恩创工业防火墙

用户手册

AVCOMM 恩创®

工业防火墙

用户手册

关于此用户手册

此用户手册旨在指导专业安装人员安装和配置工业防火墙。包括帮助避免意外发生问题的步骤。

注意:

只有合格且经过培训的人员才能对此产品进行安装、检查和维修。

免责声明

AVCOMM 保留随时更改本手册或产品硬件的权利，恕不另行通知。此处提供的信息目的是为了保证其准确可靠。但是可能不会涵盖所有的细节和更改，也并未提供在安装、操作或维护过程中遇到的所有可能的意外情况。如需更多信息，或出现未完全包含在此手册中的特定问题，应将此提交给 AVCOMM。用户有责任确定手册是否有任何针对添加的新信息和/或纠正可能的无意造成的技术或印刷错误进行的不定期更新和修订。AVCOMM 对其被第三方使用不承担任何责任。

AVCOMM 在线技术服务

在 AVCOMM，您可以使用在线服务表来请求支持。提交的服务表保存在服务器上，供 AVCOMM 团队成员分配任务并监控您的服务状态。如遇任何困难，请随时发邮件至 sales@n-tron.com.cn

目录

1. 概述

1.1 产品概述

恩创工业防火墙产品的硬件与软件均拥有完全自主知识产权，坚决杜绝后门的隐患，本产品拥有多种网络接入模式(同时支持电口和光口)，管理形式上采用集中管理分散部署的方式。对工业防火墙进行配置管理的统一安全工业防火墙是产品不可分割的一部分，该平台采用 B/S 架构，管理员可在任意连通到工业防火墙的机器上便捷的访问和管理，大幅提高运维效率，有效降低维护成本。产品硬件采用完全符合工业标准的自主设计，可以部署和应用到各种复杂的工业生产环境，硬件经过 CE，CB 和 FCC 等业内顶级标准认证，可以稳定长期不间断运行，大幅减少客户的系统停车时间。工业防火墙软件采用完全自主可控的架构设计，各主要功能模块互相配合，对流通在客户工控网络中的所有数据进行全方位的解析、判断和控制，有效保障客户正常生产数据的传输，完全杜绝非法数据和病毒在客户工控网络中的分散和传播，最大程度上保证了客户生产的长期安全稳定运行。

1.2 外观与说明（S2124)

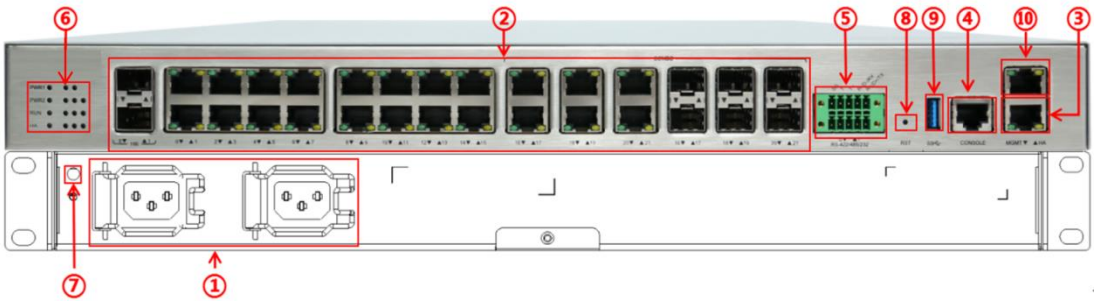


图 **错误!文档中没有指定样式的文字。**-1 产品系列中 S2124 的外观

①双路 220V 冗余电源输入
②2 个 10000M SFP+业务光口；16 个 10/100/1000M 自适应业务 GE 口；6 个 10/100/1000M 自适应 Combo 光电互斥业务接口
③1 个 10/100/1000M 自适应 RJ45 管理口
④1 个 RS232 转 RJ45 调试串口
⑤2 个 RS485/422/232 自适应业务串口，采用凤凰端子
⑥指标灯
⑦接地
⑧reset 按键，短按设备重启，长按(5s 以上)设备恢复出厂设置
⑨1 个 USB3.0 接口
⑩1 个 10/100/1000M 自适应 RJ45 HA 接口
当设备工作在接口对模式时，紧连在一起的为一对，如 0、1GE 口为一对。一对中的任意一个可以做为入口，另外一个作为出口。两对之间不可交叉。注意当开启端口同步(可关闭)时，成对的物理端口状态会保持一致，遵循下表的行为：

表 **错误!文档中没有指定样式的文字。**-1 端口同步状态表

场景	端口状态	备注
物理端口全部不接线	全部 down	
物理端口仅有一个接线	全部 down	
物理端口全部接线但对端没有连接	全部 down	
物理端口全部接线但对端仅有一个连接	全部 down	
物理端口全部接线且对端全部连接	全部 up	

1.3 指示灯说明（S2124）

设备上有 4 个主要的指示灯，分别为 PWR1、PWR2、RUN、HA 指示灯,还有 11 路的 BP 指示灯及各个网口自身的指示灯。

表 **错误!文档中没有指定样式的文字。**-2 工业防火墙指示灯说明

指示灯	面板丝印	状态	说明
电源指示灯 1	PWR1	常灭	电源未接入或电源模块故障
		绿色常亮	电源正常工作
电源指示灯 2	PWR2	常灭	电源未接入或电源模块故障
		绿色常亮	电源正常工作
系统灯	RUN	常灭	系统未运行
		绿色常亮	系统处于上电加载或复位启动状态
		绿闪每 2 秒一次	设备正常运行
		绿闪每秒 4 次	系统处于启动中
		红色常亮	系统故障 如整机上电自检、电压、温度检测出现异常
HA 灯	HA	常灭	未开启双机热备功能
		绿色常亮	双机热备正常工作，此设备为主设备
		绿闪每 2 秒一次	双机热备正常工作，此设备为从设备
		红灯常亮	双机热备出现故障
旁路指示灯	BP	常灭	未启动 BPYASS 功能
		常亮	启动 BYPASS 功能
以太网电接口指示灯	MGMT	常灭	对应接口处于未连接状态
		指示灯颜色	绿色表示当前工作在千兆速率下

			橙色表示当前工作在十兆或百兆速率下
		指示灯常亮	接口已经建立连接
		指示灯闪烁	接口正在收发数据
	业务口（GE 0-15、Combo 16-21）	常灭	对应接口处于未连接状态
		指示灯颜色	绿色表示当前工作在千兆速率下 橙色表示当前工作在十兆或百兆速率下
		指示灯常亮	接口已经建立连接
		指示灯闪烁	接口正在收发数据
以太网光接口指示灯	业务（SFP+ 0-1、Combo 16-21）	常灭	对应接口处于未连接状态
		绿色常亮	接口已经建立连接
		绿色闪烁	接口正在收发数据

1.4 技术规格

表 **错误!文档中没有指定样式的文字。**-3 工业防火墙技术规格

技术指标项	S2124	S2112	S2106
硬件要求指标	采用工业级 64 位 ARM 四核处理器，配置自研操作系统		
	16 个千兆电口、6 个千兆 Combo 口和 2 个万兆光口	8 个千兆电口和 4 个千兆 Combo 口	6 个千兆 Combo 口
	1 个 RJ45 MGMT 带外管理口和 1 个 RJ45 HA 接口		1 个 RJ45 MGMT 带外管理口
	1 个 RJ45 Console 管理口		
	配置 2 个 RS485/422/232 三合一串口		
	支持 11 组 bypass	支持 6 组 bypass	支持 3 组 bypass
	支持断电 Bypass 和看门狗		
	bypass 切换时间≤3S		
	配置冗余双电源；		

		MTBF≥250,000 小时；		
		防护等级≥IP40		
		密闭无风扇设计		
		机架式安装		DIN 导轨和壁挂式安装
性能要求指标	整机功耗	≤50W		≤25W
	OPC 数采点数	≥200000 点		≥100000 点
	时延	90%吞吐量条件下配置策略后时延≤200us		
	整机最大吞吐	10Gbps	10Gbps	6Gbps
	最大并发	≥100 万	≥100 万	≥30 万
	每秒新建连接	≥10000	≥10000	≥5000
工作温度		-10℃～60℃		-40℃～75℃
功能指标	部署方式	支持路由、交换、接口对和混合模式部署		
	工作模式	支持学习、告警、防护，三种工作模式		
	管理方式	支持自管理		
		支持统一集中管理		
		支持通过工业防火墙实现安全产品的自动升级		
		支持通过图形化方式进行设备的远程配置		
	状态检测	支持默认禁止原则，除非明确允许，否则就禁止		
		支持基于五元组的安全策略：源、目的 IP，源、目的端口，协议类型的部分或全部组合		
		支持基于 MAC 地址的访问控制		
		支持用户自定义的安全策略，包括 MAC 地址、IP 地址、端口的部分或全部组合		
		支持用户指定包过滤策略在特定网口、网桥或者 VLAN 上生效的功能		
		基于连接状态的检测结果来决定允许或拒绝数据流通过		
	白名单	支持 OPC、Modbus TCP、Siemens S7、Ethernet/IP(CIP)、IEC104、Profinet、OMRON Fins、MMS、DNP3 等工业协议的深度解析，支持指令功能码、寄存器值、动态端口、读写操作异常报文的识别和控制		

		支持 OPC、Modbus TCP、S7 协议值域控制
		支持 OPC 基金会发布的 OPC 3.0 规范
		可自定义工业协议在现场的服务器使用的具体端口号
	串口白名单	支持对串口参数进行配置
		支持“MODBUS_RTU”协议的串口白名单
		支持“MODBUS_RTU”协议的值域控制
		支持串口白名单的自学习
		支持语法检查
	启发式白名单自学习	支持学习数据的统计及实时展示
		支持学习进度提示功能，对下一步工作给出合理建议
	解码引擎	快速支持工控协议解析，无需二次开发
		针对定制协议具备深度解析每个报文字节的能力
	设备管理	可以添加和编辑系统中的设备
		可通过 IP 认证、IP + MAC 绑定方式实现只有允许的可信主机才能访问目前设备系统
	拓扑管理	编辑、显示当前系统拓扑；
		防火墙设备自发现，并自动出现在右侧设备列表中；
		显示出防火墙的在线、离线状态和告警状态；
	实时监控	支持事件实时监控，并支持事件导出功能；
		支持日志监控功能；
		支持未知设备监测，对系统内未知的设备接入进行实时告警，迅速发现系统中存在的非法接入，并能够支持阻断功能
		可实时查看网络会话表
	路由功能	支持静态路由功能，路由表条数 1000 条
		支持 VLAN 透传、封装、解封装，提供 802.1Q 模式。
	告警管理	支持消息告警、声音告警等告警方式
	日志审计	支持白名单告警日志、地址欺骗日志、防火墙告警日志、运行日志
		支持给电网安全监测装置发送 Syslog 日志
	安全策略	支持手动配置 5 元组访问控制规则；
		支持基于白名单的访问控制策略；
		支持自学习创建白名单规则，学习时间可自行调节；
		支持 IP/MAC 地址绑定规则；
		支持主机白名单功能，发现流经网络的未知设备；

		支持 ACL 时间段控制；支持 ACL 快速查找，支持自定义 ACL，ACL 规则数量达到 1000 条
	配置管理	支持学习模式、测试模式和工作模式，且用户可自主配置；
		支持报表功能，用户通过报表可查看事件、日志和审计的统计数据，支持报表下载；
		支持一键远程恢复出厂设置；
		IP 认证及 IP + MAC 绑定；
	VPN	支持以 IPSec VPN
		支持隧道配置、隧道监控
		支持预共享密钥和 X.509 数字证书两种认证方式进行 VPN 认证
	NAT	支持双向 NAT：SNAT 和 DNAT；
		SNAT 可实现“多对一”地址转换，使得内部网络主机访问外部网络时，其源 IP 地址被转换。
		DNAT 可实现“一对多”地址转换，将 DMZ 的 IP 地址/端口映射为外部网络合法 IP 地址/端口，使外部网络主机通过访问映射地址和端口实现对 DMZ 服务器的访问。
	抗 Dos	支持识别和拦截 TCP Flood、UDP Flood、ICMP Flood 等洪泛攻击
		支持识别和拦截 Land、Teardrop、Ping of Death 等包攻击
	扫描防护	支持检测和记录扫描行为，包括对防火墙自身和受保护网络的扫描
		支持网络扫描防护：tcp 扫描、udp 扫描、ICMP 扫描、文件共享扫描，主机抑制时长（秒级可配）
	IPS	支持基于特征的恶意报文检测与防护
		支持不少于 3000 条特征库，且支持工业安全事件特征库
		白+黑双检测机制，支持白名单过滤后的报文检测
	带宽管理	支持带宽保障功能，使得在带宽出现拥堵时，能够保障重要终端的网络通信
	流量监测	通过 IP 地址、网络服务、时间和协议类型等参数或它们的组合对流量进行正确的统计；
		实时或者以报表形式输出流量统计结果
		流量超过预警值的行为进行告警
	高可用性	支持双机热备
		支持 Bypass，切换时间不超过 3 秒
	网络诊断	支持 Ping 和 Tracert 等网络诊断
	远程维护	支持远程维护功能（开启/关闭 SSH）

2. 启动和登录

2.1 设备启动

确保工业防火墙的电源接头正常，将其与要求的电源接通后，工业防火墙将开始正常启动。

2.2 cli 的使用

CLI（Command Line Interface，命令行接口）是用户与设备之间的文本类指令交互界面。用户输入文本类命令，通过输入回车键提交设备执行相应命令，从而对设备进行配置和管理，并可以通过查看输出信息确认配置结果。

工业防火墙支持命令行接口界面，通过串口登录设备后使用默认的用户名为：cli，默认密码为：Cmd@753 如下图所示。进入命令行接口界面，设备的命令行接口界面下图 2-1 所示。

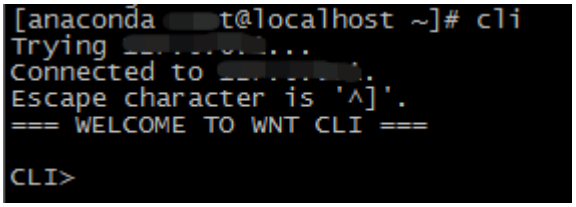


图 **错误!文档中没有指定样式的文字。**-2 命令行界面

工业防火墙设备也支持通过 SSH（此服务默认关闭）登录设备后进入命令行接口界面。

2.2.1 帮助

CLI>help

显示帮助信息。

2.2.2 系统统计信息相关

CLI>show pkt stat

查看各层次报文统计信息

CLI>show mgmtip

查看管理口 IP 地址信息

CLI>show mem pool

查看 mem pool 内存信息

2.2.3 进入系统配置视图

CLI> config

进入系统配置视图。

2.2.4 更改管理口的 IP 地址

注意：在自管理界面，除了 Web 可以更改管理口的地址外，也可以通过 Cli 命令进行更改。如果进行配置，需先使用 config 命令进入系统视图

CLI#set mgmtip <ip> [netmask]

更改设备管理口的 IP 地址

例如:将工业防火墙 A 管理口的 IP 地址更改为 192.168.8.6,掩码 255.255.255.0 的完整命令如下:

CLI# set mgmtip 192.168.8.6 255.255.255.0

2.2.5 设置集中管理平台的地址

CLI>show serverip

查看工业防火墙上配置的集中管理平台的 IP 地址

CLI#set serverip <IPV4ADDR:serverip>

设置工业防火墙需要连接到的统一安全管理平台的 IP 地址，

例如：管理平台的地址为 192.168.8.8，那么完整命令如下：

CLI> set serverip 192.168.8.8

CLI#set mgmtgw <IPV4ADDR:serverip>

设置工业防火墙网关命令，

例如：需要增加网关地址为 192.168.1.1，那么完整命令如下：

CLI# set mgmtgw 192.168.1.1

& 注意：

将 Serverip 设置为 127.0.0.1 时，设备将只能进行自管理，自管理和集中管理二者同时只能选择一种。

2.2.6 设置独立日志管理平台的地址

CLI> show ext stat

STATUS: OFF

SERVER IP:

SERVER PORT: 0

查看日志服务器配置状态， STATUS：OFF 表示没有开启，ON 表示处于开启状态

CLI# set ext enable

All done!

开启日志服务器上传方式

CLI# set ext disable

All done!

关闭日志服务器上传方式

CLI# set ext localip <IP>

设置管理口第二个 IP 段地址，用于日志服务器的连接。

CLI# set ext serverip <IP>

设置日志服务器地址

CLI#set ext serverport <PORT>

设置日志服务器端口

2.3 设备的启动

按照安装手册的说明，检查设备硬件已经正确配置完毕后，将电源线接通，设备将开始启动。请将网线与 MGMT 接口连接（此为设备的管理口），初始 **IP 地址默认是 192.168.8.8**（此为设备默认管理 IP 地址，后续可根据需要自行修改）。

设备启动完成后，在网络可达设备的主机上开启浏览器（推荐使用谷歌浏览器），并输入如下类似的网址：https://192.168.8.8:8440

即可以管理设备，进行后续的登录和配置。

&说明：

如果浏览器报如下图的错误，您只需要点击浏览器页面下面的“高级”，然后再选择“继续前往192.168.[illegible]（不安全）”即可。

图 **错误!文档中没有指定样式的文字。**-3 安全提示

启动正常的设备在输入以上地址后将打开如下的登录界面：

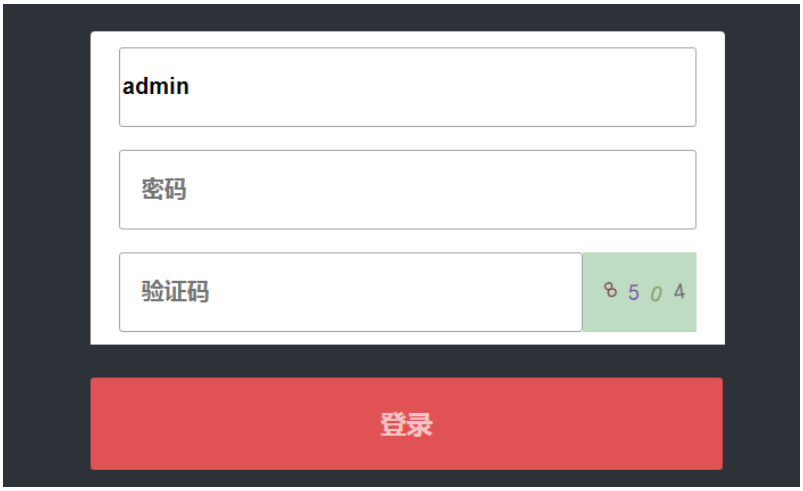


图 **错误!文档中没有指定样式的文字。**-4 设备登录界面

2.4 设备的登录

设备启动后，在上述所示的登录界面，输入正确的用户名、密码和验证码，点击<登录>，将进入系统的配置页面。

目前工业防火墙支持三种角色的用户，如果是首次登录管理系统，将以默认的用户“admin”和默认密码“Admin@123”进行登录操作，进入系统后，不同角色的用户拥有不同的权限。可以创建其它角色的用户为系统操作员，但创建后需要经过系统审核员批准后才会真正的生效。

系统内置的角色有：系统操作员、配置管理员、审计管理员。如下表：

表 **错误!文档中没有指定样式的文字。**-4 系统内置账户信息

用户名	默认密码	角色
admin	Admin@123	配置管理员
audit	Admin@123	审计管理员
Sysoperator	Admin@123	系统操作员

如果配置了自定义的用户，后续可以使用这些用户进行分权分级管理。管理账户登陆后，如图 2-4 所示：

图 **错误!文档中没有指定样式的文字。**-5 管理账户登陆

3. 系统面板

3.1 统计及监控

系统面板的统计包括告警统计、网络流量监控统计、并发会话监控统计，如图 3-1 所示:

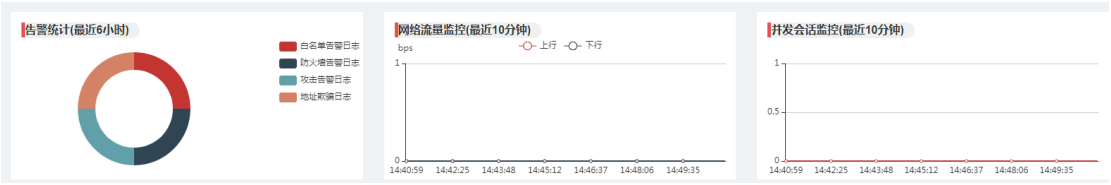


图 **错误!文档中没有指定样式的文字。**-6 系统状态统计图表

3.2 系统资源使用率

系统资源使用率实时展示目前系统资源包括 CPU、内存、硬盘的实时使用情况。如图 3-2 所示:

图 **错误!文档中没有指定样式的文字。**-7 系统资源使用率

3.3 接口信息

接口及设备信息包括了接口的部署模式、IP 地址及当前状态等内容，如下图 3-3 所示：

接口信息

接口	ip地址	状态
eth0	192.168.1.81/24	down
eth1		down
eth2		down
eth3		down
eth4		down
eth5		down
eth6		down
eth7		down
eth8		down
eth9		down
eth10		down
eth11		down

图 **错误!文档中没有指定样式的文字。**-8 接口信息

3.4 设备基本信息

设备基本信息展示了设备的名称、编号、工作模式及上次启动时间等基本信息。如图 3-4 所示

设备基本信息

系统信息
防火墙名称:新增防火墙202127008
防火墙编号:202127008
防火墙工作模式: 测试模式
上次启动时间:2021-03-26 12:47:14

图 **错误!文档中没有指定样式的文字。**-9 消息提示

4. 基础防火墙

4.1 ACL 策略

4.1.1 简介

工业防火墙作为防火墙类的产品，ACL（访问控制列表）是其基础功能之一，目前工业防火墙采用状态检测防火墙的机制实现相应的控制。

简单介绍一下状态检测防火墙。它采用了状态检测包过滤的技术，是传统包过滤上的功能扩展。状态检测防火墙在网络层有一个检查引擎截获数据包并抽取出与应用层状态有关的信息，并以此为依据决定对该连接是接受还是拒绝。这种技术提供了高度安全的解决方案，同时具有较好的适应性和扩展性。

状态检测防火墙一般也包括一些代理级的服务，它们提供附加的对特定应用程序数据内容的支持。状态检测技术最适合提供对 UDP 协议的有限支持。它将所有通过防火墙的 UDP 分组均视为一个虚连接，当反向应答分组送达时，就认为一个虚拟连接已经建立。状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性，不仅仅检测“to”和“from”的地址，而且不要求每个访问的应用都有代理。

& 注意：

默认情况下 ACL 会拒绝所有

4.1.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[基础防火墙>ACL 策略]，点击菜单进入配置页面，如图 **错误!文档中没有指定样式的文字。**-10 所示：

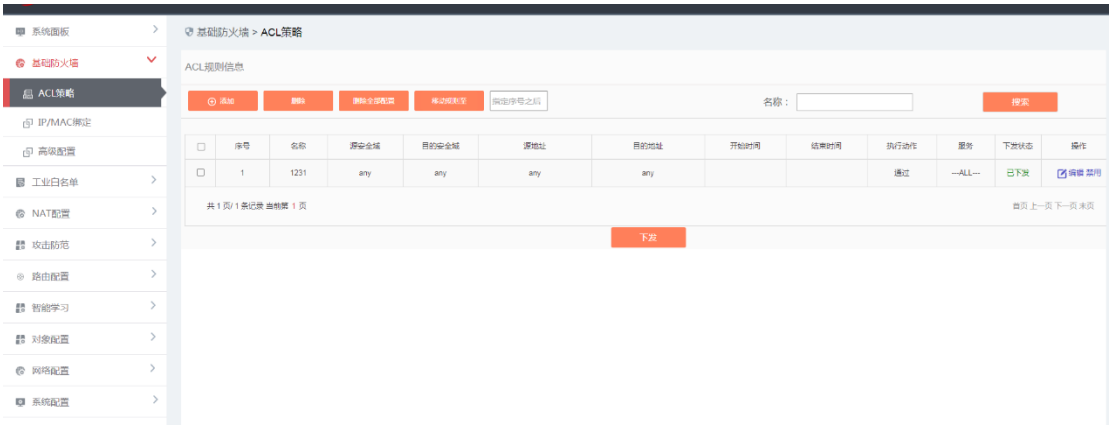


图 **错误!文档中没有指定样式的文字。**-10 ACL 策略

4.1.3 添加规则

进入[ACL 策略]页面后，点击左侧的<添加>按钮，将弹出[添加 ACL 策略]页面，如图 错误**!文档中没有指定样式的文字。-11** 所示：

图 **错误!文档中没有指定样式的文字。**-11 添加 ACL 安全策略

表 **错误!文档中没有指定样式的文字。**-5 ACL 规则各列说明

项目名称	说明
名称	每条策略起个名字，不可重复，最大 32 个字符
源安全域	发起数据请求的安全区域，以“any”表示全匹配
目的安全域	数据请求的目的安全区域，以“any”表示全匹配
源地址	发起数据请求的地址或地址组，地址或地址组的格式定义请参考相应章节
目的地址	数据请求到达的目的地址或地址组，地址或地址组的格式定义请参考相应章节
开始时间	规则生效的起始时间点
结束时间	规则失效的最后时间点
执行动作	命中该规则时防火墙对包的处理，通过、阻断、通过并记录日志或阻断不记录日志

服务	规则所支持的服务类型	
入侵防御	是否开启入侵防御功能	
操作	保存	确认所有的信息填写正确将被保存到数据库，但注意并**不生效**，同时返回到 ACL 策略列表显示页面
	保存并复制	确认所有的信息填写正确将被保存到数据库，但注意并**不生效**，同时停留在当前页面以方便继续添加新的策略
	返回	忽略所有的添加，返回到 ACL 策略列表显示页面

4.1.4 修改规则

进入[ACL 策略]页面后，点击某个 ACL 策略规则右侧操作列下的<修改>按钮，将打开[编辑 ACL 策略]的页面，就可以更改某个 ACL 策略规则的源安全域、目的安全域、源地址、目的地址，开始时间，结束时间，执行动作、服务和入侵防御，修改后点击<保存>按钮即可。

图 **错误!文档中没有指定样式的文字。**-12 ACL 策略修改

图 **错误!文档中没有指定样式的文字。**-13 ACL 策略编辑修改页面

4.1.5 删除规则

进入[ACL 策略]页面后，先选中需要删除的 ACL 策略规则，再点击列表上面左侧的<删除>按钮，可以删除对应的 ACL 策略规则。如图所示：

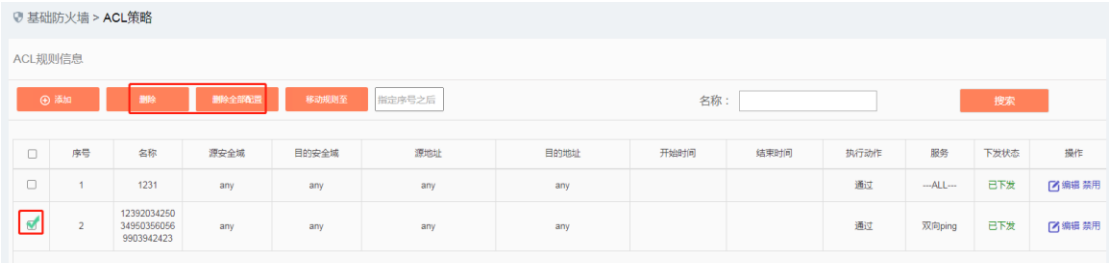


图 **错误!文档中没有指定样式的文字。**-14 ACL 策略删除

不用点击表格第一列的复选框，直接点击<删除全部规则>按钮，则可清空当前全部的 ACL 规则，在弹出的对话框中点击<确定>按钮即可

4.1.6 调整规则优先级

ACL 策略可以由多条“通过 | 阻断”语句组成。每一条语句描述的规则都不相同，这些规则可能存在重复或矛盾的地方。因此在将数据流和 ACL 规则进行匹配的时候，需要按照一定顺序进行规则匹配。

