Computer Science and Application 计算机科学与应用, 2022, 12(8), 2036-2040
Published Online August 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.128206

Hans汉斯

网闸在淄博市气象局网络安全架构中的应用

郭　旗，刘　芳，葛瑞婷，曾麒麟

山东省淄博市气象局，山东　淄博

收稿日期：2022年7月20日；录用日期：2022年8月19日；发布日期：2022年8月24日

摘　要

随着气象部门信息化水平的快速发展，终端、系统、应用等对信息网络的依赖性越来越高，网络环境的安全性尤其值得关注。如今网络安全形势之严峻，对气象部门的网络安全提出了更高的要求。本文主要分析了网闸在气象部门网络安全架构中的应用，网闸实现的内外网强逻辑隔离保障了淄博市气象局网络安全的同时，也满足了跨网数据交换、业务应用及办公需求。

关键词

气象，网络安全，网闸，安全隔离

Application of Network Gatekeeper in the Network Security Architecture of Zibo Meteorological Bureau

Qi Guo, Fang Liu, Ruiting Ge, Qilin Zeng

Zibo Meteorological Bureau, Zibo Shandong

Received: Jul. 20th, 2022; accepted: Aug. 19th, 2022; published: Aug. 24th, 2022

Abstract

With the rapid development of the information level of meteorological departments, terminals, systems, and applications have increasing dependence on information networks, and the security of network environment is particularly concerned. Nowadays, the network security situation is really severe, and it sets higher demands on the network security of meteorological departments. The article mainly analyzes the application of network gatekeeper in the network security architecture of meteorological departments, and the strong logical isolation between the meteorological network and the internet realized by the gatekeeper not only guarantees the network security

文章引用: 郭旗, 刘芳, 葛瑞婷, 曾麒麟. 网闸在淄博市气象局网络安全架构中的应用[J]. 计算机科学与应用, 2022, 12(8): 2036-2040. DOI: 10.12677/csa.2022.128206

of Zibo Meteorological Bureau, but also meets the need of cross-network data exchange, meteorological business application, and work.

Keywords

Meteorology, Network Security, Gatekeeper (GAP), Security Isolation

1. 引言

近年来，气象信息化和气象现代化的步伐不断加快，气象部门的业务系统与应用、办公系统以及对外服务手段等对信息网络的依赖程度大幅提高，随之而来网络安全议题的重要性日益显著。气象业务内网与互联网物理隔离的方式相对来说安全性更高，却难以满足日常业务和办公的需求。为了方便业务与办公，实现数据的跨网交换，同时又能满足网络安全防护的要求，本文引入了基于安全隔离网闸的强逻辑隔离方法，并已在淄博市气象局部署实施，该安全隔离技术相比于单纯通过防火墙进行内外网边界隔离的方法，进一步提高了网络安全性，保证了气象业务专网与电子政务外网之间数据信息交换的安全性和可靠性，同时保证了业务和办公效率。

2. 淄博市气象部门网络安全架构分析

当前淄博市气象局信息网络系统包括省－市－县气象业务内网与市电子政务外网，市级已取消与运营商直连的互联网，仅保留一个通过市大数据局接入的电子政务外网出口。市大数据局在电子政务外网域已经做过专门的边界安全防护，相较于运营商直连的互联网来说，安全级别提高了很多，不再是直接暴露在互联网上，且市级电子政务外网与政府及各部门之间是可以互访的，也可以访问省级电子政务外网上部署的业务，这些通过运营商直连的互联网是无法联通访问的。市电子政务外网的接入，既提高了气象部门外网层面的安全性，又满足了市县级的一些业务和工作需要，以及与政府各部门之间的业务和数据共享交换的需求。县级气象部门实行业务内网与电子政务外网、互联网物理隔离。气象业务内网中，市级承担着上联省局、下联区县局的关键节点角色，因此做好网间边界防护[1]，进一步防护可能从电子政务外网进入的攻击，至关重要。

淄博市气象局在进行网络改造之前，气象业务内网与市电子政务外网之间仅通过一台防火墙设备进行逻辑隔离，存在一定的安全风险。按照中国气象局的要求，市县级应实现业务内网与外网的物理隔离或强逻辑隔离，强逻辑隔离也就是使用相应的强逻辑隔离设备(网闸等)实现网络隔离。强逻辑隔离比逻辑隔离的安全性更高，同时能实现与逻辑隔离相接近的功能，具有数据交换方便等优点。

