云安全防护平台
管理员手册

版本编号：V2.1

北京国信网联科技有限公司

■ **版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，版权均属所有，受到有关产权及版权法保护。任何个人、机构未经的书面授权许可，不得以任何方式复制或引用本文的任何片段。

■ **版本变更记录**

时间	版本	说明	修改人
2022-4-1	2.0	创建文档	
2022-0823	2.1	功能更新	

■ **适用性声明**

本模板用于撰写内外各种正式文件，包括技术手册、白皮书等文档使用。

北京国信网联科技有限公司

目 录

北京国信网联科技有限公司

北京国信网联科技有限公司

北京国信网联科技有限公司

北京国信网联科技有限公司

1.产品简介

传统的等级保护解决方案需要客户采购大量的安全产品，部署复杂的安全策略，并基于这些安全基础设施建立有效的安全运维流程和制度。这些工作需要投入大量资源，实施周期也很长，尤其在云计算、物联网等新新兴场景中，传统安全产品组成的安全解决方案无法有效部署而导致等级保护建设项目无法落地。此时迫切需要一个云等保管理平台，作为在公有云、政务云、IDC 托管等业务场景下的新型等保合规解决方案，为云计算上的信息系统运营单位、使用单位、安全服务机构，提供可以快速落地的云等保合规支撑平台。

云安全防护平台是一套用于云计算的一站式等保合规解决方案，作为云计算环境等级保护基础管理平台，产品开发围绕等级保护相关政策及信息系统等级保护基本要求，融合多种安全组件、云化接入、简易部署，可以满足企业在云等保合规的场景需求，如应用部署在 IDC 机房、阿里云、腾讯云、华为云、政务云等大型公有云平台，满足企业等保二级、三级合规的要求。

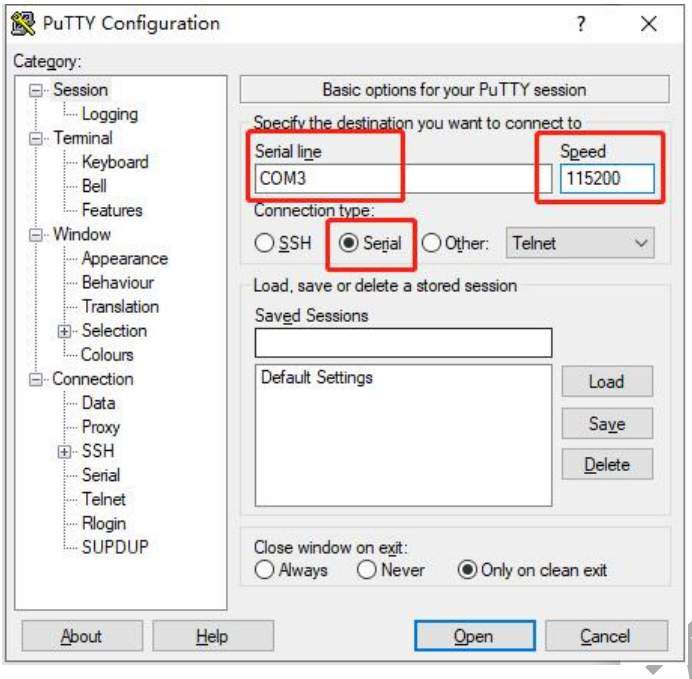
2.初始化登录

2.1. 硬件连接设备的Console口（部分设备具有）

Console 功能可以对系统进行维护，特别是当系统 Web 管理界面无法访问，或者系统出现异常时。可以通过使用 Console 用户登录，对系统进行查看，配置等。

1. 用 Console 线连接 PC 机和设备的 Console 口；
2. 运行支持 COM 口通讯的软件（如 PuTTY、SecureCRT 等）连接设备，连接状态选择“串口”，波特率设置为 115200；

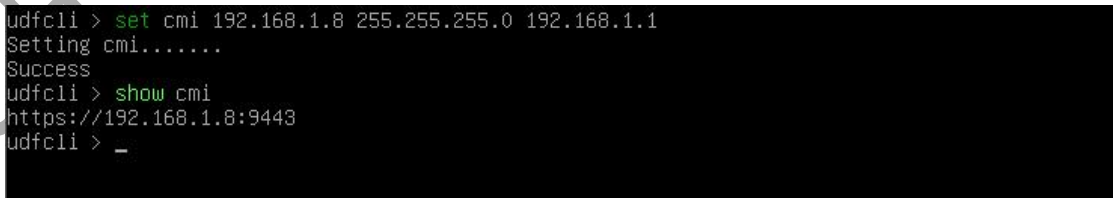
北京国信网联科技有限公司



3. 置好参数，点击【Open】按钮连接，输入用户名 udfcon，密码 udfcon，登录系统，进入命令操作欢迎界面。输入 help 并按回车获取命令帮助提示，可对系统进行查看，配置等操作。如需退出命令操作，请按 Ctrl+D 退出。

4. 初始化管理 IP，输入 show cmi 命令，查看当前系统 CMI 管理口访问地址。

5. 设置管理口 IP 命令示例，输入 set cmi 192.168.1.8 255.255.255.0 192.168.1.1，即可修改 CMI 管理口 IP 地址，如图所示。



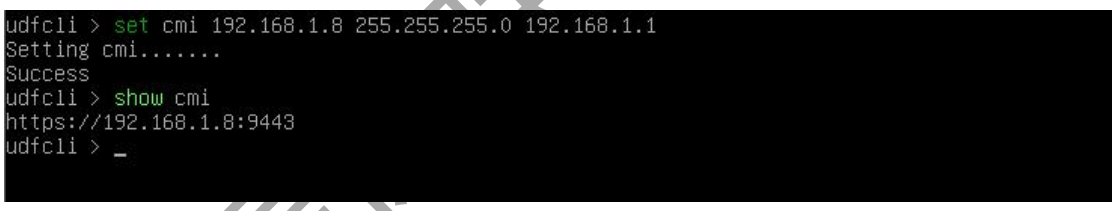
6. 设置网络后，用浏览器打开管理口访问地址，开始使用。

北京国信[illegible]科技有限公司

2.2. 虚机使用虚拟机控制台功能

如果系统安装在虚拟机中，请通过虚拟化平台提供的控制台功能，进入 Console 管理界面，根据提示输入用户名 udfcon，密码 udfcon，登录系统，进入命令操作欢迎界面。输入 help 并按回车获取命令帮助提示，可对系统进行查看，配置等操作。如需退出命令操作界面，请按 Ctrl+D 退出。

1. 初始化管理 IP，输入 show cmi 命令，查看当前系统 CMI 管理口访问地址。
2. 设置管理口 IP 命令示例，输入 set cmi 192.168.1.8 255.255.255.0 192.168.1.1，即可修改 CMI 管理口 IP 地址，如图所示。



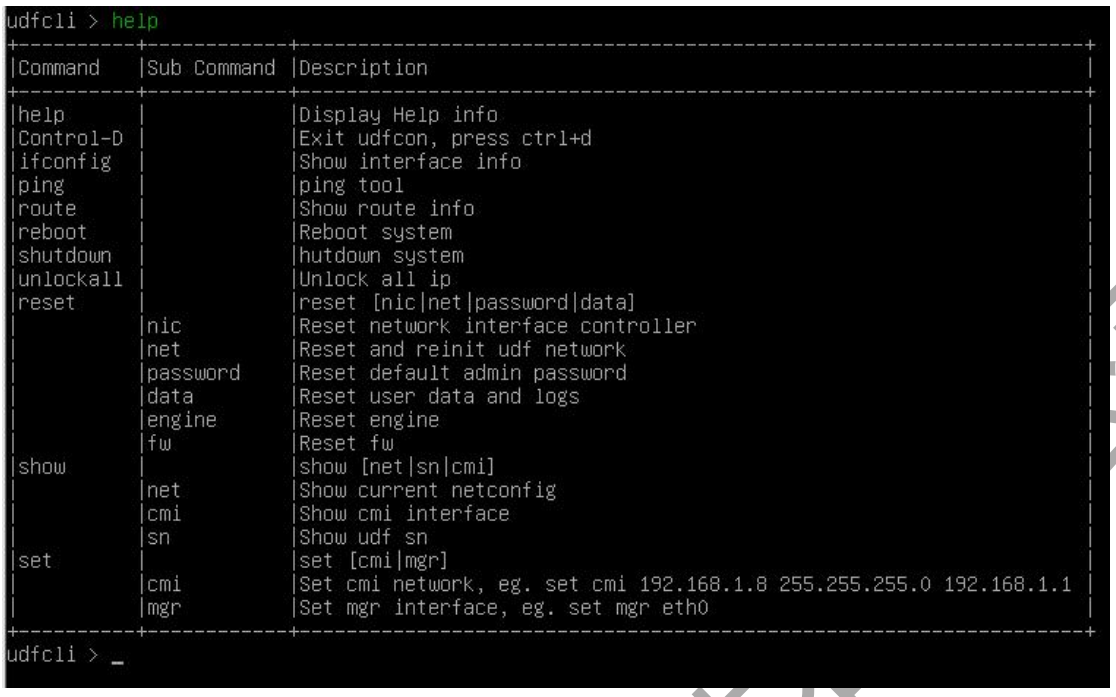
3. 设置网络后，用浏览器打开管理口访问地址，开始使用。

3.命令行操作帮助

3.1. Console功能帮助

系统提供命令行操作 Console 功能，可以使用命令对系统进行查看和配置，输入 help 并按确认键获取帮助说明，即可看到如下图所示。

北京国信[illegible]科技[illegible]公司



如上图所示，目前 Console 界面包含以下几项功能。

help：显示帮助

Control-D：退出 Console 功能，按 Ctrl+D

ifconfig：显示当前系统网卡配置信息

ping：检查网络是否可以连通

route：显示当前系统路由表信息

reboot：重启系统

shutdown：系统关机

unlockall：解锁所有被封锁的 IP

reset nic：重置网络接口控制器，该操作会重新识别网卡，一般不建议操作

reset net：重置并重新初始化网络，该操作会重新检测网卡

reset password：重置前台管理员用户名密码

reset data：重置并清除所有用户数据，此操作不可逆

reset engine：重置后台引擎，一般不建议操作

北京国信网联科技有限公司

reset fw：重置并清除管理口白名单

show net: 查看当前网络配置信息

show cmi: 查看当前系统管理口访问地址

show sn: 查看当前系统的序列号和产品二维码

set cmi: 设置当前系统的管理口 IP 地址，示例 set cmi 192.168.1.8 255.255.255.0 192.168.1.1

set mgr: 设置普通网络接口为系统管理口，示例 set mgr eth0

3.2. 重置管理员密码

当管理员忘记 Web 管理界面密码时，可通过 Console 功能，输入命令 reset password，重置前台管理员用户名密码，重置为 admin/udfadmin，操作命令如下图所示。

3.3. 恢复出厂设置

如需对系统进行恢复出厂设置操作，可通过 Console 管理功能，输入命令 reset data，重置并清除所有用户数据。系统复位后所有配置和运行数据将全部恢复到出厂状态，操作命令如下图所示。

注意：此操作不可逆，请提前备份系统配置并导出重要数据。

北京国信网安科技有限公司

4.开始使用

4.1. 系统登录

在浏览器中打开已经设置好的 CMI 管理口访问地址，浏览器可能会提示“您的连接不是私密连接”，如下图所示。

出厂默认管理地址：https://192.168.1.8:9443

点击【继续前往（不安全）】，然后显示系统登录界面。输入正确的用户名和密码，点击【确定】即可登录进行操作。

4.1.1. 管理员登录

管理员【admin】只负责对系统的安全策略配置及日常维护管理，不能进行日志审计的查看和管理，不能用于创建管理员、普通用户、审计管理员账号。

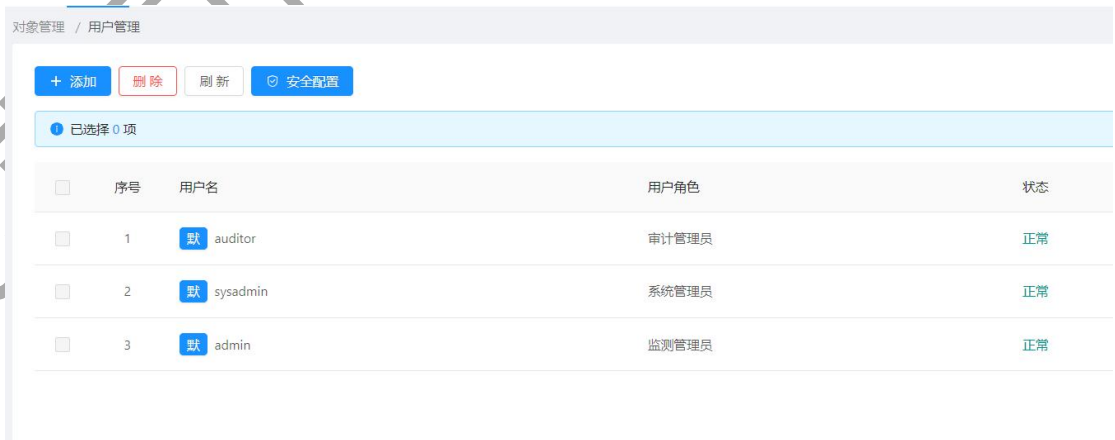
管理员初始使用内置的 admin/udfadmin 账号进行登录，第一次登录要求修改初始密码并重新登录，如下图所示。