匹配原则如下：

•规则号小的规则被优先匹配。

数据流一旦与一条规则匹配成功，将不再继续向下匹配。工业防火墙将根据该规则的动作，对数据流进行后续操作。

进入[ACL 策略]页面后，先选中需要调整优先级的 ACL 策略规则，之后输入要调整到的位置，点击<移动规则至>，将弹出移动结果。如图 错误!**文档中没有指定样式的文字。-15** 所示：

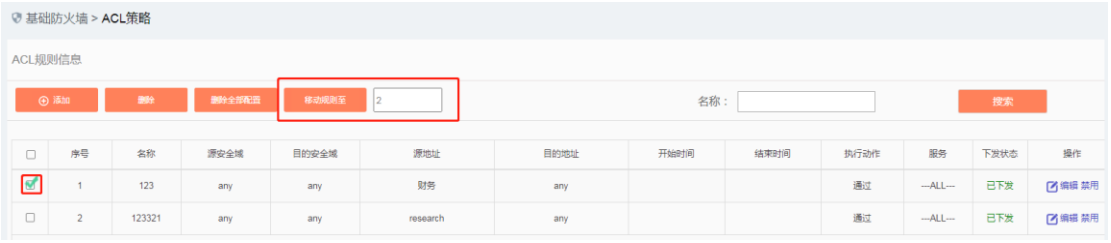


图 **错误!文档中没有指定样式的文字。**-15 ACL 策略规则优先级调整

4.1.7 禁用/启用规则

进入[ACL 策略]页面后，直接点击某个 ACL 策略规则最右侧操作列下的<禁用/启用>按钮，可以禁用或启用对应的 ACL 策略规则。禁用后该条规则以灰色背景显示。如图 **错误!文档中没有指定样式的文字。**-16 所示：

图 **错误!文档中没有指定样式的文字。**-16 ACL 策略规则启用/禁用

4.1.8 规则命中统计

在 ACL 规则查看页面可以查看到每条规则的命中情况，对于长时间未命中的策略，可以将其删除，以便节约宝贵的系统资源。但注意需要确定未命中的策略在业务现场确实没有需要。

图 **错误!文档中没有指定样式的文字。**-17 ACL 策略规则命中统计

4.2 IP/MAC 绑定

4.2.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[基础防火墙/IP/MAC 绑定]，点击菜单进入配置页面，如图 错误!**文档中没有指定样式的文字。-18** 所示：

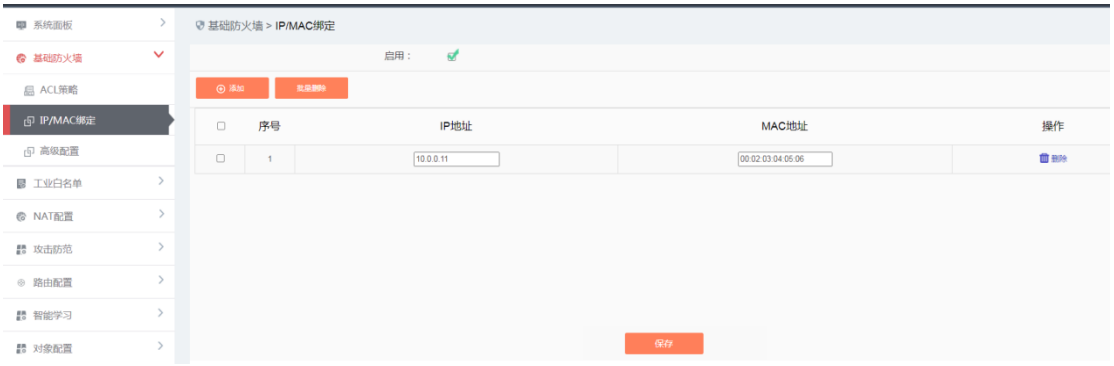


图 **错误!文档中没有指定样式的文字。**-18 IP/MAC 配置

4.2.2 规则配置

要使用此功能，需要勾选启用按钮。

如果启用了“IP/MAC 绑定”，点击<添加>按钮，表格会增加一行，编辑 IP 和 MAC 地址。如图 错误**!文档中没有指定样式的文字。-19** 所示:

图 **错误!文档中没有指定样式的文字。**-19 规则配置页面

点击 删除，删除当前规则，点击<保存>按钮，保存规则。也可勾选需要删除的规则，点击上方的<批量删除>按钮进行批量删除。

4.2.3 学习数据

参考智能学习章节，可直接使用学习到的数据辅助配置规则。

4.3 高级配置

4.3.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[基础防火墙/高级配置]，点击菜单进入配置页面，如图 错误**!文档中没有指定样式的文字。-20** 所示:

图 **错误!文档中没有指定样式的文字。**-20 高级配置

4.3.2 策略配置

4.3.2.1 会话老化时间设置

当前高级配置支持配置 TCP\UDP 老化时间，配置完点击<保存并应用>按钮，如图所示：

图 **错误!文档中没有指定样式的文字。**-21 高级配置之会话老化时间配置

表 **错误!文档中没有指定样式的文字。**-6 会话老化各列说明

项目名称	**说明**
TCP老化时间	配置TCP会话的老化时间，支持范围：1-120分钟
UDP老化时间	配置UDP虚连接的老化时间，支持范围：1-120分钟

4.3.2.2 状态检测配置

通过状态检测功能来对报文的链路状态进行合法性检查，丢弃链路状态不合法的报文。高级配置支持配置状态检测，配置完点击<保存并应用>按钮，如图所示：

图 **错误!文档中没有指定样式的文字。**-22 高级配置之状态检测配置

5. 工业白名单

5.1 工业白名单

5.1.1 简介

工业控制系统的安全问题有别于传统 IT 网络安全问题，更注重的是可用性、可靠性，因此在技术理念和产品实现上也完全不同。

工业控制系统强调的是确定性，所以什么样的流量应该在网络中传输是必须要明确和可控的，而传统的“黑名单”思想更注重的是威胁的识别和阻拦，这种思想一是需要频繁更新产品的“黑名单特征库”；二是对于新威胁往往事故发生了才能够提取特征和识别；三是这种产品经常出现漏报和误报。为了解决这些问题，工业防火墙利用工业协议深度包解析技术，实现强大的工业协议白名单功能，通过智能学习引擎，帮助客户识别、定义和控制流通在工业现场中的合法指令，而对于未知的，无论是否对工业现场造成伤害，都不允许其“穿墙而过”，防护从“被动”受到伤害后增加黑名单特征转变为“主动”定义合法流量，防止未知威胁攻击，与工业现场要求的确定性和可控性完全吻合。

工业防火墙防护思想从“黑”到“白”，从“被动防御”到“主动防护”，完全并特别适用于各种工业生产网络系统现场。因此，工业防火墙重要的一个创新就是白名单管理功能。

工业防火墙的白名单管理功能就是方便用户查看、编辑和使用白名单。

5.1.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[工业白名单/工业白名单]，点击菜单进入配置页面，如图 错误!**文档中没有指定样式的文字。-23** 所示:

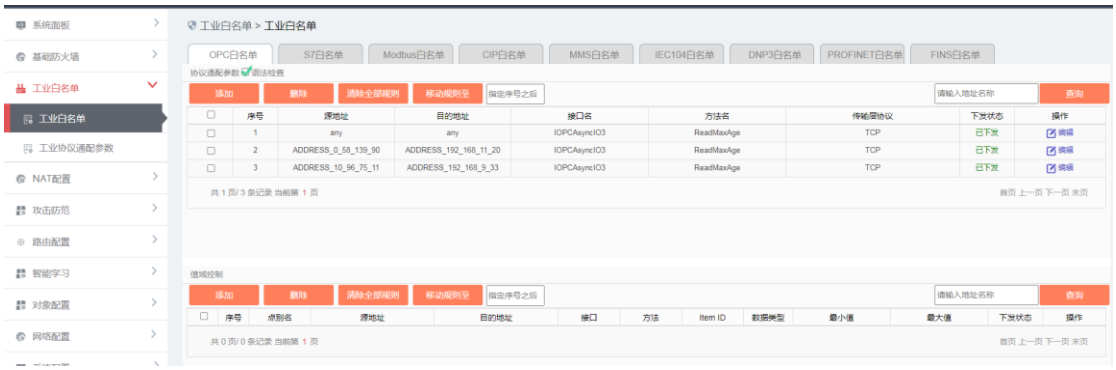


图 **错误!文档中没有指定样式的文字。**-23 会话管理

5.1.3 规则配置

5.1.3.1 OPC 白名单

添加规则

OPC 白名单配置页面，如图 错误!**文档中没有指定样式的文字。-24** 所示:

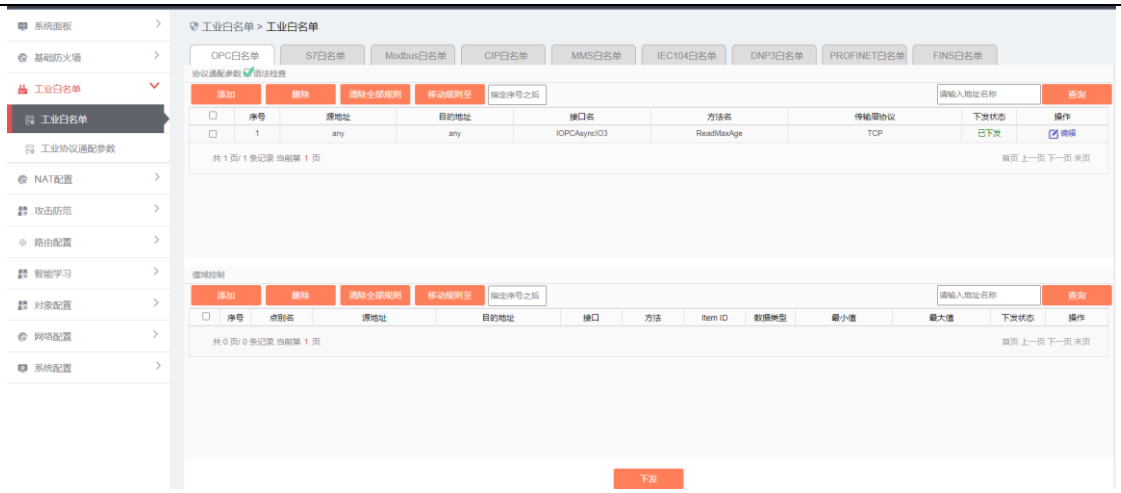


图 **错误!文档中没有指定样式的文字。**-24 OPC 白名单配置页面

添加 OPC 白名单，如图 错误**!文档中没有指定样式的文字。-25** 所示：

图 **错误!文档中没有指定样式的文字。**-25 OPC 添加白名单

表 **错误!文档中没有指定样式的文字。**-7 OPC 白名单规则各列说明

项目名称	**说明**
协议基础配置	语法检查：勾选，对OPC协议做语法检查，确保只有合法的报文通过
源地址	发起数据请求的地址或地址组，地址或地址组的格式定义请参考相应章节
目的地址	数据请求到达的目的地址或地址组，地址或地址组的格式定义请参考相应章节
开始时间	策略生效的开始时间，即从这个时间开始，策略生效
结束时间	策略生效的结束时间，即从这个时间开始，策略无效

接口名	OPC协议所包含的接口	
方法名	已选接口所包含的方法	
传输协议	默认TCP	
操作	确认	确认所有的信息填写正确将被保存到数据库，但注意并**不生效**，同时返回到策略列表显示页面
	保存并复制	确认所有的信息填写正确将被保存到数据库，但注意并**不生效**，同时停留在当前页面以方便继续添加新的策略
	取消	忽略所有的添加，返回到策略列表显示页面

添加 OPC 值域控制，如图 **错误!文档中没有指定样式的文字。**-26 所示：

图 **错误!文档中没有指定样式的文字。**-26 OPC 添加值域控制

表 **错误!文档中没有指定样式的文字。**-8 OPC 值域规则各列说明

项目名称	**说明**
点别名	值域名称
源地址	发起数据请求的地址或地址组，地址或地址组的格式定义请参考相应章节

目的地址	数据请求到达的目的地址或地址组，地址或地址组的格式定义请参考相应章节	
开始时间	策略生效的开始时间，即从这个时间开始，策略生效	
结束时间	策略生效的结束时间，即从这个时间开始，策略无效	
接口	OPC 协议所包含的接口	
方法	已选接口所包含的方法	
Item ID	协议点的统一 ID	
数据类型	包含 Boolean、Char 等	
最小值	值域范围最小值	
最大值	值域范围最大值	
操作	确认	确认所有的信息填写正确将被保存到数据库，但注意并不生效，同时返回到策略列表显示页面
	保存并复制	确认所有的信息填写正确将被保存到数据库，但注意并不生效，同时停留在当前页面以方便继续添加新的策略
	取消	忽略所有的添加，返回到策略列表显示页面

修改规则

进入[工业白名单]页面后，点击[OPC 白名单]tab 页，之后点击某个规则右侧操作列下的<编辑>按钮，将打开[编辑规则]的页面，就可以更改某个规则的源地址、目的地址、开始时间、结束时间、接口名、方法名，修改后点击<保存>按钮即可。

图 **错误!文档中没有指定样式的文字。**-27 OPC 规则编辑

图 **错误!文档中没有指定样式的文字。**-28 OPC 规则编辑页面

删除规则

进入[工业白名单]页面后，点击[OPC 白名单]tab 页，先选中需要删除的规则，再点击列表上面左侧的<删除>按钮，可以删除对应的规则。如图 错误**!文档中没有指定样式的文字。-29** 所示：

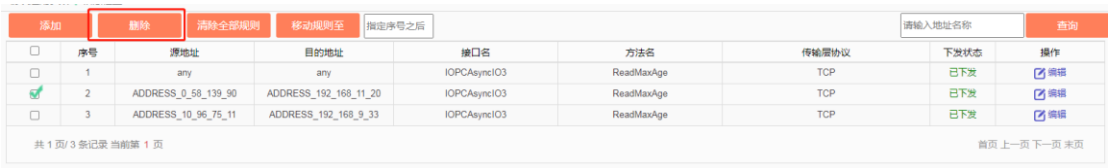


图 **错误!文档中没有指定样式的文字。**-29 规则删除

不用点击表格第一列的复选框，直接点击<清除全部规则>按钮，则可清空当前全部的规则，在弹出的对话框中点击<确定>按钮即可。

调整规则优先级

类似 ACL 策略，工业协议的白名单策略也有多个规则组成。因此在将数据流和规则进行匹配的时候，需要按照一定顺序进行规则匹配。

匹配原则如下：

•规则号小的规则被优先匹配。

数据流一旦与一条规则匹配成功，将不再继续向下匹配。

进入[工业白名单]页面后，点击[OPC 白名单]tab 页，先选中需要调整优先级的策略规则，之后输入要调整到的位置，点击<移动规则至>，将弹出移动结果。如图 错误**!文档中没有指定样式的文字。-30** 所示：

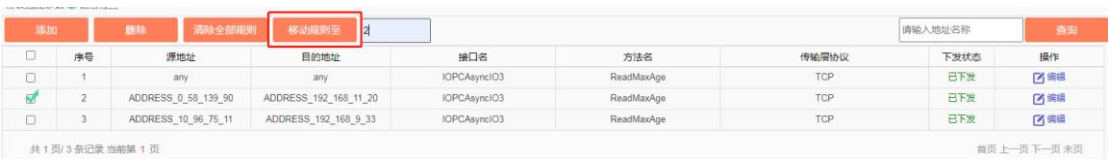


图 **错误!文档中没有指定样式的文字。**-30 策略规则优先级调整

规则命中统计

在 OPC 规则查看页面可以查看到每条规则的命中情况，对于长时间未命中的策略，可以将其删除，以便节约宝贵的系统资源。但注意需要确定未命中的策略在业务现场确实没有需要。

图 **错误!文档中没有指定样式的文字。**-31 OPC 白名单策略规则命中统计

S7 白名单：请参考上述 OPC 白名单配置。

Modbus 白名单：请参考上述 OPC 白名单配置。

CIP 白名单：请参考上述 OPC 白名单配置。

MMS 白名单：请参考上述 OPC 白名单配置。

IEC104 白名单：请参考上述 OPC 白名单配置。

DNP3 白名单：请参考上述 OPC 白名单配置。

Profinet 白名单：请参考上述 OPC 白名单配置。

Fins 白名单：请参考上述 OPC 白名单配置。

5.2 工业协议通配参数

5.2.1 简介

白名单配置模板中往往需要使用自定义功能码等可添加字段，目前 CIP 下拉菜单中通过自定义项进行添加，只支持添加功能。在工业防火墙学习过程中可能学习到用户使用的新的自定义字段，这时需要重新修改字段描述，同时用户自定义的字段也有删除的需求。为此，工业防火墙通过专门的工业协议通配参数配置页面，方便用户管理某些工业协议特有的功能特性。

5.2.2 页面导航

系统管理员登录，点击左侧导航栏的[工业白名单/工业协议通配参数](如图 错误**!文档中没有指定样式的文字。-32** 所示)，进入[工业协议通配参数]的页面（如图 错误**!文档中没有指定样式的文字。-33** 所示）。

图 **错误!文档中没有指定样式的文字。**-32 选择工业协议通配参数

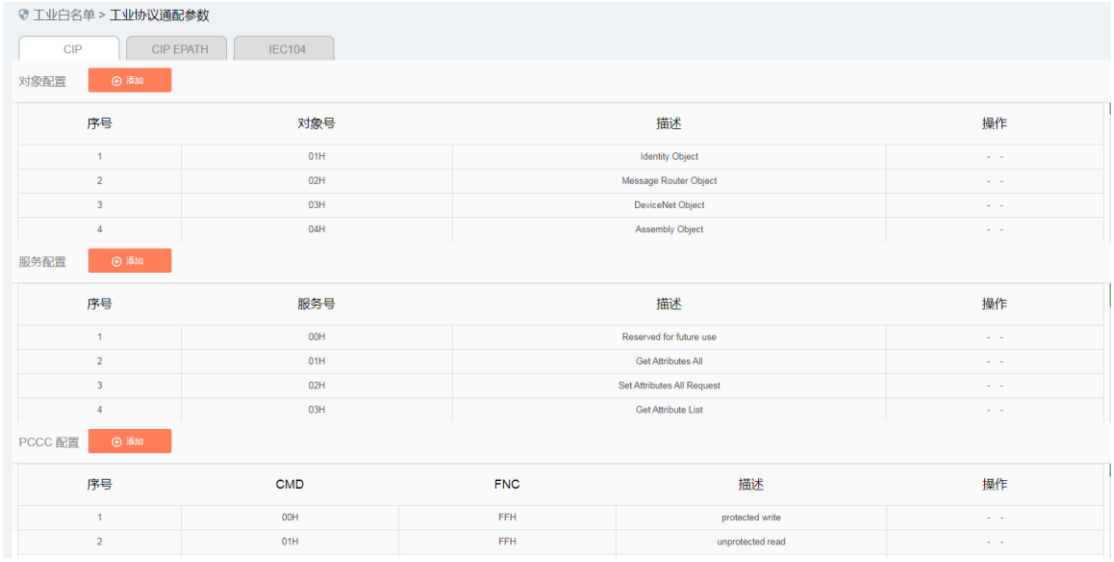


图 **错误!文档中没有指定样式的文字。**-33 工业协议通配参数配置页面

此处用户可以针对 CIP 协议进行如下三种参数的配置：

- 对象配置
- 服务配置
- PCCC 配置

下面分别说明这三种配置每个字段的含义。

表 **错误!文档中没有指定样式的文字。**-9 CIP 协议对象配置字段说明

项目名称	说明	
对象号	CIP 协议定义的标准对象以及在工业现场用户自定义的对象，以十六进制值显示	
描述	对象所代表的具体意义	
操作	修改	修改用户自定义对象的描述信息，CIP 标准对象的描述信息无法修改
	删除	删除用户自定义的对象，CIP 标准对象无法删除

表 **错误!文档中没有指定样式的文字。**-10 CIP 协议服务配置字段说明

项目名称	说明	
服务号	CIP 协议中提供的标准服务以及在工业现场用户自定义的服务，以十六进制值显示	
描述	服务的具体意义	
操作	修改	修改用户自定义的 CIP 服务的描述信息，CIP 标准服务的描述信息无法修改
	删除	删除用户自定义的 CIP 服务，CIP 标准服务无法删除

表 **错误!文档中没有指定样式的文字。**-11 CIP 协议 PCCC 配置字段说明

项目名称	说明	
CMD	CIP 协议内嵌的 PCCC 格式的报文中的 CMD 号，以十六进制值显示	
FNC	CIP 协议内嵌的 PCCC 格式的报文中的 FNC 号，以十六进制值显示	
描述	PCCC 中的 CMD 和 FNC 的组合唯一确定的方法描述	
操作	修改	重新定义 CMD 和 FNC 的组合唯一确定的方法，PCCC 定义的标准方法无法修改
	删除	删除用户自定义的由 CMD 和 FNC 的组合唯一确定的方法，PCCC 定义的标准方法无法删除

5.2.3 CIP 配置添加

点击每个配置列表左侧的<添加>按钮，（如图 错误**!文档中没有指定样式的文字。-34** 所示）的对象配置中的<添加>按钮，将打开对象配置添加页，(如图 错误**!文档中没有指定样式的文字。-35** 所示)。

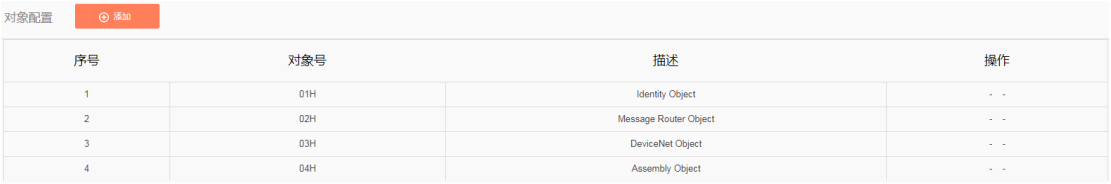


图 **错误!文档中没有指定样式的文字。**-34 CIP 协议对象配置添加按钮

图 **错误!文档中没有指定样式的文字。**-35 CIP 协议对象配置添加页面

点击<保存>将把增加的自定义对象保存到后台，然后跳转到工业协议通配参数页面。

点击<返回>将不保存编辑的自定义对象，直接返回到工业协议通配参数页面。

5.2.4 CIP 配置修改

请参考上述工业协议通配参数操作列下的修改说明。

5.2.5 CIP 配置删除

请参考上述工业协议通配参数操作列下的修改说明。

5.2.6 CIP EPATH 配置添加

点击 tab 页标签跳转到 CIP EPATH 配置页面，（如图 错误**!文档中没有指定样式的文字。-36**）点<添加>按钮添加一条规则。

图 **错误!文档中没有指定样式的文字。**-36 CIP EPATH 配置页面

5.2.7 CIP EPATH 配置删除

点击<删除>按钮删除一条规则，（如图 错误**!文档中没有指定样式的文字。-37**）。

图 **错误!文档中没有指定样式的文字。**-37 CIP EPATH 删除操作

5.2.8 CIP EPATH 配置保存

点击<保存>按钮保存配置，（如图 错误**!文档中没有指定样式的文字。-38**）。

图 **错误!文档中没有指定样式的文字。**-38 CIP EPATH 保存操作

5.2.9 IEC104 配置

点击 tab 页标签跳转到 IEC104 配置页面(如图 错误**!文档中没有指定样式的文字。-39**)。

图 **错误!文档中没有指定样式的文字。**-39IEC104 配置页面

5.2.10 IEC104 配置保存

点击<保存>按钮，保存页面配置(如图 错误**!文档中没有指定样式的文字。-40**)。

图 **错误!文档中没有指定样式的文字。**-40IEC104 保存

6. NAT配置

6.1 NAT 地址池配置

6.1.1 简介

介绍转换地址池的配置过程。

6.1.2 页面导航

系统管理员登录，点击左侧导航栏的[NAT 配置/NAT 地址池配置](如图 错误**!文档中没有指定样式的文字。-41** 所示)，进入[NAT 地址池配置]的页面 (如图 错误**!文档中没有指定样式的文字。-42** 所示)。

图 **错误!文档中没有指定样式的文字。**-41 选择 NAT 地址池配置

图 **错误!文档中没有指定样式的文字。**-42NAT 地址池配置页面

6.1.3 添加地址池

进入页面后，点击左侧的<添加>按钮，将转到[添加地址池]页面，如图 错误**!文档中没有指定样式的文字。-43** 所示：

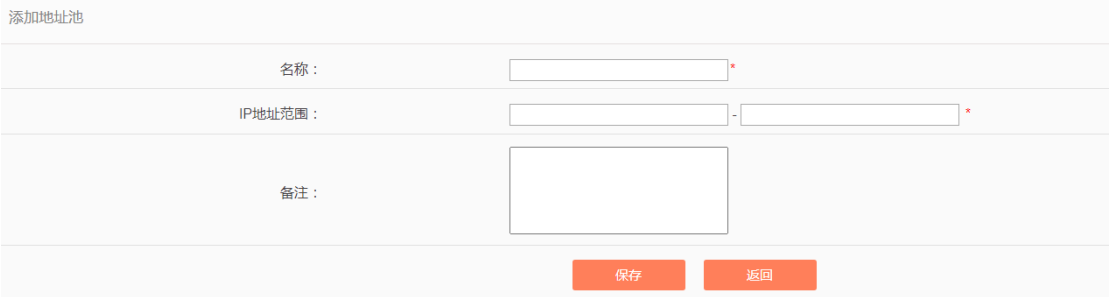


图 **错误!文档中没有指定样式的文字。**-43 添加 NAT 地址池

表 **错误!文档中没有指定样式的文字。**-12 NAT 地址池添加各列说明

项目名称	说明	
名称	输入 NAT 地址池的名称，最大 32 个字符	
IP 地址范围	输入可使用的地址范围的起始 IP 和结束 IP。结束 IP 必须大于等于起始 IP。支持将地址池配置为仅包含单个 IP 地址。	
操作	保存	确认所有的信息填写正确将被保存到数据库，同时返回到列表显示页面
	返回	忽略所有的添加，返回到列表显示页面

