李军．地市级气象通信网络拓扑演变和网络安全实践[J]．陕西气象，2023(6)：55-58.
文章编号：1006-4354(2023)06-0055-04

地市级气象通信网络拓扑演变和网络安全实践

李　军
（西安市气象局，西安　710016）

摘　要：近年来，随着西安气象事业的发展，气象通信网络规模迅速扩张，网络安全建设亟待加强。以西安市气象局气象通信网络为例，介绍了多部门、多种业务、覆盖范围大的气象通信网络如何在实际业务运行中进行组网和资源规划，以及网络安全建设工作，以期为气象部门网络规划和信息化建设提供借鉴。

关键词：网络拓扑；网络安全；防火墙
中图分类号：TP393.08　　**文献标识码**：A

信息高效处理和及时传输在气象业务中扮演着非常重要的作用。随着大数据、云计算、虚拟化等新技术在气象信息化进程中的不断融合发展，气象部门与各相关部门的联系日渐紧密，气象通信网络呈现迅速扩张的趋势，网络安全问题凸显。优化设计和改造气象信息网络系统，不断加强网络安全建设，才能适应现代气象业务发展，保障气象业务高效、稳定运行。

1　西安市气象局通信网络现状

2014 年，西安市气象局建立了全新的气象通信网络（见图 1）。气象局域网采用二层扁平化架构，构建了万兆骨干、千兆接入、双光纤冗余架构的网络传输系统[1]，采用两台高性能企业级三层交换机作为核心交换机，双机热备，进行局域网数据交换。西安市气象局与陕西省气象局及西安市各区（县）气象局之间的广域网系统均采用双设备（两台边界路由器）、双链路（中国电信、陕西广电）互联，进行气象数据传输。两台边界路由器上运行虚拟路由器冗余协议[2]，实现路由热备份和线路故障时自动切换。建立了覆盖整个业务大楼的无线局域网，在大楼布设无线 AP、无线控制器以及无线网络安全管理等相关软硬件设备。互联网百兆专线接入，政务网千兆专线接入，在网络边界部署一台天融信防火墙实现气象网、政务网和互联网之间的访问控制和安全防护。

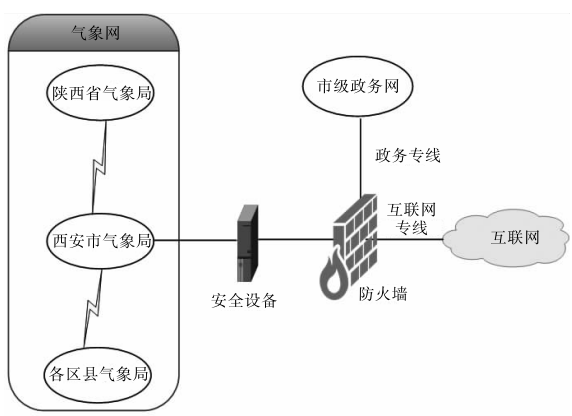

图 1　西安市气象局网络拓扑结构

网络安全建设方面，除了基本的防火墙之外，同时在防火墙和核心网络之间串接深信服入侵防御系统、绿盟上网行为管理系统，防范互联网对内网的恶意入侵，并管控内网用户互联网行为。在服务器区域之前部署网页防篡改系统保证对内部 web 服务的安全访问[3]。另外，在互联网接入处

收稿日期：2022-12-15
作者简介：李军（1980—），男，汉族，陕西高陵人，硕士，工程师，主要从事气象通信网络规划、数据库建设、新型气象探测设备观测技术研究。
基金项目：陕西省大气探测技术保障中心自立科研项目（2020S-8）

旁路接入深信服 SSL VPN 网关，以便外出人员远程办公。可将这一拓扑概括为单防火墙的网络架构。

此网络自 2015 年投入使用后，负载了所有的业务系统和办公应用，包括省市县高清视频天气会商、台站实景监控系统、曙光高性能计算机集群以及视频连线等，显著提高了主要业务系统(CMACast 卫星广播系统、天气会商系统)的运行稳定性和网内主机的桌面访问速度。

2 西安市气象局通信网络存在的问题

近年内，气象业务急剧增长，同外部门的合作进一步加强，数据互访互传激增。网络负载和规模迅速扩张，具体表现在以下四个方面。

(1)2019 年接入政务网专线，与西安交通广播电台、西安市秦岭生态环境保护管理局网络对接，跨部门系统互访，大容量数据交换(如西安市雪亮工程、视频会议)成为常态化。在网络运行保障中，每一次专线接入都需要网络结构的调整[4-5]。以“雪亮工程”为例，通过部署基于网络传输的高清视频系统，可访问全市 6 万个点位的全景实时视频，系统初次对接气象网络后视频卡顿严重。经过排查分析发现，网络瓶颈在防火墙硬件设备上，天融信防火墙因使用年限过长，包转发速率已经无法满足实时高清视频传输要求[5]。更换防火墙之后，视频传输质量有明显改善，但仍然有卡顿出现。进一步排查分析发现，大容量视频数据在局域网上传输，存在和其他应用抢占带宽资源的现象，表现为视频流不稳定，有时出现“慢动作”和系统宕机的情况，对其他大流量业务也有影响。

