触这些信息而在内网进行传播,造成恶劣的影响。可以安装非法信息过滤系统,设置非法 IP 过滤和非法字段过滤有效屏蔽 Internet 上的不良信息。

2.5 建立安全评估策略

网络安全不能仅仅依靠防火墙和其他网络安全技术,而需要仔细考虑系统的安全需求,建立相应的管理制度,并将各种安全技术与管理手段结合在一起,才能生成一个高效、通用、安全的网络系统。使用安全评估工具是进行安全评估的一种手段,可以对各方面进行检测和反馈信息收集,进而制定策略。

3 网络安全升级改造原则

经过调研协商，我局网络安全改造应遵循如下原则。

3.1 以需求为导向，统一规划原则

网络安全拟改造成一个高效的树形拓扑结构，满足网络管理数据对高性能、高可靠性的要求。

3.2 高可靠性、兼容性原则

网络安全必须采用具有高可靠性的总体设计，采用相对成熟的技术和设备。同时为确保线路畅通，建议设计网络拓扑时，每个节点考虑线路冗余。

3.3 前瞻性、经济性原则

在充分考虑此次网络安全改造设计带宽、使用技术、设备选型要满足未来几年信息化发展趋势时，在满足网络通信需求和确保网络正常运行的条件下，尽可能降低网络的安全改造成本和运行费用。

3.4 流量合理分布传输时延最小原则

要充分利用所有的网络线路资源和设备资源，避免出现某些设备负载过重或是载过轻，某些线路过于拥挤或是路空闲的情况。尽可能减少网络节点间的数据传输时延，避免传输经过不必要的节点数，保障网管数据的快速转发[3]。

4 网络改造升级方案

综上所述，经过调研讨论，广西气象局网络安全改造升级之后的网络拓扑应如下图 2 所示，具体改造升级分为以下几个方面进行：

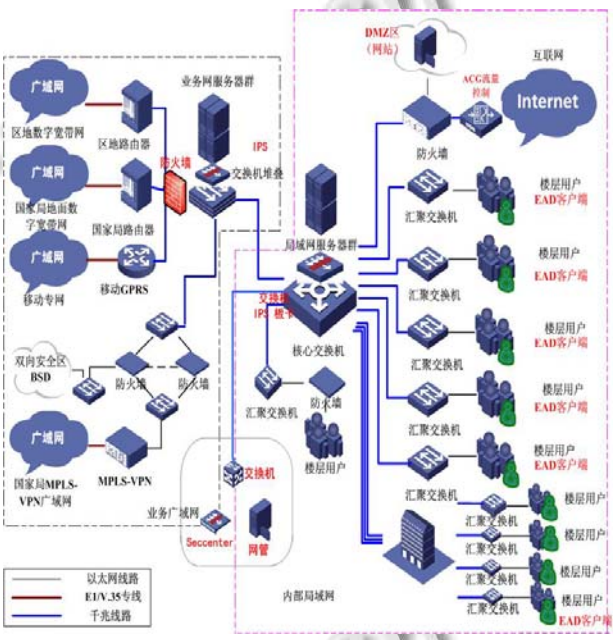

图 2 网络安全改造升级后拓扑图

4.1 外网 Internet 出口

在 Internet 出口部署 ACG（应用控制网关）[4]。此高性能应用控制网关，能对网络中的 P2P/IM 带宽滥用、网络游戏、炒股、网络视频、网络多媒体、非法网站访问等行为进行精细化识别和控制，保障网络关键应用和服务的带宽，对网络流量、用户上网行为进行深入分析与全面的审计，进而帮助用户全面了解网络应用模型和流量趋势，优化其带宽资源，开展各项业务提供有力的支撑。

而对于向 Internet 提供的服务（WEB）的服务器放置在防火墙的 DMZ 区域；根据当前的网络结构，防火墙直接连接至核心交换机，而且各个接入交换机也直接接入核心交换机，在核心交换机上部署 IPS（入侵防御系统）插卡，从而实现对所以经过核心交换机的数据进行 4-7 层的安全过滤。

