# 某自然资源局不动产登记系统政务外网数据交换建设方案

2020年8月

# 目录

# 1.建设需求分析

- 1.1 政策需求
- 根据自然资源和规划局不动产登记系统跨网迁移业务需求，自然资源部办公厅和省自然资源厅办公室发布了《关于完善信息平台网络运维环境推进不动产登记信息共享集成有关工作的通知》（自然资办函〔2019〕1041号）、《山东省自然资源厅办公室关于做好全省不动产登记“一网通办”便民服务平台建设和对接工作的通知》（鲁自然资办字〔2020〕5号），针对自然资源和规划局专网与电子政务外网的跨网信息交换做了指导规范。
- 自然资源局在与电子政务外网进行数据交互过程中，需按照国家信息安全等级保护三级重要信息系统技术标准和以上通知中的相关要求对软硬件及整体网络架构进行部署，确保自然资源局办公专网的网络安全。
- 按照《关于完善信息平台网络运维环境推进不动产登记信息共享集成有关工作的通知》（自然资办函〔2019〕1041号）的要求：“互联网与政务外网之间通过双向网闸、政务外网与业务内网之间通过单向网闸和离线摆渡方式实现数据互通”
- 按照《山东省自然资源厅办公室关于做好全省不动产登记“一网通办”便民服务平台建设和对接工作的通知》（鲁自然资办字〔2020〕5号）要求：“各地在开展不动产登记系统跨网迁移时，电子政务外网公共服务域与自然资源业务网之间应通过单向网闸和离线摆渡方式实现数据互通”

# 目前存在的问题和差距

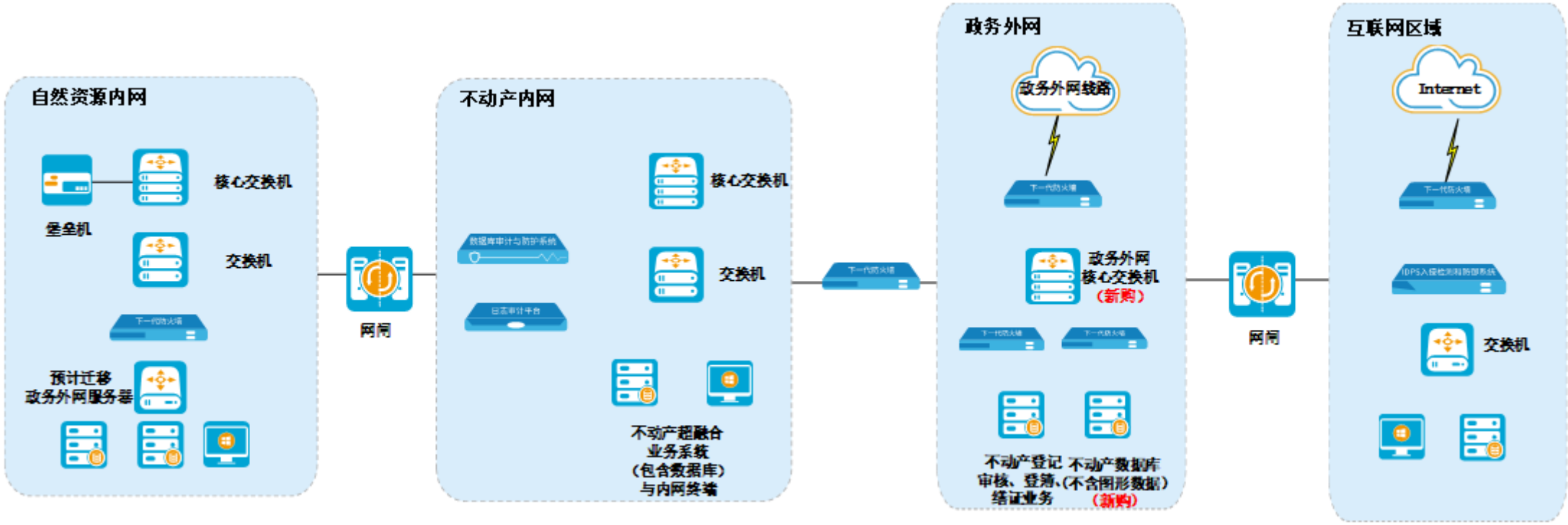
- 对外交互业务系统交互手段分散，安全防护不足
- 自然资源局专网内的业务系统与外部网络、互联网等进行交互的数量很多，但是都是各系统独立交互，没有统一的出口和安全审计检测手段，多数是直接与外部网络互联，中间没有安全防护，存在极大隐患。
- 已有安全防护基础设施陈旧，难以满足当前与未来的需要
- 现有的安全防护数量太少，且设施存在设施简陋、故障率高、功能简单以及安全防护体系不健全等问题，难以在此基础上增加新的安全防护策略，严重影响到自然资源局今后工作的开展。
- 对外数据交换不合规
- 现有自然资源局专网安全防护缺失，不满足国家等级保护的要求和网络安全法的要求，对外数据交换不满足当下标准的数据交互的要求。
- 因此建设规范的、安全的、易用的自然资源局与政务外网之间的数据交换平台，满足自然资源部的规范，通过该平台实现跨网数据交互，满足不动产登记业务系统的迫切需要，是现阶段自然资源局信息化建设的重要工作。