北京国信冠

注意：初始密码修改包含 admin 管理员账号，sysadmin 系统管理员账号，auditor 审计管理员账号，请妥善保管账号及新密码。

4.1.2. 系统管理员登录

系统管理员【sysadmin】只负责对系统的用户管理，角色管理以及相关安全配置。用户管理可添加、删除管理员账号，可解除账号登录失败锁定。



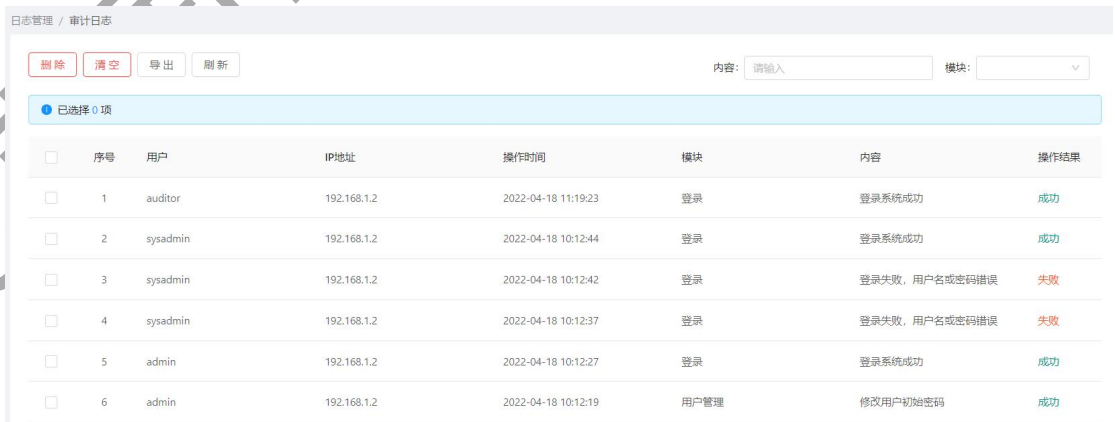
点击【安全配置】进行相关参数设置，如下图所示。

版权所有，注意保密

安全配置可进行登录超时时间，用户锁定次数，IP 锁定次数，锁定时间，密码复杂度，密码有效期等配置。

4.1.3. 审计管理员登录

审计管理员【auditor】只负责对系统的日志审计管理，可查询详细的登录日志及操作日志及导出日志信息。



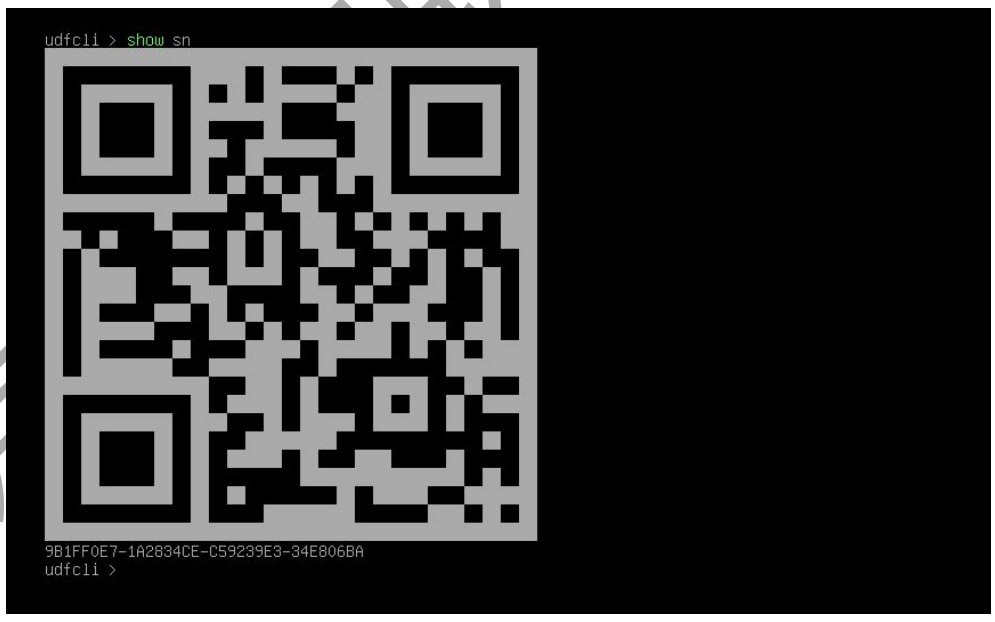
北京信网联科技有限公司

4.2. 申请授权

产品授权申请需要提供客户名称和产品序列号，可通过以下两种方式获取序列号。

1. 通过 Web 管理功能在【授权管理】页面，获取产品序列号。

2. 通过 Console 管理功能，输入 show sn 命令，获取产品序列号，手机扫描二维码可复制序列号信息。

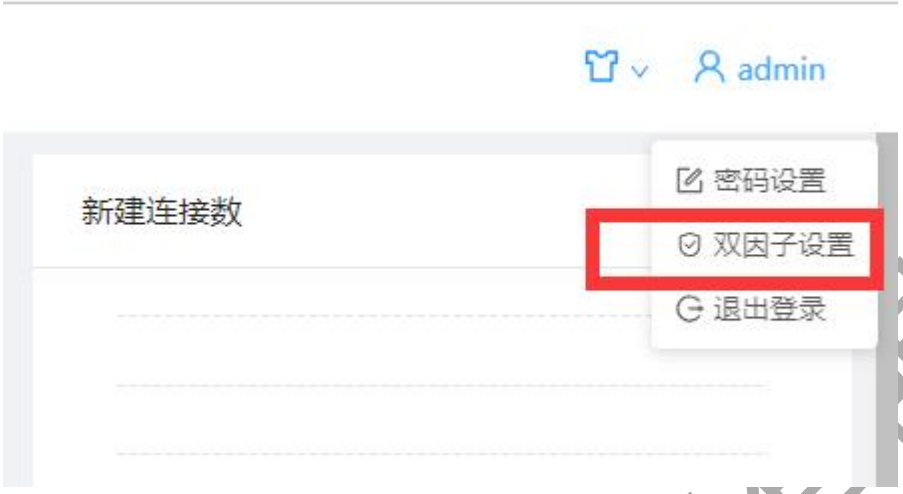


注意：产品授权无效时，功能将无法正常使用，请及时联系厂商人员申请授权。

北京[illegible]联科[illegible]公司

4.3. 双因子认证设置

在 admin 账户下，点击右上角 admin 标识可显示双因子认证设置。



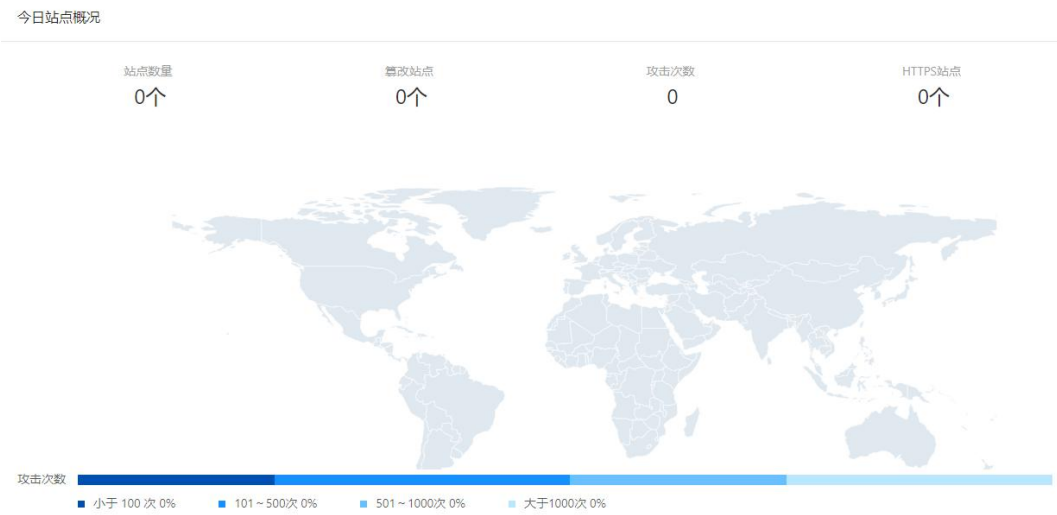
1. 开启双因子认证开关，根据帮助文档进行相关设置。（内置 Google 身份验证器）