6.1.4 修改地址池

进入页面后，点击某个地址池右侧操作列下的<编辑>按钮，将打开[编辑地址池]的页面，就可以更改地址池的名称和 IP 地址范围，修改后点击<保存>按钮即可。

6.1.5 删除地址池

进入页面后，先选中需要删除的地址池对象，再点击列表右侧操作列下的<删除>按钮，可以删除对应的地址池对象。

点击表格第一列的复选框，选中多个地址池对象，点击列表上方的<批量删除>按钮，则可批量删除地址池对象。

6.2 源 NAT

6.2.1 简介

源 NAT 用来解决内网用户访问互联网时，IP 资源短缺的问题，源 NAT 模块将内网用户的 IP 地址转换成网关的公网 IP 地址。

& 注意：

源 NAT 在配置时只能 LAN-WAN，所以需要在接口配置时提前指定接口为 LAN 或 WAN

6.2.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[NAT 配置/源 NAT]，点击菜单进入配置页面，如图 错误**!文档中没有指定样式的文字。-44** 所示：

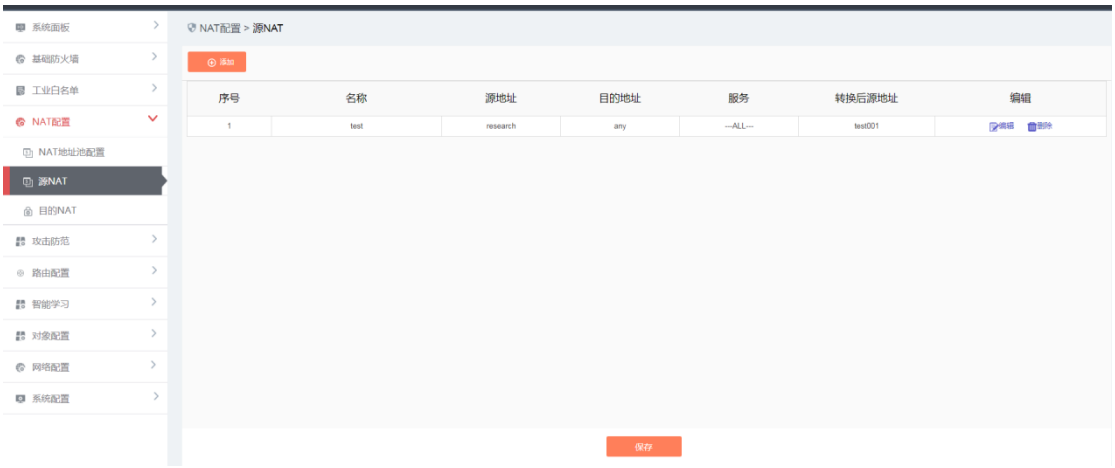


图 **错误!文档中没有指定样式的文字。**-44 源 NAT 策略管理

6.2.3 添加规则

点击<添加>按钮，弹出源 NAT 配置界面，如图 错误**!文档中没有指定样式的文字。-45** 所示：

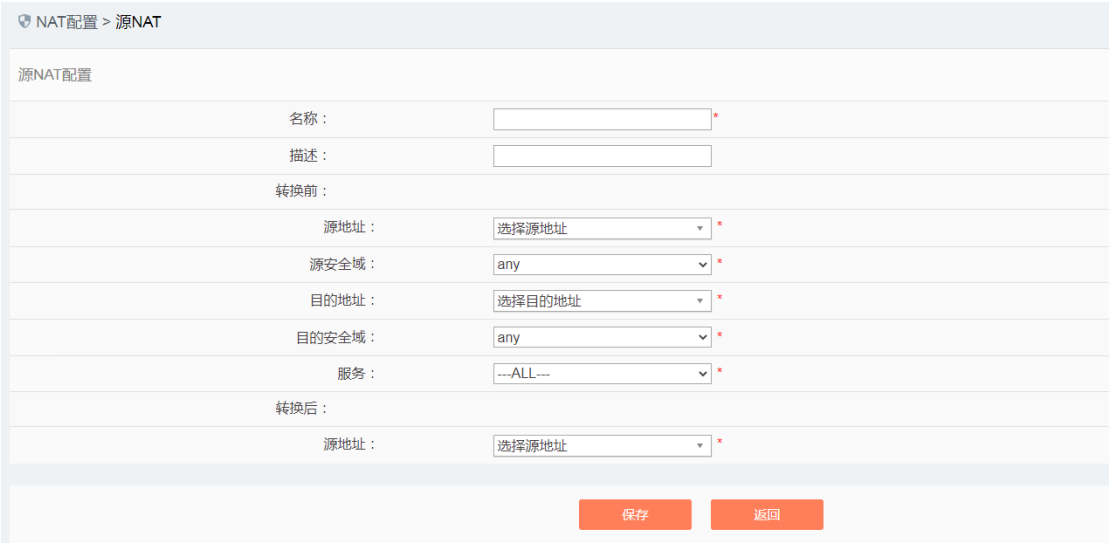


图 **错误!文档中没有指定样式的文字。**-45 源 NAT 配置

表 **错误!文档中没有指定样式的文字。**-13 源 NAT 添加各列说明

项目名称	**说明**
名称	不允许为空，只允许输入汉字、数字、字母、下划线和连接符，其总长度不超过 32 位
描述	源 NAT 配置描述性内容
转换前-源地址	转换前的源地址。注：转换前源地址地址范围与转换后需要一致，要么 1 对 1，要么多对 1.
转换前-源安全域	转换前的报文来自于此安全域
转换前-目的地址	转换前的目的地址

转换前-目的安全域	转换前的报文发往此安全域
服务	需要转换的服务
转换后-源地址	转换后的源地址
保存	保存源 NAT 配置
返回	不保存，返回源 NAT 配置列表

6.2.4 修改规则

在[源 NAT]配置列表页面中，点击<编辑>按钮，可以进入源 NAT 配置编辑页面，编辑已经保存的 NAT 配置，如图所示：

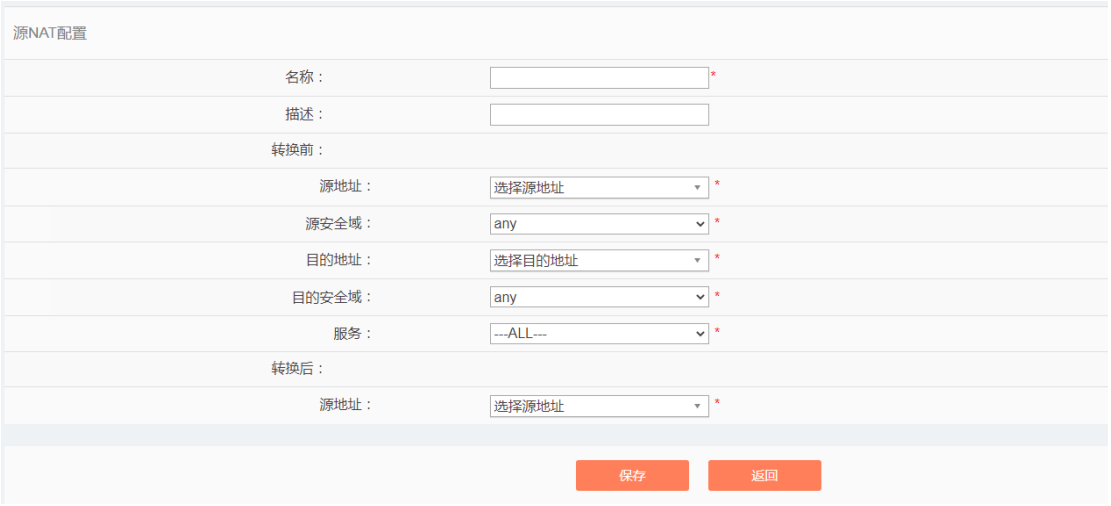


图 **错误!文档中没有指定样式的文字。**-46 编辑源 NAT 配置

参数等同于添加源 NAT 配置。

6.2.5 删除规则

点击某条源 NAT 配置后面的<删除>按钮，可以删除对应的源 NAT 配置。

6.2.6 应用规则

新建、编辑、删除源 NAT 列表后，点击<保存>按钮，可以保存并应用源 NAT 配置列表，如图所示：

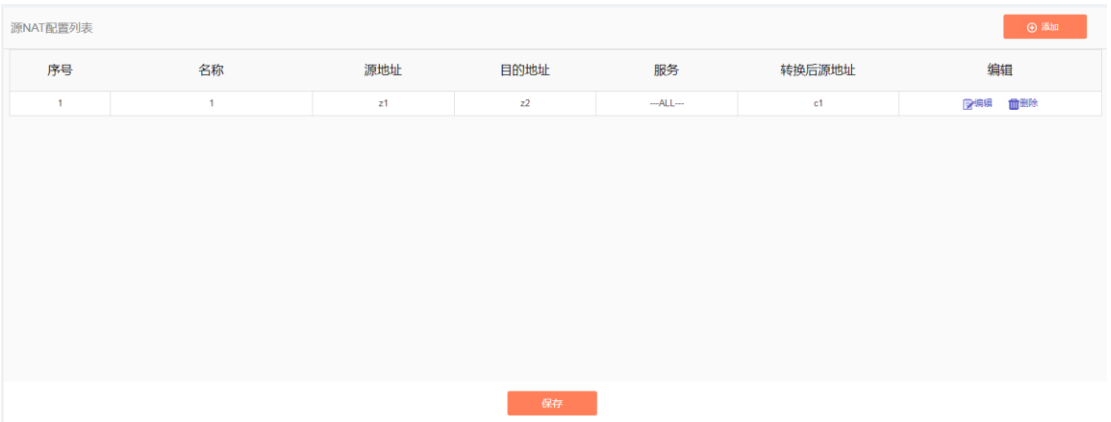


图 **错误!文档中没有指定样式的文字。**-47 保存源 NAT 配置列表

6.2.7 规则命中统计

在源 NAT 规则查看页面可以查看到每条规则的命中情况，对于长时间未命中的策略，可以将其删除，以便节约宝贵的系统资源。但注意需要确定未命中的策略在业务现场确实没有需要。

图 **错误!文档中没有指定样式的文字。**-48 源 NAT 策略规则命中统计

6.3 目的 NAT

6.3.1 简介

DNAT 主要用于在公网上的用户，需要访问内网的服务器时，通过 DNAT 将内部服务器映射到外网。

& 注意：

目的 NAT 在配置时只能 WAN-LAN，所以需要在接口配置时提前指定接口为 LAN 或 WAN

6.3.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[NAT 配置/目的 NAT]，点击菜单进入配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-49 目的 NAT 策略管理

6.3.3 添加规则

点击<添加>按钮，弹出目的 NAT 配置界面，如图所示：

图 **错误!文档中没有指定样式的文字。**-50 目的 NAT 配置

项目名称	说明

名称	不允许为空，只允许输入汉字、数字、字母、下划线和连接符，其总长度不超过 32 位
描述	目的 NAT 配置描述性内容
公网地址	选择相应地址
私网地址	选择相应地址
协议	支持 TCP，UDP，ICMP
公网端口	公网端口
私网端口	私网端口
转换前-源安全域	转换前的报文来自于此安全域
保存	保存目的 NAT 配置
返回	不保存，返回目的 NAT 配置列表

表 **错误!文档中没有指定样式的文字。**-14 目的 NAT 添加各列说明

6.3.4 修改规则

在[目的 NAT]配置列表页面中，点击【编辑】按钮，可以进入目的 NAT 配置编辑页面，编辑已经保存的 NAT 配置，如图所示：

图 **错误!文档中没有指定样式的文字。**-51 编辑目的 NAT 配置

参数等同于添加目的 NAT 配置。

6.3.5 删除规则

点击某条目的 NAT 配置后面的<删除>按钮，可以删除对应的目的 NAT 配置。

6.3.6 应用规则

新建、编辑、删除目的 NAT 列表后，点击【保存】按钮，可以保存并应用规则，如图所示：

图 **错误!文档中没有指定样式的文字。**-52 保存目的 NAT 配置列表

6.3.7 规则命中统计

在目的 NAT 规则查看页面可以查看到每条规则的命中情况，对于长时间未命中的策略，可以将其删除，以便节约宝贵的系统资源。但注意需要确定未命中的策略在业务现场确实没有需要。

图 **错误!文档中没有指定样式的文字。**-53 目的 NAT 策略规则命中统计

7. 攻击防范

7.1 异常报文检测

通过异常报文检测，可以检测 Land 攻击、Teardrop 攻击、Ping of Death 攻击。

7.1.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[攻击防范/异常报文检测]，点击菜单进入配置页面，如图所示：

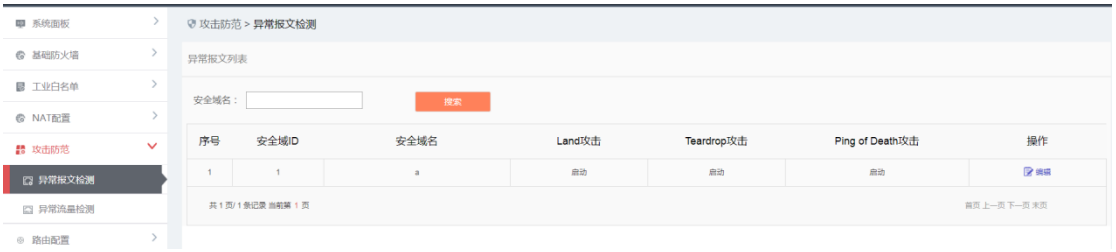


图 **错误!文档中没有指定样式的文字。**-54 异常报文检测

7.1.2 异常报文检测配置

点击安全域后面的<编辑>按钮，弹出异常报文基本信息界面，通过勾选需要检测的攻击开启相应的攻击检测功能，如图所示：

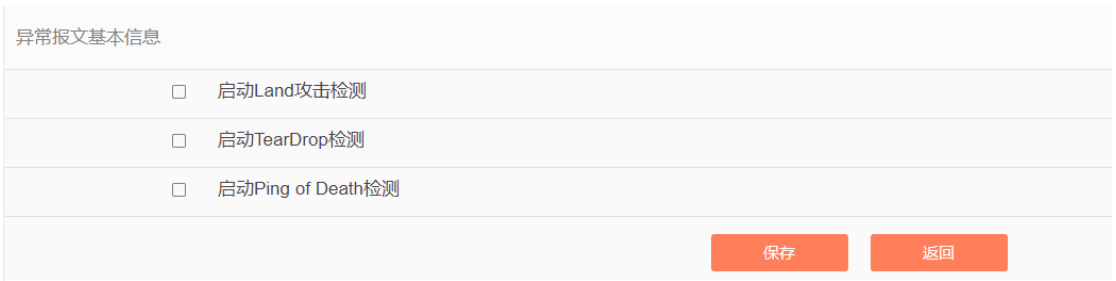


图 **错误!文档中没有指定样式的文字。**-55 异常报文检测配置

7.2 异常流量检测

通过异常流量检测可以检测 SYN Flood 攻击、Ping Flood 攻击、UDP Flood 攻击。

7.2.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[攻击防范/异常流量检测]，点击菜单进入配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-56 异常流量检测

7.2.2 异常流量检测配置

点击安全域后面的<编辑>按钮，弹出异常流量基本信息界面，通过勾选要检测的攻击和设置阀值配置异常流量检测规则，如图所示：

图 **错误!文档中没有指定样式的文字。**-57 异常流量检测配置

8. 路由配置

8.1 静态路由

8.1.1 静态路由配置页面

静态路由配置页面，如图所示

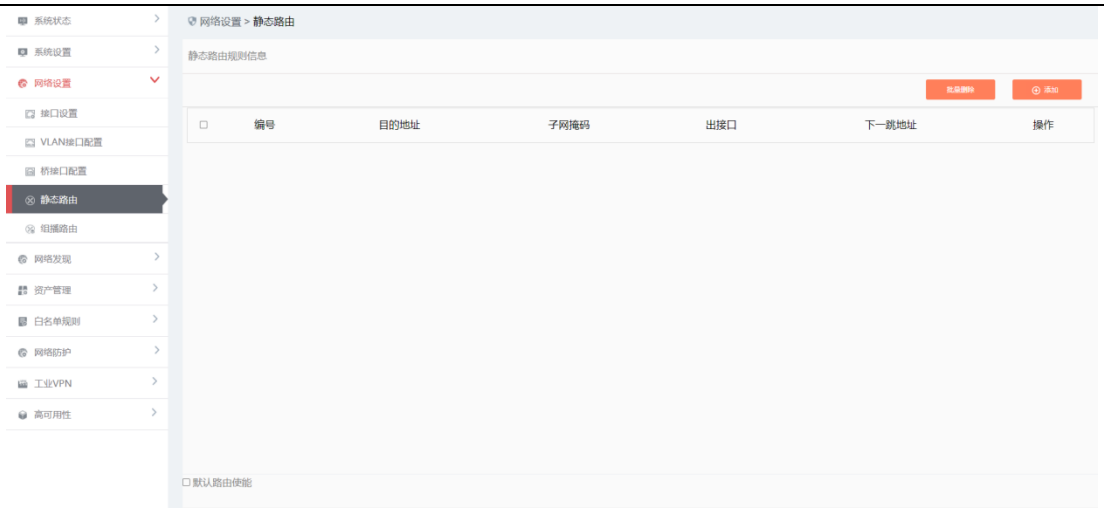


图 **错误!文档中没有指定样式的文字。**-58 静态路由配置页面

默认路由使能页面，如图所示：

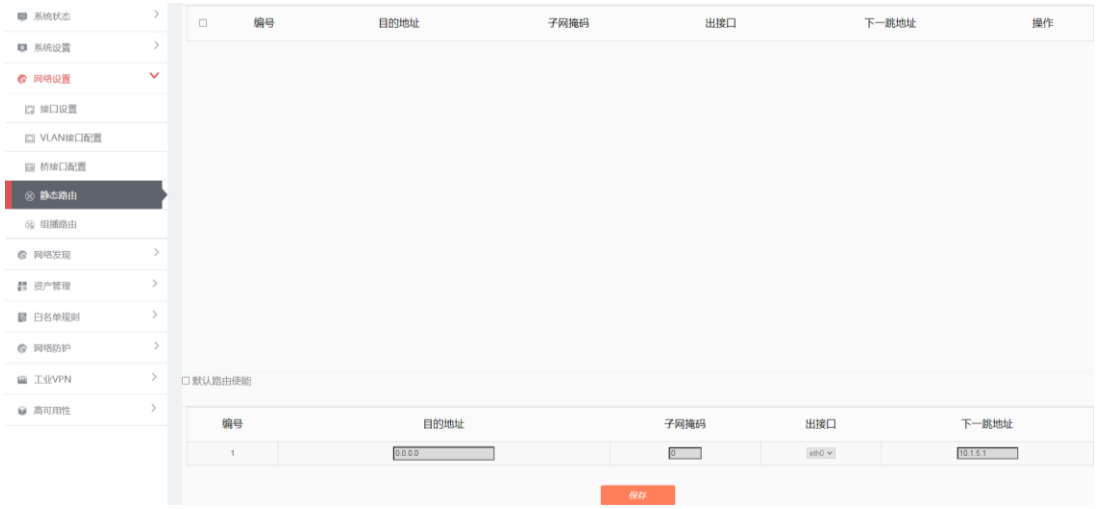


图 **错误!文档中没有指定样式的文字。**-59 默认路由配置页面

& 注意：

当去往某一目的地的静态路由具有“黑洞”属性时，无论配置的下一跳地址是什么，该路由的出接口均为 NULL0 接口，任何去往该目的地的 IP 报文都将被丢弃，并且不通知源主机。在网络遭受攻击的情况下，可以通过配置黑洞路由丢弃去往目的地址的报文。

8.1.2 静态路由配置

进入[静态路由]点击左侧的<添加>按钮，可直接添加静态路由信息，如图所示：

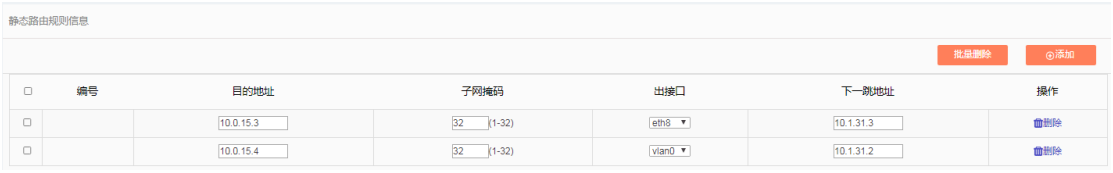


图 **错误!文档中没有指定样式的文字。**-60 添加静态路由

当静态路由没有配置或者无法找到路由的时候，可以使用默认路由，如图所示：

图 **错误!文档中没有指定样式的文字。**-61 默认路由配置

表 **错误!文档中没有指定样式的文字。**-15 路由表各列说明

项目名称	**说明**	
编号	编号	
目的地址	路由的目的地址	
子网掩码	子网掩码位数	
出接口	路由的物理出接口	
下一跳地址	下一跳的 IPv4 地址	
操作	<添加>	添加一条路由规则
	<批量删除>	删除所有选中的条数
	<删除>	将所在行的路由规则删除
	<保存>	保存所有配置选项

9. 智能学习

9.1 简介

开启智能学习功能，启动防火墙智能学习模式，能够自动发现网络中的设备地址，识别设备之间的网络连接关系，识别网络中的协议类型，智能分析工业协议并自动生成防护规则。智能学习包括地址、IP/MAC、工业协议白名单三大部分。工业协议白名单包括 OPC、S7、Modbus、CIP、IEC104、DNP3、MMS、Profinet、Fins。

9.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[智能学习/智能学习]，点击菜单进入智能学习页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-62 智能学习页面

9.3 智能学习控制

点击左侧的<启动>按钮，防火墙将进入学习模式，将所学习的数据按类划分至三个选项卡中。

9.3.1 地址选项卡

地址选项卡页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-63 地址选项卡页面

表 **错误!文档中没有指定样式的文字。**-16 智能学习各列说明

项目名称	说明
<启动>	开始学习
地址名称	设备地址的名称
IP 地址	设备的 IP 地址，点分十进制表示
<搜索>	按着搜索条件进行搜索
<清空>	清空学习到的所有地址信息
<删除>	删除一条学习数据

9.3.2 IP/MAC 绑定选项卡

IP/MAC 绑定选项卡页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-64IP/MAC 绑定选项卡页面

表 **错误!文档中没有指定样式的文字。**-17 IP/MAC 绑定选项卡各列说明

项目名称	说明
<启动>	开始学习
IP 地址	设备的 IP 地址，点分十进制表示
MAC 地址	设备的 MAC 地址，以 00:01:02:03:04:05 格式展示
<搜索>	按着搜索条件进行搜索
<生成策略>	把选中的 IP/MAC 地址对的学习数据生成策略规则
<删除>	删除一条学习数据
<刷新>	刷新显示
<全部生成策略>	把所有 IP/MAC 地址对的学习数据生成策略规则
<全部删除>	删除所有学习数据

9.3.3 工业协议白名单选项卡

工业协议白名单选项卡页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-65 工业协议白名单选项卡页面

9.3.3.1 OPC 学习数据

工业白名单选项卡的第一个 tab 页即 OPC 协议学习数据，其中各列的含义如下表所示：

表 **错误!文档中没有指定样式的文字。**-18 OPC 协议学习数据各列说明

项目名称	说明

源地址	发起数据请求的地址或地址组
目的地址	数据请求到达的目的地址或地址组
传输层协议	实际使用的传输层协议
接口名	OPC 接口名称，用于搜索的选项之一
方法名	OPC 方法名称，用于搜索的选项之一
<搜索>	按着搜索条件进行搜索
<生成策略>	把选中的 OPC 学习数据生成策略
<删除>	删除一条学习数据
<刷新>	刷新显示
<生成全部策略>	把所有的 OPC 学习数据生成策略
<全部删除>	删除所有的 OPC 学习数据

S7 学习数据：请参考上述 OPC 学习数据配置。
Modbus 学习数据：请参考上述 OPC 学习数据配置。
CIP 学习数据：请参考上述 OPC 学习数据配置。
MMS 学习数据：请参考上述 OPC 学习数据配置。
IEC104 学习数据：请参考上述 OPC 学习数据配置。
DNP3 学习数据：请参考上述 OPC 学习数据配置。
Profinet 学习数据：请参考上述 OPC 学习数据配置。
Fins 学习数据：请参考上述 OPC 学习数据配置。

9.4 学习时间配置

在[智能学习]页面，点击<学习时间配置>按钮，打开防火墙智能学习的时间配置。如下图：

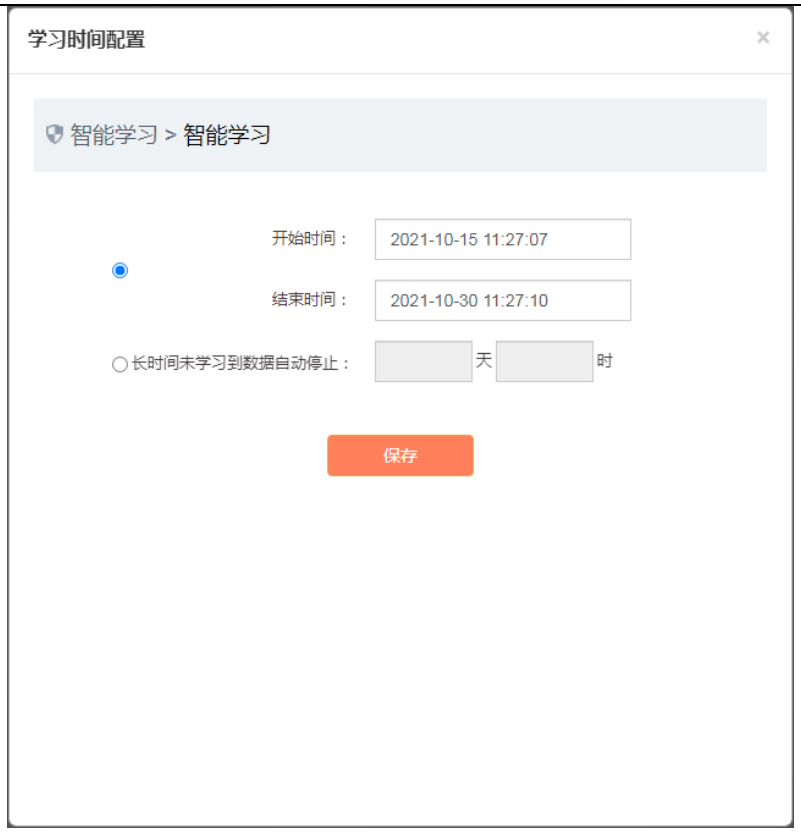


图 **错误!文档中没有指定样式的文字。**-66 学习时间配置页面

对于需要使用智能学习的现场，可根据：

- 业务的周期设置学习的开始时间和结束时间；
- 根据学习数据的趋势，在多长时间没有新的学习数据时自动停止。

同时只能选择一种时间设置方式。

表 **错误!文档中没有指定样式的文字。**-19 学习时间配置各项说明

项目名称	说明
开始时间	设置开始学习的时间，精确到秒，适用于知道业务周期的场景
结束时间	设置结束学习的时间，精确到秒，适用于知道业务周期的场景
长时间未学习到数据自动停止	学习数据不再有变化，持续时间设置，精确到小时，适用于不清楚业务周期的场景
<保存>	保存时间设置