# 2.总体建设方案概述

- 2.1 方案总体概述
- 在完成不动产登记系统的业务迁移后，自然资源业务网（内网）中只保留“不动产权籍调查成果审核业务”以及不动产登记数据库（空间图形数据）两部分业务。“不动产登记审核、登簿、缮证业务”以及不动产登记数据库部署在政务外网的服务器中运行。
- 认真贯彻落实两项通知要求精神，严格按照信息系统安全等级保护建设的要求，在自然资源专网与市级电子政务外网的边界处，部署数据交换前后置机，单向光闸设备进行数据交换；在政务外网与互联网之间通过部署双向网闸进行数据交换。严格规范“跨网”数据交换的权限管控、网络访问行为细粒度管控、网络攻击行为管控保障不动产登记相关信息的网络安全性。
- 通过省“一网通办”平台，实现互联网申请、电子政务外网审核、自然资源业务网管理权籍信息的三网并行模式。

# 方案拓扑图

2.2 整体安全规划建设拓扑如图所示：



# 3.区域划分与部署设备描述

- 整个系统被分为自然资源业务网区、不动产内网、政务外网区、互联网区四个区域。
- 自然资源内网到不动产内网可以通过网闸来进行数据的交换。不动产内网与政务外网可以通过防火墙来实现隔离。
- 网闸对不同网络或信息系统之间所交换的数据进行应用层细颗粒度过滤和隔离摆渡，结合安全标记和可信增强模块技术对传输过程进行深层次的安全防护，确保相互之间所有数据的安全可靠。
- 网闸用于进行业务处理。可支持协议交换、文件同步、数据库同步以及视频业务处理。交换前置机作为业务的终结点，会对标准协议进行阻断，随后将数据进行打包，在通过单向隔离部件进行传输。在进行数据传输时，每一侧的互联前置，只使用一台单向光闸发送数据，用另一台单向光闸接受数据。从而保证信息以单向链路进行传输，确保同一链路上无反馈。

# 网闸

- 从最初的完全断开，到物理隔离，再到逻辑隔离，以及今天常讲的“安全隔离”（Security Isolation），安全隔离技术随着时代发展迅速演化。当前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，这与单机系统间的隔离是有所区别的。安全隔离产品务必要满足现实应用当中的安全需求，对于电子政务建设而言，在实践中总结提炼出来的政策性的要求更应该被严格遵守。正是这样一款产品，它从设计理念、功能实现等都紧密结合电子政务建设中的安全隔离需求。
- 基本功能主要体现在这些方面：在保持内外网络有效隔离的基础上，实现了两网间安全的、受控的数据交换。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。系统中的数据交换业务可以灵活配置和快速定制，数据交换可以单向也可以双向。除了必须要开放的用于数据交换的特定应用通道外，网闸不提供任何对外的服务。此外，独特的结构设计和所支持的双机热备功能，更在极大程度上保证了网络系统间信息交换的安全性和可靠性，增强了产品的竞争力。

# 堡垒机

- 智慧的运维风险管理的核心是通过利用新一代运维堡垒机技术，以一种更智慧的方法来改变运维人员和IT设备交互的方式，以便提高交互的安全性、合规性、效率、灵活性和响应速度。通过智慧的风险管理解决方案，使得风险管理设备与IT基础设施的完美结合，运维人员可以进行更高效的操作，做出更明智的决策，降低运维操作风险，提高企业工作效率，保障信息安全。
- 采用先进的面向服务的设计理念和消息机制，确保应用和系统的灵活性和稳定性。
- 采用为运维管理业务量身定制的NoSQL数据库，灵活高效、吞吐率高，在数据库的定制、升级和迁移过程中不需更改库表结构。
- 实现了高效的磁盘读写保护机制，采用多重数据内容保护措施，当进行数据库插入和更新操作，不需重建索引，并使用高效缓存机制，降低磁盘读写次数。
- 独创的虚拟网络服务机制，能够实现对单一端口的高效复用，使得设备对外只暴露单一端口，从而有效降低堡垒机的安全隐患。

- 是业界设备系统支持协议最全的堡垒机，支持的协议包括：
- 文本协议：Telnet、SSH、(S)FTP；图像协议：RDP、VNC、X11；Web协议：HTTP、HTTPS；数据库协议：Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix、MySQL；
- 应用协议：Weblogic、EMC、F5、Radware、VMware vSphere Client、ADS、NetApp、Symantec pcAnywhere。
- 具有业界最完备和安全的运维端到堡垒机的访问机制，采用强加密的SSL传输控制命令，完全避免可能存在的嗅探行为，确保数据传输安全。同时，产品还支持一次一密动态口令的认证方式。
- 能支持超长SQL查询语句（大于4K）识别，以及Telnet、SSH超长命令识别。
- 提供智能的设备凭证托管服务，可以在登录时自动填入已授权的设备账户凭证，并在受委托的情况下定期去修改账户凭证。通过大量地研究和分析各类系统登录和改密机制，使得产品可以自适应绝大部分系统，不需要定制相关脚本。
- 管理员事先将设备账号及其密码保存在堡垒机，运维人员登录堡垒机并经过认证授权后就可以直接访问目标设备，无须再次手工输入设备账号和密码信息，无须记忆多个设备账号和密码，实现真正意义上的单点登录（SSO），提高运维人员工作效率、改善用户体验

# 防火墙

- 载自主可控的防火墙系统，融合了丰富的网络特性，在满足IPv4/IPv6双协议栈的同时，配合智能路由和DDNS等，可在802.1Q、RIP、OSPF等各种复杂的网络环境中灵活组网；具备与第三方系统对接，数据共享，提升业务价值。产品具备优秀的适应性，适用各种复杂场景，更符合业务需要。
- 领先的多核架构及分布式搜索检测引擎，配合高性能的处理器，多业务并行处理，确保在各种大流量、复杂应用的环境下，仍能具备快速高效的业务处理和防护能力。
- 产品集防火墙、负载均衡、入侵防御、病毒过滤、应用识别、行为控制、VPN接入、业务可视、安全认证等功能于一体，为用户提供了一个灵活、高效、全面的网络解决方案。