(2)2020 年之后接入西安超算中心专线、网络存储器。因为模式运算数据体量大，需要在外网(西安超算中心)和内网(气象台高性能计算机)之间频繁传输中间数据，骨干网和防火墙之间的传输负载过大，为充分保障业务，减轻网络传输和设备负载，对数据进行分流处理势在必行。

(3)2021 年引进网络存储器(network attached storage，NAS)、ZStack 超融合专有云平台对接西安超算中心网络，系统之间频繁进行的大容量数据交互传输造成骨干网数据吞吐量剧增。

(4)2022 年远距离相控阵雷达系统的建成使得物理范围本局限于西安市气象局业务楼内的气象局域网拓展成为城域网。随着进行短时临近监测的 7 部相控阵雷达陆续接入西安市气象局网络，网络物理范围不再局限于业务大楼，而是延伸成为覆盖城乡、跨地区(渭南金堆集)的城域网。运营商专线成为局域网的组成部分。实践表明，原有的网络拓扑已经不能满足新业务的基本需求，改造势在必行。另一方面，信息化的快速推进在促进气象业务发展的同时，也带来了新的网络安全风险，网络安全建设亟待加强。

3 西安市气象局新的网络拓扑

2022 年基于数据分流和网络安全考虑，对原有的网络拓扑重新改造，形成了“双防火墙、双互联网出口”架构(图 2)。

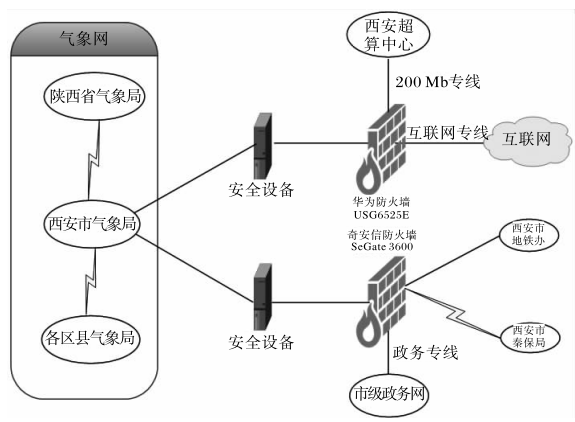

图 2 西安市气象局新的网络拓扑

新的网络拓扑通过在网络边界部署两台防火墙设备，将进出西安市气象局内网的流量分成两路进行传输，并进行负载均衡配置，实现数据分流。实践证明，这一改造确保了雪亮工程、模式计算等大流量业务的流畅运行，有效解决了新业务剧增带来的网络传输瓶颈问题，进一步发挥了双核心骨干万兆网络的性能。与改造之前相比，核心交换机资源和内存使用率从 60%下降至 20%左右，恢复到低位运行，明显降低了网络设备压力。

目前途经两路防火墙的主要业务和专线连接拓扑包括：(1)通过华为防火墙进行的超算中心模式运算、互联网访问、西安市气象自动站数据回

传。(2)通过奇安信防火墙进行的雪亮工程、西安市地铁办、政府相关部门与市气象局的数据交互。改造体现了网络设计的高性能原则,为系统的扩容留下了空间,可满足未来数年西安市气象局业务的发展需求[6-7]。

4　西安市气象局网络安全建设

在网络拓扑改造的同时,参考近年来网络安全技术发展趋势以及气象部门网络安全实践经验,按照国家网络安全等级保护制度 2.0 标准进行网络安全设计布局[8],进一步加强了网络安全建设。

4.1　安全设备的部署

如前所述,除了在互联网、政务网之间架设两道防火墙之外,同时部署了深信服入侵防御系统、绿盟上网行为管理系统、网页防篡改三套硬件设备,以加强对跨网络流量的监控[9]。

2022 年,为进一步加强内网安全建设,除了原有的安全设备外,还在内网以旁路监听方式部署一套软硬件结合的深信服“安全态势感知系统”,该系统包含漏洞扫描(负责对全网设备、终端进行漏洞扫描,汇总扫描流量发送至安全感知平台)、威胁探针(负责对网络流量进行采集,分析潜在威胁,分析后的数据上传给安全感知平台)、日志审计(集中采集网络设备各种日志,以统一的形式集中存储,并对日志进行实时事件分析和审计分析,形成分析结果上传至安全感知平台)和安全感知。安全感知作为“安全态势感知系统”的大脑,集检测、可视、响应处置于一体。它汇总漏洞扫描、威胁探针和日志审计发来的立体数据,采用大数据关联分析、机器学习等技术,以可视化方式展现全网的资产、威胁和攻击、可疑流量等。“安全态势感知系统”的四个模块协同工作,对局域网内服务器、用户终端、网络设备等进行不间断扫描(漏洞、弱口令、病毒)和报警;四个模块能够联动,自动解决部分比较初级的安全问题,面对复杂问题(失陷主机、僵尸资产等)时,能够通过界面提供清楚的问题清单,以供管理人员进行人工处置。西安市气象局新的网络安全设备部署如图 3 所示。