9.5 学习趋势分析

实时查看学习的趋势可辅助运维人员快速完成学习过程进入到其它工作模式。

1. 支持对最近 1 个月、1 天、1 小时的学习数据个数进行统计趋势分析。
2. 最近一个月学习数据个数的统计展示图的 x 轴单位为天，最近 1 天学习数据个数的统计展示图的 x 轴单位为小时，最近 1 个小时学习数据个数的统计展示图的 x 轴单位为 5 分钟。
3. 学习数据超过 30 分钟不到 6 小时不变化时，提示用户：“距离上次学习数据变化已过去了 XX

小时 XX 分钟”；超过 6 小时以上没有学习到数据时，页面提示“距上次学习到新数据已过去：XX 小时 XX 分钟，建议停止学习进入告警模式！ ”的提示信息。

如下图所示：

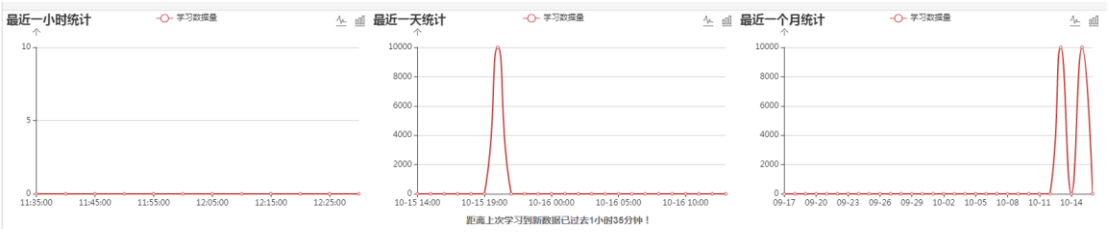


图 **错误!文档中没有指定样式的文字。**-67 学习趋势展示

10. 流量监测

10.1 简介

工业防火墙具备流量统计功能，通过 IP 地址、网络服务、时间和协议类型等参数或它们的组合对流量进行正确的统计，实时或者以报表形式输出流量统计结果，还对流量超过预警值的行为进行告警。

10.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[对象配置/监测对象]，点击菜单进入监测对象的配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-68 监测对象的配置页面

在左侧导航栏找到[流量监测/流量监测]，点击菜单进入流量监测的规则配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-69 流量监测规则配置页面

10.3 监测对象

在设置监测对象前，可提前针对不同类型的监测对象设置分类，如果没有特殊的分类，可使用系统

默认的“default”分类。如下图所示:

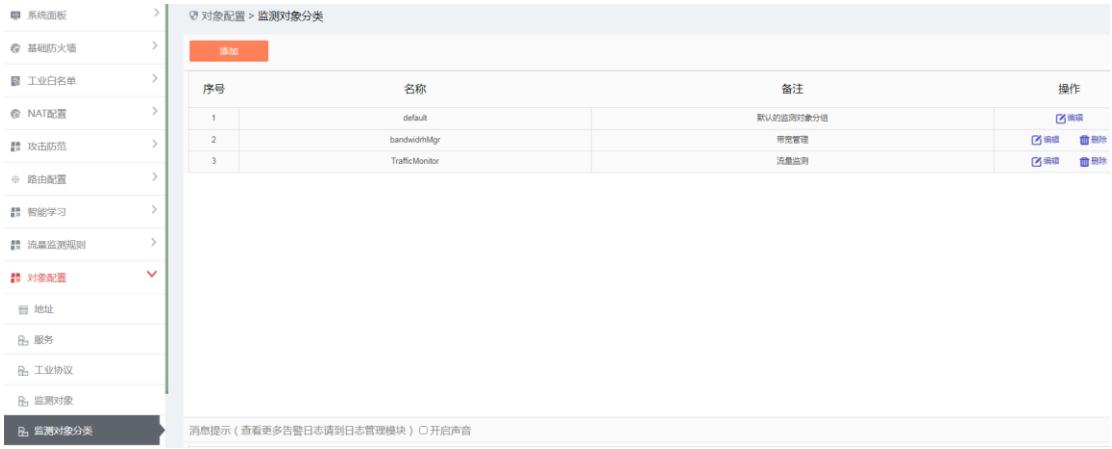


图 **错误!文档中没有指定样式的文字。**-70 流量监测对象分类配置页面

配置好不同的分类后，可根据 IP 地址、网络服务、时间和协议类型等参数或它们的组合设置不同的监测对象并对它们的流量进行实时或以报表形式输出统计结果。

10.3.1 添加监测对象

在[监测对象]配置页面，点击左侧的<添加>按钮，将直接在列表增加一条默认对象，如图所示:

图 **错误!文档中没有指定样式的文字。**-71 监测对象添加

表 **错误!文档中没有指定样式的文字。**-20 监测对象各列说明

项目名称	**说明**
ID	监测对象的唯一标识符，是一个不超过 3000 的整数数字
名称	监测对象的名称。如果输入的名称使用特殊字符，仅支持使用键盘上有的特殊字符。
源地址	发起数据请求的地址或地址组，地址或地址组的格式定义请参考相应章节
目的地址	数据请求到达的目的地址或地址组，地址或地址组的格式定义请参考相应章节
服务	要监测的服务
分类	监测对象所属的分类
<保存>	保存一条地址项

10.3.2 修改监测对象

在[监测对象]配置列表页面中，可直接修改对应监测对象的各个字段的取值，之后点击<保存>即可

使修改生效。

10.3.3 删除监测对象

点击某条监测对象后面的<删除>按钮，可以删除对应的监测对象。

点击表格第一列的复选框，选中多个监测对象，点击列表上方的<批量删除>按钮，则可批量删除地址对象。

10.4 流量监测

根据不同的流量监测对象进行个性化的流星监测行为。

10.4.1 添加监测规则

在[流量监测]配置页面，点击左侧的〈添加〉按钮，将直接在列表增加一条默认监测规则，如图所示：

图 **错误!文档中没有指定样式的文字。**-72 流量监测规则添加

表 **错误!文档中没有指定样式的文字。**-21 流量监测规则各列说明

项目名称	说明
监测对象	本条规则对应的要监测流量的监测对象
上行流量阈值(Kbps)	流入监测对象的流量阈值，超过后可根据“执行动作”进行相应的处理
下行流量阈值(Kbps)	流出监测对象的流量阈值，超过后可根据“执行动作”进行相应的处理
总流量阈值(Kbps)	流入流出监测对象的总流量阈值，超过后可根据“执行动作”进行相应的处理
执行动作	告警或监测，监测时只统计流量，告警时对超出阈值时将产生事件日志 注意：告警时，当处于防护模式下，流量超出的部分报文将被丢弃
操作	<删除>，删除对应的规则

10.4.2 修改监测规则

在[流量监测]配置列表页面中，可直接修改对应流量监测规则的各个字段的取值，之后点击<保存>即可使修改生效。

10.4.3 删除监测规则

点击某条流量监测规则后面的<删除>按钮，可以删除对应的流量监测规则。

点击表格第一列的复选框，选中多个流量监测规则，点击列表上方的<批量删除>按钮，则可批量删除流量监测规则。

10.5 流量统计

可实时查看流量统计结果。

在[监测对象]配置页面，点击操作列下的<查看流量>按钮，将打开对应监测对象的实时流量统计页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-73 实时查看流量

11. 对象配置

11.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[对象配置/地址]，点击菜单进入地址配置页面，如图所示：

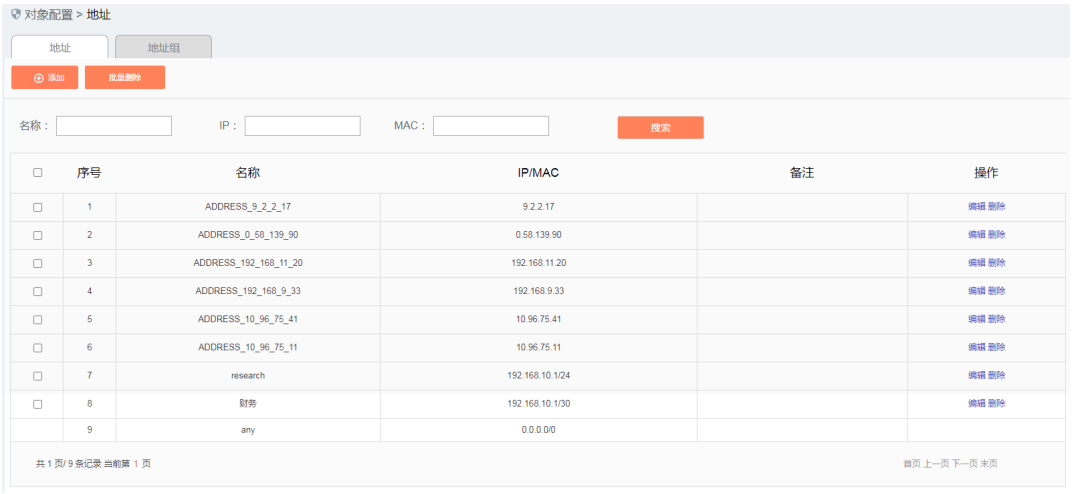


图 **错误!文档中没有指定样式的文字。**-74 地址管理页面

11.2 地址

11.2.2 地址

地址选项卡，如图所示：

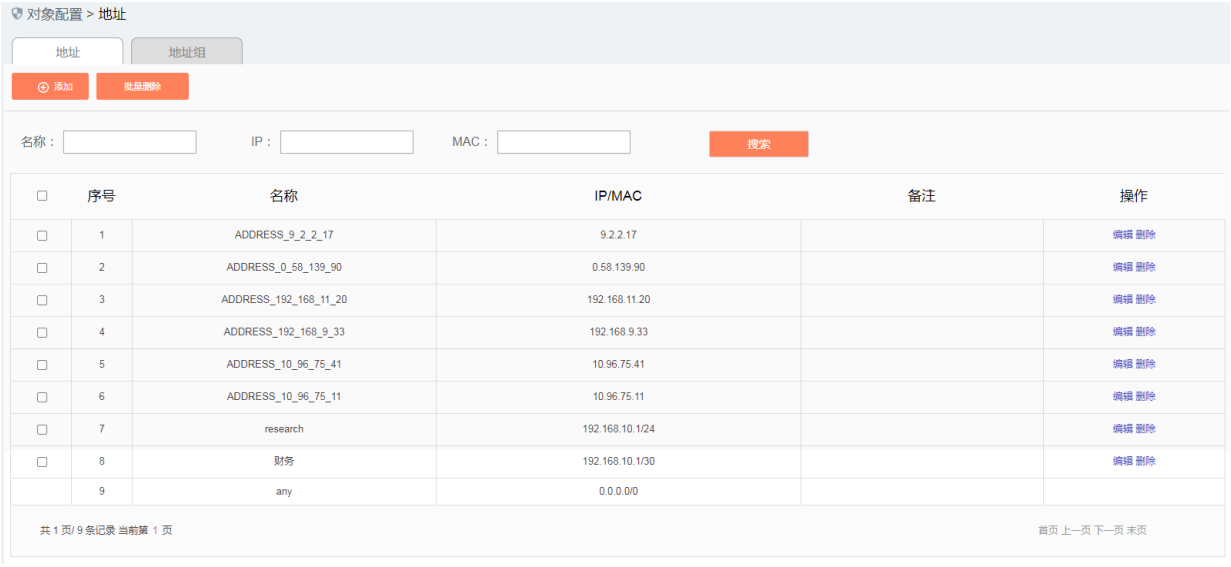


图 **错误!文档中没有指定样式的文字。**-75 地址选项卡

表 **错误!文档中没有指定样式的文字。**-22 地址选项卡各列说明

项目名称	**说明**
名称	地址的名称
IP/MAC	地址对象的 IP 地址或 MAC 地址，仅支持单个地址
备注	添加地址的备注说明
<添加>	添加一条地址项
<批量删除>	删除选中的所有地址项
<搜索>	按着搜索条件进行搜索
<编辑>	编辑选中的地址对象
<删除>	删除一条地址对象

11.2.2.1 添加地址

点击左侧的<添加>按钮，进入添加地址配置界面，如图所示：

图 **错误!文档中没有指定样式的文字。**-76 地址配置

表 **错误!文档中没有指定样式的文字。**-23 添加地址各列说明

项目名称	**说明**
名称	地址对象的名称。如果输入的名称使用特殊字符，仅支持使用键盘上有的特殊字符。
定义地址方式	可以按着“IP 地址/范围”或“MAC 地址”来定义地址，二选一
IP 地址/范围	添加 IPv4 地址，格式可以为 10.1.1.2、10.1.1.2/24、10.1.1.2/255.255.255.0、10.1.1.2\0.0.0.255 或 10.1.1.2-10.1.1.10 格式。当输入单个 IPv4 主机 IP 地址时，系统下发时自动追加 32 位掩码。
MAC 地址	添加 MAC 地址，格式可以为 XX:XX:XX:XX:XX:XX（其中 X 是 1 位十六进制数）
备注	对添加地址的备注说明
<保存>	保存一条地址项
<返回>	返回到上一级菜单

11.2.2.2 修改地址

在[地址]配置列表页面中，点击【编辑】按钮，可以进入地址对象的编辑页面，编辑已经保存的地址对象，如图所示：

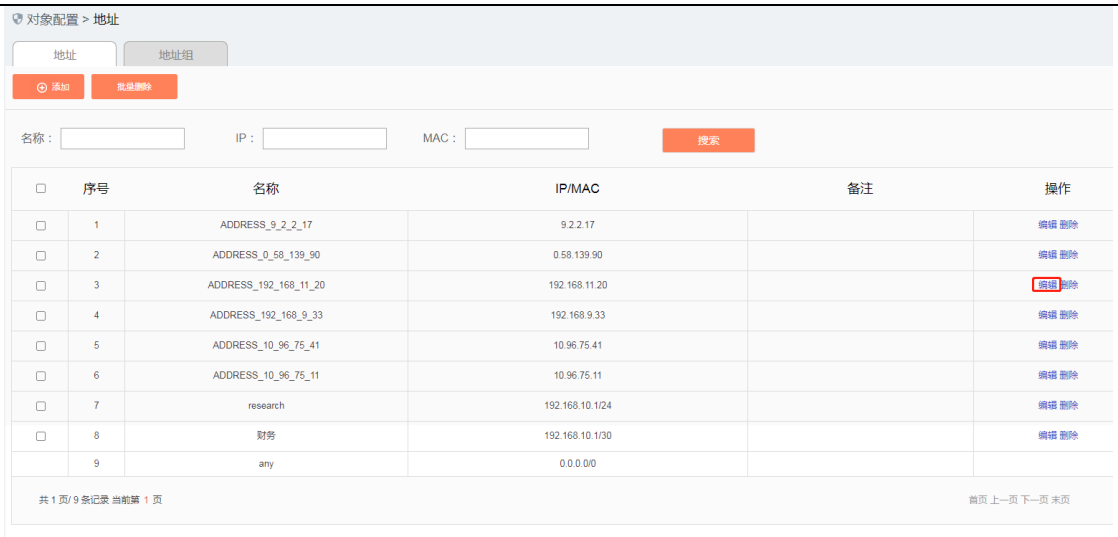


图 **错误!文档中没有指定样式的文字。**-77 编辑地址对象

参数等同于添加地址对象，请参阅上节。

11.2.2.3 删除地址

点击某条地址对象后面的<删除>按钮，可以删除对应的地址对象。

点击表格第一列的复选框，选中多个地址对象，点击列表上方的<批量删除>按钮，则可批量删除地址对象。

11.2.3 地址组

地址组选项卡，如图所示：

图 **错误!文档中没有指定样式的文字。**-78 地址组选项卡

表 **错误!文档中没有指定样式的文字。**-24 地址组各列说明

项目名称	**说明**
名称	地址组的名称
成员	地址组包含的地址对象
备注	地址组的备注说明
<添加>	添加一条地址组项
<批量删除>	删除选中的所有地址组
<搜索>	按着搜索条件进行搜索
<编辑>	编辑选中的地址组对象

<删除>	删除一条地址组对象

11.2.3.1 添加地址组

点击左侧的<添加>按钮，进入添加地址组配置界面，如图所示：

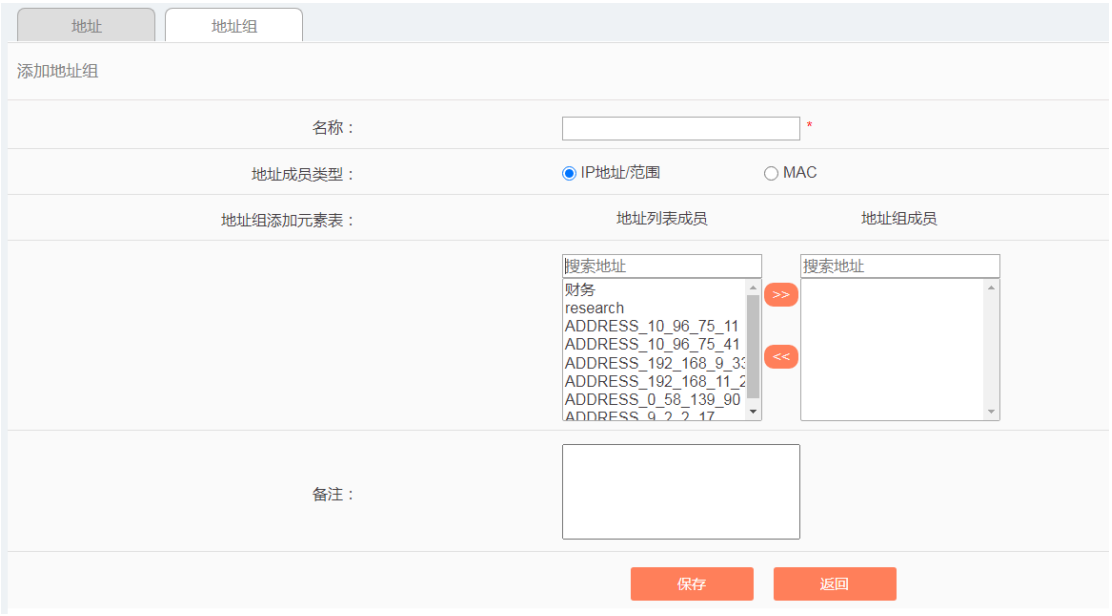


图 **错误!文档中没有指定样式的文字。**-79 地址组添加页面

表 **错误!文档中没有指定样式的文字。**-25 地址组添加各列说明

项目名称	**说明**
名称	地址组的名称
地址组添加元素表	可以从“地址列表成员”通过>>添加到“地址组成员”或从“地址组成员”通过<<移除到“地址列表成员”
备注	对添加地址的备注说明
<保存>	保存一条地址组项
<返回>	返回到上一级菜单

11.2.3.2 修改地址组

在[地址组]配置列表页面中，点击【编辑】按钮，可以进入地址组对象的编辑页面，编辑已经保存的地址组对象，如图所示：

图 **错误!文档中没有指定样式的文字。**-80 编辑地址对象

参数等同于添加地址组对象，请参阅上节。

11.2.3.3 删除地址组

点击某条地址组对象后面的<删除>按钮，可以删除对应的地址组对象。

点击表格第一列的复选框，选中多个地址组对象，点击列表上方的<批量删除>按钮，则可批量删除地址组对象。

11.3 服务

除了可以使用预先定义好的服务外，用户还可以自己定义网络中其它服务器提供的服务。

11.3.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[对象配置/服务]，点击菜单进入配置页面，如图所示：

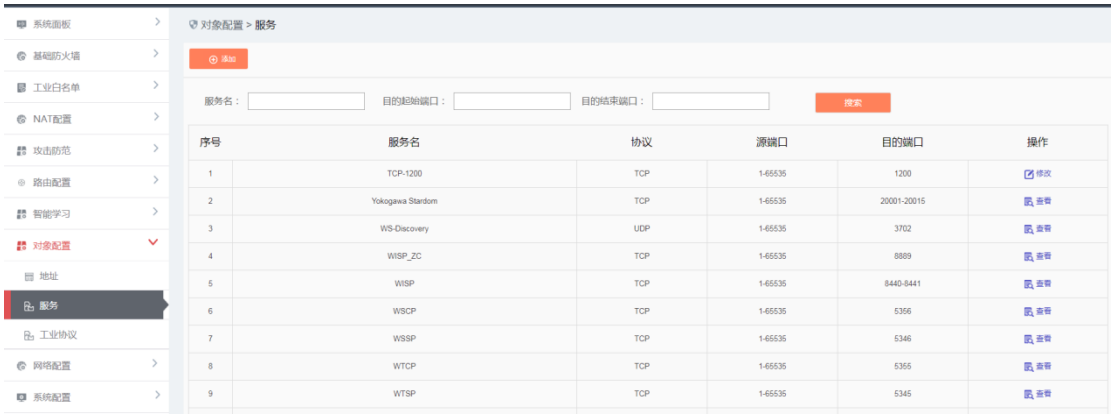


图 **错误!文档中没有指定样式的文字。**-81 服务页面

11.3.2 添加服务

进入[服务]页面后，点击左侧的<添加>按钮，如图 **错误!文档中没有指定样式的文字。**-82 所示，将弹出自定义服务添加页面，如图 **错误!文档中没有指定样式的文字。**-83 所示：

图 **错误!文档中没有指定样式的文字。**-82 添加服务

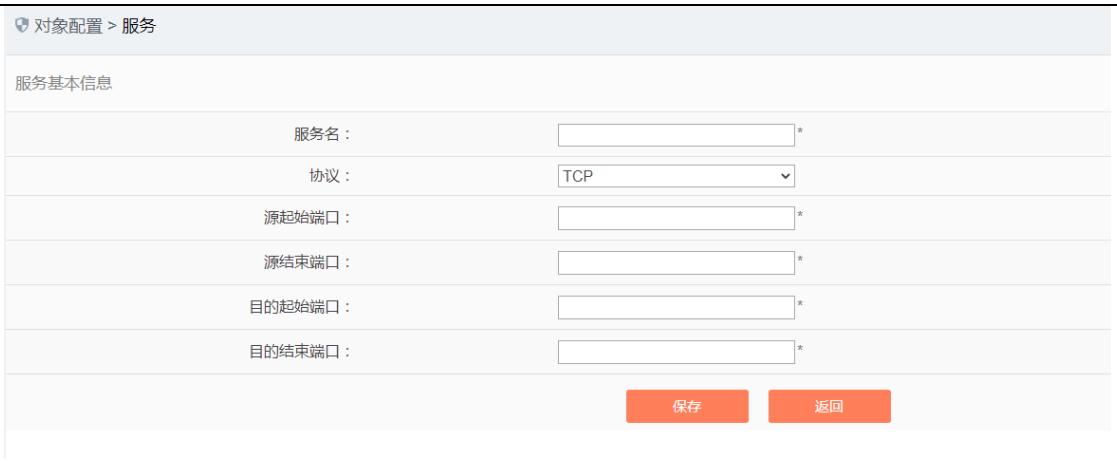


图 **错误!文档中没有指定样式的文字。**-83 服务添加页面

表 **错误!文档中没有指定样式的文字。**-26 服务添加各列说明

项目名称	**说明**	
服务名	自定义的服务名称，不能与现有的冲突	
协议	下拉选择该服务所依赖的传输层协议	
源起始端口	服务所使用的源起始端口，从 1 到 65535，没有则输入 1	
源结束端口	服务所使用的源结束端口，从 1 到 65535，没有则输入 65535	
目的起始端口	服务所使用的目的起始端口，从 1 到 65535	
目的结束端口	服务所使用的目的结束端口，从 1 到 65535，只有一个端口则与目的起始端口相同	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到服务列表显示页面
	返回	忽略所有的修改，返回到服务列表显示页面

11.3.3 查看服务

进入[服务]页面后，即可查看到当前系统内置和已经自定义过的服务。

11.3.4 修改服务

进入[服务]页面后，点击操作列下的<修改>按钮，即可以修改自定义服务，修改页面如图所示:

图 **错误!文档中没有指定样式的文字。**-84 修改服务

每个字段的含义请参考 011.3.2 添加服务。

11.3.5 删除服务

进入[服务]页面后，直接点击某个自定义服务最右侧的<删除>按钮，可以删除对应的自定义服务。如图所示：

图 **错误!文档中没有指定样式的文字。**-85 删除自定义服务

注：无法删除正在被某个安全策略使用的自定义服务。

11.4 工业协议

11.4.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[对象配置/工业协议]，点击菜单进入配置页面，如图所示：

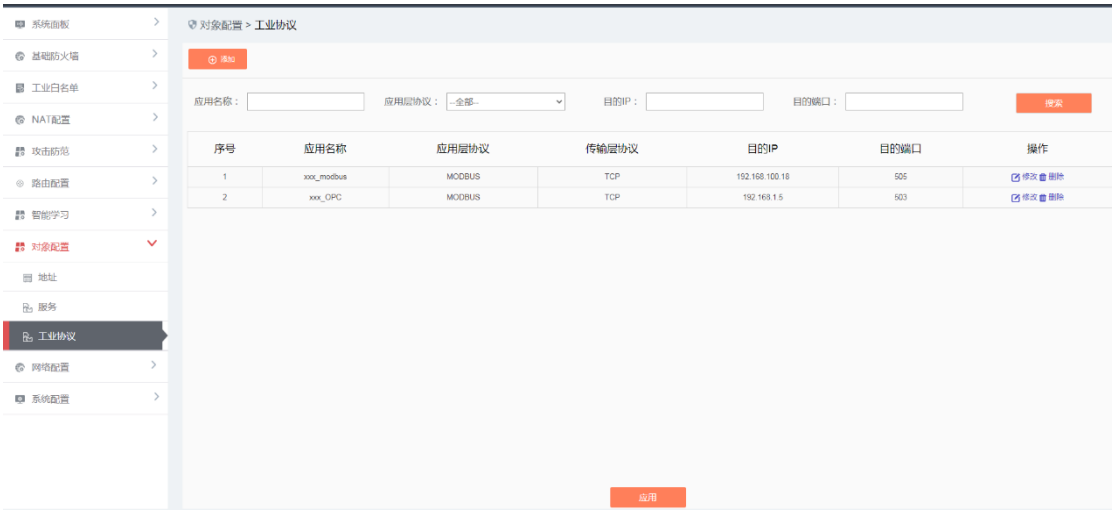


图 **错误!文档中没有指定样式的文字。**-86 工业协议

11.4.2 添加工业协议

进入[工业协议]页面后，点击左侧的<添加>按钮，将弹出工业协议添加页面，如图所示：

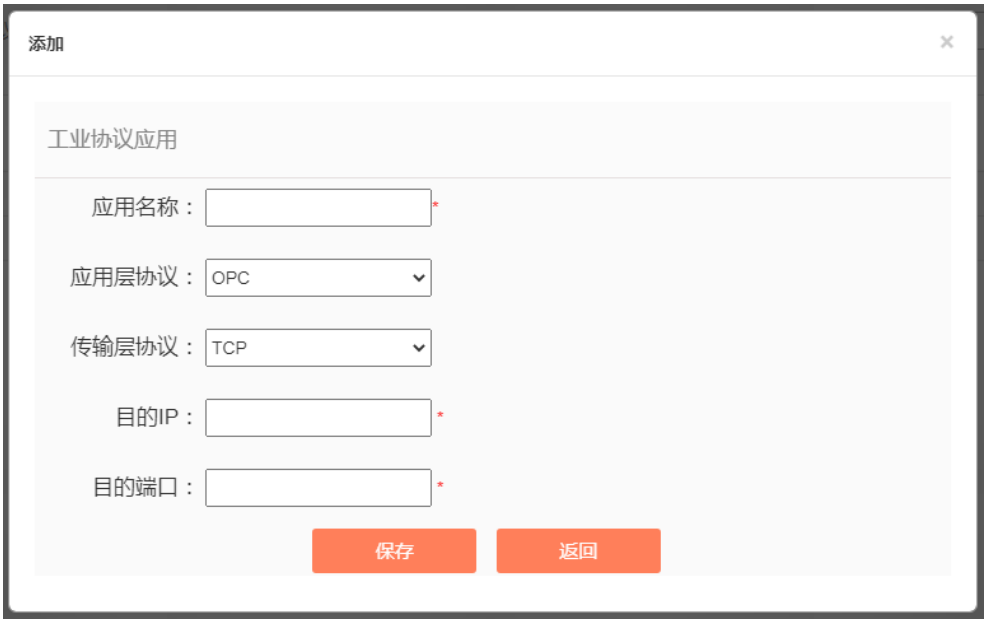


图 **错误!文档中没有指定样式的文字。**-87 工业协议添加页面

表 **错误!文档中没有指定样式的文字。**-27 工业协议添加说明

项目名称	说明
应用名称	自定义的工业协议的名称，不能与现有的冲突
应用层协议	下拉选择要自定义的工业协议
传输层协议	下拉选择该协议所依赖的传输层协议
目的 IP	提供协议服务端的设备 IP 地址

