——漏洞屏蔽系统——

说

明

书

2023 年 9 月

目录

1 产品发展背景 1

1.1 业务需求 1

2 产品介绍 1

2.1 市场定位 2

2.2 目标客户群体 2

3 产品属性 3

3.1 产品迭代 3

4 产品体系架构 3

4.1 系统拓扑图 3

4.2 业务流程图 4

5 产品功能 4

5.1 风险发现 4

5.2 风险预警 4

5.3 风险屏蔽 4

5.4 漏洞保护 5

5.5 日志审计 5

6 产品后台 5

6.1 运行环境 5

6.2 部署方式 5

7 产品应用 6

7.1 降低黑客对漏洞的利用 6

7.2 延长漏洞修复时间 6

7.3 合规性检查 6

8 产品价值 6

1 产品发展背景

随着数字化转型的加速推进，企业和组织在网络上存储、处理和传输大量敏感数据，因此成为黑客和恶意攻击者的主要目标。针对系统和应用程序的漏洞攻击成为了日益增长的安全威胁，给各行各业带来了严重的风险和损失。传统的漏洞扫描工具通常用于发现已知漏洞并提供修补建议。然而，这些工具在面对新的未知漏洞时往往束手无策，同时也存在误报的问题。此外，漏洞修复过程繁琐耗时，会导致服务中断或性能降低，给业务运营带来不便和经济损失。企业和组织在追求网络安全的同时，亦需要保持业务的正常运行。传统的漏洞修复方式往往会导致业务停机或功能降级，给组织造成重大影响。随着网络攻击技术的不断演进，高级威胁如零日漏洞和 APT 攻击等变得越来越多样化和隐蔽化。这些攻击利用未知漏洞进行入侵，往往能够在传统安全防御措施下不被察觉。因此，市场急需一种能够在不中断业务的情况下提供漏洞安全保障的解决方案。

基于上述市场需求和挑战，漏洞屏蔽系统应运而生。该系统通过采取一系列措施来隐藏系统和应用程序中的漏洞，从而减少遭受攻击的风险，同时保持业务的正常运行。这种新颖的安全策略为企业和组织提供了更加全面、高效的网络安全保障。

1.1 业务需求

1） 漏洞修复过程繁琐耗时

漏洞修复时可能导致服务中断或性能降低，给业务运营带来不便和经济损失。传统的漏洞修复方式需要将系统或应用程序暂停运行并进行升级或补丁安装，这会影响业务正常运行，给企业和组织造成重大影响。

2） 存在被攻击的风险

当漏洞暴露在外部环境时，黑客更容易发现它们，可以利用这些漏洞来入侵目标系统并进行详细分析和利用。公开的系统或应用程序通常会受到更多关注，吸引了黑客的兴趣，因此漏洞暴露的风险也相应增加。

3） 合规检查需求

上级单位定期对企业和组织的系统和资产进行安全评估，其评估方向之一是采用漏洞扫描设备对企业和组织的系统漏洞进行合规检查，能让企业了解自身的网络安全状况，查漏补缺、提前整改，防患于未然。

2 产品介绍

漏洞屏蔽系统能够实现不暴露漏洞的情况下对企业和组织提供安全保障，避免了漏洞被攻击者利用的风险，并且不会对业务的正常运行造成任何影响。通过

屏蔽外界攻击风险，可以大幅降低被攻击的概率，并有效防范高级威胁的入侵。这种新颖的安全策略填补了传统漏洞修复方式的不足，为市场提供了一种更加灵活、智能的安全解决方案，有助于保护企业的敏感数据和业务运作，提升整体网络安全的水平，帮助企业和组织更好地应对不断增长的网络威胁。

2.1 市场定位

作为一种高级的网络安全解决方案，专注于帮助企业和组织保护其系统和应用程序免受恶意攻击和未知漏洞的威胁。其核心目标是提供一种更加全面、高效和无缝的安全保障，以满足客户对安全性和业务连续性的需求。