北京[illegible]技术[illegible]公司

5.概览

概览页面包含以下信息：

1) 今日站点概况，包含站点数量，攻击次数，https 站点数量信息。

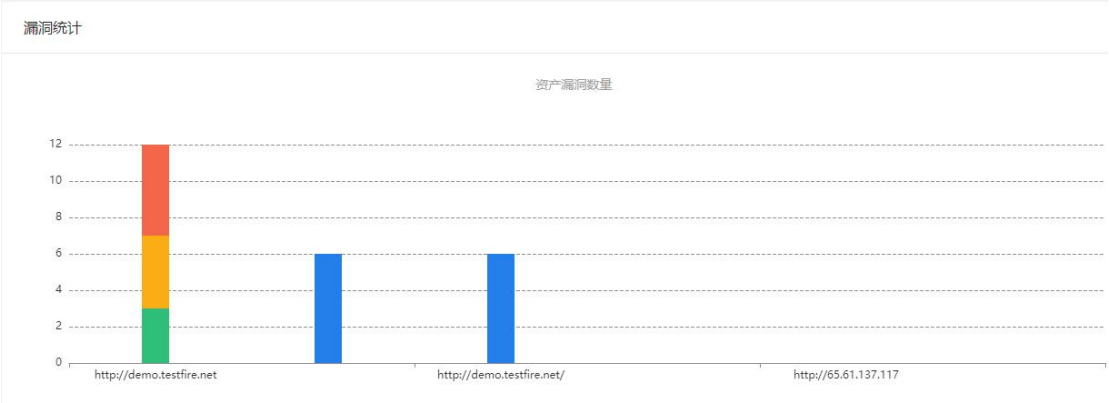


2) CPU 使用率，内存使用率，磁盘使用率。

3) 新建连接数，展示当前新建连接数趋势。

北京未科

4) 漏洞统计，展示站点漏洞情况。



6.动态感知

6.1. 流量统计

1) 网卡流量

可根据时间查看数据接入口流量统计数据。

北京国信网联公司

2) 分析流量趋势

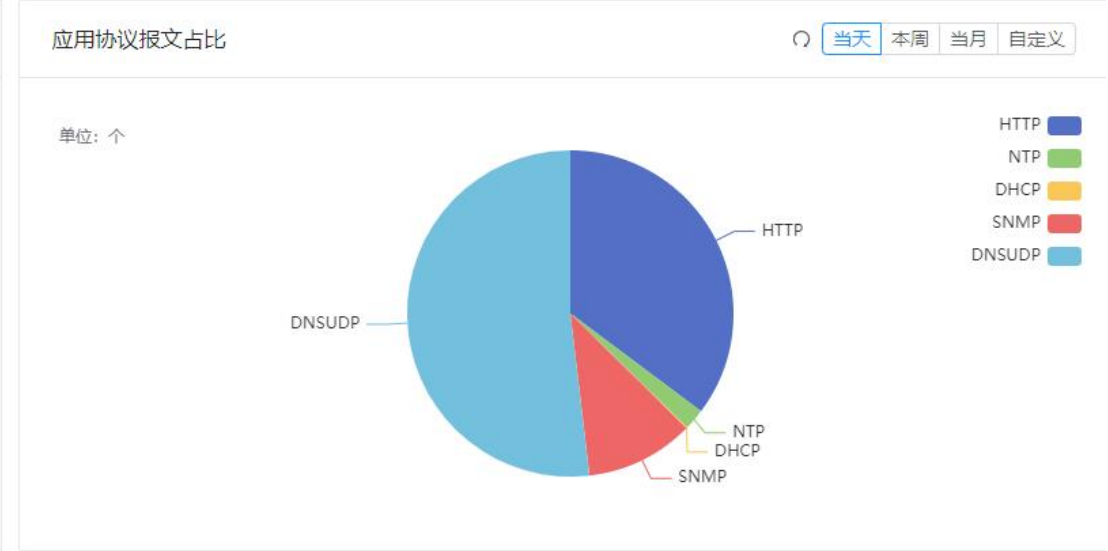
可根据时间查看已经分析的数据流量情况。

3) 协议报文趋势

可根据时间查看已经分析的协议报文趋势。

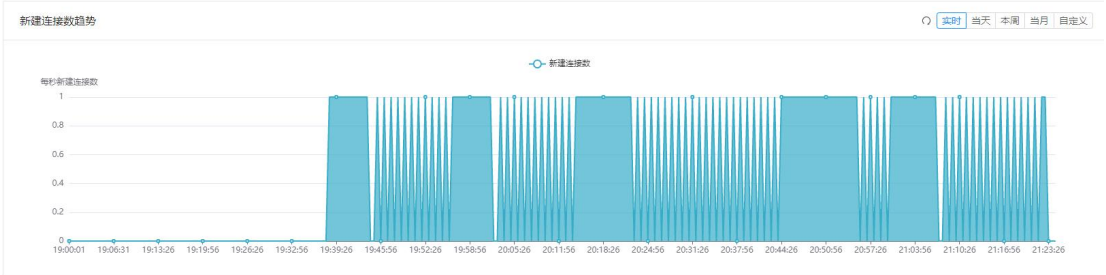
4) 应用协议报文占比

可根据时间查看已经分析的协议报文占比。



5) 新建连接数趋势

可根据时间查看新建连接数趋势。



北京国

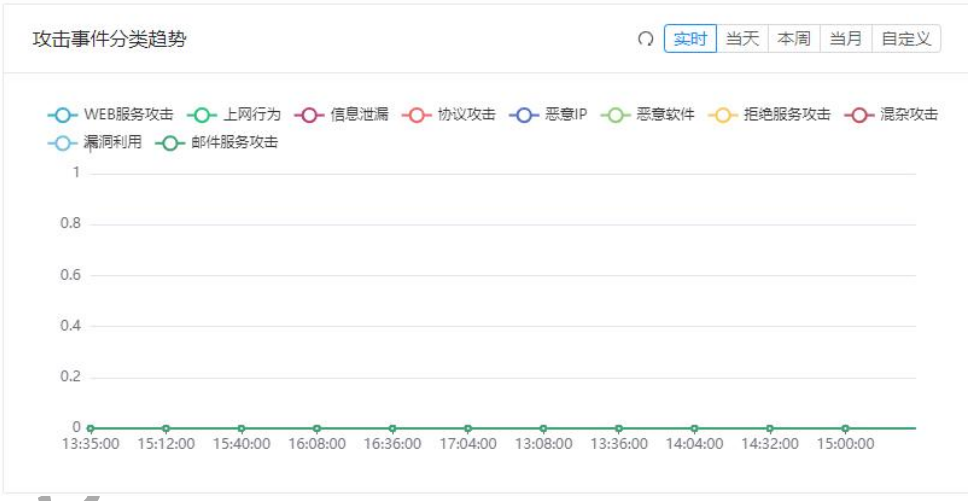
6.2. 攻击流量

1) 攻击事件协议趋势

可根据时间查看攻击事件包含的协议趋势。

2) 攻击事件分类趋势

可根据时间查看攻击事件的分类趋势。



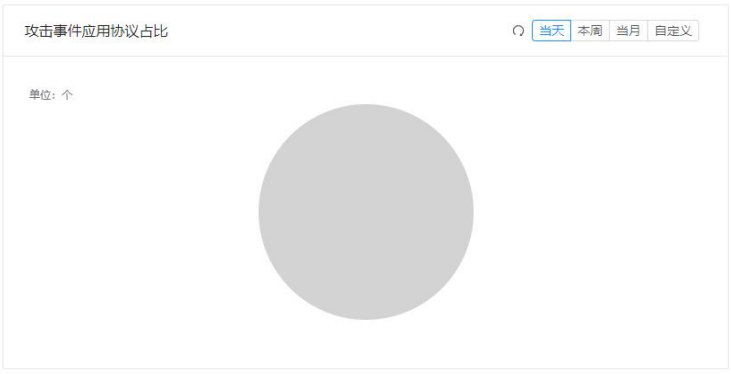
3) TOP10 区域攻击事件

可根据时间、世界/中国查看 TOP10 区域攻击事件。

北京[illegible]科技有限公司

4) 攻击事件应用协议占比

可根据时间查看攻击事件应用协议占比。



7.资产管理

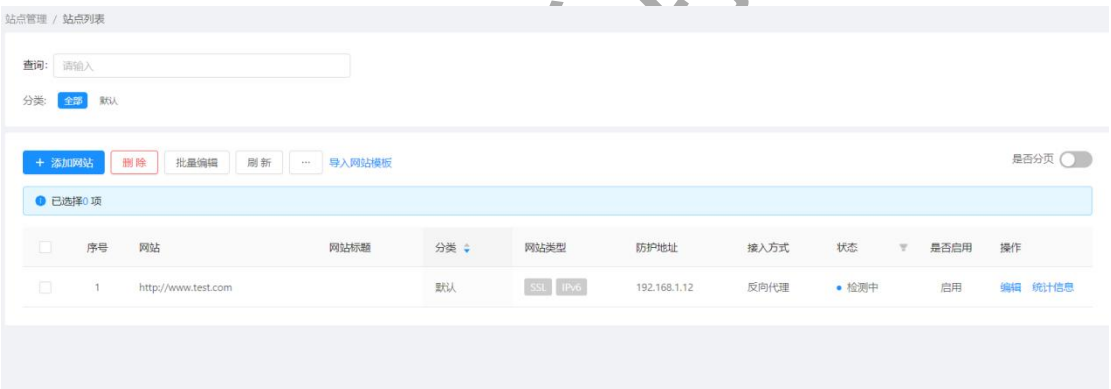
7.1. 资产列表

7.1.1. 添加网站

资产列表可对资产进行添加，删除，批量编辑，一键启用禁用，一键开启关闭防护，导出导入网站等操作。

北京国信网联科技有限公司

资产列表页面列出了当前系统所添加的网站信息，可展示网站域名，网站标题，网站分类，接入方式，后端防护地址，健康状态等内容。



点击【添加网站】添加需要防护的网站域名及网站服务器 IP 和端口，如下图所示。

北京国信

网站域名

- 协议类型：支持 http 和 https；
- 网站域名：填写网站对外服务的真实域名，多个域名请用换行分割；

防护地址

- 协议类型：支持 http 和 https；
- 防护地址：填写网站服务器的真实 IP 地址，支持 IPv4 和 IPv6 地址；
- 端口：填写网站服务器的真实端口；

(1) 添加分类

在添加网站页面，点击【高级配置】可添加网站所属分类，点击【+号】添加分类，填写分类名称，选择上级分类，选择网站所属分类。

北京国信网联科技有限公司

(2) 支持IPv6

在添加网站页面，点击【高级配置】可开启网站支持 IPv6 访问，该功能默认启用无需配置，如下图所示。

注意：支持 IPv6 访问，前提需要在解析口属性的网卡配置添加 IPv6 地址，并在 DNS 服务器添加 AAAA 类型的域名解析记录。

(3) 负载均衡

在添加网站页面，点击【高级配置】可开启网站负载均衡功能，开启负载均衡支持添加多个后端服务器地址，可选择均衡算法支持轮询、IP 哈希、X-Real-IP 哈希，如下图所示。

北京国信 有限公司

(4) 合规配置

在添加网站页面，点击【HTTP 头合规配置】可进行 HTTP 安全配置，如下图所示。

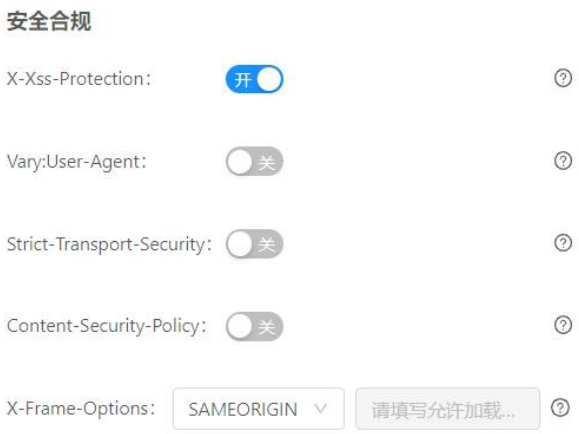
基础配置

Server：一般用于备注服务器信息，建议隐藏。

X-Author：一般用于备注作者信息，建议隐藏。

X-Powered-By：一般用于展示应用版本信息，建议隐藏。

北京国[illegible]技有限公司



安全合规

X-Xss-Protection：可在检测到反射的跨站点脚本 XSS 攻击时阻止页面加载，对浏览器版本有要求，推荐启用。

X-Frame-Options：用来指示浏览器是否应该被允许在一个以<iframe>内呈现页面，确保其内容未嵌入其他网站，可以使用此功能来避免点击劫持攻击。

支持以下四种配置：

- 与源网站一致：表示采用源站的 X-Frame-Options 配置不做修改。
- SAMEORIGIN：表示该页面可以在相同域名页面的<iframe>中展示，推荐启用。
- DENY：表示该页面不允许在<iframe>中展示，即便是在相同域名的页面中嵌套也不允许。
- ALLOW-FROM：表示该页面可以在指定来源的<iframe>中展示。

北京国信网联科技有限公司

HTTP 代理

X-Forwarded-For 和 X-Real-IP：一般用于记录真实发起请求的客户端 IP，使后端服务器可以通过 X-Forwarded-For 和 X-Real-IP 字段识别真实来源 IP 地址。

支持以下三种配置：

- 访问 IP：表示将发起请求的 IP 做为字段值。
- 放行：表示不对原字段值做任何修改。
- 真实客户端 IP：表示将真实用户 IP 做为字段值。

真实 IP 来源：当发起请求的 IP 不是真实 IP 时，可以选择从 X-Forwarded-For 和 X-Real-IP 字段，获取真实来源 IP 地址，一般用于前端有 CDN 或负载均衡的场景。

Host：指定请求服务器的域名/IP 地址和端口号，可选择不包含端口，包含用户输入端口，包含后端服务器端口。

CDN 白名单：填写获取真实来源 IP 的信任地址，一般填写 CDN 地址。

7.1.2. 导入网站模板

如遇到网站较多的情况，可根据网站模板进行批量导入。格式如下图：

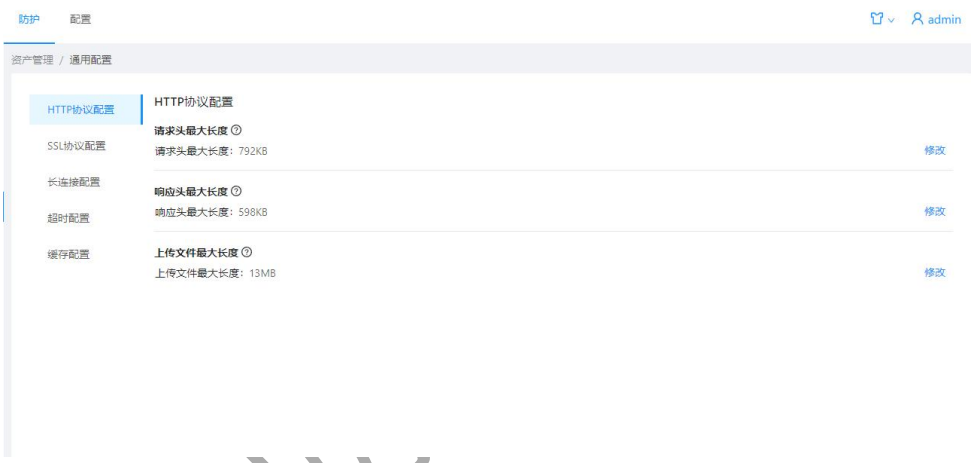
北京国信网联科技有限公司

	A	B	C	D	E	F	G	H
1	网站模式	网站域名	网站端口	防护模式	防护地址	防护端口		
2	http	www.test.	80	http	192.168.1	80		
3								
4								
5								

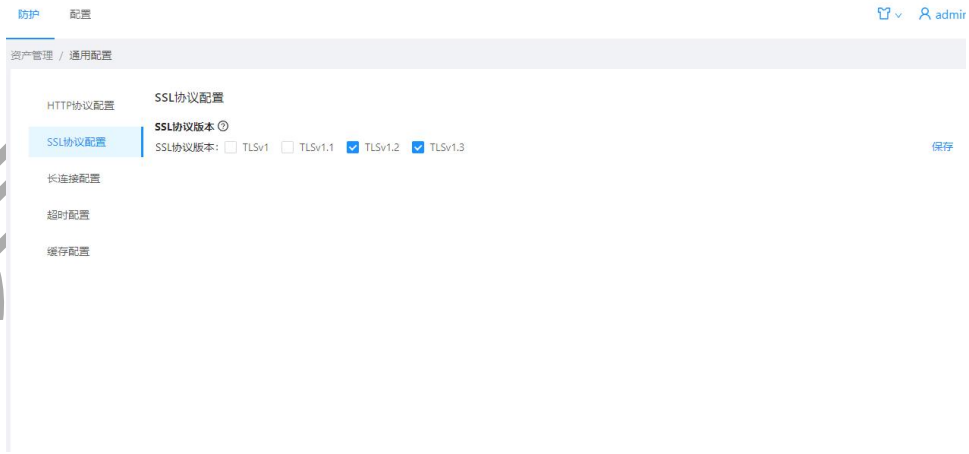
7.2. 通用配置

通用配置一般不需要修改，特殊场景下可以根据需要进行配置。

1) HTTP 协议配置，支持三个字段长度配置，分别为：请求头最大长度、响应头最大长度、上传文件最大长度。

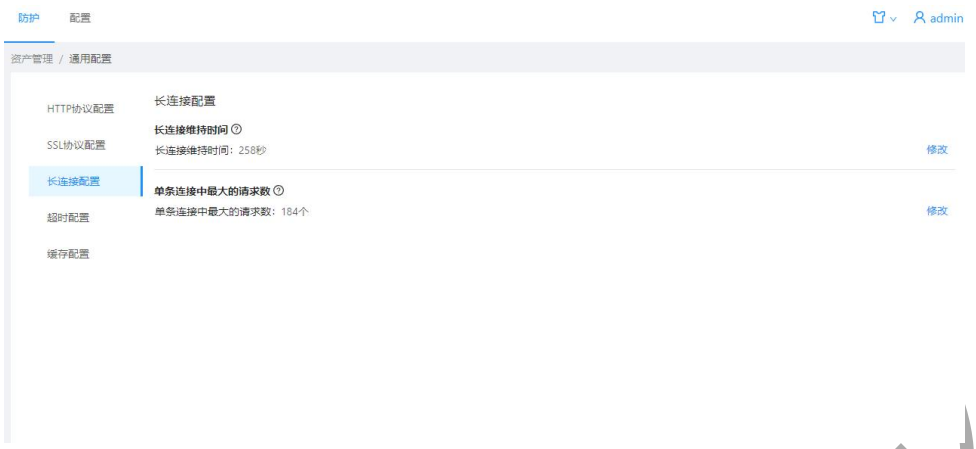


2) SSL 协议配置，支持多种 SSL 协议版本配置，至少选择一种。

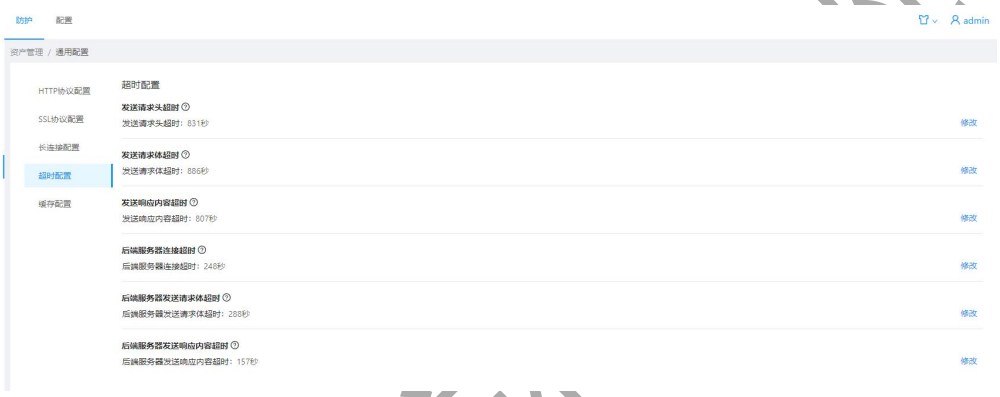


3) 长连接配置，支持长连接维持时间和单条连接中最大请求数的配置。

北京[illegible]有限公司



4) 超时配置，可配置请求和后端服务器相关的超时时间。



5) 缓存配置，用以是否保留内存缓冲区开关。

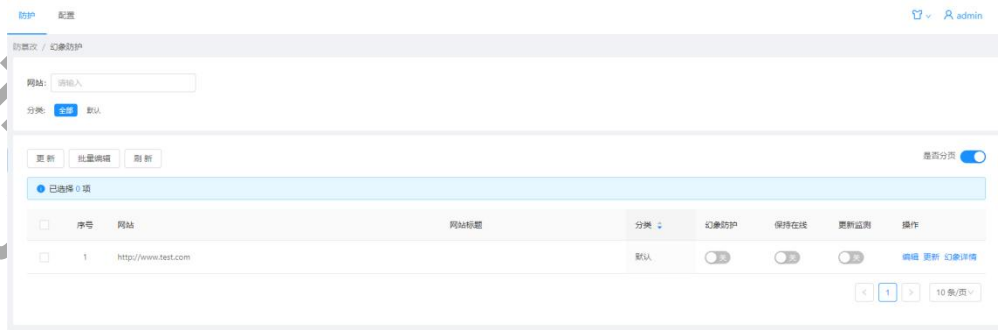
6) 域名配置，控制是否允许未配置的域名访问。

版权所有，注意保密

8.防篡改

8.1. 幻象防护

防篡改可以对网站提供幻象防护功能，开启后自动生成当前网站的幻象快照，可实现对网站页面的静态保护，能够使访问者无法看到真实的网站内容，始终对外展示某一时间点的网站幻象，保护网站内容安全。支持生成多个幻象快照，用户可以根据需要切换不同的快照提供访问。