目的端口	替换此协议默认端口的新的端口	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到工业协议列表显示页面
	返回	忽略所有的修改，返回到工业协议列表显示页面

11.4.3 查看工业协议

进入[工业协议]页面后，即可查看到当前已经自定义过的工业协议。

11.4.4 修改工业协议

进入[工业协议]页面后，点击操作列下的<修改>按钮，即可以修改工业协议，修改页面，如图所示：

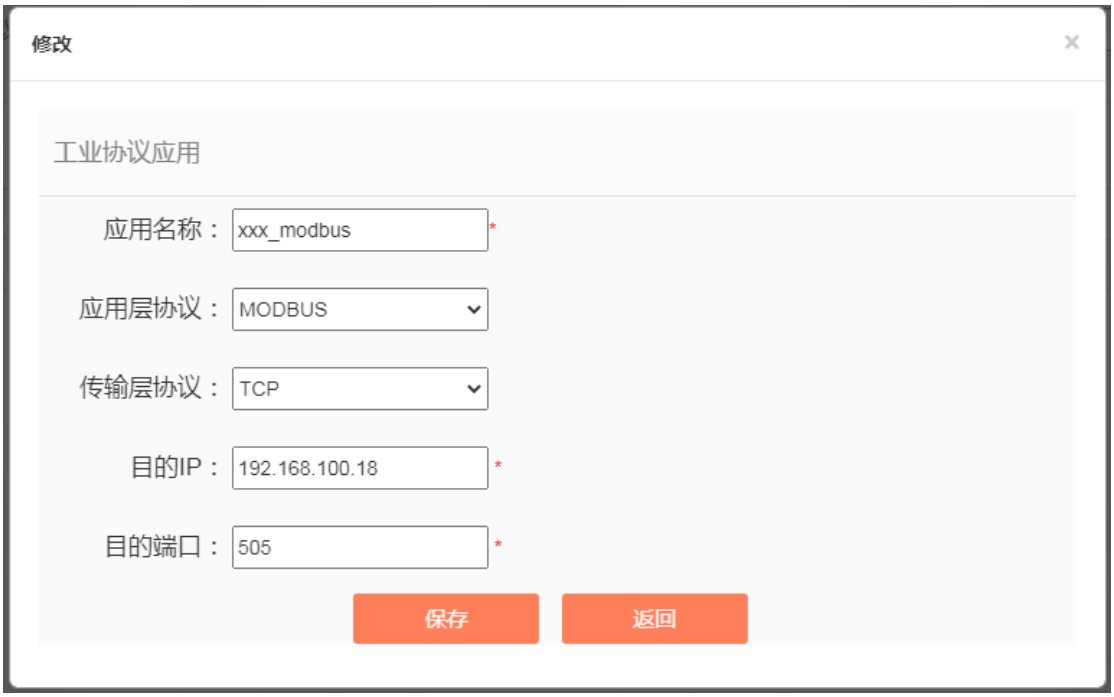


图 **错误!文档中没有指定样式的文字。**-88 工业协议修改页面

每个字段的含义请参考添加工业协议。

11.4.5 删除工业协议

进入[工业协议]页面后，直接点击某个工业协议最右侧的<删除>按钮，可以删除对应的工业协议。如图所示：

图 **错误!文档中没有指定样式的文字。**-89 删除工业协议

注：无法删除正在被某个策略使用的工业协议。

11.5 监测对象

参考 010.3 监测对象部分的介绍。

11.6 监测对象分类

参考 010.3 监测对象部分的介绍。

11.7 工艺序列

具体请参考 017.2.6 工艺序列

12. 网络配置

12.1 简介

网络配置部分集成了所有和网络配置相关的模块包括接口配置、VLAN 接口配置、安全域管理。

& 注意：

当启用 ARP 代理功能时,尽量不要使用默认路由，以防现网环境通信受影响。可以明确指定静态路由

12.2 物理接口配置

12.2.1 接口状态

型号不同的设备接口数不同，以 S2124 为例说明。

设备共包括 24 个接口，命名为 eth0~eth23，接口配置可以针对每个接口进行相关配置。如图所示：

图 **错误!文档中没有指定样式的文字。**-90 网络接口状态

表 **错误!文档中没有指定样式的文字。**-28 网络接口各列说明

项目名称	说明
接口名称	接口名称包括 eth0~eth23
IP 地址	接口的 IP 地址/掩码，可配置多个显示的时候用逗号（,）隔开
模式	接口的工作模式，包括路由、交换和接口对三种模式
连接类型	在交换模式下可以选择 Access 和 Trunk 两种类型
VLAN ID	VLAN ID
Trunk Vlan ID	Trunk Vlan ID 仅在接口类型为 Trunk 的时候可选
操作	编辑接口的相关配置选项

12.2.2 接口配置

点击接口状态页面中，编辑选项，可进入接口配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-91 编辑接口

表 **错误!文档中没有指定样式的文字。**-29 接口编辑各项说明

项目名称	说明
接口名称	接口名称包括 eth0~eth23 不可编辑
链路工作模式	包括自适应、全双工、半双工三种配置
Combo 接口	当“链路工作模式”为非“自适应”时，需要选择当前工作的接口类型是“电口”还是“光口”,默认是“电口”
链路速度	当选择全双工和半双工的时候可配置
工作模式	接口的工作模式，包括路由、交换和接口对三种模式
IP 地址/掩码	当选择静态 IP 地址的时候可用，配置完毕后点击添加按钮后保存，最大支持 8 个
ARP 代理	ARP 代理功能开关，仅在路由模式下可用
连接到	接口的出口位置，包括 Wan 和 Lan 两种配置选项
启用管理	仅在路由模式下可用
启用 ping	启用 ping 功能，仅在路由模式下可用
启用 traceroute	启用 traceroute 功能，仅在路由模式下可用
<保存>	保存所有配置
<返回>	返回到上级菜单

12.3 VLAN 接口

12.3.1 简介

在逻辑上将一个局域网 LAN (Local Area Network) 划分成多个子集，每个子集形成各自的广播域，即虚拟局域网 VLAN（Virtual Local Area Network）。简单地说，VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。

当 VLAN 内的主机需要与网络层的设备通信时，可以在设备上创建基于 VLAN 的逻辑接口，即 VLAN

接口。VLAN 接口在功能上与普通三层物理接口基本相同，可实现配置 IP 地址等多种三层特性。

12.3.2 VLAN 接口配置

VLAN 接口配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-92VLAN 接口配置页面

12.3.3 添加 VLAN 接口

进入[VLAN 接口配置]点击左侧的<添加>按钮，进入添加 VLAN 接口配置界面，如图所示：

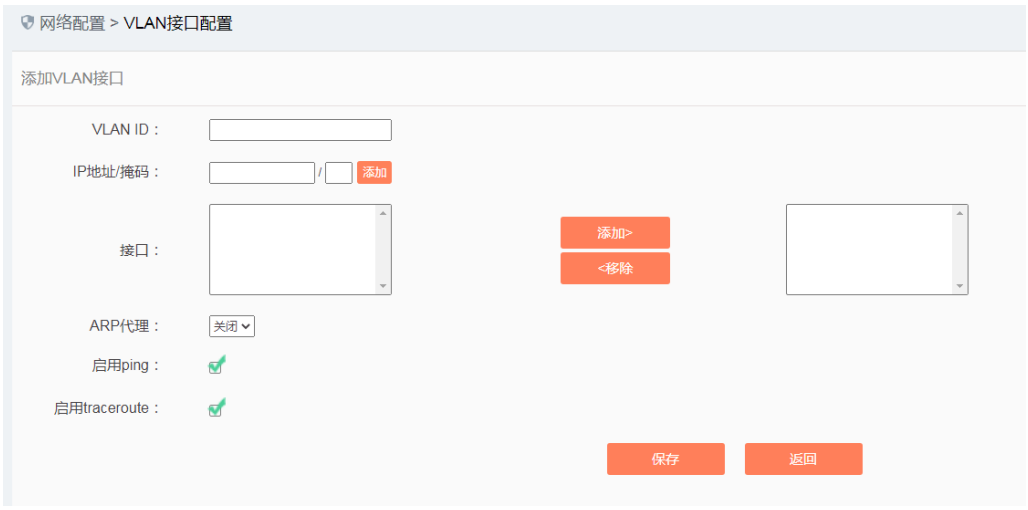


图 **错误!文档中没有指定样式的文字。**-93 添加 VLAN 接口

表 **错误!文档中没有指定样式的文字。**-30 添加 VLAN 接口各项说明

项目名称	说明
VLAN ID	VLAN ID 合法范围 1~4094
IP 地址/掩码	配置 IP 地址及 IP 地址掩码位数
接口	<添加>和<移除>接口
ARP 代理	ARP 代理功能开关
启用 ping	启用 ping 功能
启用 traceroute	启用 traceroute 功能
<保存>	保存当前配置

<返回>	返回上一级菜单

完成配置后，点击<保存>按钮，可在 VLAN 接口配置页面，查看 VLAN 接口信息。

12.3.4 修改 VLAN 接口

进入[VLAN 接口配置]页面后，点击操作列下的<修改>按钮，即可以修改 VLAN 接口，修改页面，如图所示：

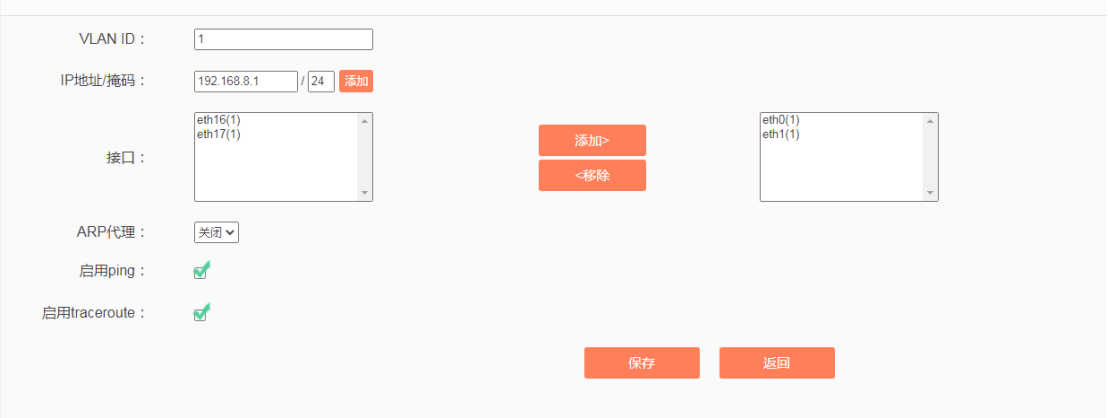


图 **错误!文档中没有指定样式的文字。**-94VLAN 接口修改页面

每个字段的含义请参考添加 VLAN 接口。

12.3.5 删除 VLAN 接口

进入[VLAN 接口配置]页面后，直接点击某个 VLAN 接口最右侧的<删除>按钮，可以删除对应的 VLAN 接口。

12.4 安全域管理

12.4.1 简介

传统基于接口的策略配置方式需要为每一个接口配置安全策略，给网络配置管理员带来了极大的负担，安全策略的维护工作量成倍增加，从而也增加了因为配置引入安全风险的概率。和传统防火墙基于接口的策略配置方式不同，业界主流防火墙通过围绕安全域（Security Zone）来配置安全策略的方式解决上述问题。

所谓安全域，是一个抽象的概念，它有两种划分方式：

- 按照接口划分。

安全域可以包含三层普通物理接口和逻辑接口，也可以包括二层物理 Trunk 接口+VLAN，划分到同一个安全域中的接口通常在安全策略控制中具有一致的安全需求。

- 按照IP 地址划分。

根据 IP 地址划分不同的安全域，以实现按业务报文的源 IP 地址或目的 IP 地址进行安全策略控制。

引入安全域的概念之后，安全配置管理员将安全需求相同的接口或 IP 地址进行分类（划分到不同的域），能够实现策略的分层管理。通过引入安全域的概念，不但简化了策略的维护复杂度，同时也实现了网络业务和安全业务的分离。

工业防火墙采用接口划分的方式，实现安全域的管理。

注：安全域的接口选择只支持物理口（eth0~eth8）。

12.4.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[网络配置/安全域　管理]，点击

菜单进入配置页面，如图所示：

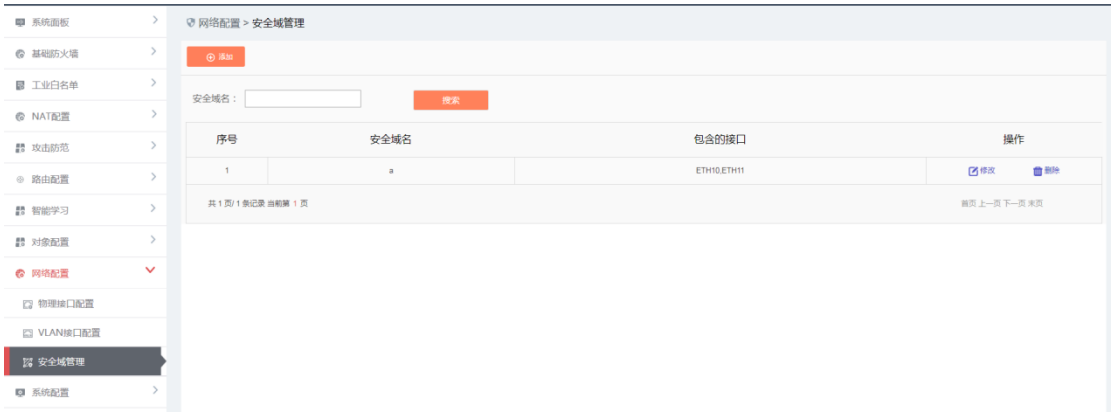


图 **错误!文档中没有指定样式的文字。**-95 安全域管理

12.4.3 添加安全域

点击 [安全域管理]安全域列表标签左侧的<添加>按钮，将弹出安全域添加页面，如图所示：

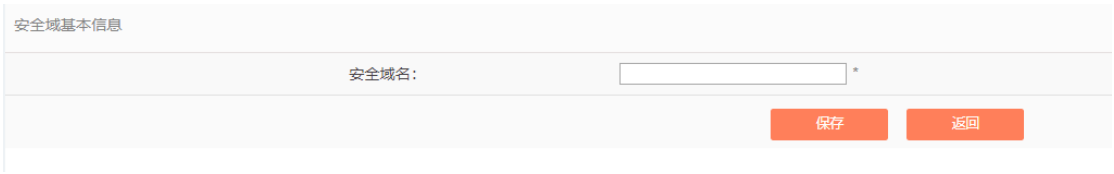


图 **错误!文档中没有指定样式的文字。**-96 添加安全域

12.4.4 查看安全域

点击左侧导航栏的[网络配置/安全域管理]，进入[安全域管理]的页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-97 安全域管理页面

安全域有两种基本类型，一种是由系统内置的安全域，一种是用户自己创建的安全域。用户自定义创建的安全域。两者除 ID 外，可以修改其它所有属性。此处可以查看到系统内所有安全域的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-31 安全域各项说明

项目名称	说明	
安全域名	便于记忆的安全域的名称	
包含的接口	安全域包含的所有防火墙接口	
操作	修改	对安全域的信息进行修改和设置
	删除	删除安全域

12.4.5 修改安全域

点击[安全域管理]安全域列表中操作列下的<修改>按钮，将打开[安全域基本信息]修改页面（如图

所示），可以修改安全域的基本信息。

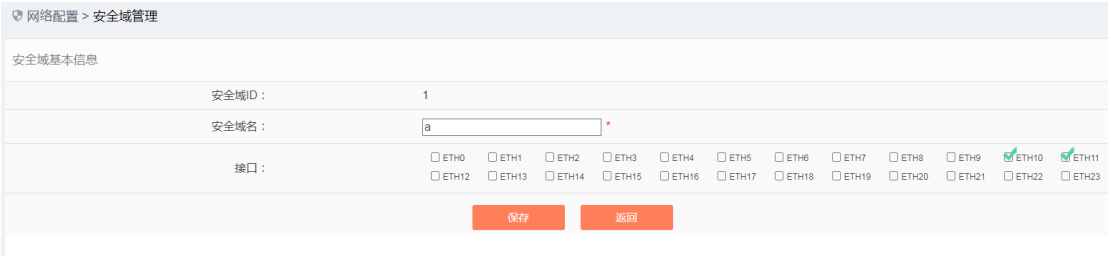


图 **错误!文档中没有指定样式的文字。**-98 修改安全域信息

安全域包含了防火墙的哪个接口，此接口所连接的网络就属于此安全域。例如：如果安全域 Trust 包含了接口 eth1，而某个安全策略包含了一条从 Trust 到 any 安全域的通过策略，则意味着从 eth1 发起的会话都会通过。

12.4.6 删除安全域

点击[安全域管理]安全域列表操作列下的<删除>按钮，可以把不再使用的安全域进行删除。

注意：无法删除正在被安全策略规则使用的安全域。

12.4.7 检索安全域

在[安全域管理]安全域显示列表页面中，可以根据条件对安全域进行检索，如图所示：

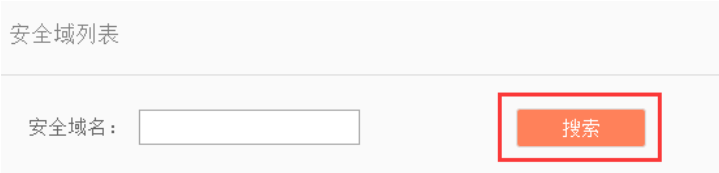


图 **错误!文档中没有指定样式的文字。**-99 检索安全域

13. VPN

13.1 简介

虚拟专用网（Virtual Private Network， VPN）提供了一种在公共网络上建立专用数据通信网络的方法。通过基于共享的 IP 网络，VPN 为用户远程访问、外网和内网之间的通信提供了安全而稳定的 VPN 隧道。

对于构建 VPN 来说，网络隧道（Tunneling）技术是个关键技术。网络隧道技术指的是利用一种网络协议来传输另一种网络协议，它主要利用网络隧道协议来实现这种功能。VPN 隧道通常在企业的两个本地局域网，或远程用户和本地局域网之间使用，根据应用场景的不同，相应地分为点到点 VPN 以及点到多点 VPN。

13.2 基本配置

13.2.1 页面导航

配置管理员登录管理平台后，点击[VPN 配置/基本配置]，如图所示。

图 **错误!文档中没有指定样式的文字。**-100VPN 基本配置导航

13.2.2 配置流程

主要设置 VPN 全局配置，控制 VPN 功能的启用/禁用和 NAT-T 功能的启用/禁用。

启用 VPN 功能：复选框，默认不勾选。用于控制 VPN 功能的启用/禁用。

启动 NAT-T 功能：复选框，默认不勾选。用于控制 NAT 穿越功能的启用/禁用。

13.3 隧道配置

13.3.1 页面导航

配置管理员登录管理平台后，点击[VPN 配置/隧道配置]，如图所示。

图**错误!文档中没有指定样式的文字。**-101 VPN 隧道配置导航

13.3.2 配置点到点 VPN

点到点 VPN 即局域网到局域网的 VPN（LAN to LAN VPN），该场景中，本端希望与另一台 VPN 网关建立隧道，以使两台设备所连的私网可以相互通信。如果希望本端可以主动发起访问，那么就要求对端网关需要拥有固定的 IP 地址。如果两端网关都拥有固定的 IP 地址，这样两者就可以相互发起访问。

单击隧道列表页<添加>按钮，打开 VPN 隧道添加页面，选择“点到点”的场景，如下图所示：

图**错误!文档中没有指定样式的文字。**-102 配置点到点 VPN 隧道

之后按照下面的步骤进行配置：

第 1 步：隧道的基本信息

表 **错误!文档中没有指定样式的文字。**-32 隧道基本配置各项说明

列名称	说明
隧道名称	输入 VPN 隧道的名称，由 1-32 个字母、数字、下划线组成，不能重复、必填项。
本端接口	从下拉列表中选择建立 VPN 隧道使用的接口。本端接口必须为配置 IP 地址的 WAN 口，可以是物理接口、VLAN 接口。物理接口应为本端与对端相连的接口，通常为设备的公网接口。本端将使用该接口与对端建立隧道。
本端地址	输入本端设备与对端设备建立隧道所使用的 IP 地址。当“本端接口”配置了多个 IP 地址时，可以从中任选一个，只要对端可以正常访问此 IP 地址即可。在双机热备组网中，请选择本端接口对应的虚拟 IP 地址。
对端地址	输入对端网关所使用的 IP 地址，支持 IP 和 IP/MASK 两种格式。
网关地址	本端网关与对端网关不在同一网段建立隧道时，需要配置网关地址。
默认网关	对端地址没有固定的 IP 地址（不配置或者配置全匹配 0.0.0.0/0）时，需要配置网关地址并勾选默认网关复选框。

说明：当本端接口选择虚拟口（VLAN 接口）时，请注意配置要求：不支持包含 Trunk 口的虚拟口；虚拟口数量不能大于透明口数量；同一 VLAN ID 只能配置一条。

第 2 步：认证参数

VPN 隧道支持预共享秘钥和 RSA 签名两种认证方式，不同方式需要配置的参数略有差异。

表 **错误!文档中没有指定样式的文字。**-33 预共享秘钥各项说明

列名称	说明
预共享秘钥	输入双方管理员约定的密钥字符串

本端 ID	本端 ID 用于标识本端设备的身份，供对端设备认证自身的合法性。类型和值都要与对端设备上设置的“对端 ID”参数保持一致。
对端 ID	对端 ID 用于认证对端设备的身份，此参数需要向对端管理员获取。类型与值都需要与对端设备上设置的“本端 ID”参数保持一致。如果不需要认证，接受任意 ID 的请求，请选择“接受任意对端 ID”。

表 **错误!文档中没有指定样式的文字。**-34 RSA 签名各项说明

列名称	**说明**
本地服务器证书	必须为.crt 或.cer 或.pem 的文件，证书管理请参考 020.9 证书管理中的具体内容
本地服务器私钥	必须为.pem 或.der 的文件
对端 CA 证书	必须为.crt 或.cer 或.pem 的文件
本端 ID	本端 ID 用于标识本端设备的身份，供对端设备认证自身的合法性。类型和值都要与对端设备上设置的“对端 ID”参数保持一致。
对端 ID	对端 ID 用于认证对端设备的身份，此参数需要向对端管理员获取。类型与值都需要与对端设备上设置的“本端 ID”参数保持一致。如果不需要认证，接受任意 ID 的请求，请选择“接受任意对端 ID”。

第 3 步：配置隧道需要加密的数据流

通常情况下只有部分数据流需要进入隧道发往对端私网，还有一部分数据流需要直接进入 Internet。为了避免这些本来需要访问 Internet 的数据流进入隧道，需要配置流量规则来限定可以进入隧道的数据流。在流量规则列表中最多可以添加 10 条规则，流量将从上到下依次匹配规则，匹配成功则进入隧道，不再继续匹配后续的规则。

表 **错误!文档中没有指定样式的文字。**-35 加密的数据流各项说明

列名称	**说明**
本端子网	输入允许进入隧道的数据流的源地址，支持 IP/MASK 格式，通常为本端内网中需要保护的私网网段。
本端端口	输入允许进入隧道的数据流的源端口号，当协议为 TCP/UDP 时该参数有效，0 表示全匹配。
对端子网	输入允许进入隧道的数据流的目的地址，支持 IP/MASK 格式，通常为对端内网中需要访问的私网网段。

对端端口	输入允许进入隧道的数据流的目的端口号，当协议为 TCP/UDP 时该参数有效，0 表示全匹配。
协议	下拉选择允许进入隧道的数据流的协议，支持 ANY、ICMP、IGMP、IP-IN-IP、TCP、UDP、OSPF 和 SCTP，ANY 表示全匹配。

说明：点到点场景对端子网不能为全匹配（0.0.0.0/0）；当本端接口选择虚拟口（VLAN 接口）时，本地子网不能为全匹配（0.0.0.0/0）。

第 4 步：配置安全提议中高级参数（可选）

系统预置了多组默认的安全提议参数，可反选【采用默认配置】复选框并展开“高级”选项查看。如果默认提议不能满足协商要求，可以修改“高级”中的参数。要求除“SA 超时时间”之外，所有参数需要两端存在相同选项。

安全提议中的算法支持多选。同时选择了多个算法，隧道双方在 IKE 协商时，会根据算法安全性由高到低的顺序逐个进行匹配，安全性高的算法被优先使用。算法安全性的高低顺序，在 Web 界面上按照从右至左的顺序排列。例如加密算法中，最右边的加密算法 AES256 的安全性最高，其次是 AES192，...，安全性最低的是 3DES。

第 5 步：配置“高级”参数

表 **错误!文档中没有指定样式的文字。**-36 高级选项各项说明

列名称	**说明**
IKE 参数	
IKE 版本	选择“v1”或“v2”来确定与对端进行 IKE 协商时所使用的协议版本。同时选择两种版本表示可响应 v1 和 v2 两个版本的 IKE 请求，但是主动发起请求时只使用 v2 版本。
协商模式	当“IKE 版本”选择了“v1”时会出现本参数，选择 IKEv1 的协商模式。 •主模式：强制使用主模式协商，主模式更安全。 •野蛮模式：强制使用野蛮模式协商，野蛮模式更快速。
加密算法	选择满足需要的加密算法，AES 算法的安全性和复杂度都比 3DES 算法高。
认证算法	当“IKE 版本”选择了“v1”时会出现本参数，选择保证数据发送源可靠的认证算法，仅 IKE v1 支持此参数。
PRF 算法	当“IKE 版本”选择了“v2”时会出现本参数，选择保证数据发送源可靠的认证算法，仅 IKE v2 支持此参数。
DH 组	选择密钥交换方法。