1） 高级安全解决方案

是一种高级网络安全解决方案，强调在漏洞修复以外提供有效的安全防御措施。通过虚化系统和应用程序中的漏洞，屏蔽任意角度的异常攻击、扫描等行为，防止黑客利用已知和未知的漏洞进行入侵攻击。

2） 保护关键资产

系统专注于保护企业和组织的关键资产，包括敏感数据、知识产权和商业机密等。它提供一个安全的屏障，确保这些关键资产不会因漏洞被攻击者利用而受到损害。

3） 业务连续性

与传统的漏洞修复方式不同，漏洞隐藏系统可以在不中断业务的情况下提供安全保障，无需停机或升级系统，确保企业和组织的业务能够持续进行。

2.2 目标客户群体

1） 高度依赖网络

企业和组织核心业务离不开网络，业务运转也系统需要网络支撑，对网络依赖心较大的客户，本产品能够保护其系统和应用程序免受恶意攻击。

2） 数据机密性较强

企业或组织处理大量敏感用户数据的行业，如金融机构、医疗保健机构、电信运营商等，需要确保用户数据的安全性。本产品可以帮助保护这些敏感数据不会通过恶意攻击而被窃取，降低数据损失的风险。

3） 政府和公共机构

政府部门、国家重要机构和公共服务提供商需要保护国家和公众的信息安全，以及基础设施的稳定运行，本产品可以提供有效的网络安全保护，防止潜在的网络威胁。

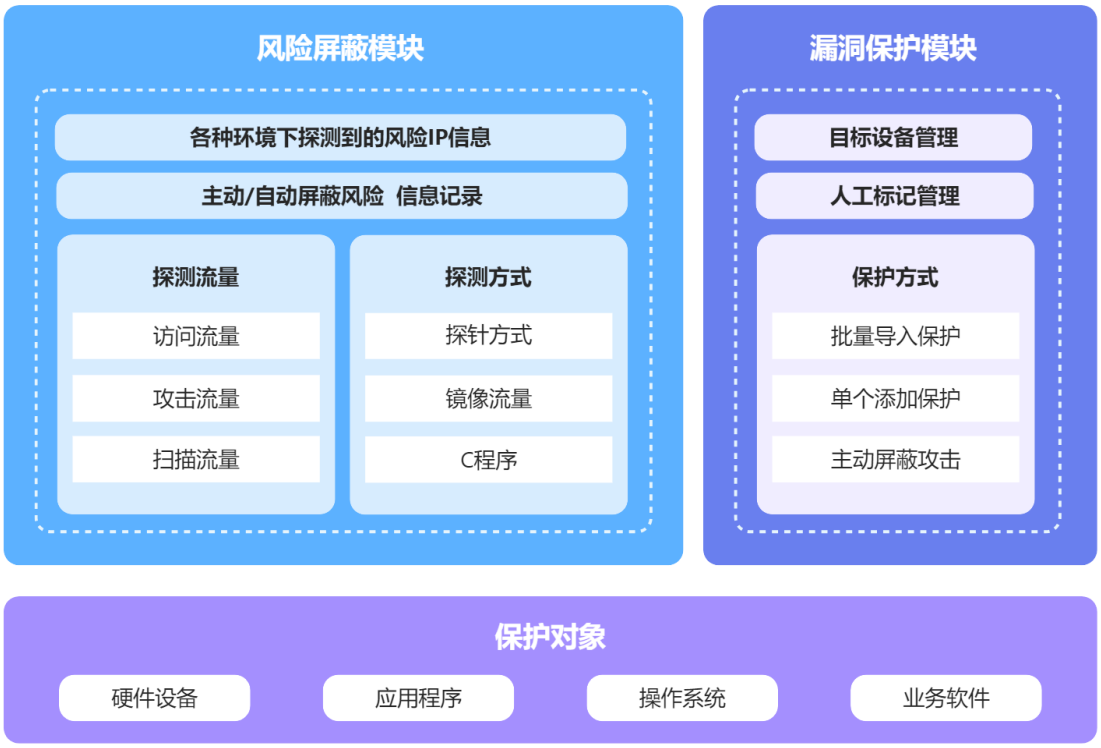
3 产品属性

3.1 产品迭代

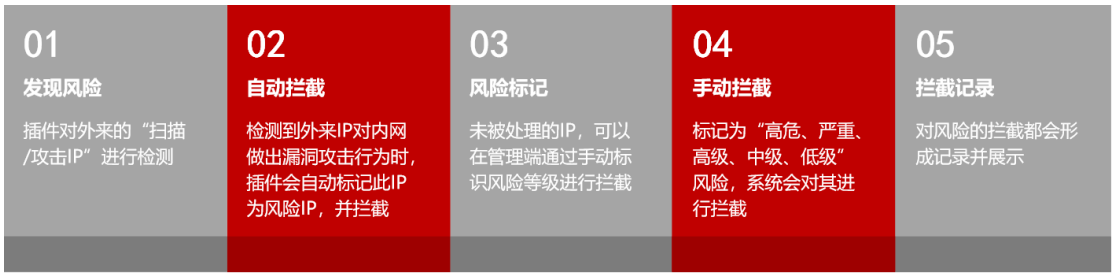
迭代版本	版本说明
迭代 1.0（目前）	添加需要保护的漏洞设备，系统自动对攻击目标设备的风险 IP 进行预警和屏蔽，使其无法对目标设备发动伤害；
迭代 2.0	自动发现需要保护的漏洞设备，并对其漏洞等级进行自动判定和排列；

4 产品体系架构

4.1 系统拓扑图



4.2 业务流程图



5 产品功能

5.1 风险发现

