文章编号：1006-4354 (2012) 02-0036-02

GAP技术在气象信息安全中的应用

李招连，陈艺宏，张 磊
(漳州市气象局，福建漳州 363000)

摘 要：利用GAP（安全隔离网闸）技术物理隔离气象内网DMZ区，确保网络安全的基础上构建相应的信息交换机制，解决了内外网络间信息交换难的问题，从而保障气象信息安全。

关键词：气象信息安全；GAP技术；物理隔离；映射控制
中图分类号：P409 **文献标识码**：B

目前，气象内外网的信息交换量不断增多，气象信息安全保障至关重要。气象部门的网络架构若采用传统物理隔离卡技术，虽能确保网络安全，却因缺乏相应的信息交换机制，信息交换受限制；若采用防火墙技术，内外网间信息虽能实现交换，但安全功能相对单一，存在安全漏洞，黑客仍可渗透或旁路防火墙攻入内部网络[1]。应用GAP技术的内外网具有“隔而不离”的效果，既能确保气象网络安全，又能构建信息交换机制，解决网络间信息交换难的问题。

1 GAP技术简介

GAP（air gap）即安全隔离网闸，其通过专用硬件使两个或两个以上网络在不连通的情况下，实现安全数据传输和资源共享。GAP采用独特的硬件设计并集成多种软件防护策略，形成整体多层面安全防护，能够显著提高内网的安全强度。GAP技术的基本原理是由两套独立的系统连接安全（内网）和非安全网络（外网），两套系统间架构安全隔离网闸，保证安全网络连通时，断开与非安全网络连接；非安全网络连通时，断开与安全网络的连接，使用两套系统中的数据通路进行数据交换，达到隔离与交换的目的[2]。GAP技术数据交换流程为切断网络间通用协议连接；将数据包分解或重组为静态数据；对静态数据进行安全审查，包括网络协议检查和代码扫描等；确认后的安全数据流入内部单元；内部用户通过严格的身份认证机制获取所需数据。

2 GAP技术在气象网络中的应用

漳州气象局原有网络有SDH专网、移动MPLS网络及政务网组成的内部局域网，同时备有一条漳州市区域站采集传输系统宽带移动专线和电信所提供的10 MB光纤为主干的外网，原有网络通过部署防火墙来保障互联与安全。气象内部网络有极高的安全性和保密性要求，只在必要时允许访问外网，内外网信息的交换亟需安全保障。虽然气象局网络外网部署有防火墙设备提供安全保护，但仍存在一些问题：①防火墙重在保障数据互联互通，在保障数据的安全方面存在局限性，容易导致内网被黑客攻击；②内网数据未进行安全等级划分，重要网络数据未加强保护。

2.1 应用GAP技术的网络构架

针对存在问题，对信息网络进行升级改造：①在原有防火墙基础上部署了VIGAP安全隔离网闸对内网进行隔离保护；②内网按数据安全级别划分不同区域，加强内网重要数据的保障。VIGAP技术的应用为气象内网提供实时隔离保护，并在信息可控状态下实现内外网间实时、适度的信息交换。根据网络构架中数据安全级别，将气象内网划分为政务区和DMZ区(气象原始观测数据等)，形成外网、政务区和DMZ区三个不同安全等级的网络，DMZ区的安全由防火墙保护改为由VIGAP保护，加强DMZ区数据的保障[3]。如图1所示，