SA 超时时间	输入“SA 超时时间”，默认：86400，范围：60-604800，单位：秒。 IKE 隧道将在建立时间达到阈值时重新协商以保证安全性，重协商不会导致当前隧道中断。
IPSec 参数	
封装模式	IPSec 的封装模式，仅支持“隧道模式”，只保护报文载荷部分，常用于 VPN 网关之间建立隧道。
安全协议	IPSec 的安全协议，仅支持“ESP”协议，提供对报文载荷的加密和认证能力。
ESP 加密算法	选择保证数据不被窃取的加密算法。
ESP 认证算法	选择保证数据发送源可靠的认证算法。
PFS	选择密钥交换方法。组号越大密钥越长，安全性越高。选择“0”表示不进行额外的密钥交换。
SA 超时时间	输入“SA 超时时间”，默认：3600，范围：60-604800，单位：秒。IPSec 隧道将在建立时间达到阈值时重新协商以保证安全性，重协商不会导致当前隧道中断。
DPD（对端状态检测）	
检测时间间隔	输入“检测时间间隔”，范围：10-3600，单位：秒。
重传时间间隔	输入“重传时间间隔”，范围：2-60，单位：秒。仅对 IKEv1 有效。

13.3.3 配置点到多点 VPN

点到多点常用于一个总部与多个分支建立 VPN 的场景，该场景中，本端希望与多台 VPN 网关、客户端（如：便携计算机等）同时建立多条隧道，实现这些设备或所连私网的互联。这些设备的 IP 地址通常是不固定的。这种场景常用于总部与出差员工之间建立 VPN，要求总部拥有固定的 IP 地址，由出差员工发起访问。

单击隧道列表页<添加>按钮，打开 VPN 隧道添加页面，选择“点到多点”的场景，如下图所示：

图**错误!文档中没有指定样式的文字。**-103 配置点到多点 VPN 隧道

之后按照下面的步骤进行配置：

第 1 步：选择客户端类型

根据实际需要接入的设备在“对端接入类型”中选择客户端类型

- 分支网关：使用 IPSec 协议接入的 VPN 网关。
- 拨号客户端：使用 IKE v2 协议接入的客户端，例如：PC（Win7/Win10）等

第 2 步：配置隧道的基本信息

具体各项信息请参考 013.3.2 配置点到点 VPN 的相同部分

第 3 步：配置隧道双方的认证参数

VPN 隧道支持预共享秘钥和 RSA 签名两种认证方式，不同方式需要配置的参数略有差异。

具体各项信息请参考 013.3.2 配置点到点 VPN 的相同部分

第 4 步：配置分配给用户的地址池（可选）

当“对端接入类型”勾选了“拨号客户端”时会出现本配置项，指定为用户分配私网 IP 地址的地址池，支持 IP 和 IP/MASK 两种格式，最多可配置 8 条地址池。

第 5 步：配置隧道需要加密的数据流

具体各项信息请参考 013.3.2 配置点到点 VPN 的相同部分

第 6 步：配置安全提议中高级参数（可选）

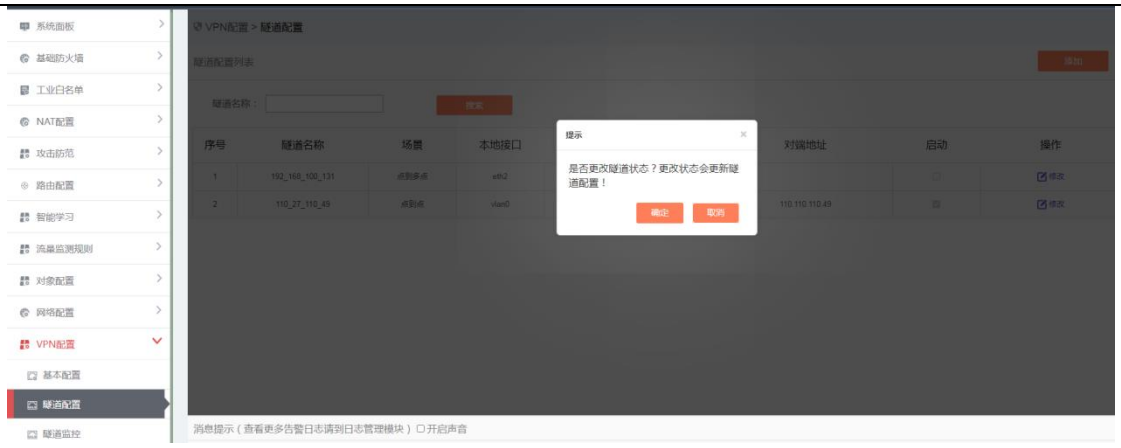
具体各项信息请参考 013.3.2 配置点到点 VPN 的相同部分

第 7 步：配置“高级”参数

具体各项信息请参考 013.3.2 配置点到点 VPN 的相同部分

13.3.4 启动/停止隧道

成功创建 VPN 隧道后，隧道默认为停止状态，需要手工启动隧道，启动后隧道才能生效。在隧道配置列表中，勾选某隧道对应的<启动>复选框，确定后即可启动相应的隧道。在隧道列表中， 反选某隧道对应的<启动>复选框，确定后即可停止相应的隧道。如图所示。



图**错误!文档中没有指定样式的文字。**-104 启动/停止隧道

13.3.5 修改/删除隧道

成功创建 VPN 隧道后，在启动和停止状态下都可以修改隧道配置，在隧道配置列表中，点击某条隧道对应的<修改>按钮即可进入相应的隧道配置页面；只有隧道处于停止状态时才可以执行删除操作，在隧道配置列表中，点击某条隧道<删除>按钮，确定后即可删除相应的隧道。如图所示：

图**错误!文档中没有指定样式的文字。**-105 修改/删除隧道

13.4 隧道监控

配置管理员登录管理平台后，点击[VPN 配置/隧道监控]，如图所示

图**错误!文档中没有指定样式的文字。**-106 VPN 隧道监控导航

通过隧道监控功能，配置管理员可以查看到当前已经建立的 VPN 隧道状态信息，支持查看的 VPN 隧道信息如下所示。

表 **错误!文档中没有指定样式的文字。**-37 监控各项说明

列名称	说明
隧道名称	显示 VPN 隧道名称
连接 ID	显示隧道连接 ID
状态	显示隧道连接状态
本端地址	显示隧道本端接口的 IP 地址
对端地址	显示隧道对端接口的 IP 地址
IKE SA 倒计时（秒）	显示最近一次隧道建立至今剩余 IKE SA 超时时间（单位：秒）
IPSEC SA 倒计时（秒）	显示最近一次隧道建立至今剩余 IPSEC SA 超时时间（单位：秒）
发送流量（B）	显示最近一次隧道建立至今发送的流量（单位：字节）
接收流量（B）	显示最近一次隧道建立至今接收的流量（单位：字节）

14. 双机热备

14.1 功能介绍

高可用性即双机热备功能、是基于防火墙之间的热备，即：一台防火墙出现故障，另一个防火墙能接替故障防火墙的工作，完成业务的转发和防护工作。

当防火墙处于备用状态或者故障状态时，它在网络中是透明的。

当防火墙处于主用状态时，该防火墙需完成业务转发和防护工作。

当主用防火墙出现故障时，备用防火墙切换成主用防火墙接替业务转发和防护工作。

说明：双机的配置需要保持一致性，以保证主用防火墙故障时，业务的连续性。

14.2 双机热备配置

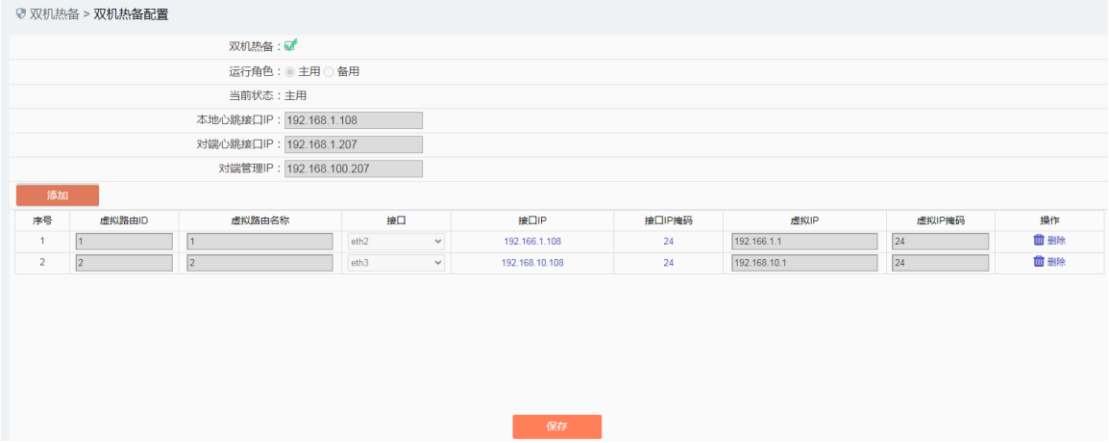
14.2.1 页面导航

配置管理员登录管理平台后，点击[双机热备/双机热备配置]，如图所示：

图**错误!文档中没有指定样式的文字。**-107 双机热备导航

14.2.2 双机热备配置

点击[双机热备/双机热备配置]后，打开的配置界面如下图所示：



图**错误!文档中没有指定样式的文字。**-108 双机热备配置界面

表 **错误!文档中没有指定样式的文字。**-38 双机热备配置各项说明

列名称	说明
双机热备	禁用/启用双机热备功能
运行角色-主用	主用代表防火墙的优先级较高，在竞选 active 时，有较大的概率成为 active 防火墙。

	备用代表防火墙的优先级较低，在竞选 active 时，有较大的概率成为 standby 防火墙。
当前状态	显示当前防火墙的双机热备的状态
本地心跳接口 IP	用于数据同步，保证切换时业务稳定。只支持单 IP 路由口。
对端心跳接口 IP	数据同步需要填写另一个防火墙心跳口的 IP 地址，两者需要在同一网段。
对端管理 IP	配置同步需要通过管理口进行，这里需要配置对端防火墙的管理口 IP 地址

除配置基础信息外，还需要配置 VRRP 的分组。

表 **错误!文档中没有指定样式的文字。**-39 VRRP 分组配置各项说明

虚拟路由 ID	虚拟路由的 ID 号，取值范围 1-255，不可重复。
虚拟路由名称	虚拟路由名称，支持汉字、数字、字母、下划线和连接符，长度不超过 32。
接口	目前支持 vlan、路由接口
虚拟 IP	虚拟路由的 IP 地址，支持 ARP。
虚拟 IP 掩码	虚拟 IP 的掩码

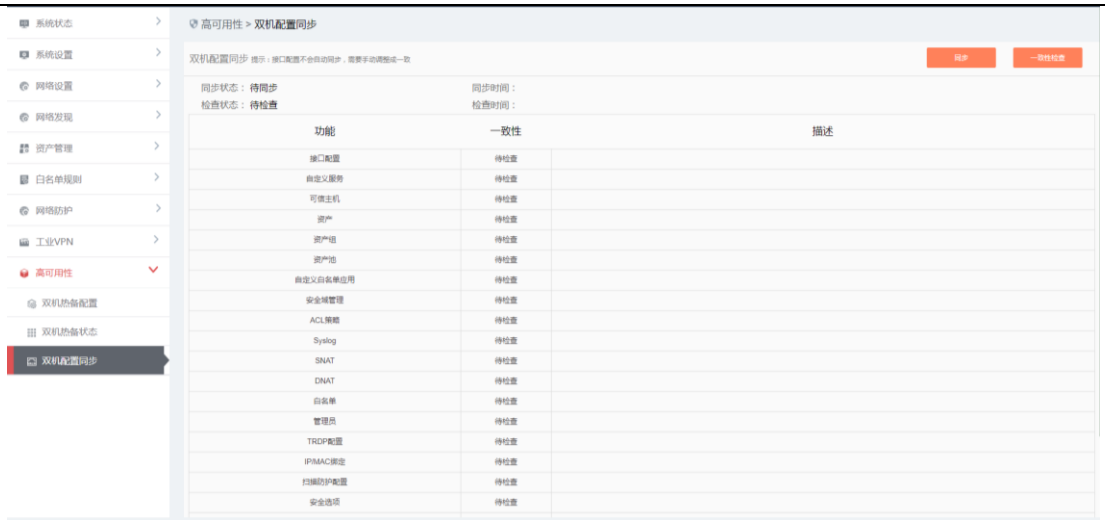
注：最大虚拟路由数 最多支持 64 条虚拟路由。

表 **错误!文档中没有指定样式的文字。**-40 工业防火墙主备状态说明

列名称	**说明**
主用状态	当前防火墙处于 active 状态，负责业务转发及心跳同步工作。
故障状态	当前防火墙已配置的接口中包含 linkdown 状态，防火墙处于故障状态。
备用状态	当前防火墙处于 standby 状态，监听主用防火墙心跳。
关闭状态	双机热备功能未启用。

14.3 双机热备同步

双机热备同步页面，如图所示：



图**错误!文档中没有指定样式的文字。**-109 双机热备同步页面

列名称	说明
同步	两台防火墙之间会定时进行数据同步，也支持手动就行同步。 同步方向：active 防火墙-->standby 防火墙
一致性检查	同步条件检查。

15. 扫描防护

通过工业防火墙开启扫描防护，可以检测网络中是否有 TCP 扫描、UDP 扫描、ICMP 扫描和文件共享扫描等行为。

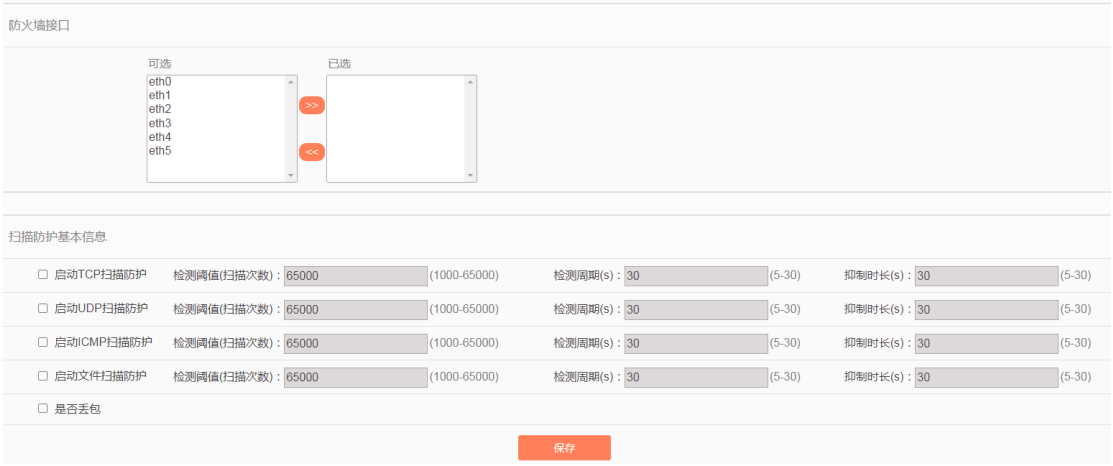
15.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[扫描防护/扫描防护]，如图所示：

图**错误!文档中没有指定样式的文字。**-110 扫描防护

15.2 扫描防护配置

进入[扫描防护]配置界面，首先设置需要启用的防火墙接口，然后通过勾选要启用的扫描防御、配置阈值来开启相应的防护，配置完点击<保存>按钮，如图所示：



图**错误!文档中没有指定样式的文字。**-111 扫描防护配置

16. 诊断中心

诊断中心包括 Ping 诊断、Tracert 诊断。通过诊断中心配置，管理员可以进行相应的故障处理和排查。

16.1Ping 诊断

16.1.1 简介

最常见的用于检测网络设备可访问性的调试工具，它使用 ICMP 的 echo 信息来决定：

- 远程设备是否可用。
- 与远程主机通信的来回旅程（round-trip）的延迟（delay）。
- 包（packet）的丢失情况。

Ping 诊断主要用于检查网络连接及主机是否可达。

16.1.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[诊断中心/诊断中心]，如图所示：

图**错误!文档中没有指定样式的文字。**-112 诊断中心左侧导航

16.1.3 使用方法

进入[诊断中心]使用界面，默认打开的就是 Ping 诊断，在“目的主机 IP 地址”中输入需要诊断的 IP 地址，点击后面的<Ping>按钮，界面将显示诊断结果，如图所示：

图**错误!文档中没有指定样式的文字。**-113Ping 诊断使用

16.2 Tracert 诊断

16.2.1 简介

Tracert 诊断用于测试数据包从发送主机到目的地所经过的网关，主要用于检查网络连接是否可达以及分析网络什么地方发生了故障

16.2.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[诊断中心/诊断中心]，如图所示：

图**错误!文档中没有指定样式的文字。**-114 诊断中心左侧导航

16.2.3 使用方法

进入[诊断中心]使用界面，打开[Tracert 诊断]，在“目的主机 IP 地址”中输入需要诊断的 IP 地址，点击后面的<Tracert>按钮，界面将显示诊断结果，如图所示：

图**错误!文档中没有指定样式的文字。**-115Tracert 诊断使用

17. 工艺异常检测

17.1 功能介绍

针对存在私有协议的工控现场，需要精准化控制业务，对偏离业务的微小行为都要进行识别和控制，可以使用本功能。工业防火墙支持对通用协议和用户私有协议进行周期、工艺序列、协议字段、序列号、协议长度字段、包长度进行检测，对于偏离规则的异常行为及时进行识别和控制。

17.2 规则配置

17.2.1 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[工艺异常检测/工艺异常检测]，如图所示：

图**错误!文档中没有指定样式的文字。**-116 工艺异常检测左侧导航

点击打开[工艺异常检测]页面后，如下图所示：

图 **错误!文档中没有指定样式的文字。**-117 工艺异常检测规则配置

17.2.2 添加规则

在[工艺异常检测]配置页面，点击左侧的<添加>按钮，将直接在列表增加一条默认规则，如图所示：

图 **错误!文档中没有指定样式的文字。**-118 工艺异常检测规则添加

表 **错误!文档中没有指定样式的文字。**-41 工艺异常检测各项说明

列名称	说明
源 IP	会话源 IP
目的 IP	会话目的 IP
源端口	会话源端口
目的端口	会话目的端口
通讯周期	检查会话报文的通讯周期是否合法。当报文间的时间间隔不符合配置参数值时，告警或阻断。 支持以下配置子项： 周期： 会话报文周期 容忍度：会话报文间隔容忍度

工艺序列对象	检查会话报文序列是否为预定义的合法工艺序列。 比如预定义合法功能码序列为 A->B->C，那么 A->C->B、B->C->A 的报文序列都是非法的。
协议字段	检查协议字段值是否合法。 支持以下配置子项： OFFSET：协议字段位置的起始 OFFSET 位置； 长度：协议字段长度（单位：BYTE） 端序：大小端 类型：协议字段类型（数字/字符串） 取值：协议字段合法值
序列号	检查会话序列号是否按预定值递增。 支持以下配置子项： OFFSET：序列号字段位置的起始 OFFSET 位置； 长度：序列号字段长度（单位：BYTE） 端序：大小端 递增步长：序列号递增步长 容错阈值：序列号容错阈值
报文长度匹配	检查会话序列号是否按预定值递增。 支持以下配置子项： OFFSET：报文长度字段位置的起始 OFFSET 位置； 长度：报文长度字段长度（单位：BYTE） 端序：大小端 差值：报文长度字段值与报文应用层长度值之间的差值（如果两者一致，则配置该差值为 0）
包大小取值范围	检查报文应用层长度是否合法。
协议类型	支持 any、SFP、RSSPI、RSSPI(互联互通版)四种配置。

	当配置为 SFP 时，则该协议建链动作会被识别出来，并产生建链告警信息； 当配置为 RSSPI（互联互通版）时，则该协议建链、时序校正动作都会被识别出来，并产生相应告警信息；
执行动作	支持告警拦截、告警不拦截两种配置。 防火墙设备的工艺序列检测，当配置为告警不拦截时，违反工艺异常检测的报文不会被阻断。

17.2.3 删除规则

点击[工艺异常检测]规则列表操作列下的<删除>按钮，可以把不再使用的检测规则进行删除。

注意：无法删除正在被设备使用的工艺异常检测规则。

17.2.4 修改规则

在[工艺异常检测]配置列表页面中，可直接修改对应规则的各个字段的取值，之后点击<保存>即可使修改生效。

17.2.5 应用规则

规则配置完成后，点击页面下方的<保存并应用>按钮，对应的规则将生效。

17.2.6 工艺序列

客户现场的一个业务操作对应的是一系列固定顺序的报文功能码，此时可定义这一系列固定顺序的功能码为指定的一种工艺序列，只有符合这种业务操作的行为才是正常的，否则视为异常。

17.2.7 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[对象配置/工艺序列]，如图所示：

图**错误!文档中没有指定样式的文字。**-119 工艺序列左侧导航

点击打开[工艺序列]页面后，如下图所示:

图 **错误!文档中没有指定样式的文字。**-120 工艺序列配置

17.2.8 添加工艺序列

在[工艺序列]配置页面，点击左侧的<添加>按钮，将直接在列表增加一条默认工艺序列，如图所示:

图 **错误!文档中没有指定样式的文字。**-121 工艺序列添加

表 **错误!文档中没有指定样式的文字。**-42 工艺序列各项说明

列名称	**说明**
名称	本工艺序列的名称，将在工艺异常检测规则中引用
OFFSET	指令序列功能码在报文中的起始偏移位置
长度	功能码字段的长度，单位：BYTE
指令序列	由指定的功能码顺序定义的合法工艺序列。 比如功能码有 A、B、C 三个，合法序列为 A->B->C
操作	<删除>，删除对应的工艺序列

17.2.9 配置序列

每个工艺序列支持自由配置，点击需要配置工艺序列的具体某个序列，即可打开对应的[指令序列编辑]配置界面，如下图所示：

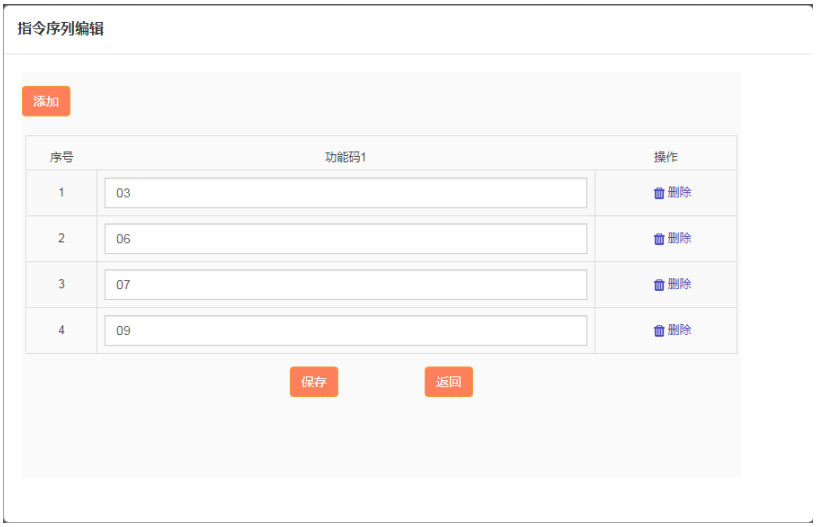


图 **错误!文档中没有指定样式的文字。**-122 工艺序列添加

17.2.10 添加序列

在[指令序列编辑]配置页面，点击左侧的<添加>按钮，将直接在列表增加一条默认的功能码，如图所示：

图 **错误!文档中没有指定样式的文字。**-123 序列添加功能码

17.2.11 删除序列

点击[指令序列编辑]序列列表操作列下的<删除>按钮，可以把不应出现在序列中的功能码进行删除。

注意：无法删除正在被设备使用的工艺序列中的具体序列。

17.2.12 修改序列

在[指令序列编辑]配置列表页面中，可直接修改对应序列的各个功能码的取值，之后点击<保存>即可使修改生效。

17.2.13 删除工艺序列

点击[工艺序列]规则列表操作列下的<删除>按钮，可以把不再使用的工艺序列进行删除。

注意：无法删除正在被设备使用的工艺序列。

17.2.14 修改工艺序列

在[工艺序列]配置列表页面中，可直接修改对应工艺序列的各个字段的取值，之后点击<保存>即可使修改生效。

17.2.15 应用工艺序列

工艺序列配置完成后，点击页面下方的<保存>按钮，对应的工艺序列将被保存。被保存后的工艺序列即可在 017.2 规则配置中使用。

18. 带宽管理

18.1 简介

工业防火墙具备带宽管理功能。基于监测对象，对通过自身的流量进行管理和控制。带宽管理是指带宽保障功能，使得在带宽出现拥堵时，能够保障重要终端的网络通信。

18.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[带宽管理/带宽管理]，点击菜单进入监测对象的配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-124 带宽管理左侧导航页面

在左侧导航栏找到[带宽管理/带宽管理]，点击菜单进入带宽管理的规则配置页面，如图所示：

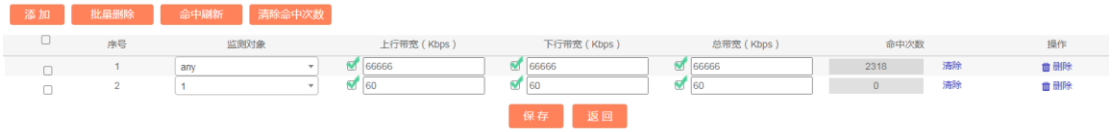


图 **错误!文档中没有指定样式的文字。**-125 带宽管理规则配置页面

18.3 监测对象

请参考 010.3 监测对象相关配置。

18.4 带宽管理

根据不同的监测对象进行个性化的带宽管理行为。

18.4.1 添加规则

在[带宽管理]配置页面，点击左侧的<添加>按钮，将直接在列表增加一条默认规则，如图所示：

图 **错误!文档中没有指定样式的文字。**-126 带宽管理规则添加

表 **错误!文档中没有指定样式的文字。**-43 带宽管理规则各列说明

项目名称	说明
监测对象	本条规则对应的要进行带宽管理的监测对象
上行带宽(Kbps)	最小上行带宽，当流量较大时，此监测对象的上行带宽的最小值
下行带宽(Kbps)	最小下行带宽，当流量较大时，此监测对象的下行带宽的最小值
总带宽(Kbps)	最小总带宽，当流量较大时，此监测对象的总带宽的最小值
命中次数	该条策略的命中统计
操作	<删除>，删除对应的规则

18.4.2 修改规则

在[带宽管理]配置列表页面中，可直接修改对应流带宽管理规则的各个字段的取值，之后点击<保存>即可使修改生效。

18.4.3 删除规则

点击某条带宽管理规则后面的<删除>按钮，可以删除对应的带宽管理规则。

点击表格第一列的复选框，选中多个流带宽管理规则，点击列表上方的<批量删除>按钮，则可批量删除带宽管理规则。

18.4.4 规则命中统计

在带宽管理查看页面可以查看到每条规则的命中情况，对于长时间未命中的策略，可以将其删除，以便节约宝贵的系统资源。但注意需要确定未命中的策略在业务现场确实没有需要。

19. 入侵防御

19.1 简介

工业防火墙具备入侵防御功能。入侵防御是一种安全机制，通过分析网络流量，检测入侵（包括缓冲区溢出攻击、木马、蠕虫等），并通过一定的响应方式，实时地中止入侵行为，保护企业工控系统和网络架构免受侵害。