幻象防护：开启后则启动防护，关闭则失效。

保持在线：开启后即使源站关闭了，仍然可以基于设备内的快照提供网站访问。

北京网信网联科技有限公司

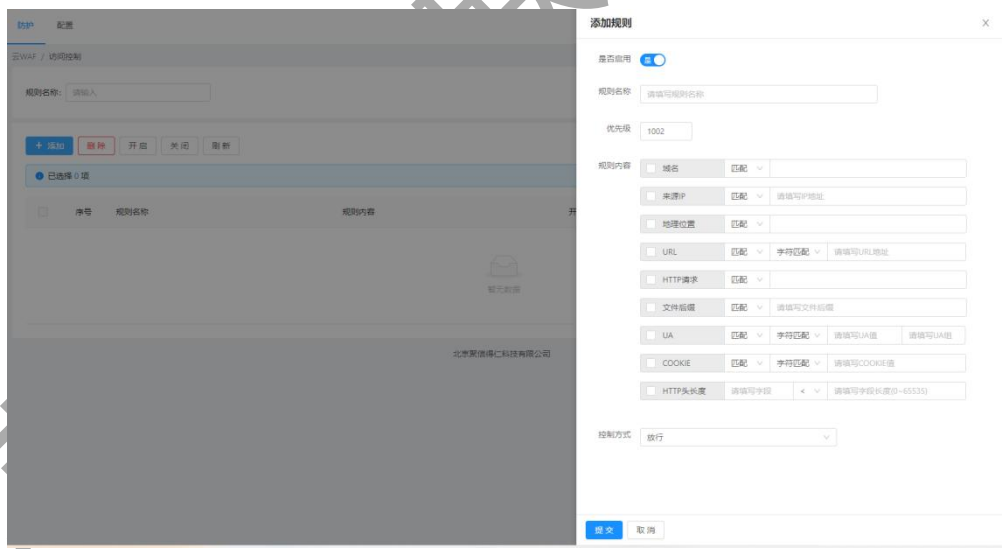
更新监测：开启后自动监测源站页面是否有改动。

9.云WAF

9.1. 访问控制

展示云 WAF 中创建的相关规则，可根据规则名称进行检索。提供添加，删除，开启，关闭规则的操作。

点击【添加】如下图所示。



是否启用：可选择此规则是否启用。

规则名称：可自定义规则名称。

优先级：定义规则优先级，数字越大优先级越高。

规则内容：可使用域名、来源 IP、地理位置、URL、HTTP 请求、文件后缀、UA、COOKIE、

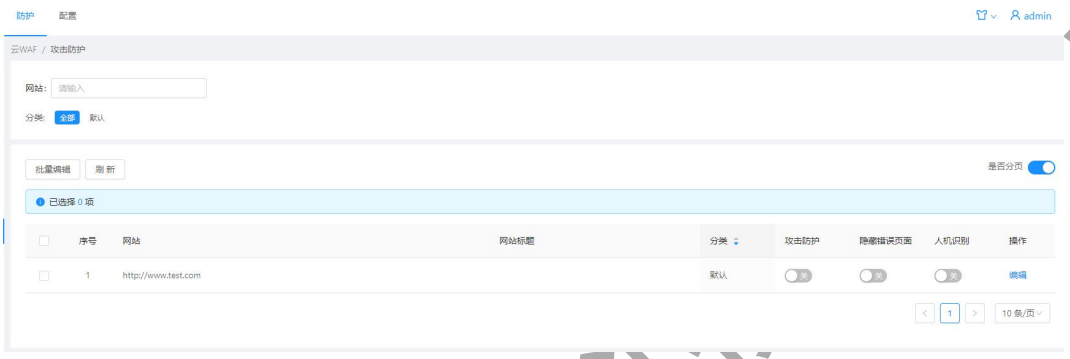
版权所有，注意保密

HTTP 头长度来进行访问控制，可选择一项或多选进行组合控制。

控制方式：可选放行、关闭幻象防护、检测、重定向、拦截、set-cookie 放行。

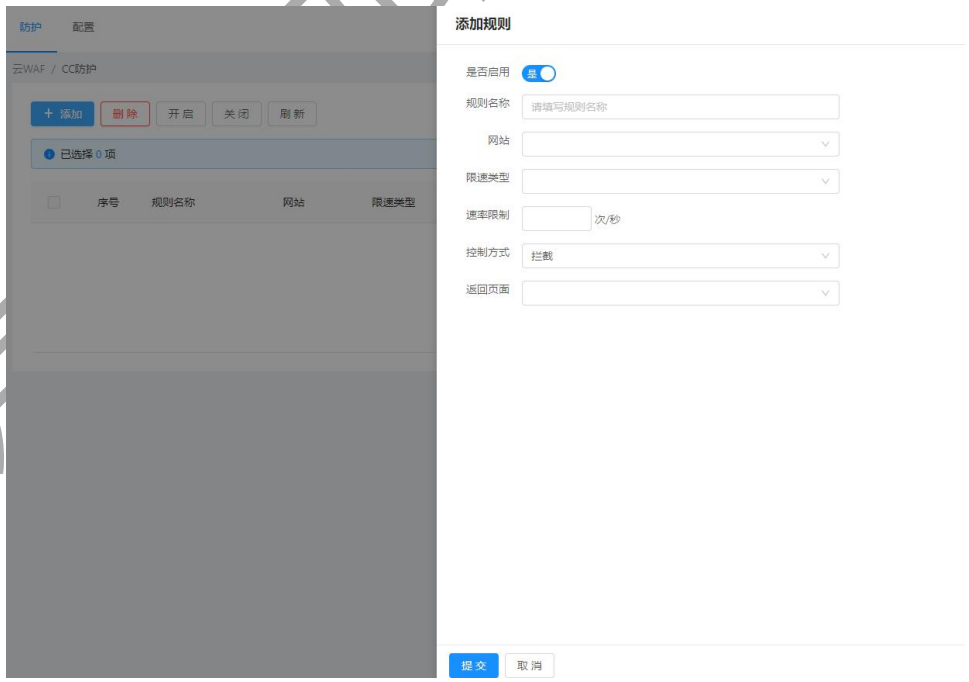
9.2. 攻击防护

对已经添加的业务进行防护控制，可选择开关攻击防护功能，隐藏错误页面功能，人机识别功能。



9.3. CC防护

在云 WAF 的 CC 防护页面，点击【添加】CC 防护规则。



是否启用：设置此条策略是否启用。

规则名称：自定义规则名称。

网站：选择已添加的网站。

限速类型：可选择根据 IP 限速或根据 URL 进行限速。

速率限制：N 次/秒。

控制方式：可选拦截/重定向。

返回页面：可选网站升级中、网站维护中。

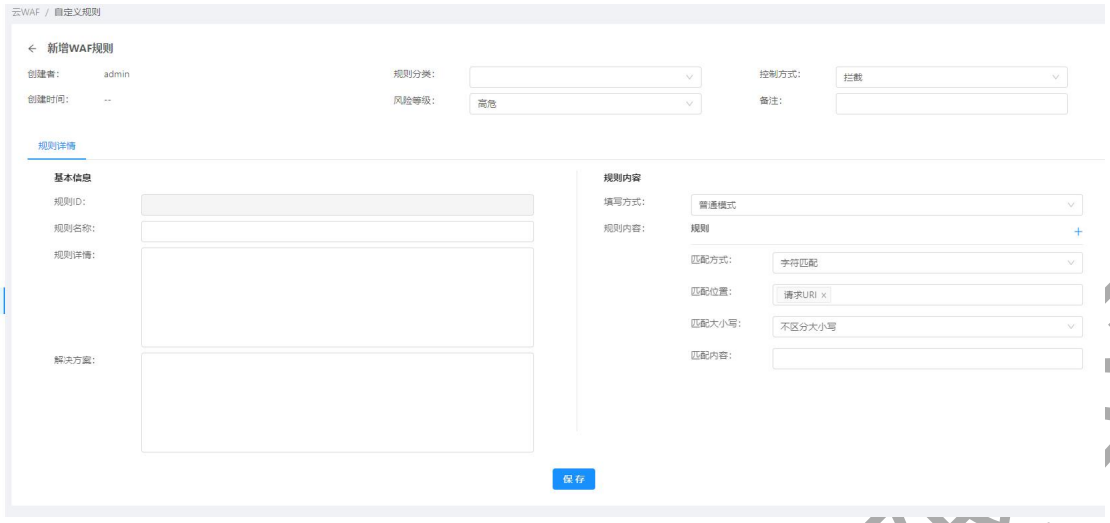
9.4. 防护策略

此页面展示内置规则策略，内置策略可以克隆为新建自定义策略进行试用。新建策略可进行导入或导出为模板。

9.5. 自定义规则

可根据需要编写 WAF 自定义规则。

北京国信



9.6. 防护日志

可使用网站信息，攻击类型，源 IP，日期范围进行检索 WAF 防护日志。防护日志展示规则 ID，发现时间，源 IP，地理位置，攻击类型，User Agent，目标，日志内容，级别，次数。