系统利用先进的网络安全技术和算法，对设备的网络和流量进行实时探测和分析，以便及时发现互联网对设备的攻击或扫描行为。

1） 探测机制

通过持续的流量探测，检测异常的网络活动，主动分析每个网络数据包，并与已知恶意行为模式进行比对，快速识别出可能的攻击行为。无论是来自外部的端口扫描、漏洞利用还是恶意代码传输，系统都能准确地捕捉到异常风险行为。

2） 判断机制

具备实时更新的异常规则库，其中包含了各种已知的攻击和扫描行为的特征信息。系统通过与库中行为进行实时对比和匹配，可以及时发现最新的攻击手法和恶意行为，确保设备在不断变化的网络威胁环境下保持安全。

5.2 风险预警

通过实时监测和分析网络流量以及设备行为，能够对互联网攻击行为进行准确判断，一旦发现异常行为，系统将立即触发预警机制，以保护设备免受攻击。系统能够根据预定的警报规则和算法，对异常情况进行预警，并提供系统捕捉到的相关异常信息，帮助管理员快速响应和防范潜在的安全威胁，保护设备的安全性和稳定性。

5.3 风险屏蔽

系统通过自研的高新技术手段，能够对各种环境下的恶意攻击、扫描、访问行为进行屏蔽，使风险 IP 无法捕捉到系统需要保护的目标设备。这种方法可以使攻击者无法准确判断目标系统的真实状态和漏洞情况，从而降低他们对系统进行有针对性的攻击的能力。

1） 自动屏蔽

通过网络和流量分析，判断环境内的攻击行为，符合攻击规则，则半丁为风

险 IP，系统自动进行屏蔽处理。

2） 手动屏蔽

系统自动记录所有对目标设备进行访问的 IP。支持通过人工干预和操作对 IP 进行屏蔽处理，使其无法扫描目标设备内的漏洞信息。

5.4 漏洞保护

将系统中的漏洞或弱点隐匿起来，使攻击者难以察觉和利用。本产品提供的解决方案仅作为综合安全策略的一部分来降低攻击风险。组织应该采取多层次、多维度的安全防护措施，定期评估和改进安全措施，以应对不断变化的威胁环境。