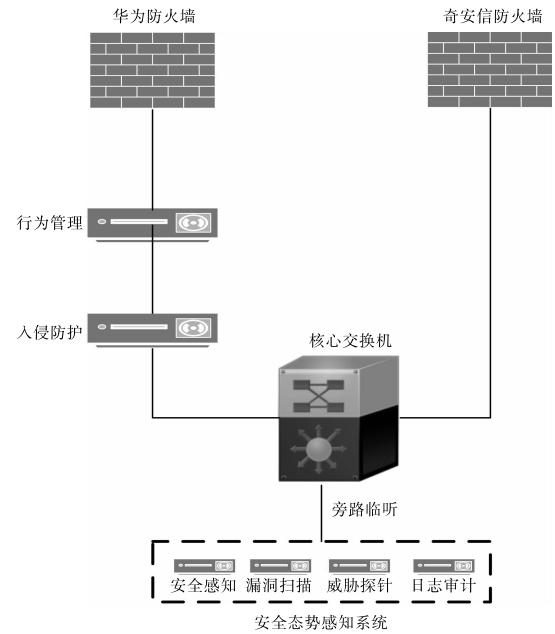

图 3　西安市气象局网络安全设备部署

第十四届全国运动会举办期间,安全态势感知系统在西安市气象局网络中检测出 10 台风险主机,主要的风险包括病毒、下载恶意文件、黑客工具、蠕虫病毒等。防火墙拦截外部攻击 420 次,涉及服务器 29 台。共处理安全事件 20 起,有效防护了网络安全。

4.2　网络权限的划分

一些基础性的技术仍然是非常有效的安全防护手段,针对楼层各单位现状,对局域网的 VLAN 划分了不同的访问权限。通过在核心交换机建立访问策略,禁止非必要网段访问服务器网段,禁止网络打印机配置网关,禁止无线局域网 WIFI 访问内网。通过安全态势感知平台检测发现,这些措施明显提升了网络安全性能。

4.3　网络安全管理规章制度的进一步完善

自 2009 年起,先后建立了《西安市气象局通信网络管理办法》、《网络科管理制度》《机房管理办法》、《网络安全管理制度》等,并不断进行细化。同时,制定系统安全技术措施,网络安全应急演练制度;对于各直属单位,每台计算机落实到人,安全责任到人,禁止各办公室私自搭建无线 WIFI。参与公安部、国省两级气象部门的网络安全演练,进一步提高网络安全意识和防范技能。

5 结语

西安市气象局新建网络无论是传输还是网络节点设备都具有充分的扩容能力，未来几年能够充分满足业务需求，但网络及安全建设方面仍有一些问题需要考虑：(1)当前网络局域网内预报模式计算数据传输量大，加之部分程序无节制抢占带宽资源，考虑可对预报模式系统建立独立的数据传输网络，以释放局域网带宽资源；(2)政府部门对气象数据产品需求日渐增大，充分利用现有政务专线为政府部门提供实时气象数据是未来需要解决的重点问题；(3)区县局业务主机是病毒的高发区，如何利用现有安全设备加强对区县局网络安全监管需要进一步探索。

参考文献：

[1] 王春虎．国家级气象高速骨干网络的系统设计[J]．应用气象学报，2002，13(5)：638-640.

[2] 李军，李光，邸永强，等．基于虚拟路由冗余协议和双向转发检测的基层气象通信网络设计和实现[J]．气象科技，2017，45(2)：381-384.

[3] 中华人民共和国国家互联网信息办公室．2019年我国互联网网络安全形势分析[R/OL]．(2016-02-05)[2022-11-25]．http://www.cac.gov.cn/2016-02/05/c_1118003198.htm.

[4] 燕东渭，杨艳，王垒．面向业务保障的省级气象广域网络优化升级[J]．气象科技，2015，43(2)：211-215.

[5] 徐慧洋，白杰，卢红旺．华为防火墙技术漫谈[M]．北京：人民邮电出版社，2015：12-15.

[6] LAMMLET. CCNA学习指南(640-802)(第7版)[M]．袁国忠，徐宏，译．北京：人民邮电出版社，2013：370-378.

[7] 郭晓佳，江彩英．市级气象专网网络管理与气象数据维护[J]．网络安全技术与应用，2020(11)：1-4.

[8] 曹玉静，谢博思，付硕，等．气象部门网络安全等保2.0建设浅析[J]．网络安全和信息化，2022(7)：140-143.

[9] 鲍磊磊，吴瑞涛，姜淑杨．地市级气象信息网络安全架构标准化设计研究[J]．网络安全技术与应用，2022(1)：103-105.