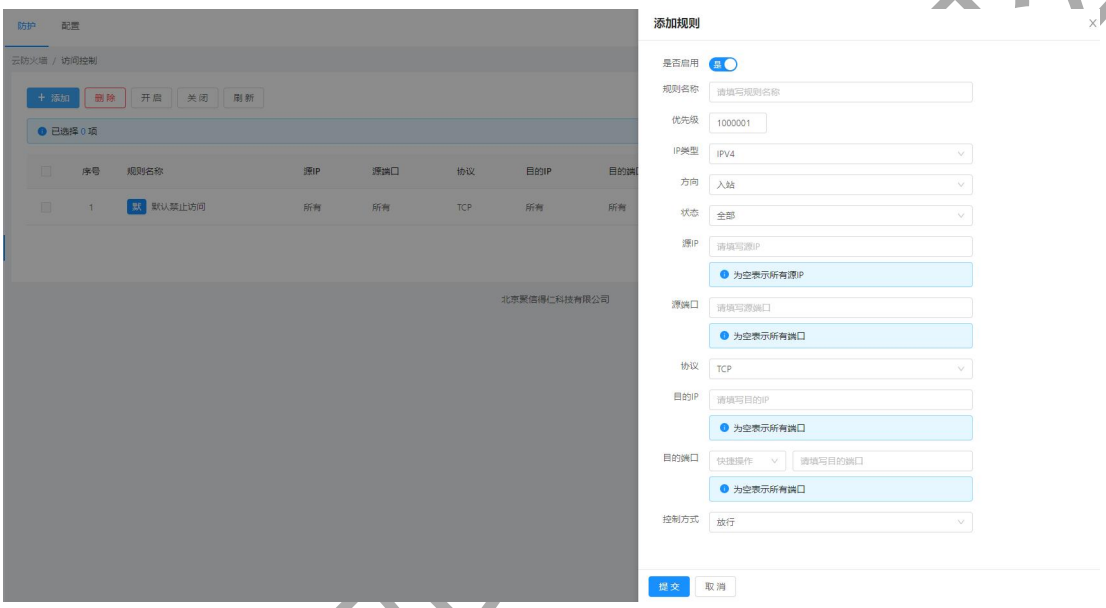
10. 云防火墙

10.1. 访问控制

访问控制默认情况下是对所有的 IP 拦截的，如果想要某一个 IP 放行，必须对其配置相应的访问控制策略。

北京国科技有限公司

点击【添加】进行访问控制策略配置，支持多种条件的访问控制规则，策略匹配按照优先级顺序匹配。



是否启用：控制是否启用此条规则。

规则名称：可自定义规则名称。

优先级：设置策略优先级，数字越大优先级越高。

IP 类型：可选择使用 IPv4 或 IPv6。

方向：选择策略是控制入站方向还是出站方向。

状态：可选择全部，新建，失效，无效。

源 IP：设置来源 IP。

源端口：设置来源端口。

协议：设置协议为 TCP/UDP/ICMP。

北京国信网

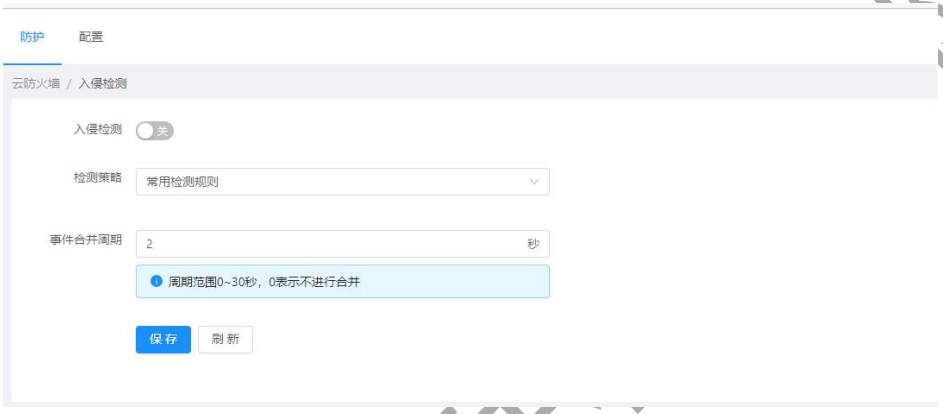
目的 IP：设置目的 IP。

目的端口：设置目的端口。

控制方式：可选择放行/封禁。

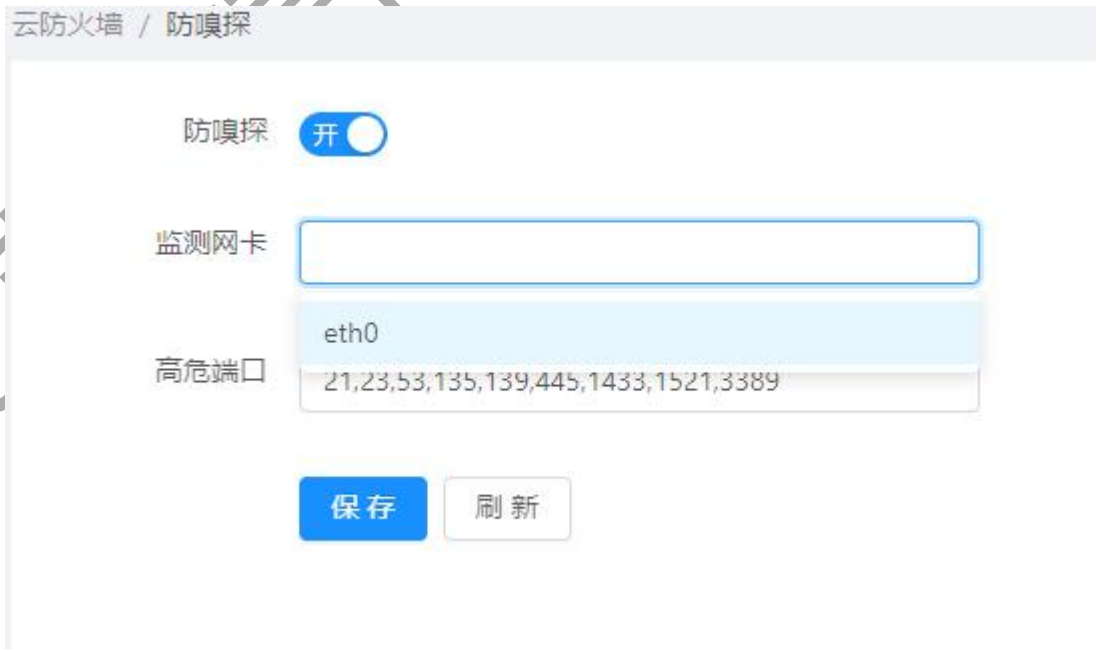
10.2. 入侵检测

此页面提供入侵检测开关功能，检测策略可选择常用检测策略/全部检测策略，事件合并周期可选择将在一定时间内发生的相同安全事件进行合并。



10.3. 防嗅探

可设置监测网卡及端口进行扫描防护。



北京网联浪公司

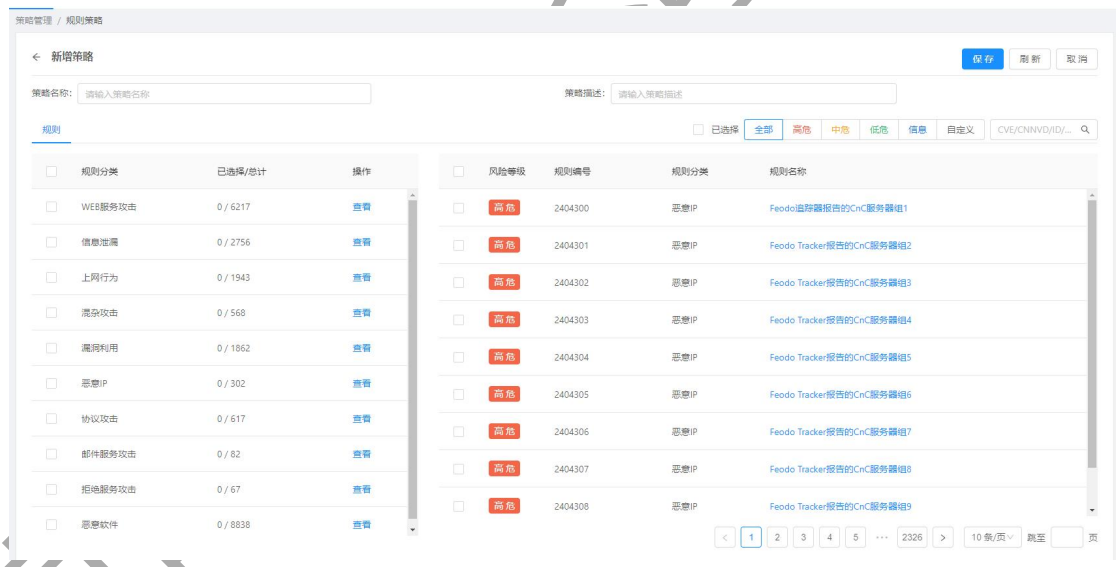
10.4. 防护策略

1) 内置规则

包含常用检测规则和所有检测规则。内置策略可以克隆为新建自定义策略进行试用。新建策略可进行导入或导出为模板。

2) 新建策略

可根据内置规则，手动定义监测内容。



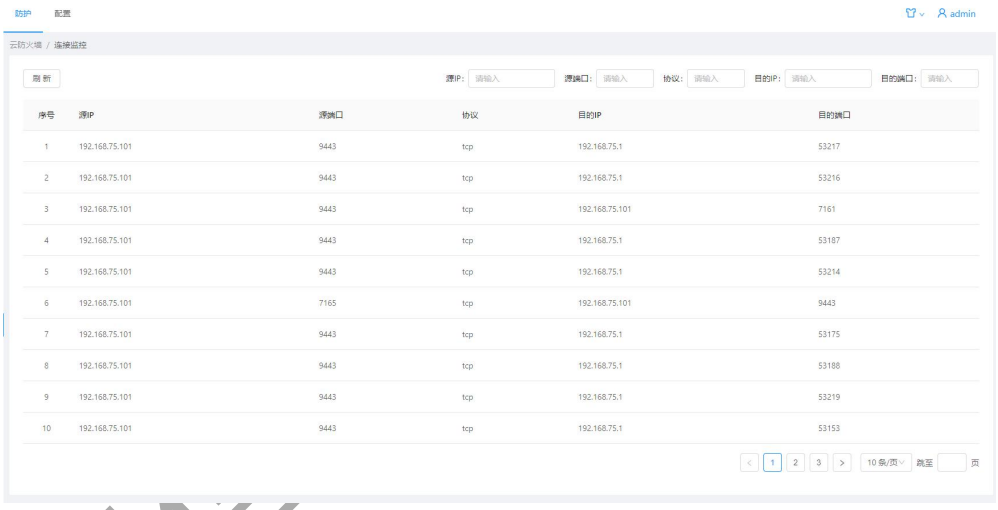
10.5. 入侵记录

可根据源 IP，源端口，目的 IP，目的端口，名称，等级，分类，ID，日期范围，协议，应用协议或合并条件的方式对已有安全事件进行筛选。

北京...技有限公司

10.6. 连接监控

对经过设备的所有请求进行监控，可根据以下信息进行搜索及展示：源 IP，源端口，协议，目的 IP，目的端口。

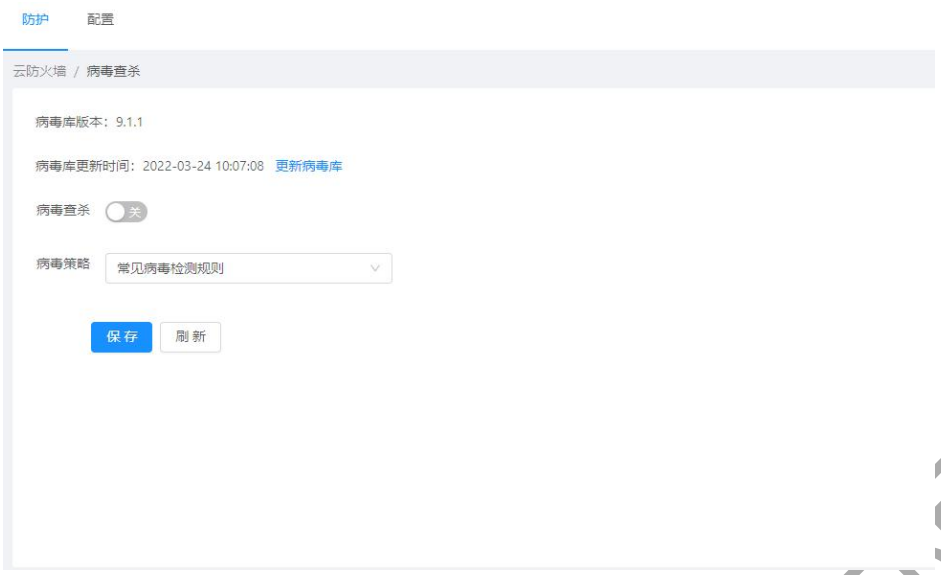


11. 防病毒

11.1. 病毒查杀

此页面展示当前病毒库版本信息，病毒库更新时间。提供更新病毒库按钮，点击后自动进行病毒库更新，病毒查杀功能开关（默认关闭此功能，开启后会消耗部分性能）；病毒策略可选择常见病毒规则或所有病毒检测规则。

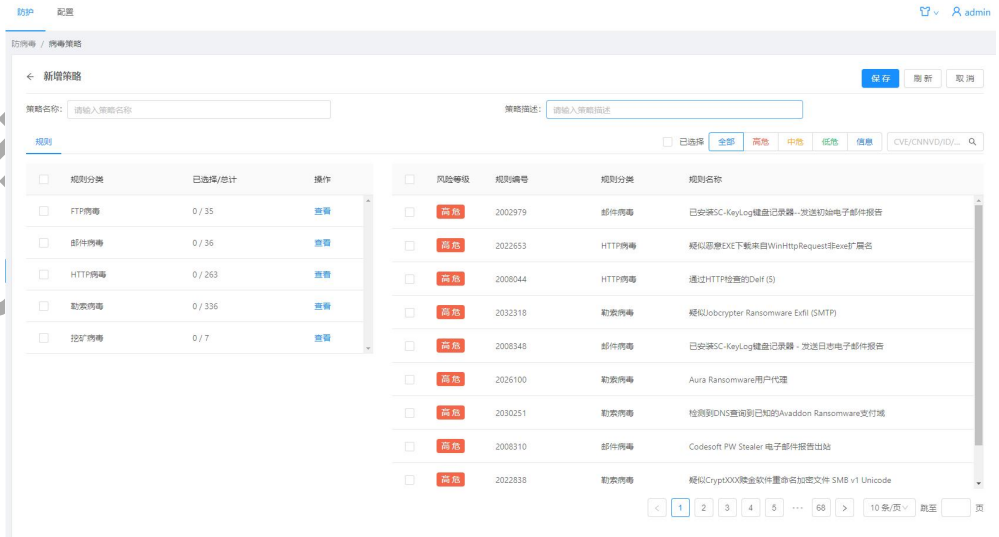
北京国信有限公司



11.2. 病毒策略

此页面展示内置规则策略，内置策略可以克隆为新建自定义策略进行试用。新建策略可进行导入或导出为模板。

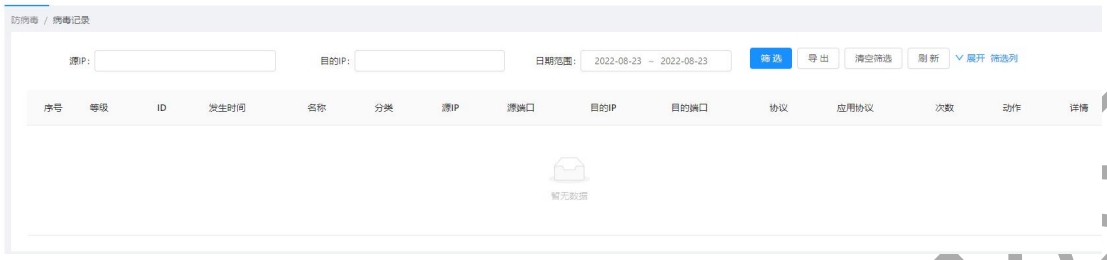
新建策略：可自定义策略中包含哪些规则。



北京某某科技有限公司

11.3. 病毒记录

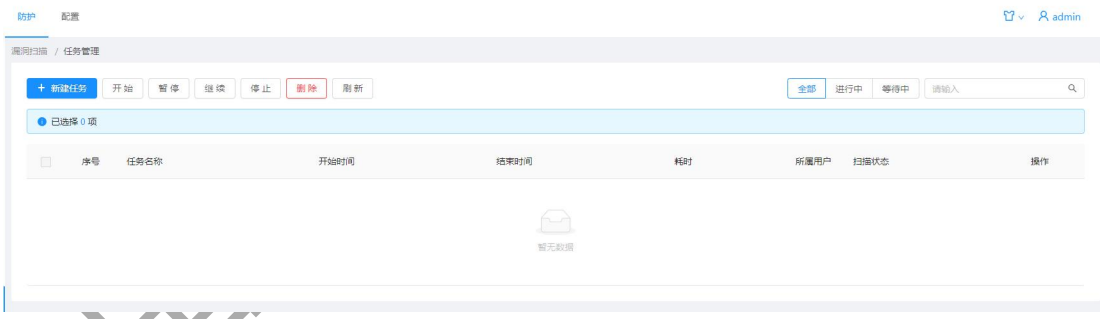
可展示对病毒防护的相关信息。



12. 漏洞扫描

12.1. 任务管理

此页面提供新建任务功能，同时可对任务进行开始，暂停，继续，停止，删除，刷新任务列表动作。可选择查看全部任务，进行中任务，等待中任务。列表展示任务序号，任务名称，开始时间，结束时间，耗时，所属用户，扫描状态，操作信息。