5.5 日志审计

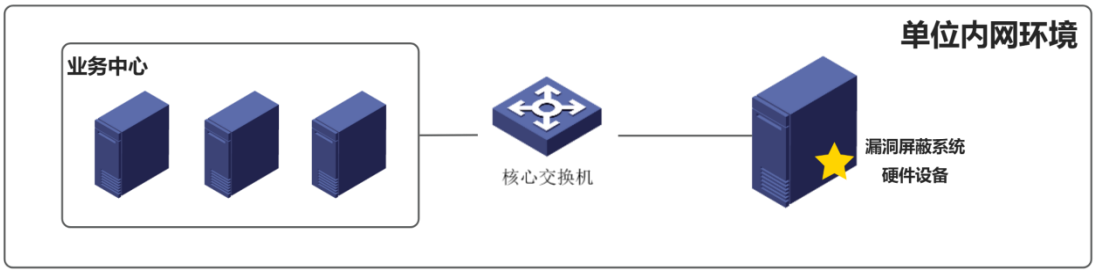
建立并启用日志记录功能，跟踪和追溯系统中用户或管理员的操作行为，以便进行审计、故障排查和安全调查的技术手段。系统会记录用户或管理员的各类操作行为，包括登录、注销、文件访问、数据库查询、系统配置修改等。每个操作都将被时间戳记录下来，并与操作者的身份信息关联。记录详细的操作信息，实现溯源功能可追踪一个操作或一系列操作的来源。例如，通过记录 IP 地址、用户名、会话 ID 等关键信息，可以追溯到操作的发起者或相关联的其他操作，这样可以提供足够的细节，帮助后续的审计和调查工作。

6 产品后台

6.1 运行环境

序号	设施	环境参数
1	虚拟机	Linux 操作系统； CPU：4 核；内存：8G 或以上；存储：100G 以上；
2	服务器	Linux 操作系统； CPU：64 核；内存：12G；存储：1T

6.2 部署方式



7 产品应用

7.1 降低黑客对漏洞的利用

黑客想要对内网进行攻击时，需要提前拿漏扫工具对内网进行扫描，扫出来一些漏洞后，能够利用漏洞从而对内网进行攻击。本产品可以降低黑客对漏洞的利用，实现方式：漏扫工具对内网进行扫描时会产生流量信息，系统自动带有攻击行为的漏扫攻击进行屏蔽，使其无法获取到“漏洞设备”的实际信息。

7.2 延长漏洞修复时间

企业和组织近段时间无法对漏洞进行维护和修复时，可将漏洞进行保护，使得其他环境下的人员和设备无法扫描到目标设备存在的漏洞，由此可以延长漏洞的修复时间。

7.3 合规性检查

需要合规检查时，上级单位会提供漏扫设备对客户单位进行扫描。本系统可以帮助企业达到合规要求，实现方式：将漏扫设备的 IP 在系统界面内标记为无风险，系统自动对无风险 IP 无条件放行，使漏扫设备能够正常扫描内网漏洞，通过我司专利技术手动，能够使其无法扫描到被保护的目标设备，从而实现对攻击的屏蔽。