3. 网闸的基本功能特点与技术原理

网闸实现的安全隔离技术一般指两个或两个以上可路由的网络借助不可路由的协议来进行数据交换而达到隔离的目的。在保持内外网络有效隔离的基础上，网闸实现了两网间安全的、受控的数据交换[2] [3]。数据交换由发起方以客户机身份与网闸连接，网闸再以客户机身份与数据交换的另一方建立连接，实现数据交换。

3.1. 网闸的基本功能特点

网闸的具体功能特点包括以下几个方面。

1) 网间安全隔离。网闸采用多机系统结构，以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换。

2) 协议中断，信息落地。网闸的内/外端机是内/外网络各自通用协议(即 TCP/IP 协议)的终点，一方的网络协议不可向对方延伸。所有过往的应用层信息都从 TCP/IP 协议包中剥离，被还原为应用层信息。

3) 受控的信息交换。由网闸连接的内外网络之间，所有信息交换活动都在预先建立的有效安全通道上进行，这些协议通道借助严格的安全策略进行控制，因此能防范恶意攻击和敏感信息的泄漏。

4) 基于用户的访问控制。内外网络之间，只有合法用户的特定信息交换活动才允许通过。协议通道的建立、通信、断开，都是在严格的基于用户的访问控制之下进行的。

5) 防范各类攻击和信息泄漏。借助用户访问控制、安全协议通道的建立、安全策略的设定，网闸可以发现、过滤并阻塞各种已知和未知的攻击，特别是很多基于应用的攻击手段，例如 Web 脚本攻击、病毒和蠕虫等恶意代码，有效保护内部网络系统的安全性。与此同时，借助严格的内容控制，也可以防止内部敏感信息外泄。

6) 应用级的安全审计。借助预先设定的审计策略，网闸可以对所有信息交换过程中出现的问题进行审计记录，便于及时获知“谁在何时做了何事”。

综上所述，网闸一方面可以防止来自外部网络的恶意攻击，另一方面也能防止内部网络重要信息的泄漏，在保证安全性的前提下，最终实现了灵活的网间信息交换。

3.2. 网闸的技术原理

“2 + 1”系统架构的网闸，由内端机、外端机和数据迁移控制单元三部分组成。内端机和外端机具有独立的存储和运算单元，并具有独立总线。内外端机之间采用了具有互斥效果的数据迁移控制单元进行连接，数据迁移控制单元使用专用的私有协议与内外端机进行通信，且其驱动程序模块也是独立编写的，在这种情况下，即使有人试图通过代码分析破解一端机的接口，也无法通过控制单元攻击到另外一端机，也就无法攻击到另一端网络。“2 + 1”系统架构的网闸结构如图 1 所示。

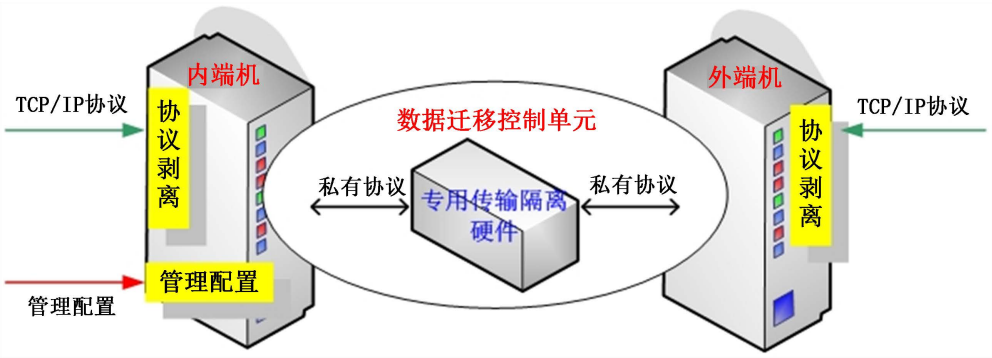

Figure 1. Diagram of the “2 + 1” system gatekeeper (GAP) structure
图 1. “2 + 1”系统架构的网闸结构图

内端机和外端机分别是内网和外网网络协议的终点。网闸的技术原理即所有过往的应用层数据都从内网和外网的 TCP/IP 协议中剥离，被剥离的数据再通过数据迁移控制单元在内外端机之间进行传输。内端机与外端机之间采用专用传输隔离硬件和专用协议相连，从而阻断了任何从一端机攻击另外一端机的