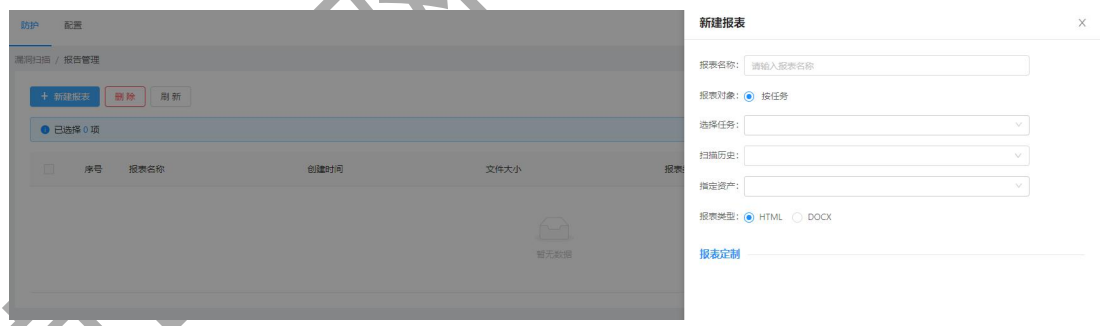
点击【新建任务】新建扫描任务，需填写任务名称，扫描类型为网站扫描/主机扫描，任务目标中选择需要进行扫描的资产。

北京[illegible]科技有限公司

12.2. 报告管理

报告管理界面提供新建报表，删除，刷新动作。可以根据报表名称检索已生成的报表，可展示报表序号，报表名称，创建时间，文件大小，报表类型，状态，操作信息。

点击【新建报表】进行生成报表操作。



报表名称：填入生成报表的名称。

报表对象：支持按照任务生成。

选择任务：可选择漏扫任务中的一个或多个来进行生成报表。

扫描历史：可根据扫描的历史数据生成报表。

指定资产：可根据一个或者多个资产进行生成报表。

北京[illegible]有限公司

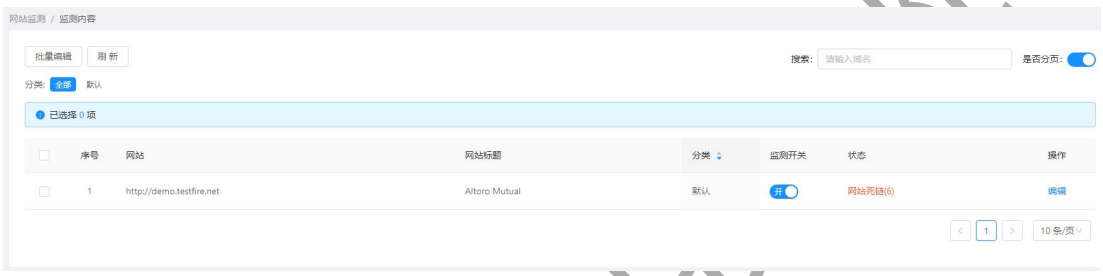
报表类型：可选择 HTML 格式或 DOCX 格式。

报表定制：可自定义报表标题名称。

13. 网站监测

13.1. 监测内容

可对资产是否开启监测进行开关。



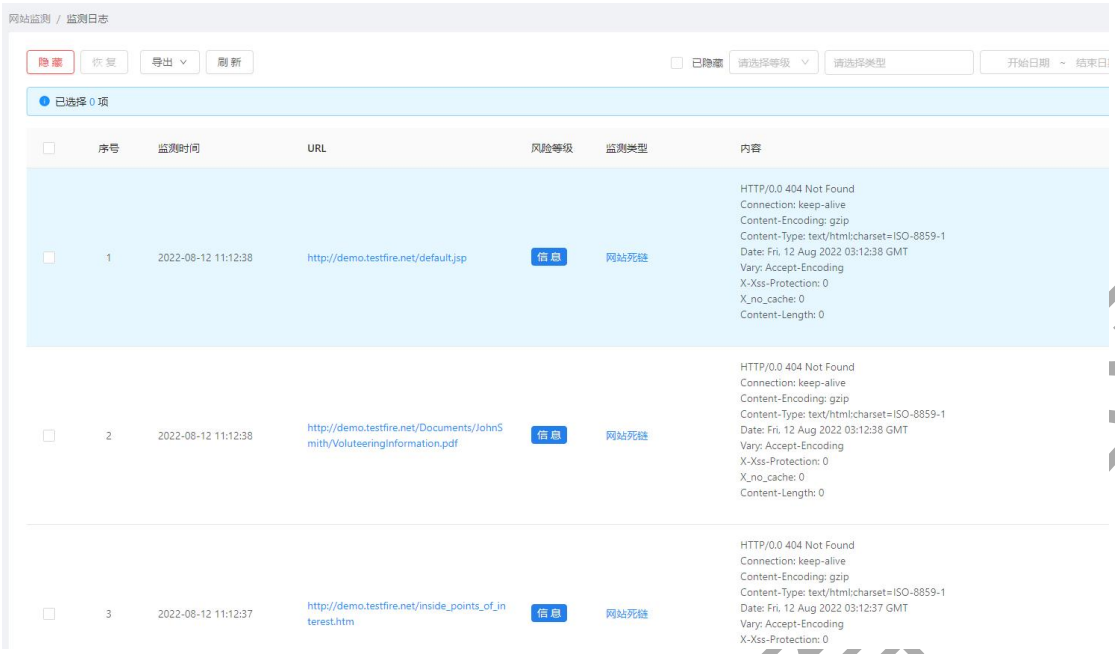
13.2. 监测策略

可选择监测内容，也可进行自定义策略编辑。

13.3. 监测日志

对检测到的异常内容进行展示。

北京聚信得仁科技有限公司



14. 日志审计

14.1. 日志查阅

14.2. 日志源

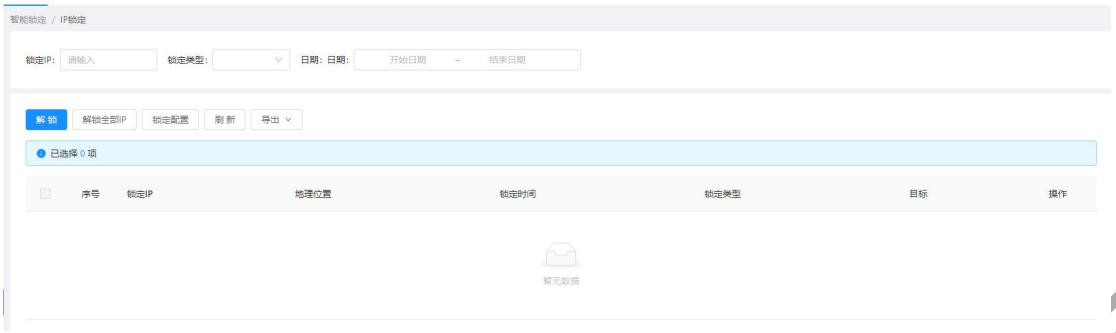
14.3. 采集服务

15. 智能锁定

15.1. IP锁定

在智能锁定的【IP 锁定】页面，可进行查看和解除当前被锁定阻断的 IP 地址，查看被锁定的时间，锁定 IP 及地理位置，阻断原因，攻击目标等详细信息。

北京国信网联科技有限公司



锁定 IP：可输入需要进行锁定的 IP。

锁定类型：可定义锁定 IP 类型为端口扫描/暴力破解/目录遍历。

日期：可选锁定 IP 时间范围，开始如期 - 结束日期。

解锁：可对选中 IP 进行解锁。

解锁全部 IP：可对列表中所有 IP 进行解锁。

点击【锁定配置】，可进行锁定时间和 IP 白名单的相关参数配置。

锁定时间：可设定锁定时间为一小时/一天/七天。

IP 白名单：可输入单个 IP 或 IP 段，支持 IPv6 地址。

16. 防护白名单

16.1. 白名单

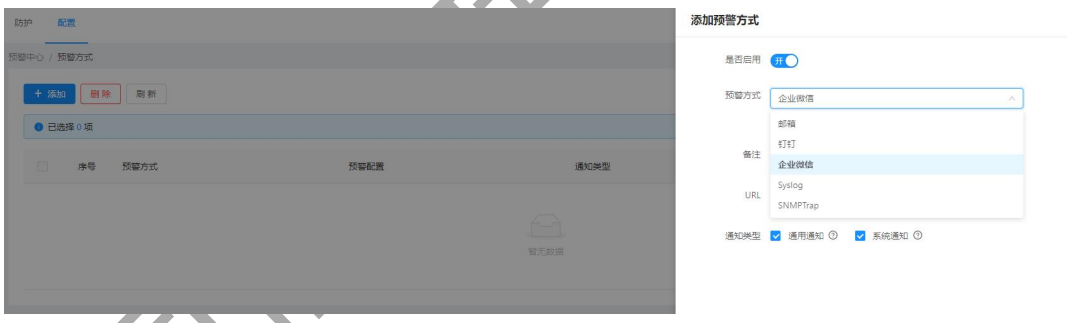
可根据防护类型进行 IP 添加白名单操作。

北京国信

17. 预警中心

17.1. 预警方式

在预警中心的【预警方式】页面，可选择使用邮箱，企业微信，钉钉，Syslog，SNMP Trap 发送预警，通知类型可选择通用通知或系统通知（相关内容可点击系统中功能后对应的在线帮助）。