8 产品价值

1） 防止恶意利用

阻止攻击者利用已知漏洞进行攻击，减少系统遭受恶意活动的风险。

2） 延长修复时间

使攻击者在发现和利用漏洞之间的时间延长，给安全团队更多时间来检测、分析和修复漏洞。

3） 符合规范要求

某些行业或法规要求保护漏洞以确保用户数据和隐私的安全。遵守这些要求可以降低法律风险。

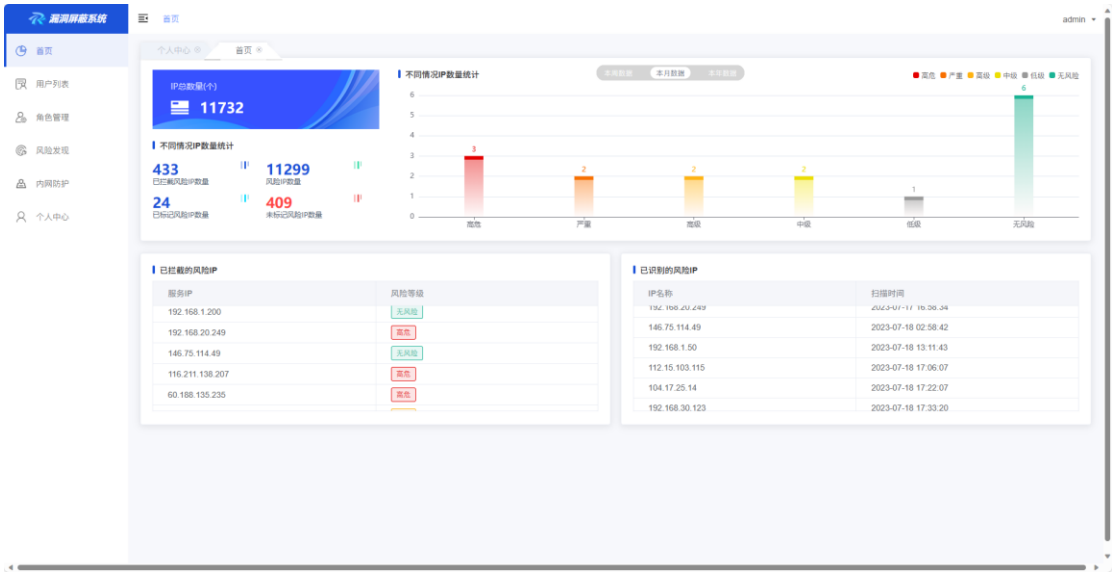
4） 维护组织声誉

及时保护漏洞可以避免公众对系统或组织安全性的质疑，维护组织声誉。

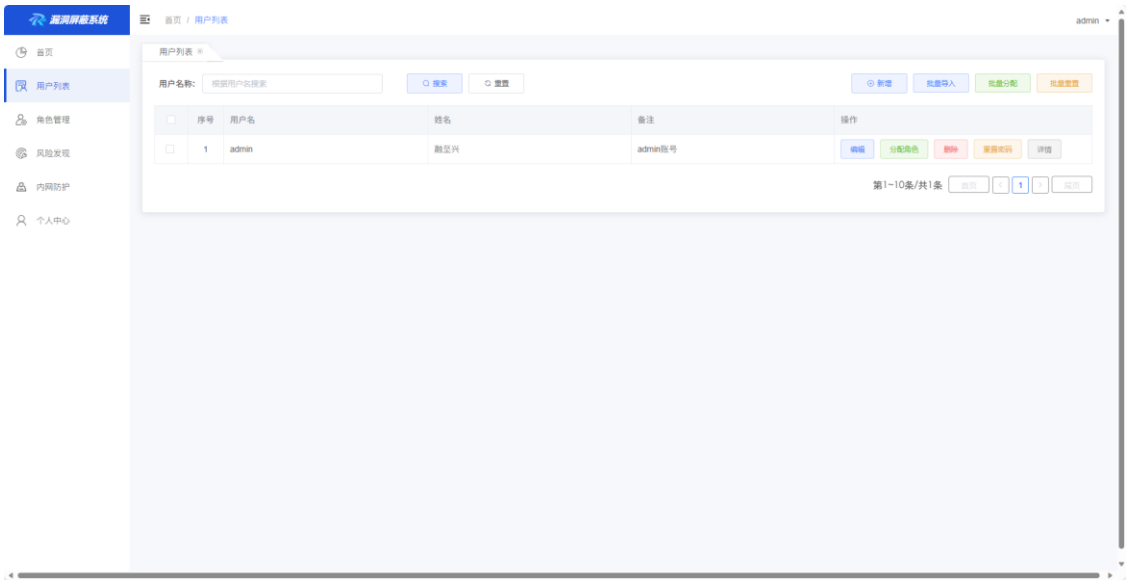
9 系统主要功能截图

9.1 登录界面

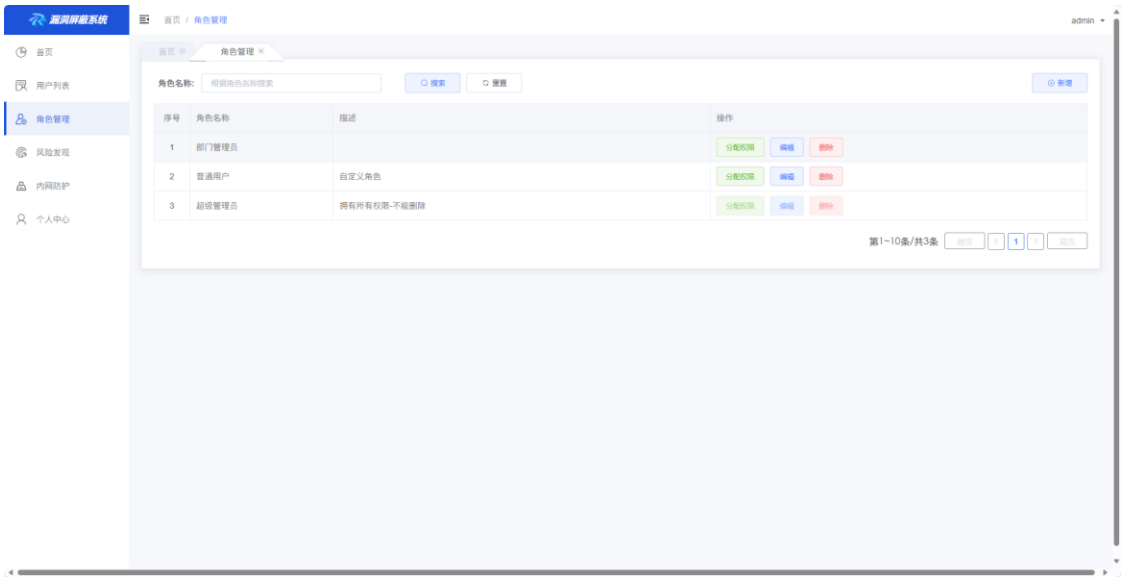
9.2 系统首页