收稿日期：2011-05-16

作者简介：李招连（1985—），男，福建周宁人，学士，助理工程师，从事专业气象服务、气象网络维护。

漳州气象局网络架构由DMZ区、政务区、外网、交换机、防火墙和VIGAP安全隔离网闸组成，直接用网闸加强DMZ区安全保障。

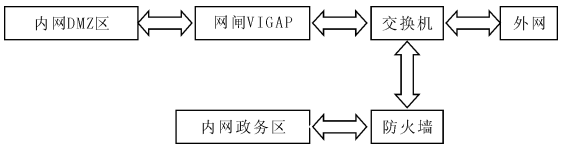

图1　漳州气象网络架构图

2.2　VIGAP的特点

采用的安全隔离与信息交换系统VIGAP 300（简称VIGAP）具有4特点。①采用电子开关通断技术。VIGAP包含硬件电子开关动作系统，使连接内网与外网的两组高速电子开关配合气象系统数据流分时“接通”、“断开”，实现信息网络间数据的安全交换。②采用反射GAP技术。VIGAP的内部反射GAP系统完全基于硬件体系，不依赖任何通信协议和操作系统服务，具有独立的硬件逻辑电路，通过独立的总线交换数据，实现网络间数据的高速交换。③采用基于权限和数字签名的身份鉴别技术。为了防止非法访问及篡改网络信息数据，加强身份验证与反拒认的模块，有效保证访问用户身份的合法性，中断假冒和未授权用户的访问，确保传输数据文件的完整性。④采用协议终止及分析技术。网络数据流经VIGAP时，数据在VIGAP设备计算机系统被处理，经协议终止、协议检查并剥离数据包装，剥离出的裸数据被反射GAP系统传送到另一方，并重新生成协议后送达目的地，彻底杜绝黑客利用协议对内网攻击，保证网络安全。

2.3　基于VIGAP的内外网信息交换

VIGAP安装于气象内网DMZ区与外网的连接通道上，实现气象内外网安全隔离，有效地保障气象内部重要信息的安全性，满足气象信息与外网数据交换时的安全要求。VIGAP是物理断开系统，在保证物理断开的基础上支持文件交换服务。VIGAP系统由两套独立工作的计算机系统和一套反射GAP系统组成，两套计算机系统分别是连接内网的可信网络端计算机（DMZ区）和连接政务区与外网的不可信网络端计算机，通过反射GAP系统相连，处理两个网络交换数据事务。

VIGAP系统控制平台的软件系统从逻辑上分为3部分：内部代理、外部代理以及传输控制软件。内部代理连接内网DMZ区，外部代理通过交换机连接政务区与外网，两者通过传输控制软件进行信息和数据交换，传输控制采用隔断网络连接的纯数据驱动交换，数据加载控制协议，进而保障网络安全。通过VIGAP系统控制平台的映射控制，设置内网DMZ区和政务区与外网的映射配置，同时采用VIGAP的LVDS总线和高速双开关体系结构，使气象信息内外网交换及网络安全的性能显著增强。VIGAP采用新一代反射GAP技术和协议终止技术，成功实现既保证内网DMZ区和政务区与外网的物理隔断，又保证两网络间的数据实时访问，防止针对网络层和OS层已知或未知的攻击。同时利用双主机工作模式，从物理隔离阻断潜在攻击的连接，包括一系列阻断特征，如没有协议、TCP/IP连接、包转发，只有文件“摆渡”，对固态介质只有读和写两个命令，保障其结果是无法攻击、入侵和破坏。

3　结语

安全隔离网闸技术不能取代现有的防火墙、IDS及VPN等主流安全技术，只有与这些安全技术相互结合，才能构建出安全强度更高、安全隐患和漏洞更少、风险更低的安全网络，最大限度地发挥GAP技术的隔离作用[4]。另外，还必须提高用户的网络安全意识，加大整体防范网络入侵和攻击的能力，并在此基础上形成一支高素质的气象网络安全管理队伍，及时正确地应对网络安全事件，才能从根本上解决气象内部网络面临的安全威胁和困扰，保障气象信息安全。

参考文献：

[1]　杜虹．电子政务中涉密网络建设有关问题的探讨[J]．信息安全与通信保密，2001（6）：20-22.

[2]　郑挺．网络安全隔离GAP技术探析[J]．中国新技术新产品，2010（10）：29.

[3]　王佳，孙鹏，陈晓宇．广东气象网络安全物理隔离方案[J]．广东气象，2006（3）：56-57.

[4]　李江峡．隔离网闸的现状与应用[J]．网络与信息安全，2005（18）：34-35.