17.2. 预警日志

展示预警列表，提供方式、预警时间、预警内容、预警结果信息。

北京国[illegible]科技有限公司

18. 计划任务

18.1. 定时策略

在计划任务的【定时策略】页面，可看查看和管理定时策略，支持添加定时策略。

点击【添加】可进行新建定时策略。

每周：可选择一个定时策略生效的时间范围，支持多个时间段。

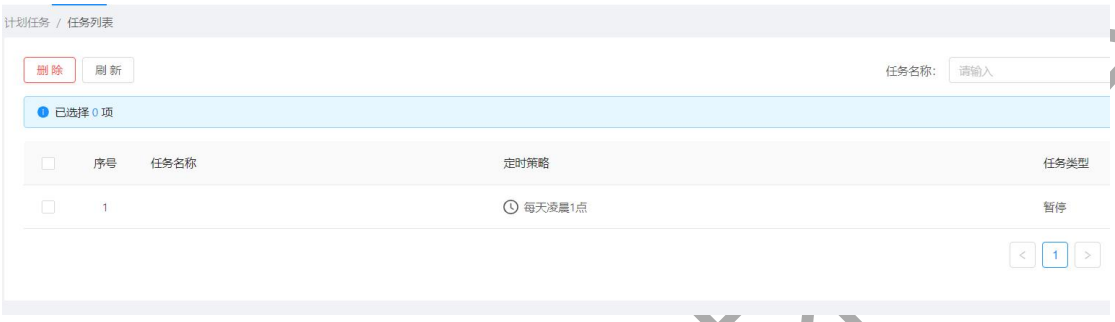
日期范围：可选择一个定时策略生效的日期范围，超过日期范围后定时策略无效。

北京有限公司

间隔小时：可选择一个间隔时间，每隔多长时间，执行定时任务。

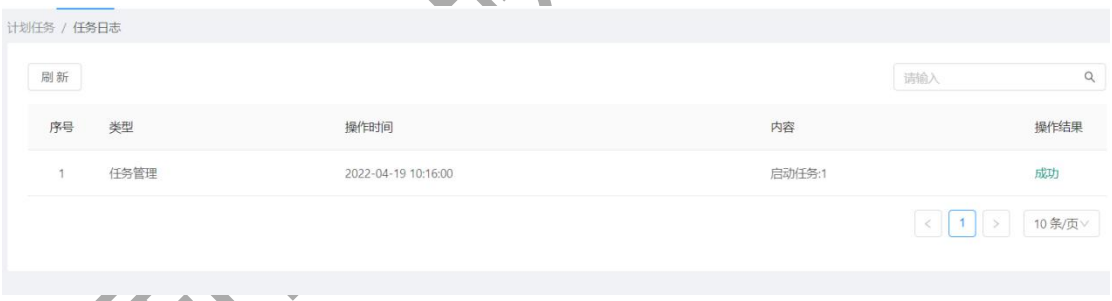
18.2. 任务列表

在计划任务的【任务列表】页面，可查看和管理所有关联了定时策略的定时任务，对于不需要的定时任务，可选择删除。



18.3. 任务日志

在计划任务的【任务日志】页面，可查看所有定时任务的执行情况，了解详细定时任务执行结果。



19. 对象管理

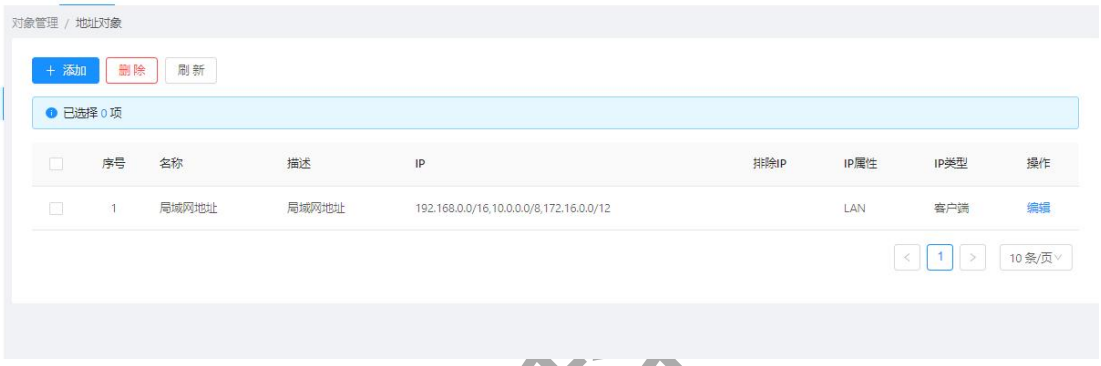
19.1. 证书管理

用于管理网站 SSL 证书，可以查看证书详细信息。

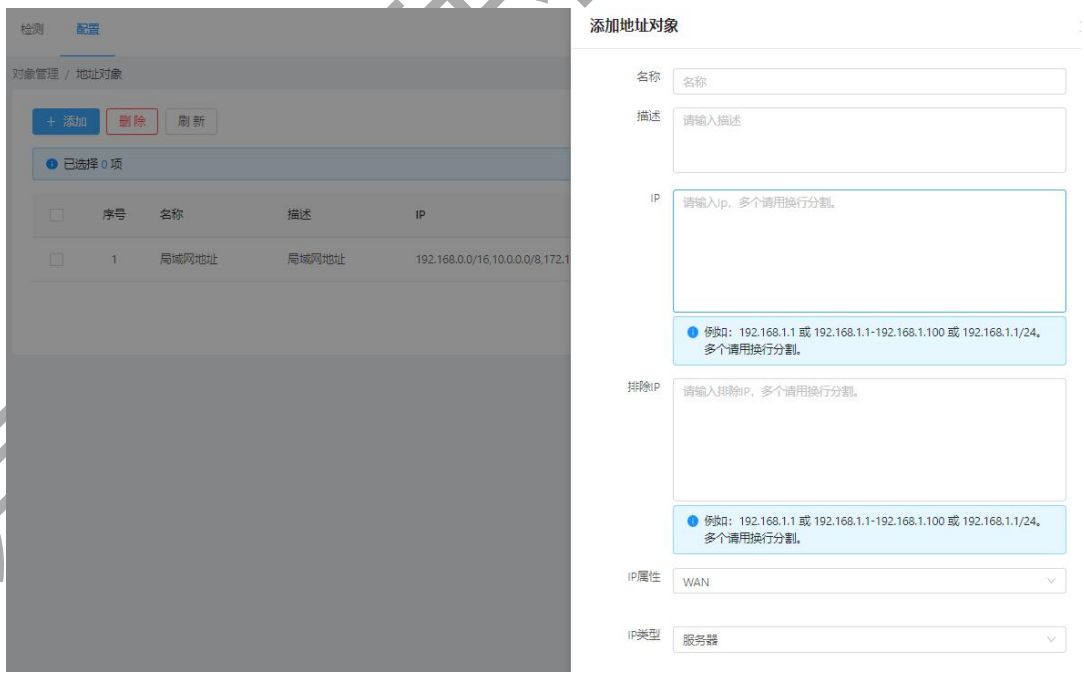
北京国咨科技有限公司

19.2. IP地址组

用于管理自定义 IP 地址组。

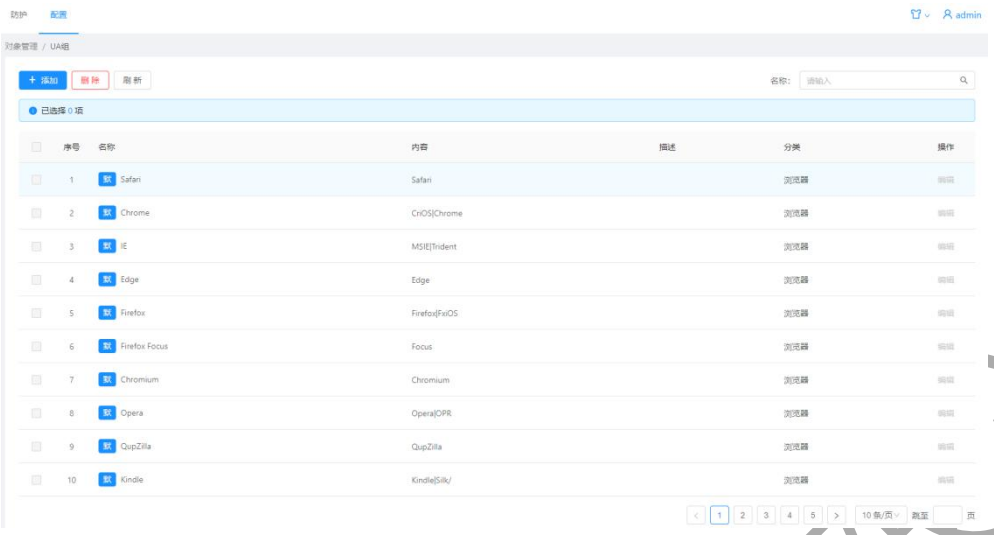


点击【添加】可新建地址组，填写地址对象名称，IP 地址，IP 属性，IP 类型。



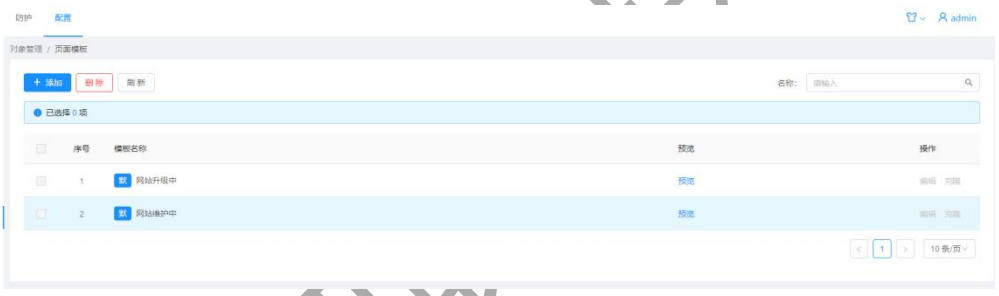
19.3. UA组

管理 UA 组，可用于访问控制。



19.4. 页面模板

用于重定向的页面模板。



20. 系统配置

20.1. 网络配置

20.1.1. 网卡配置

本页面列出了所有网络接口的工作状态，包括 IP 地址、子网掩码、网关、是否启用、工作方式、接口属性等信息。**注意：修改网络配置后，需要点击【应用】方能生效。**

北京国信网安科技有限公司

选择某个网络接口，点击【编辑】，对该网络接口进行配置，如下图所示。

网口属性

管理口：用于访问系统的 Web 管理界面，仅允许存在一个管理口。

镜像口：用于配置采集网络镜像流量的接口。

解析口：用于配置监听前端 http/https 协议的接口。

20.1.2. 路由配置

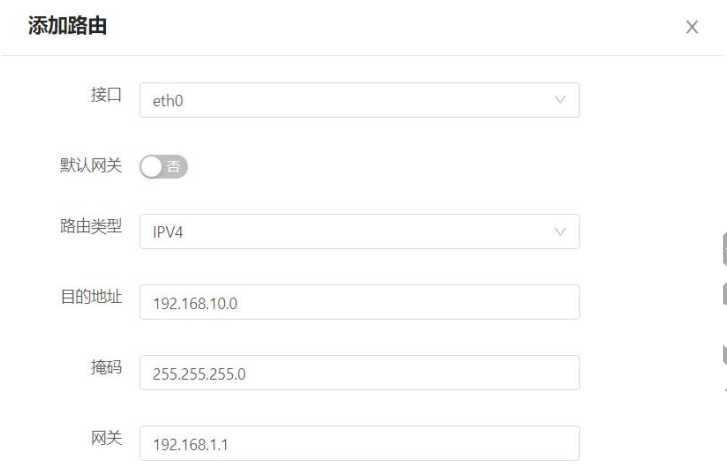
路由配置页面可以添加自定义静态路由。添加路由前，先了解部署环境网络拓扑，以免配置后导致系统网络无法连接。**注意：修改路由配置后，需要点击【应用】方能生效。**

大部分场景下，无需特别配置路由，使用默认配置即可。

默认网关：默认网关初始为管理口网关地址（不显示在路由列表中）。

北京国信网联

点击【新增】，添加静态路由进行配置，如下图所示。

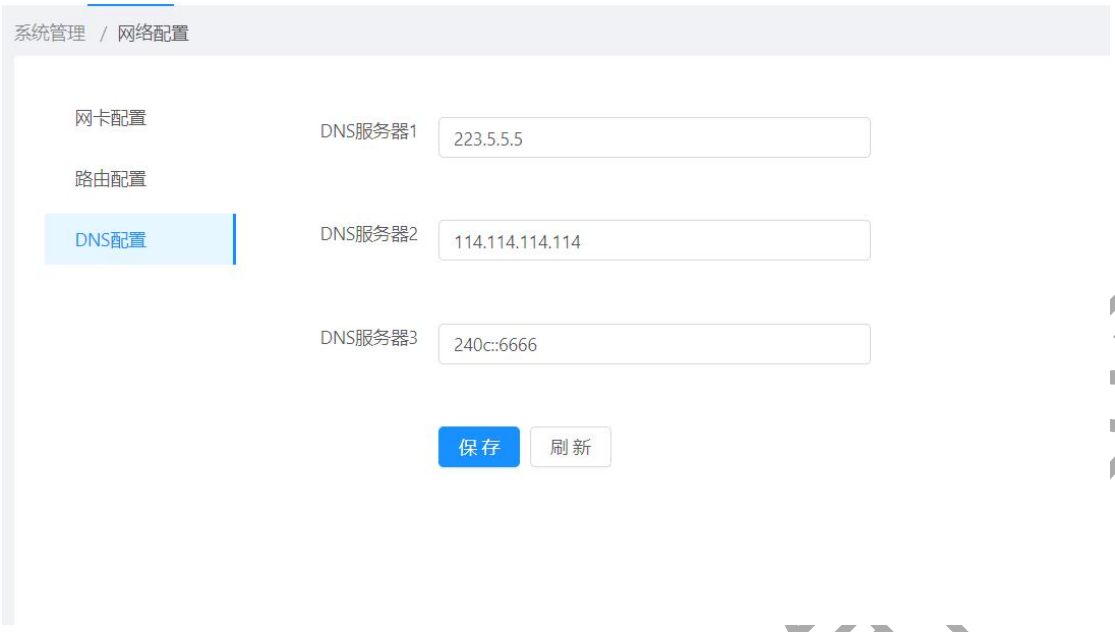


20.1.3. DNS配置

DNS 配置页面可以配置系统的 DNS 服务器，可设置 IPv4 和 IPv6 DNS 服务器。修改 DNS 地址时，根据部署环境设置正确的 DNS 服务器地址。**注意：修改 DNS 配置后，需要点击【应用】方能生效。**