19.2 页面导航

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统配置/入侵防御]，点击菜单进入监测对象的配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-127 入侵防御左侧导航页面

在左侧导航栏找到[系统配置/入侵防御]，点击菜单进入入侵防御的规则查看和配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-128 入侵防御规则查看和配置页面

19.3 入侵防御

根据不同的业务进行个性化的入侵防御配置。

19.3.1 查看和检索

打开[入侵防御]规则查看和配置页面，即可查看工业防火墙当前支持的入侵防御规则库。通过输入不同的检索条件，可检索指定的规则。

表 **错误!文档中没有指定样式的文字。**-44 入侵防御规则各列说明

项目名称	说明
名称	本条规则的名称
事件类型	入侵的事件类型，如缓冲区溢出攻击、木马、蠕虫等
事件等级	定义的本入侵的事件级别，有高、中、低
协议	本入侵的事件使用的工控协议
场景类型	行业业务类型，如工控、通用
描述	本条规则的具体描述信息
级别	本入侵事件的严重程度，包括一般、重要、严重
状态	本条规则的开启/关闭状态
日志	本入侵事件发生时是否记录日志
动作	本入侵事件发生时对报文的处理动作是拒绝/允许
操作	<配置>，配置对应的规则

19.3.2 配置规则

在[入侵防御]规则查看和配置页面中，可直接点击操作列下的<配置>按钮，配置对应入侵防御规则，打开的配置界面如下图所示：

图 **错误!文档中没有指定样式的文字。**-129 入侵防御规则配置页面

表 **错误!文档中没有指定样式的文字。**-45 入侵防御规则配置各列说明

项目名称	**说明**
名称	当前配置的规则名称
事件等级	本入侵事件的严重程度，包括一般、重要、严重
状态	启用或关闭本规则
日志	本入侵事件发生时是否记录日志
动作	本入侵事件发生时对报文的处理动作是拒绝/允许
操作	<保存>，对应的规则配置将保存并生效 <返回>，所做的修改将取消并返回到规则查看页面

19.3.3 升级规则库

点击[入侵防御]列表左侧的<升级>按钮，可升级规则库，打开的升级界面如下图所示：

图 **错误!文档中没有指定样式的文字。**-130 入侵防御规则升级页面

19.3.4 应用规则

入侵防御规则配置完成后，在需要应用的 ACL 规则添加或编辑页面，打开相应的功能即可使入侵防御生效，如下图所示：

图 **错误!文档中没有指定样式的文字。**-131 安全策略使能入侵防御页面

20. 系统配置

20.1 工作模式

20.1.1 简介

工业防火墙支持多种工作模式，支持测试模式，该模式下工业防火墙对禁止策略进行告警，但不拦截；支持工作模式，工业防火墙的正常工作模式，严格按照防护策略进行过滤等动作保护。

& 注意：

当启动智能学习时，设备工作在学习模式下，工作模式将不生效

20.1.2 工作模式配置

管理员 admin 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统配置/工作模式]，点击菜单进入配置页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-132 工作模式配置页面

表 **错误!文档中没有指定样式的文字。**-46 工作模式配置各项说明

项目名称	说明
工作模式	更改防火墙当前的工作模式
<保存>	保存工作模式的设置

20.2 系统维护

本模块主要包含系统配置的备份与恢复、恢复出厂设置、抓包管理、升级和远程维护几个功能。配置管理员可以定期对系统配置进行备份，并在需要的时候执行恢复操作。抓包管理可以方便快捷的对业务口进行抓包操作，方便查看各个接口的业务运行情况。升级功能可以实现对工业防火墙的一键升级，远程维护可开启关闭远程访问防火墙的能力。

20.2.1 页面导航

配置管理员登录工业防火墙后，点击[[系统配置/系统维护]，如图所示:

图 **错误!文档中没有指定样式的文字。**-133 系统维护导航

20.2.2 备份与恢复

点击[系统配置/系统维护]，进入到系统维护界面，默认第一个 TAB 页为备份与恢复，如图所示:

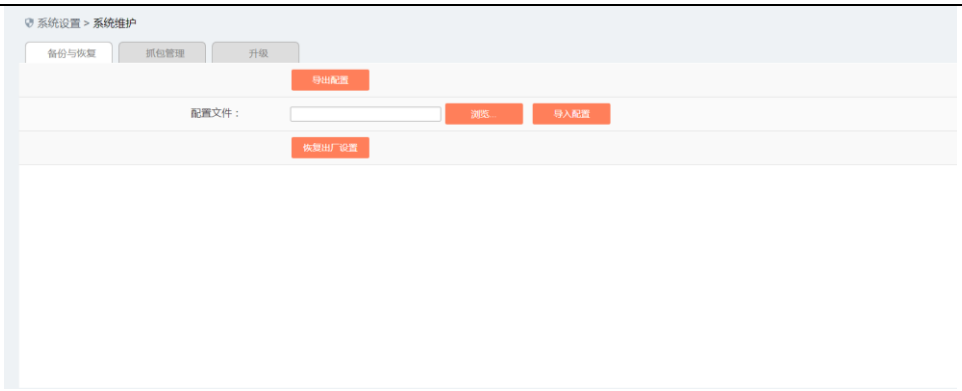


图 **错误!文档中没有指定样式的文字。**-134 系统维护备份与恢复页面

表 **错误!文档中没有指定样式的文字。**-47 系统维护备份与恢复各项说明

操作	**说明**
导出配置	点击<导出配置>则以 zip 压缩包的形式导出系统全部配置信息
配置文件	显示要导入的配置文件名称
浏览	点击浏览按钮则弹出本地磁盘，选择要导入的配置文件 zip 压缩包
导入配置	要求导入的必须为 zip 文件，导入成功后系统配置信息自动下发
恢复出厂设置	点击<恢复出厂设置>按钮，系统数据会清空，恢复默认访问 IP

20.2.3 抓包管理

点击[系统配置/系统维护]，进入到系统维护界面，切换到抓包管理 TAB 页，如图所示：

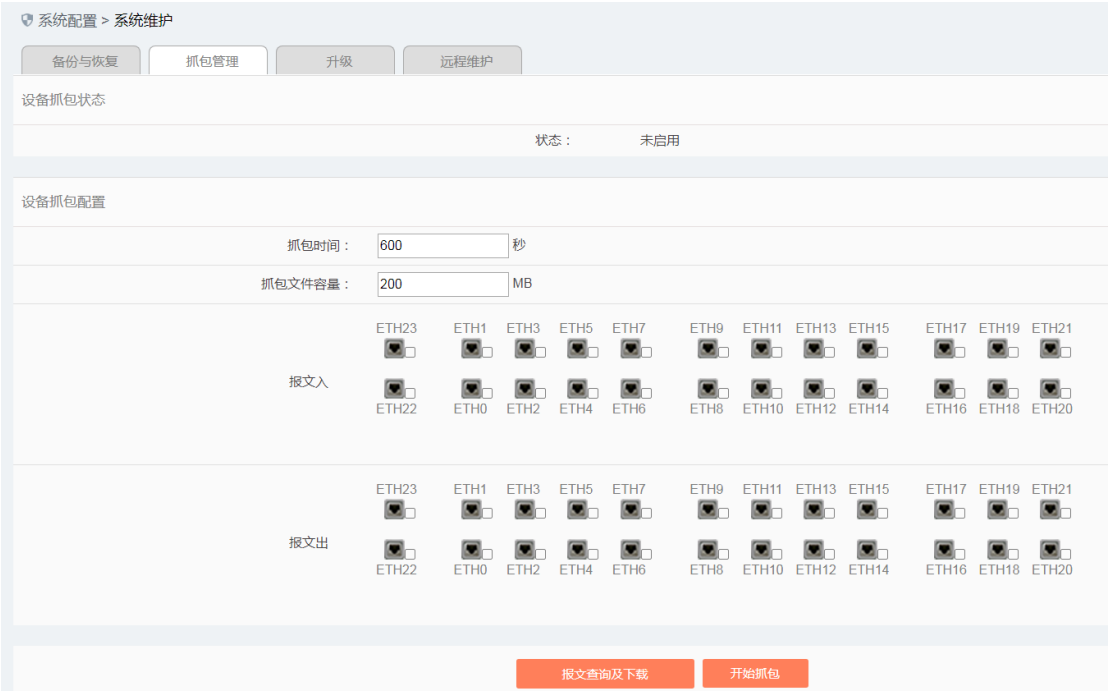


图 **错误!文档中没有指定样式的文字。**-135 抓包管理配置页面

表 **错误!文档中没有指定样式的文字。**-48 抓包管理各项说明

操作	**说明**
状态	开启抓包后，状态显示为抓包中；停止抓包，状态显示为抓包结束
抓包时间	抓包时间配置范围 1-600 秒，默认 600 秒，满足时间条件抓包自动停止
抓包文件容量	抓包容量配置范围 1-2048MB，默认 200MB，满足容量条件抓包自动停止
报文入接口	ETH0-ETH23 接口，接口状态为 UP 状态则是绿色标识，可以勾选并开启抓包，若是 DOWN 状态则是灰色标识，不可编辑
报文出接口	ETH0-ETH23 接口，接口状态为 UP 状态则是绿色标识，可以勾选并开启抓包，若是 DOWN 状态则是灰色标识，不可编辑

配置参数填写完整后，点击<开始抓包>状态显示为抓包中，按钮名称显示为<停止抓包>，点击<停止抓包>按钮则手动停止抓包，状态变更为抓包结束。

点击<报文查询及下载>进入查询及下载界面，如图所示：

图 **错误!文档中没有指定样式的文字。**-136 报文查询及下载页面

表 **错误!文档中没有指定样式的文字。**-49 报文查询及下载各项说明

项目名称	**说明**	
报文名称	报文名称以防护墙编号+接口名+in/out+时间戳命名，根据名称可以清晰的分辨出接口对应的抓包文件	
操作	下载	点击<下载>按钮则可以下载 pcap 文件进行查看
操作	删除	点击<删除>按钮则提示删除成功，文件被清除

20.2.4 升级

点击[系统配置/系统维护]，进入到系统维护界面，切换到升级 TAB 页，如图所示：

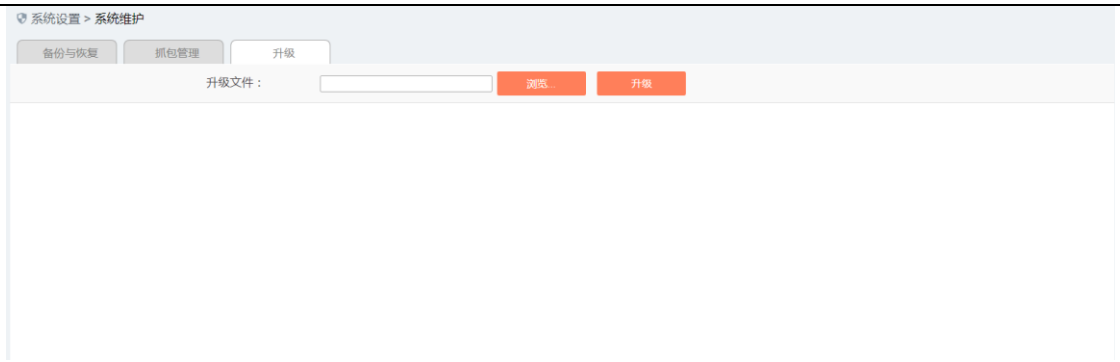


图 **错误!文档中没有指定样式的文字。**-137 升级页面

表 **错误!文档中没有指定样式的文字。**-50 升级各项说明

项目名称	**说明**	
升级文件	显示要升级的文件名称	
操作	浏览	点击<浏览>则打开本地磁盘，可以选择要升级的文件
操作	升级	点击<升级>按钮则进入升级操作

20.2.5 远程维护

点击[系统配置/系统维护]，进入到系统维护界面，切换到[远程维护]TAB 页，如图所示：

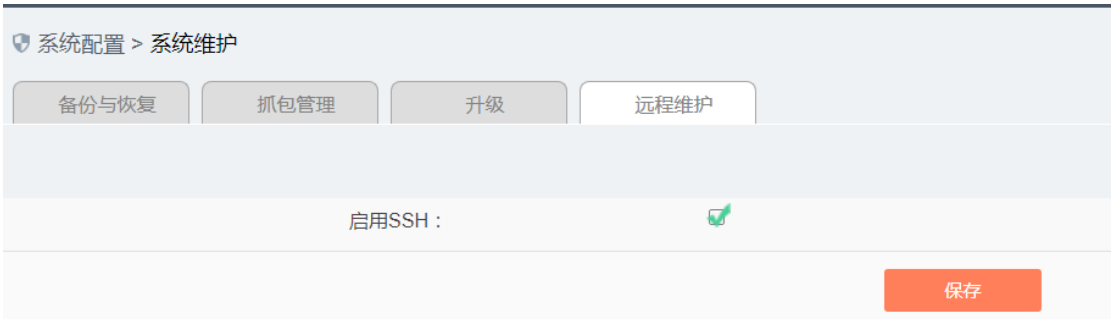


图 **错误!文档中没有指定样式的文字。**-138 远程维护页面

可远程开启/关闭 设备的 SSH 服务。

20.3 日期时间配置

20.3.1 页面导航

配置管理员登录工业防火墙后，点击[系统配置/日期时间配置]，如图所示：

图 **错误!文档中没有指定样式的文字。**-139 日期时间配置导航

20.3.2 日期时间配置

NTP 为时间同步服务器，系统默认为关闭状态。点选开启选项，输入正确的服务器 IP 地址，点击<保存>按钮，提示保存成功，则 NTP 服务器配置成功。

20.4 存储周期配置

20.4.1 页面导航

配置管理员登录工业防火墙后，点击[[系统配置/存储周期配置]，如图所示：

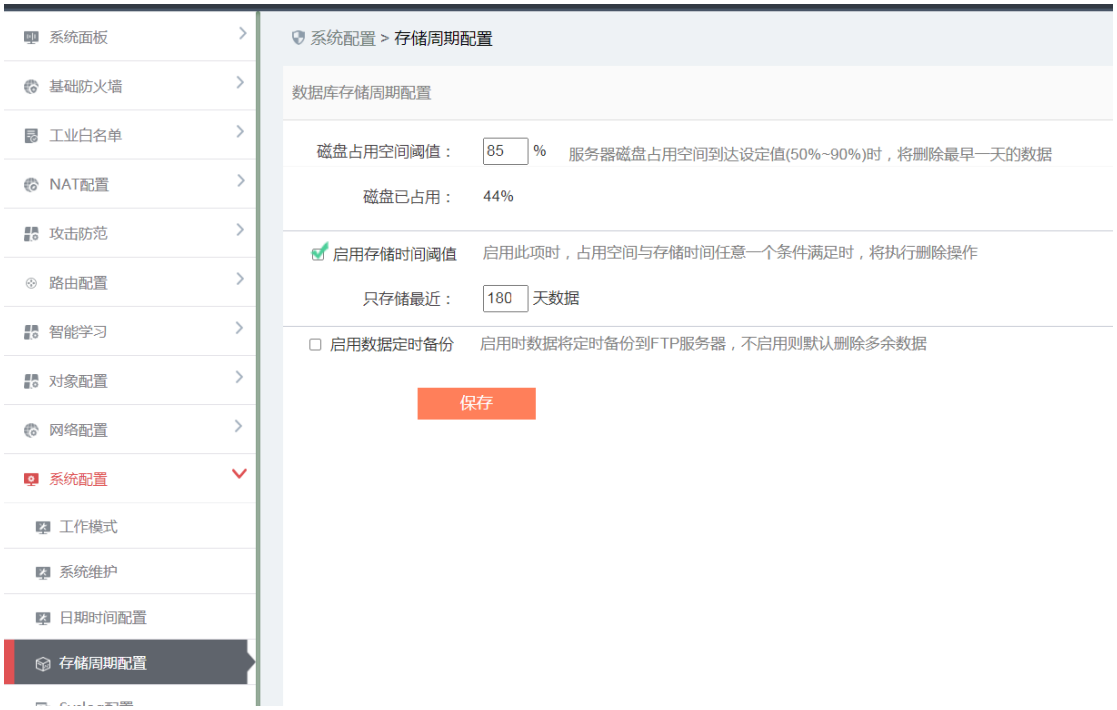


图 **错误!文档中没有指定样式的文字。**-140 存储周期配置导航

20.4.2 配置存储周期

点击[系统配置/存储周期配置]按钮，可以进入配置页面。如图所示：

图 **错误!文档中没有指定样式的文字。**-141 配置页面

服务器磁盘占用空间阈值和服务器存储时间阈值都有默认值，并且是开启状态。磁盘空间默认阈值为 85%，服务器磁盘占用空间到达设定值(50%-90%)时，将删除最早一天的数据，存储时间阈值为 30 天，占用空间与存储时间任意一个条件满足时，将执行删除操作。

启用数据定时备份默认为不开启，启用时数据将定时备份到 FTP 服务器，不启用则默认删除多余数据,勾选启用则进入配置页面。如图所示：

图 **错误!文档中没有指定样式的文字。**-142 配置页面

输入正确的服务器地址，默认为匿名用户登录，点击<测试连接>按钮，弹出校验连接提示框。如图所示：

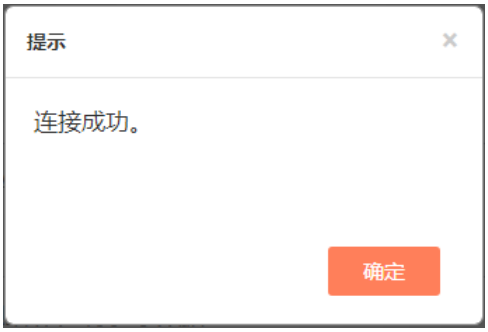


图 **错误!文档中没有指定样式的文字。**-143 连接确认页面

不勾选使用匿名用户选项，则弹出 ftp 用户认证界面（如图所示），输入 ftp 服务器用户名、密码、确认密码，点击<测试连接>按钮，验证服务器是否连通，点击<保存>按钮，存储周期配置成功。如图所示：

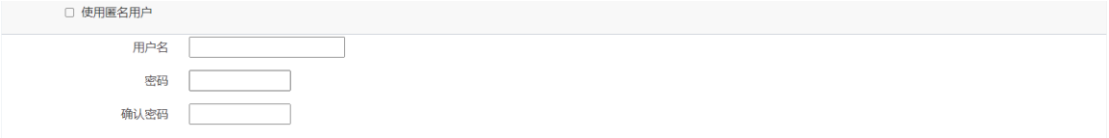


图 **错误!文档中没有指定样式的文字。**-144ftp 服务器认证页面

20.5 Syslog 配置

配置 SysLog 服务器 IP 地址与端口，发送防火墙设备产生的告警、日志及状态信息到 SysLog 服务器。

20.5.1 页面导航

配置管理员登录工业防火墙后，点击[系统配置/Syslog 配置]，如图所示：

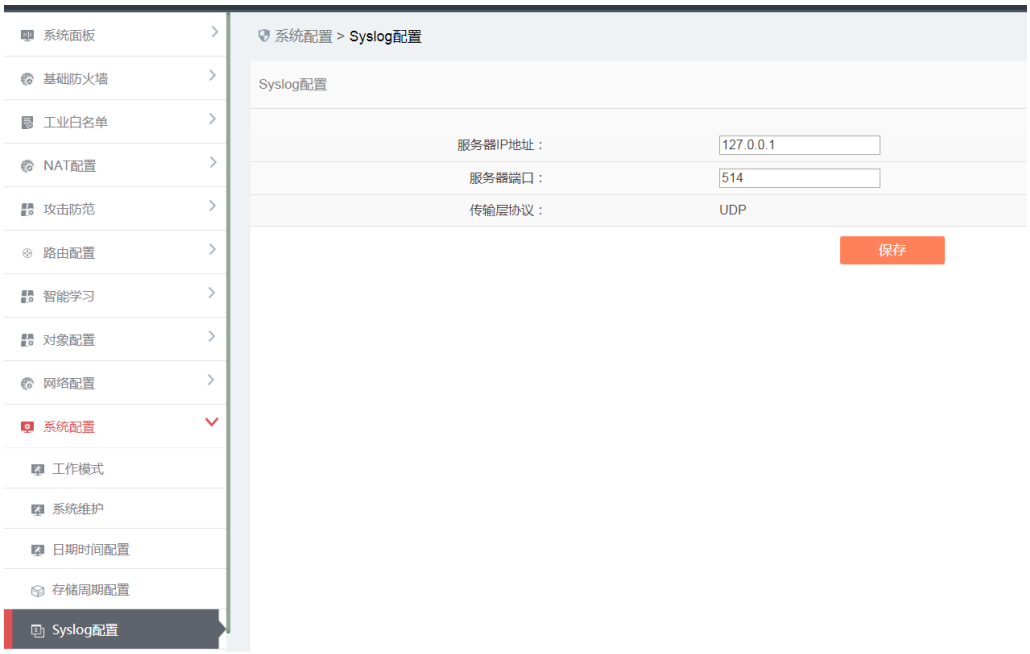


图 **错误!文档中没有指定样式的文字。**-145Syslog 配置导航

20.5.2 Syslog 配置

点击[系统配置/Syslog 配置]按钮，可以进入配置页面如图所示：

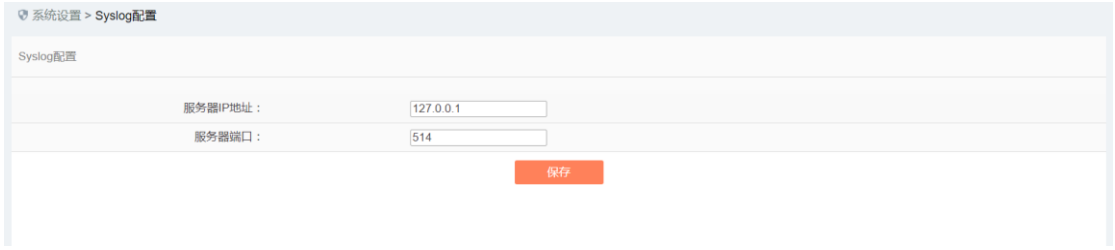


图 **错误!文档中没有指定样式的文字。**-146 Syslog 配置页面

配置页面可以设置服务器 ip 地址和端口，默认 ip 为 127.0.0.1，端口默认为 514。服务器 ip 地址和服务器端口输入框可编辑，输入新的 ip 地址和端口，点击<保存>按钮，即可保存成功。

表 **错误!文档中没有指定样式的文字。**-51syslog 配置操作各项说明

项目名称	说明
服务器 IP 地址	Syslog 服务器的 IP 地址，支持 IPv4，IPv4 时用点分十进制表示，最多同时可配置 1 个地址
服务器端口	发送 Syslog 使用的端口号，范围 1-65535

20.6 授权管理

20.6.1 简介

License 即许可证，是设备供应商对产品特性的使用范围、期限等进行授权的一种合约形式，License 可以动态控制产品的某些特性是否可用。当需要时，用户可以通过购买 License 激活产品的某些特性和

功能特性。对于本产品，每个工业防火墙设备中只能存在一个处于激活状态的 License 文件，激活新的 License 将会使旧的 License 失效。

目前设备支持以下方法激活 License：

- 手动激活

当购买或续购 License，获得 License 授权证书后，通过登录指定页面，对所管理的设备进行授权和授权的更新。

20.6.2 查看授权

点击[系统配置/授权管理]页面，将弹出具体的授权信息页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-147 授权详情查看页

此页面显示当前工业防火墙的授权详情。

- 下载文件

得到工业防火墙的授权文件，可以将此文件发给生产商，用来后续更新授权信息

- 更新授权

更新当前工业防火墙的授权信息

20.6.3 获取授权文件

在打开的工业防火墙授权详情页上，点击<下载文件>按钮，可以将授权文件下载下来。

20.6.4 更新防火墙授权信息

在打开的工业防火墙授权详情页上，点击<更新授权>按钮，将弹出授权文件选择对话框，以把用户从厂商获取到的最新的授权文件更新到指定的工业防火墙中，(如图所示)

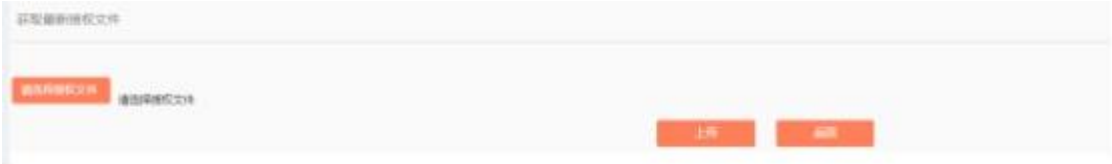


图 **错误!文档中没有指定样式的文字。**-148 选择要更新到工业防火墙的新授权文件

- 请选择授权文件

点击请选择授权文件后，将弹出文件选择对话框。

找到新的授权文件后(如：以设备 ID 为名字，后缀为“.dat”的文件)，双击文件或选择<打开>，之

后再点击<上传>按钮，浏览器将此文件首先上传到工业防火墙所在的服务器，然后通知给工业防火墙，工业防火墙将执行更新授权动作，更新成功，用户将可以在查看页面看到新的授权信息。

➢ 返回

点击<返回>将不执行任何操作，直接返回到工业防火墙授权详情页。

20.7 可信主机管理

访问工业防火墙的主机是有限制的。在初始情况下，任意一台机器只要可以连接到工业防火墙都可以访问工业防火墙。如果一旦配置了可信主机，那么将只有被加入可信主机的机器才可以访问工业防火墙。