可能。以内端机到外端机方向为例，我们来说明“2 + 1”架构网闸的技术原理，即网闸内部信息处理的整个过程。内端机接受用户发来的连接请求后，将用户连接的基本信息与管理员配置的策略进行匹配，审查其来源，连接发起源是否为合法发起源。若是合法发起源，内端机接受连接发起源发来的信息，按照既定的协议通道进行应用协议的预处理，随后交由数据迁移控制单元的策略系统进行分析处理，如未发现问题，则通过控制单元将剥离出来的应用层数据交换到外端机。外端机在收到数据之后，将数据重新组成 TCP/IP 包，发送给目的服务器，并经过控制单元向内端机发送确认消息，这样一次数据交换工作即告结束。

4. 网闸在淄博市气象局网络架构中的部署

淄博市局在加入网闸进行网络改造之前，气象业务内网与电子政务外网之间通过防火墙进行逻辑隔离，理想情况是直接用网闸替代这台防火墙[4]，但考虑到气象业务对实时性要求极高，无法等待长时间的网络中断，而网络升级改造的复杂度又非常高，网闸正式上线运行必须经过长时间的调试，因此我们先把网闸的基础配置做好，并用测试机进行测试，同时保留经过防火墙的链路，确保业务和办公不受影响。

首先用一台终端连接网闸的管理口(MAN 口)，用默认地址和账户登录后，设置新的管理口地址和管理员账户，并将 PC 设置为与管理口同网段的地址，接下来就可以通过 Web 页面登录管理口地址进行相应的配置了。网闸没有桥接模式，而是代理的工作模式，内端和外端系统都必须分配 IP 地址。内端机用于设置网闸内端系统的 IP 地址，我们选定其中一个接口 GE0/0 设置为内网的地址，用于与内网交换机相连；外端机用于设置网闸外端系统的 IP 地址，选定其中一个接口 GE0/0 设置为电子政务外网的地址，用于与政务外网交换机相连。接下来进行路由设置，网闸路由分内端路由和外端路由。内端路由仅对内端系统生效，外端路由仅对外端系统生效。两边的路由协议不会贯通，也就不存在冲突或环的问题。网闸内部仅仅摆渡应用层数据，底层的任何协议都无法穿透过去。在路由配置中添加路由，分别设置好内外端机的目的子网、子网掩码、网卡和网关信息。

配置好路由之后，需要将内外网两端任何一类信息交换都置于特定的受控协议通道上，通道是网闸的基本策略，通过建立好的通道来实现协议信息交换功能。以内到外的访问为例，内网访问源(客户端)只能访问到网闸内端系统的 IP1，而外网服务端的地址 IP2 和端口 PORT2 对于内网访问源来说是路由不可达的，也是 TCP/IP 协议无法到达的。网闸通道，就是将外网服务端 IP2 和 PORT2 映射到内端系统 IP1 的某一个端口 PORT1 上，构成一对一的映射关系。当内网客户端访问 IP1 上的 PORT1 时，就好像在外网直接访问 IP2 上的 PORT2 服务一样。通道的开启和关闭均由管理员控制。受控通道开启后，内端机/外端机开始监听通道入口 IP 上指定的端口，控制单元上相应的协议分析部件开始运作，准备处理各种流经通道的协议数据信息。

在配置网闸通道之前，事先对需要访问的内网业务地址进行详细梳理，将访问具体到端口级别，便于在网闸上添加相应的通道。通道支持的应用类型有多种协议，包括 TCP、UDP、HTTP、FTP、SMTP 等，做通道配置时选择对应协议类型即可。以从外到内的访问为例，目的地址即为内网业务的 IP 地址，连接地址为网闸内端机的 IP 地址，监听地址则为网闸外端机的 IP 地址。有时一个网页应用可能不只有一个 IP 地址，其下面的子链接又变成了其他的地址，这种情况需要再一一添加子链接对应 IP 的通道。

通道添加完成后，测试通过网闸是否能实现业务访问，网闸正式上线后，我们将防火墙调整至电子政务外网入口与外网交换机之间，对防火墙和交换机的配置进行相应的调整，可对电子政务外网起到一定的防护隔离作用。在防火墙与外网交换机之间增加全网行为管理设备，配置上网访问策略，规范用户行为，对终端访问外网的行为进行记录，并设置 IP + Mac 地址的一一绑定，实行准入控制。部署网闸并