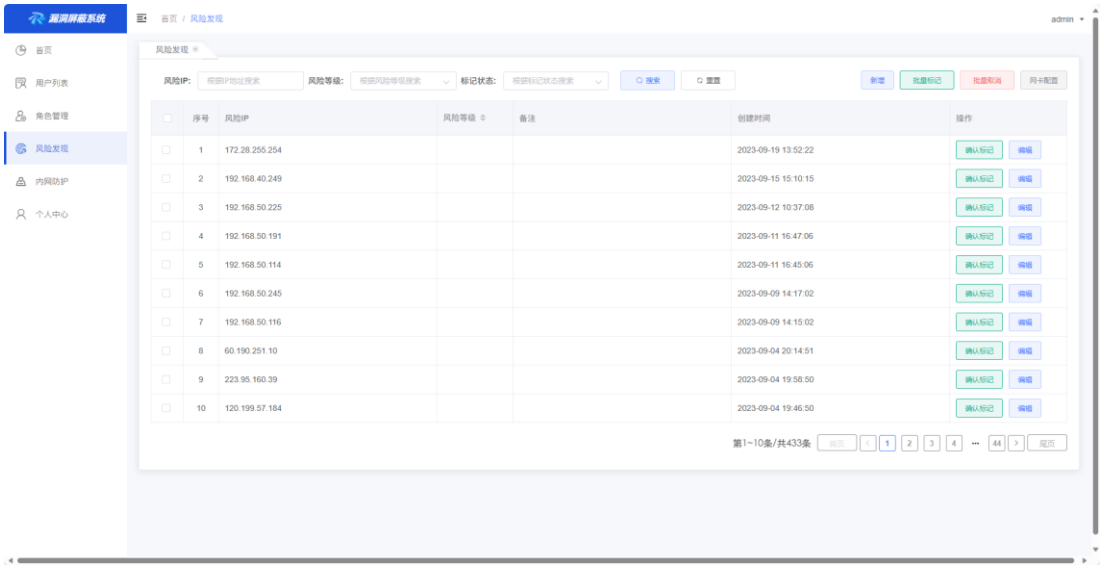
9.3 用户列表



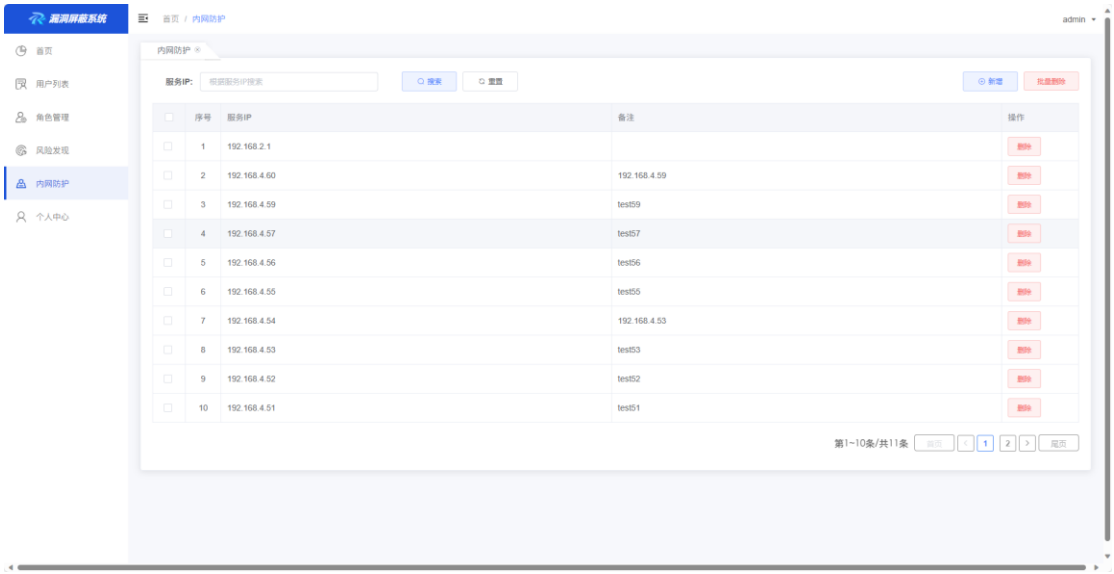
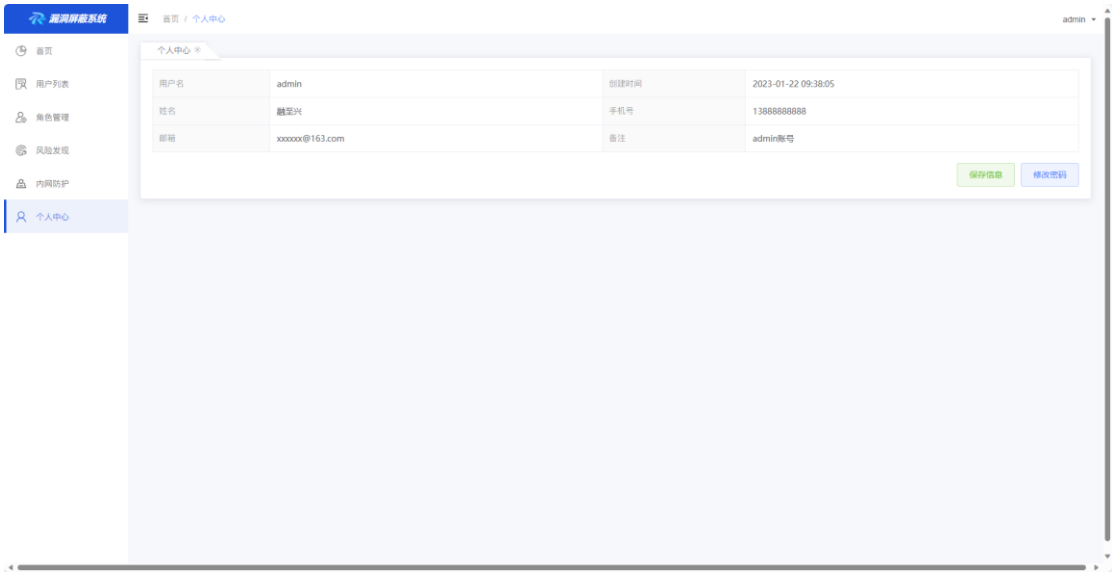
9.4 角色管理



9.5 风险发现



9.6 内网防护



9.7 个人中心