4.2 内网 PC 终端

在用户的 PC 终端部署 EAD（终端准入系统）。EAD 安全策略组件（EAD，End user Admission Domination）[4]从控制用户终端安全接入网络的角度入手，整合网络接入控制与终端安全产品，通过 iNode 智能客户端、EAD 安全策略服务器、IMC 智能管理平台平台、网络设备以及第三方软件的配合和联动，对接入网络的用户终端强制实施企业安全策略，严格控制终端用户的网络使用行为；同时在管理上，又能做到用户管理与网络设备管理、网络拓扑管理的融合，使得内网 PC 终端准入控制解决方案在有效加强用户终端主动防御能力的基础上，为企业网络管理人员更提供了有效、易用、强大的管理工具和手段[4]。

4.3 广域网出口

综合部署位置、性能及功能要求，可以将各个地市和国家局地面数字宽带网的广域网出口先连接至中档防火墙[4]，而后通过防火墙连接至区气象局内网，从而保证广域出口的 OSI2-4 层的安全防护。

4.4 关键业务安全防护

各个地市访问部署在外联区的业务网服务器群，为抵挡日益兴盛的应用层病毒和攻击，在这些业务服务器群前段应部署 OSI 的 4-7 层的安全防御设备。考虑到其访问量不是很大，可以考虑安装集入侵防御与检测、病毒过滤、带宽管理和 URL 过滤等功能与一体的 IPS（Intrusion Prevention System[4]入侵防御系统,通过深入到 7 层的分析与检测，实时阻断网络流量中隐藏的病毒、蠕虫、木马、间谍软件、网页篡改等攻击和恶意行为，实现对网络应用、网络基础设施和网络性能的全面保护。而区气象局作为全网的核心，承载着所有业务的转发，因此在核心交换机上部署 IPS 插卡，实现对所有经过核心交换机的业务数据进行安全过滤，包括局域网服务器群的核心业务。

4.5 其他

为实现对整网安全设备进行统一管理，更重要的是实现对所有安全设备的安全信息进行统计和处理，可以部署安全管理中心 SecCenter[4]。SecCenter 基于先进的深度挖掘及分析技术，集安全事件收集、分析、响应等功能为一体，解决了网络与安全设备相互孤立、网络安全状况不直观、安全事件响应慢、网络故障定位困难等问题，使 IT 及安全管理员脱离繁琐的管理工作，极大提高工作效率，能够集中精力关注核心业务。

综合上述，本网络经上述措施改进之后，便可初步形成外防内堵，集防护、监测、响应、修复等多种技术于一体的的安全网络。对于外网，它以防火墙为网络安全的第一道屏障，兼以流量控制，过滤不安全的网络服务从而降低风险并使网络能够带宽均衡；对于内网，通过设定 IPS 的安全策略，对流经的每个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析、事件关联分析等），一旦发现隐藏于其中的网络攻击，可以根据该攻击的威胁级别立即采取抵御措施，这些措施包括（按照处理力度）：向管理中心告警；丢弃该报文；切断此次应用会话；切断此次 TCP 连接等，并配合安全管理中心 SecCenter，使得网络管理员能够第一时间解决网络当前隐患，防患于未然。

5 结语

随着互联网技术不断发展和我局业务的不断拓展，网络的安全性越来越受到重视,网络环境的复杂性、多变性,以及信息系统的脆弱性,决定了网络不能仅仅依靠防火墙,还涉及到管理和技术等方方面面,需要仔细考虑系统的安全需求,建立相应的管理制度,并将各种安全技术与管理手段结合在一起,才能生成一个高效、通用、安全的业务系统网络。

参考文献

1 王秋华.网络安全体系结构的设计与实现.杭州电子科技大学学报,2005,5.

2 李鹏.王纪凤,尚玉莲等.防火墙与入侵监测系统在高校校园网中的应用.泰山医学院学报,2007,(11):906–907.

3 朱超军.浅析网络安全方案的设计.福建电脑,2010.

4 http://www.h3c.com.cn.