优化调整后的淄博市气象部门网络架构见图 2。

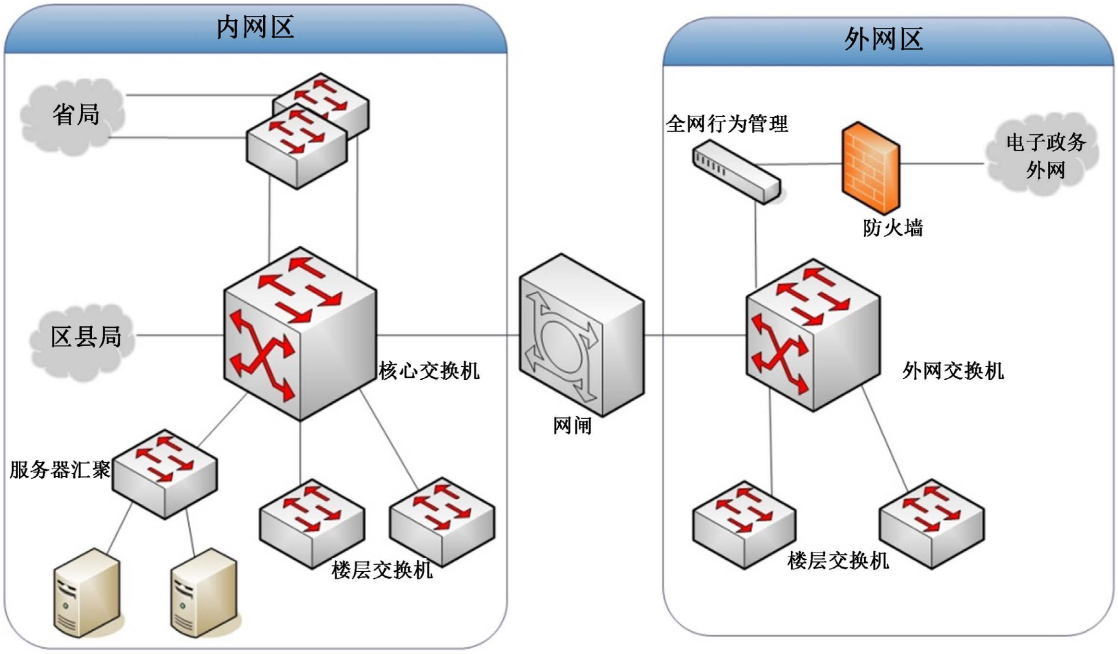

Figure 2. Diagram of the optimized network structure of Zibo Meteorological Bureau
图 2. 淄博市气象部门优化后的网络架构图

5. 结语

本文介绍了安全隔离网闸技术在淄博市气象部门网络安全架构中的部署应用，在保持气象业务内网与电子政务外网有效隔离的基础上，网闸实现了两网间安全的、受控的数据交换，配合外网边界部署的防火墙和全网行为管理设备，进一步优化了淄博市气象部门的网络安全架构，同时保障了数据的跨网交换和办公需求，为安全隔离网闸技术在气象部门及其他行业的推广应用提供了较高的参考价值。如今网络安全已成为一项值得长期关注的重要话题，各级气象部门应当充分利用网闸、防火墙等安全设备、安全隔离防护技术等，不断提升安全防护能力，才能更好地应对网络安全面临的各种挑战，进一步提高我国气象信息安全和信息化水平。

参考文献

[1] 李雪源, 李楠, 王坦帅, 宋波, 李慧. 聊城市气象局网络安全架构设计[J]. 网络安全技术与应用, 2021(8): 125-126.

[2] 谢丹, 林凯特, 郭晓佳. 市级气象网络边界安全防护系统的实现[J]. 福建电脑, 2020, 36(5): 96-98. https://doi.org/10.16707/j.cnki.fjpc.2020.05.033

[3] 盛梅, 冯志伟, 陈世春. 基于 GAP 技术的气象网络物理隔离方案的探讨[J]. 计算机安全, 2007(10): 81-82.

[4] 陈纯子, 李楠, 王允达. 网闸在气象数据跨网安全交换中的应用测试[J]. 信息系统工程, 2022(1): 73-76.