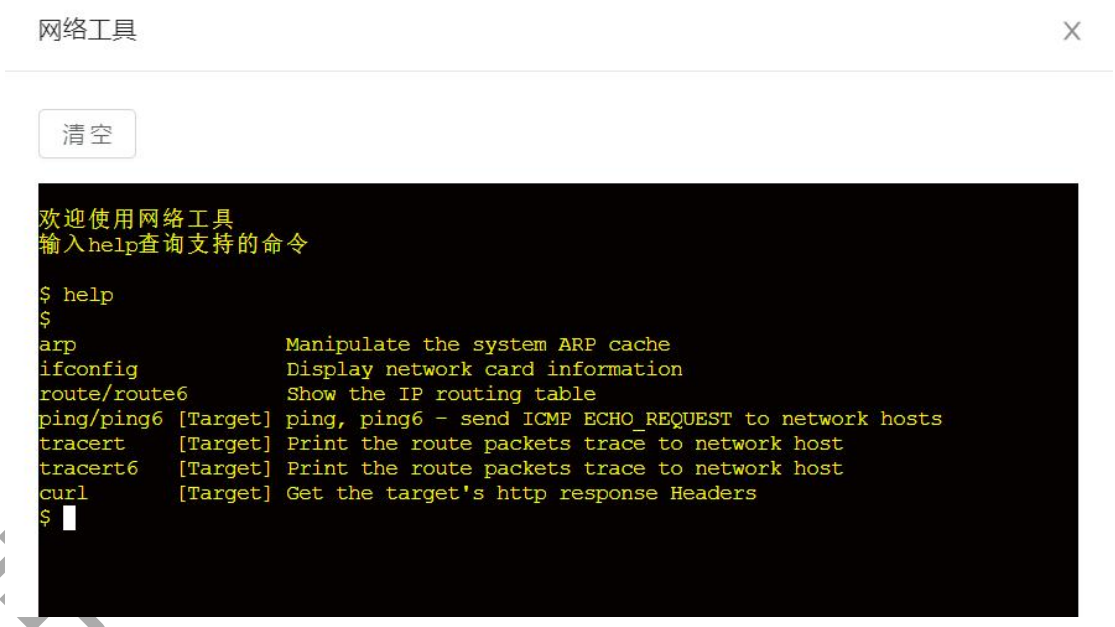
大部分场景下，无需特别配置 DNS 服务器，使用默认配置即可。

北京国信网联科技有限公司



20.1.4. 网络工具

在网络配置页面，系统提供【网络工具】功能，方便管理员进行网络测试。



如上图所示，目前【网络工具】包含以下几项功能。

help：显示帮助

arp：查看系统 ARP 信息

ifconfig：显示当前系统网卡配置信息

北京...技有限公司

route/route6：显示当前系统 IPv4/IPv6 路由表信息

ping/ping6：检查 IPv4/IPv6 网络是否可以连通

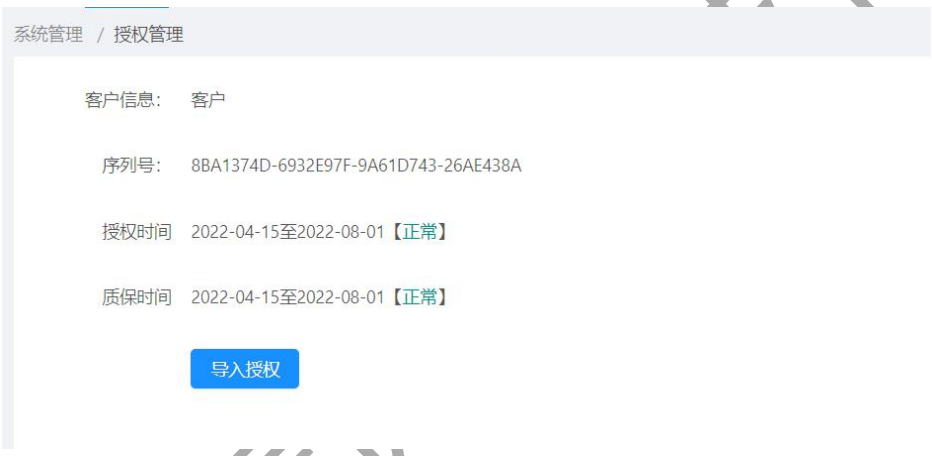
tracert/ tracert6：跟踪 IPv4/IPv6 路由所经过的路径

curl：利用 URL 获取目标的 http 响应头

20.2. 授权管理

授权管理页面用于查看和导入授权信息，用于查看客户信息、系统序列号、授权有效期等内容。

注意：授权过期后，产品功能将无法正常使用，请及时联系厂商人员更新授权。



点击【导入授权】选择授权文件进行【提交】，会校验授权信息并更新。

注意：第一次导入授权系统会进行初始化配置，耐心等待后请刷新页面。

20.3. 固件版本

20.3.1. 离线升级

固件版本页面用于查看和升级系统固件，上传固件升级文件，查看当前固件版本信息。

北京国信

手动下载固件升级包至本地电脑，并在本页面上传至系统中进行升级。

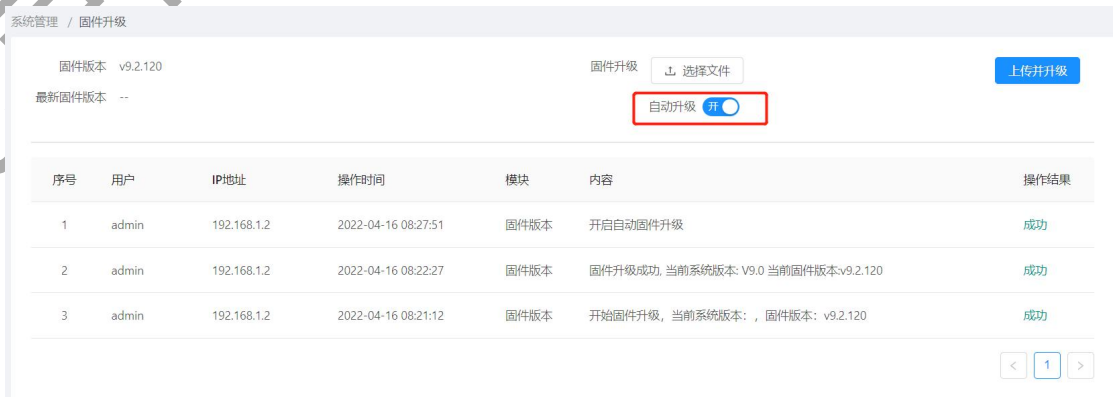
注意：如需获取固件升级包，请联系厂商人员。

点击【选择文件】，点击【上传并升级】，即进入固件升级流程。固件升级完成后，可以在日志中进行查看固件升级结果。

注意：固件升级过程中，系统无法进行配置，不要关闭系统电源，以免造成系统损坏。

20.3.2. 在线升级

在线升级固件需要打开【自动升级】开关，该功能默认关闭。通过自动检查更新获取最新固件版本信息，点击【安装】按钮自动下载和升级版本。



北京国信网安有限公司

打开后，系统会定时检查版本更新，如果检查到更新的版本，则会提示新版本相关信息。

注意：请选择恰当的时机进行固件升级，以免升级时造成业务中断。

20.4. 规则版本

20.4.1. 离线升级

规则版本页面用于查看和升级系统规则，上传规则升级文件，查看当前规则版本信息。

手动下载规则升级包至本地电脑，并在本页面上传至系统中进行升级。

注意：如需获取规则升级包，请联系厂商人员。

点击【选择文件】，点击【上传并升级】，即进入规则升级流程。规则升级完成后，可以在日志中进行查看规则升级结果。

20.4.2. 在线升级

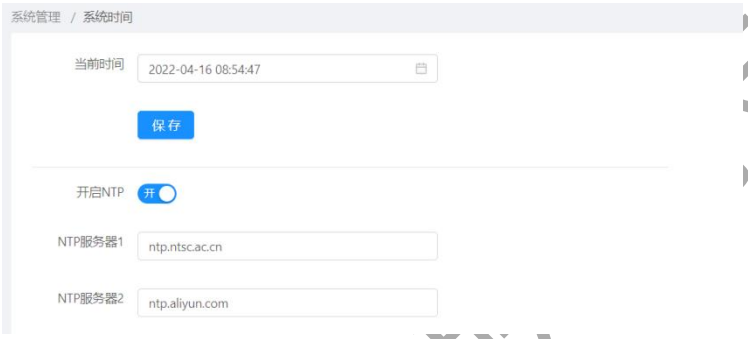
在线升级规则需要打开【自动升级】开关，该功能默认关闭。通过自动检查更新获取最新规则版本信息，点击【安装】按钮自动下载和升级版本。

版权所有，注意保密

打开后，系统会定时检查版本更新，如果检查到更新的版本，则会提示新版本相关信息。

20.5. 系统时间

系统时间配置页面用于配置系统时间以及 NTP 时间同步。



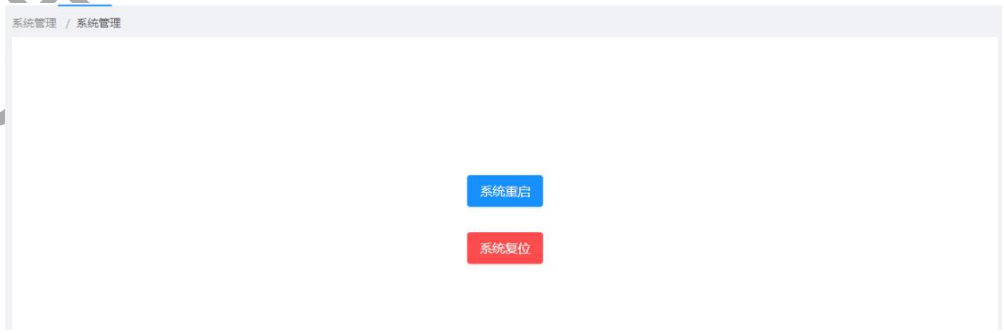
点击【当前时间】输入框，选择相应的时间后，点击保存后立即生效。

系统时间 NTP 同步服务默认自动开启，大部分场景无需特殊配置。

注意：系统时间和日志统计以及计划任务相关，请保持正确是时间配置。

20.6. 系统管理

系统管理页面用于系统重启和系统复位操作。



北京国信网安科技有限公司

点击【系统重启】进行重新启动操作，系统重启避免在设备运行的时候直接切断电源，以免造成系统损坏。

点击【系统复位】进行恢复出厂设置操作，重置并清除所有用户数据，此操作不可逆。请提前备份系统配置并且导出重要数据。

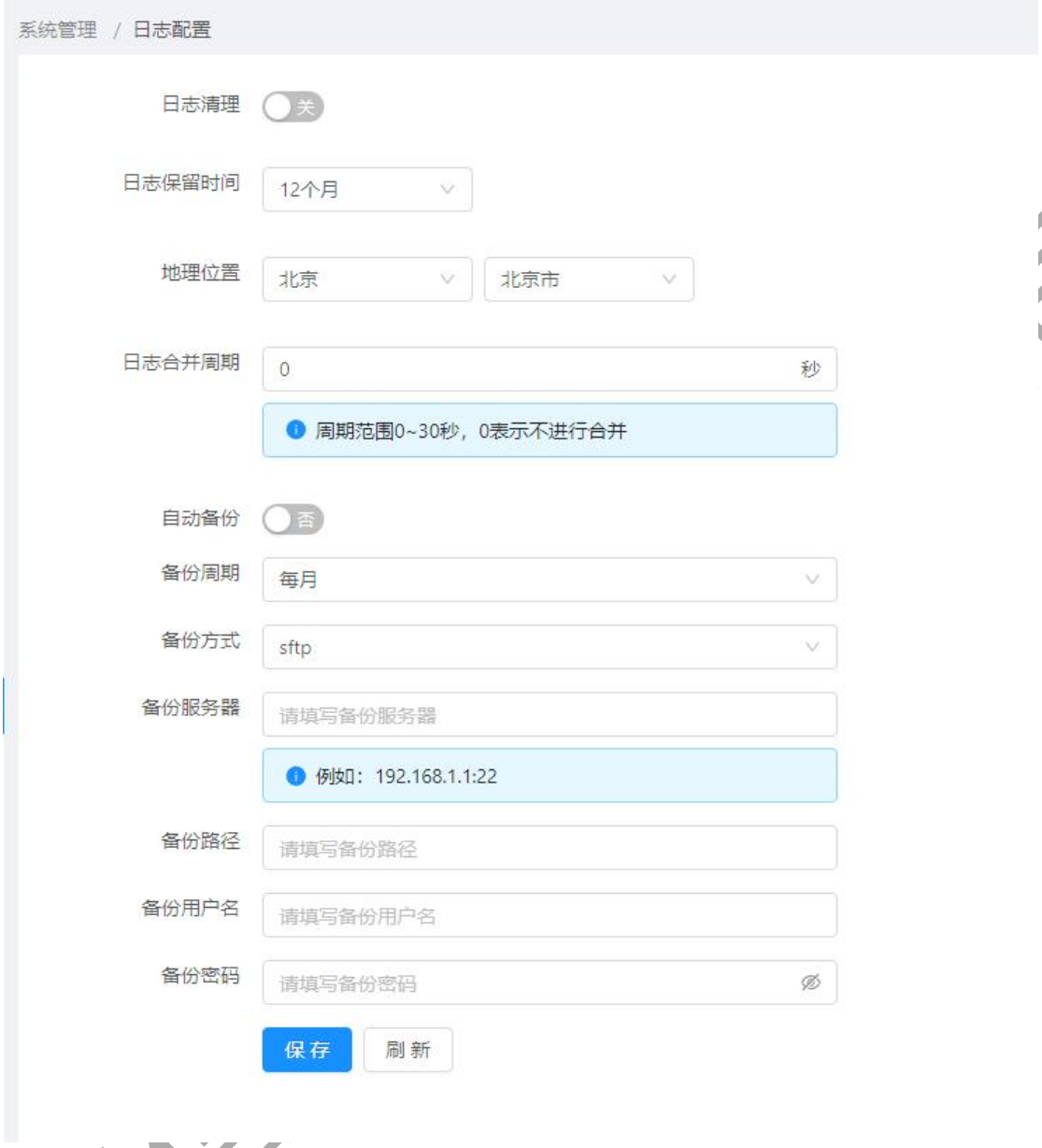
注意：系统复位后所有配置和运行数据将全部恢复到出厂状态。

20.7. 日志配置

日志清理：开启此功能后，可根据需要选择日志保留时间及日志来源地区，超出时间的日志将自动删除，也可设定合并重复日志。

自动备份：可选择使用 FTP 服务将日志备份到其他存储日志的服务器中。

北京国信网联科技有限公司



21. 集群管理

21.1. 本机信息

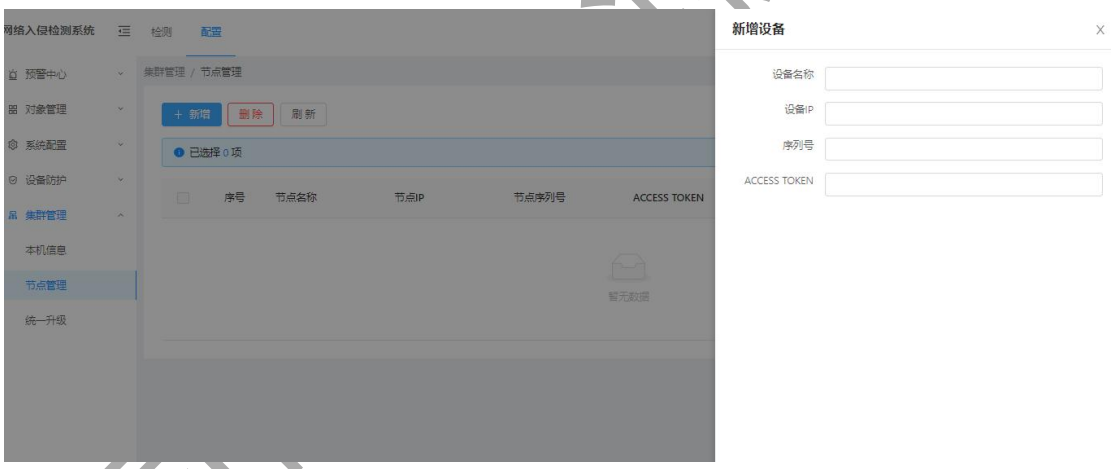
本机信息包含本机序列号，ACCESS TOKEN（加入集群需要此参数），以及本机状态。

北京国

21.2. 节点管理

在集群节点管理页面，可查看和管理节点设备信息，包括节点名称，节点 IP，节点序列号，ACCESS TOKEN，固件版本，规则版本等。

点击【新增】可添加节点设备，需填写设备名称，设备 IP，序列号，ACCESS TOKEN。



21.3. 统一升级

在统一升级页面，可进行集群统一升级操作，查看当前固件版本，规则版本，可对集群内节点设备进行统一的固件升级和规则升级操作。

北京国[illegible]科技有限公司

21.4. 数据同步

在集群状态下需配置数据同步，可保证集群内配置信息一致。

北京国信网联科技有限公司