20.7.1 页面导航

配置管理员登录工业防火墙后，点击[[系统配置/可信主机管理]，即可进入可信主机配置页面，如图所示：

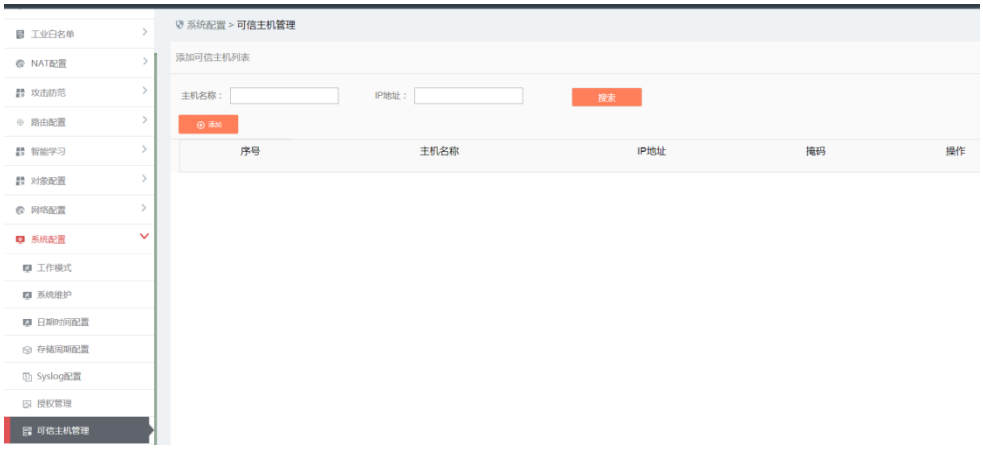


图 **错误!文档中没有指定样式的文字。**-149 可信主机导航

20.7.2 添加可信主机

点击 [系统配置/可信主机管理]可信主机列表标签左侧的<添加>按钮，将弹出可信主机添加页面，如图所示：

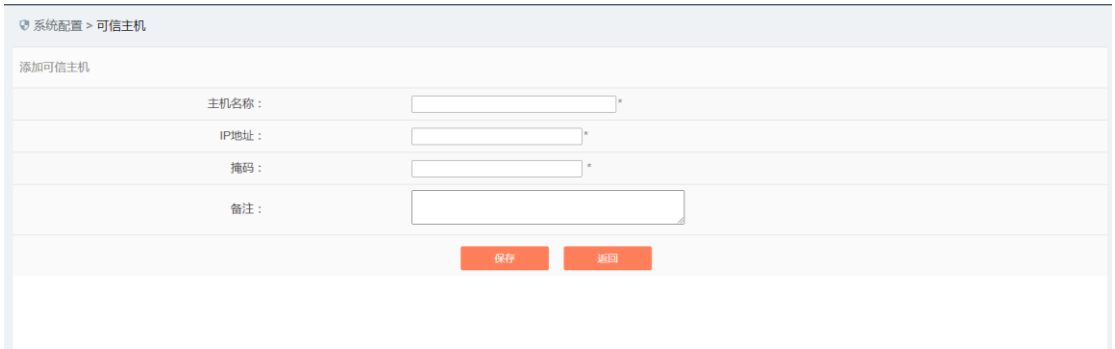


图 **错误!文档中没有指定样式的文字。**-150 可信主机添加页

表 **错误!文档中没有指定样式的文字。**-52 可信主机添加各项说明

项目名称	说明
主机名称	给可信主机定义一个容易理解、记忆且有含义的名字
IP 地址	可信主机分配到的 IP 地址，十进制格式

掩码	可配置主机对应的掩码，掩码范围 1-32	
备注	可选填，附加说明信息	
操作	保存	所有的修改信息将被保存到数据库并生效，同时返回到可信主机列表显示页面
	返回	忽略所有的修改，返回到可信主机列表显示页面

20.7.3 查看可信主机

点击[可信主机]可信主机列表中操作列下的<查看>按钮，将打开可信主机的信息展示界面，主要展示可信主机的名称、ip 地址、掩码、备注信息，如图所示:

图 **错误!文档中没有指定样式的文字。**-151 可信主机查看页

在可信主机查看页，点击<返回>按钮，则返回到可信主机列表页面。

20.7.4 修改可信主机

点击[可信主机]可信主机列表中操作列下的<修改>按钮，将打开[可信主机基本信息]修改页面，可以修改可信主机的基本信息，如图所示:

图 **错误!文档中没有指定样式的文字。**-152 可信主机基本信息修改页

20.7.5 删除可信主机信息

点击[可信主机]可信主机列表中操作列下的<删除>按钮，将弹出删除确认提示框，如图所示:

图 **错误!文档中没有指定样式的文字。**-153 可信主机删除确认页

点击<确认>按钮，则该条可信主机信息从可信主机列表中被删除。

20.8 实时消息配置

20.8.1 页面导航

配置管理员登录工业防火墙后，点击[系统配置/实时消息配置]，如图所示：

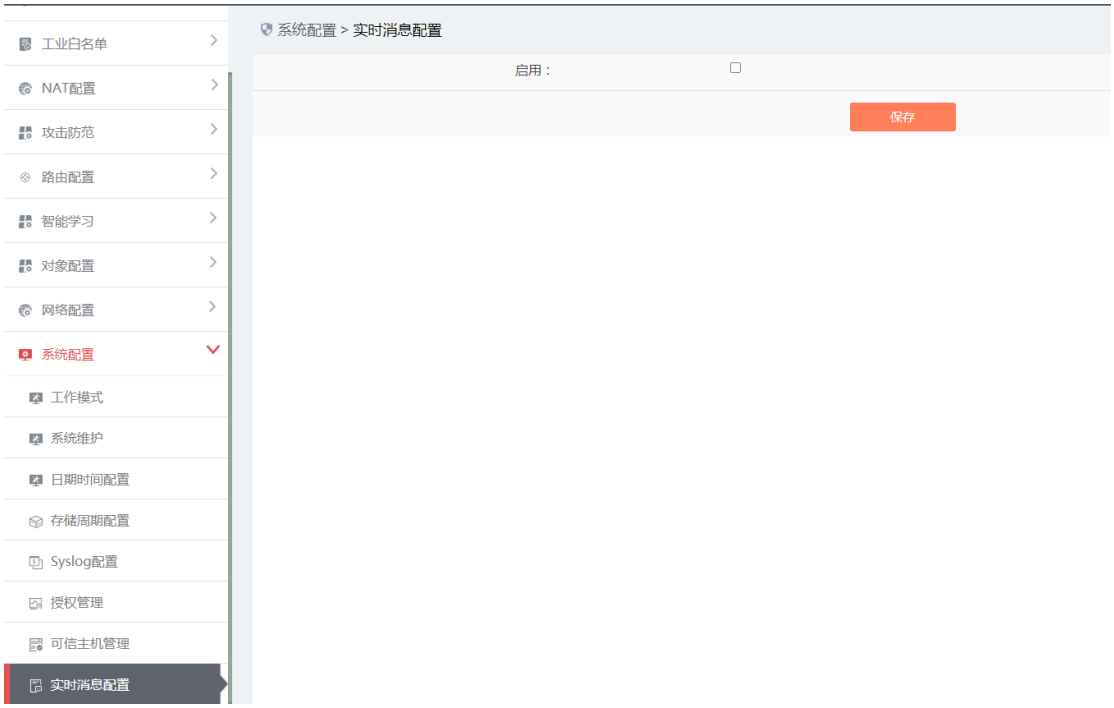


图 **错误!文档中没有指定样式的文字。**-154 实时消息配置导航

20.8.2 实时消息配置

配置页面默认为开启消息提示框，整个工业防火墙页面底部显示消息提示信息。取消勾选启用，并点击<保存>按钮，提示保存成功。如图所示：

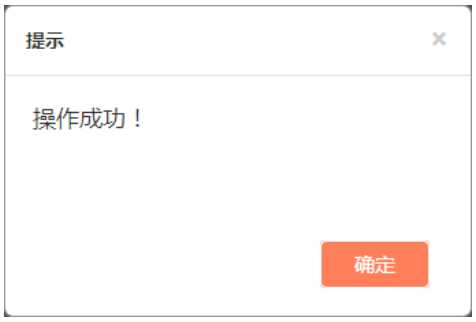


图 **错误!文档中没有指定样式的文字。**-155 操作成功确认页面

配置成功后，在页面底部实时推送的告警和配置信息将消失。

20.9 证书管理

20.9.1 页面导航

配置管理员登录工业防火墙后，点击[系统配置/证书管理]，如图所示：

图 **错误!文档中没有指定样式的文字。**-156 证书管理配置导航

20.9.2 证书管理

打开[证书管理]页面，页面显示出当前已生成的证书。

点击左侧上方的<生成证书>按钮，将打开生成证书页面，如下图所示：

图 **错误!文档中没有指定样式的文字。**-157 生成证书页面

表 **错误!文档中没有指定样式的文字。**-53 生成证书各列说明

项目名称	说明
名称	证书的名称
颁发给	证书要颁发给的机构名称
有效期(天)	证书的有效期，范围：1-9999
服务器IP	证书使用的服务器的IP地址
客户端证书数量	可以连接的客户端的数量

密码	证书使用的密码
确认密码	密码确认
操作	<保存>，将生成证书并保存 <返回>，不生成证书并返回到证书查看页面，

证书生成后，即可在 VPN 的“点到多点”的场景中使用。VPN 的配置请参考 13VPN

21. 其它配置

21.1 修改密码

密码管理页面可以修改当前用户的使用密码。

配置管理员登录工业防火墙后，点击页面右上角的<修改密码>按钮，将弹出[密码管理]页面，用户可以修改当前用户密码，如图所示:

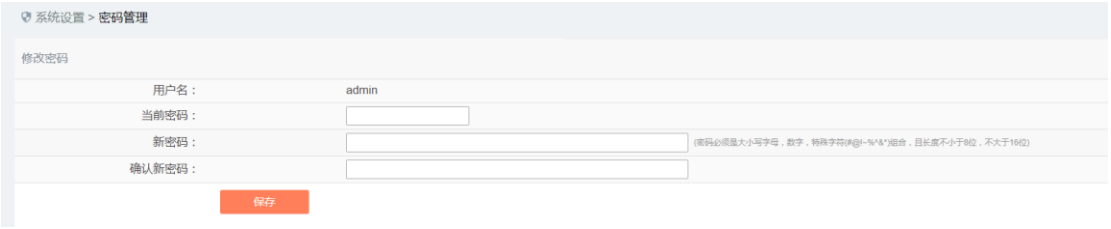


图 **错误!文档中没有指定样式的文字。**-158 密码管理页面

表 **错误!文档中没有指定样式的文字。**-54 修改密码各项说明

项目名称	**说明**	
当前密码	当前用户密码	
新密码	密码必须是大小写字母，数字，特殊字符(#@!~%^&*)组合，且长度不小于8个字符，不大于16个字符	
确认新密码	与新密码必须相同	
操作	保存	保存修改密码操作

21.2 重启

用户可随时重启工业防火墙。

配置管理员登录工业防火墙后，点击页面右上角的<重启>按钮，将弹出确认页面，用户可以重启防火墙，如图所示:

图 **错误!文档中没有指定样式的文字。**-159 重启按钮

22. 审计管理员

22.1 实时会话

会话表是设备转发报文的关键表项。所以当出现业务故障时，通常可以通过 Web 查看会话表信息，大致定位发生故障的模块或阶段。

22.1.1 会话表查询

审计管理员登录工业防火墙后，点击[实时会话/会话表查询]，将打开会话表查询页面，用户可以查看当前的实时会话信息，如图所示：

图 **错误!文档中没有指定样式的文字。**-160 会话表查询导航

图 **错误!文档中没有指定样式的文字。**-161 会话表查询结果页面

22.2 事件日志

22.2.1 白名单告警

白名单告警是流经防火墙的报文违反了防火墙上的白名单规则产生的，只有防火墙处于告警模式或

防护模式时才有可能产生此日志。

22.2.1.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/白名单告警]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-162 白名单告警日志

此处可以查看到白名单告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-55 白名单告警各项说明

项目名称	**说明**	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
源端口	发起数据请求的机器所使用的端口	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的端口	请求的目标机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
应用层协议	具体的应用类型	
告警信息	告警的描述信息	
是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别，级别说明请参考相应说明	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选右侧上部的<显示已处理日志>，将可以查看到已经被处理过的日志。如图所示：

图 **错误!文档中没有指定样式的文字。**-163 显示已处理的白名单告警日志列表页

22.2.1.2 处理日志

点击[白名单告警]显示列表中操作列下的<处理>按钮，将显示如下图所示[白名单告警日志信息]的处理页面。如图所示：

图 **错误!文档中没有指定样式的文字。**-164 白名单告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[白名单告警日志]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

对于有些白名单告警，此处可将告警直接转换为规则，只需要点击<添加到策略>即可将此条告警加入到对应协议的白名单规则中，后续将不再告警。

22.2.1.3 清空日志

工业防火墙支持对日志的批量删除功能。

用户可以批量删除无用的日志。在[白名单告警]的列表页面中，点击下方的<清空>按钮，即可完成对应日志的批量删除。如图所示：

图 **错误!文档中没有指定样式的文字。**-165 白名单告警的清空

22.2.1.4 删除日志

用户可以选择删除选中的日志。在[白名单告警]的列表页面中，点击某行日志前面的复选框选中日志，也可以点击表格头部的复选框，选中该页面所有日志，如图所示，点击<删除选中>按钮，即可完成对选中日志的删除。

图 **错误!文档中没有指定样式的文字。**-166 白名单告警的删除

22.2.1.5 导出日志

用户可以导出白名单告警日志。在[白名单告警]的列表页面中，，点击<导出日志>按钮，参考上图，即可导出日志，导出完成后，在[日志管理/日志导出下载]页面可下载该导出日志。

22.2.1.6 检索日志

在[白名单告警]的列表页面中，可以根据条件对日志进行检索。如图所示：

图 **错误!文档中没有指定样式的文字。**-167 检索白名单告警日志

22.2.2 ACL 告警

ACL 告警日志是流经防火墙的报文违反了防火墙上的 ACL 策略规则产生的，只有防火墙处于告警模式或防护模式时，报文违反了安全策略规则，才产生此类型的告警。

22.2.2.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/ACL 告警]，点击菜单进入页面，如图所示：

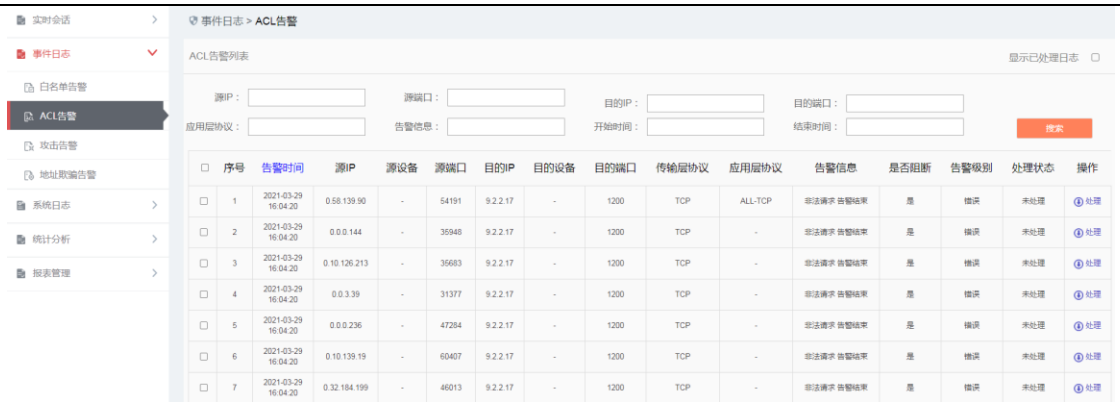


图 **错误!文档中没有指定样式的文字。**-168 防火墙告警日志列表

此处可以查看到 ACL 告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-56ACL 告警各项说明

项目名称	说明	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
源设备	无设备名称时显示为“-”，否则显示源设备的名称	
源端口	请求的目标机器所使用的源端口	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的设备	无设备名称时显示为“-”，否则显示目的设备的名称	
目的端口	请求的目标机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
应用层协议	具体的应用类型	
告警信息	告警的描述信息	
是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选列表右上方的<显示已处理日志>，将可以查看到已经被处理过的日志。如图所示：

图 **错误!文档中没有指定样式的文字。**-169 显示已处理的防火墙告警日志列表页

22.2.2.2 处理日志

点击[ACL 告警]显示列表中操作列下的<处理>按钮，将显示如下图所示[ACL 告警日志信息]的处理页面。

图 **错误!文档中没有指定样式的文字。**-170 防火墙告警处理页

点击处理状态的下拉框，选择“关闭”，并在处理意见中填写相关的意见后点击保存，即可完成对告警信息的处理，此时在[ACL 告警]页的列表中默认将不再看到此条日志。

也可以不选择“关闭”，只填写处理意见。

此处可将告警直接转换为规则，只需要点击<添加到策略>即可将此条告警加入到 ACL 策略中，后续将不再告警。

22.2.2.3 清空日志

工业防火墙支持对日志的批量删除功能。

用户可以选择清空日志。在[ACL 告警]的列表页面中，点击下方的<清空>按钮，即可完成对应日志的清空。如图所示：

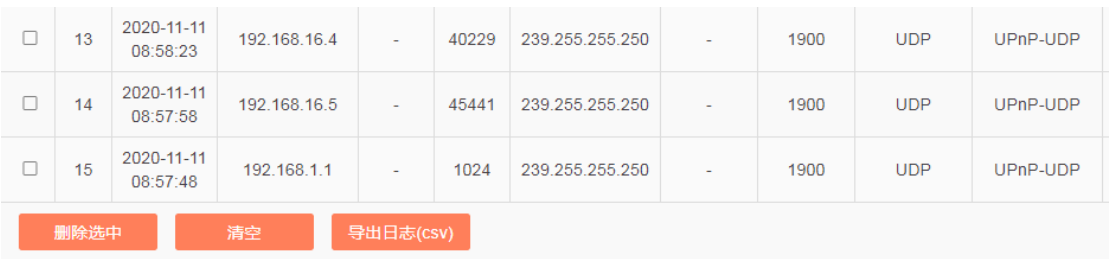


图 **错误!文档中没有指定样式的文字。**-171ACL 告警的清空

22.2.2.4 删除日志

用户可以选择删除选中的日志。在[ACL 告警]的列表页面中，点击某行日志前面的复选框选中日志，也可以点击表格头部的复选框，选中该页面所有日志，如图所示，点击<删除选中>按钮，即可完成对选中日志的删除。

图 **错误!文档中没有指定样式的文字。**-172ACL 告警的删除

22.2.2.5 导出日志

用户可以导出 ACL 告警日志。在[ACL 告警日志]的列表页面中,，点击<导出日志>按钮，即可导出日志，导出完成后，在[日志管理/日志导出下载]页面可下载该导出日志，可参考 0 节说明。

22.2.2.6 检索日志

在[ACL 告警]的列表页面中，可以根据条件对日志进行检索。如图所示：

图 **错误!文档中没有指定样式的文字。**-173 检索防火墙告警日志

22.2.3 攻击告警日志

22.2.3.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/攻击告警]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-174 攻击告警日志列表页

此处可以查看到攻击告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-57 攻击告警各项说明

项目名称	说明
目的 IP	攻击的目的 IP 地址，点分十进制格式
源 IP	攻击的源 IP 地址，点分十进制格式
是否丢包	对报文的处理动作是放行还是阻断

攻击信息	具体的攻击内容	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选攻击告警日志列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。如图所示：

图 **错误!文档中没有指定样式的文字。**-175 显示已处理的攻击告警日志列表页

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.2.4 地址欺骗日志

地址欺骗日志是流经防火墙的报文违反了防火墙上的 IP/MAC 规则产生的，只有防火墙处于告警模式或防护模式时才有可能产生此日志。

22.2.4.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/地址欺骗告警]，点击菜单进入页面，如图所示：

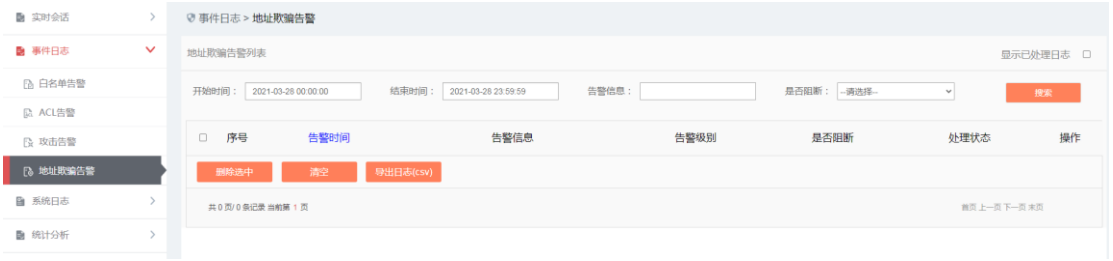


图 **错误!文档中没有指定样式的文字。**-176 地址欺骗日志列表页

此处可以查看到地址欺骗所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-58 地址欺骗告警各项说明

项目名称	说明
告警信息	告警的描述信息

是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选地址欺骗日志列表标签右侧的<显示已处理日志>，将可以查看到已经被处理过的日志。如图所示：

图 **错误!文档中没有指定样式的文字。**-177 显示已处理的地址欺骗日志列表页

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.2.5 入侵防御告警

入侵防御告警是流经防火墙的报文命中了入侵防御规则产生的，只有防火墙处于告警模式或防护模式时才有可能产生此日志。

22.2.5.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/入侵防御告警]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-178 入侵防御告警日志

此处可以查看到入侵防御告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-59 入侵防御告警各项说明

项目名称	说明	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
源端口	发起数据请求的机器所使用的端口	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的端口	请求的目标机器所使用的端口	
传输层协议	报文使用的传输层的协议类型	
告警类型	此条对应的告警具体大类型，如：暴力猜解、信息泄露、代码执行等	
告警信息	告警的描述信息	
是否阻断	对报文的处理动作是放行还是阻断	
告警级别	告警可能造成的损害级别，级别说明请参考相应说明	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选右侧上部的<显示已处理日志>，将可以查看到已经被处理过的日志。

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.2.6 流量阈值告警

当监测对象的流量超过了配置的阈值时，将产生流量阈值告警。

22.2.6.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/流量阈值告警]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-179 流量阈值告警日志

此处可以查看到流量阈值告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-60 流量阈值告警各项说明

项目名称	说明	
告警信息	告警的描述信息	
告警级别	告警可能造成的损害级别，级别说明请参考相应说明	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选右侧上部的<显示已处理日志>，将可以查看到已经被处理过的日志。

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.2.7 工艺异常告警

工艺异常告警是流经防火墙的报文违反了工艺异常检测规则产生的，只有防火墙处于告警模式或防护模式时才有可能产生此日志。

22.2.7.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/工艺异常告警]，点击菜单进入页面，如图所示：

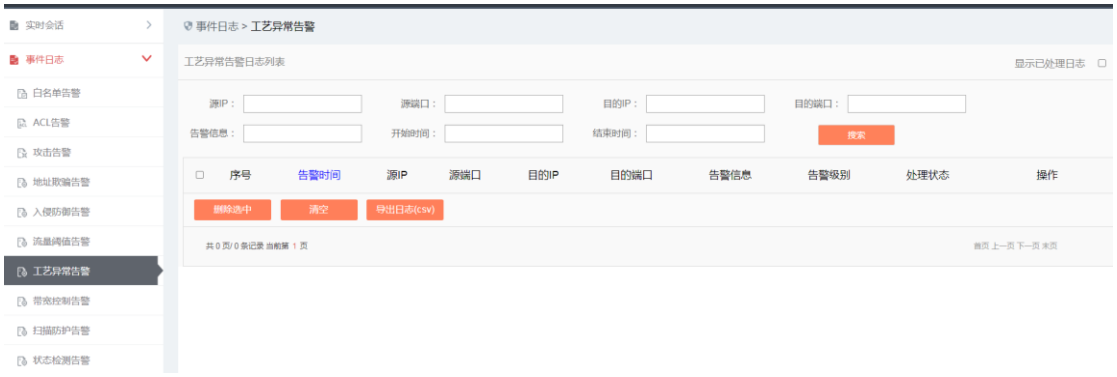


图 **错误!文档中没有指定样式的文字。**-180 工艺异常告警日志

此处可以查看到工艺异常告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-61 工艺异常告警各项说明

项目名称	说明
源 IP	发起数据请求的 IP 地址，点分十进制格式
源端口	发起数据请求的机器所使用的端口

目的 IP	请求数据的目的 IP 地址，点分十进制格式	
目的端口	请求的目标机器所使用的端口	
告警信息	告警的描述信息	
告警级别	告警可能造成的损害级别，级别说明请参考相应说明	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选右侧上部的<显示已处理日志>，将可以查看到已经被处理过的日志。

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.2.8 带宽管理告警

带宽管理告警是流经防火墙的报文违反了带宽管理规则产生的，只有防火墙处于告警模式或防护模式时才有可能产生此日志。

22.2.8.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/带宽管理告警]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-181 带宽管理告警日志

此处可以查看到带宽管理告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-62 带宽管理告警各项说明

项目名称	说明	
告警信息	告警的描述信息	
上行丢包数量	超出带宽导致的上行丢包数量统计	
下行丢包数量	超出带宽导致的下行丢包数量统计	
上行丢失字节数	超出带宽导致的上行丢失字节数统计	
下行丢失字节数	超出带宽导致的下行丢失字节数统计	
告警级别	告警可能造成的损害级别，级别说明请参考相应说明	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选右侧上部的<显示已处理日志>，将可以查看到已经被处理过的日志。

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.2.9 扫描防护告警

扫描防护告警是流经防火墙的报文命中了扫描防护规则产生的，只有防火墙处于告警模式或防护模式时才有可能产生此日志。

22.2.9.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[事件日志/扫描防护告警]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-182 扫描防护告警日志

此处可以查看到扫描防护告警所有日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-63 扫描防护告警各项说明

项目名称	说明	
源 IP	发起数据请求的 IP 地址，点分十进制格式	
目的 IP	请求数据的目的 IP 地址，点分十进制格式	
是否丢包	是否将报文进行了丢弃	
告警信息	告警的描述信息	
处理状态	是否已经查看和处理了告警	
告警时间	发生告警的时间	
操作	处理	对告警信息做进一步处理

除可以显示所有未处理的告警外，用户还可以查看已经处理过的历史告警。

勾选右侧上部的<显示已处理日志>，将可以查看到已经被处理过的日志。

处理日志：请参考其它日志处理方式。

清空日志：请参考其它日志处理方式。

删除日志：请参考其它日志处理方式。

导出日志：请参考其它日志处理方式。

检索日志：请参考其它日志处理方式。

22.3 系统日志

22.3.1 系统运行日志

系统运行日志是记录系统运行状态的日志。

22.3.1.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统日志/系统运行日志]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-183 系统运行日志列表页

此处可以查看到所有系统运行日志的信息，含义如下：

表 **错误!文档中没有指定样式的文字。**-64 系统运行日志各项说明

项目名称	说明
功能类型	哪个组件的日志，主要有平台和设备
日志的类型	主要包括上下线、bypass 切换等
操作时间	日志产生时的时间

22.3.1.2 导出日志

用户可以选择导出日志。在[系统运行日志]的列表页面中，点击下方的<导出日志>按钮，即可完成对应日志的导出。如图所示：

图 **错误!文档中没有指定样式的文字。**-184 系统运行日志的导出

22.3.1.3 检索日志

在[系统运行日志]的列表页面中，可以根据条件对日志进行检索。如图所示：

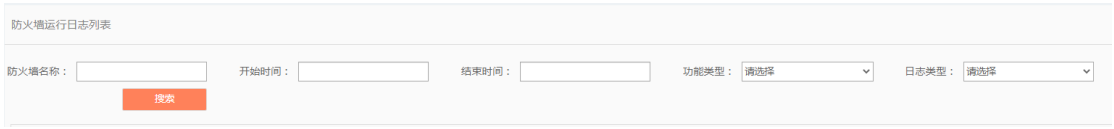


图 **错误!文档中没有指定样式的文字。**-185 检索系统运行日志

22.3.2 系统操作日志

22.3.2.1 简介

系统操作日志主要记录当前系统的所有用户的行为日志，可以导出相关日志，筛选特定日志，方便后期进行审计工作。

22.3.2.2 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统日志/系统操作日志]，点击菜单进入页面，如图所示：

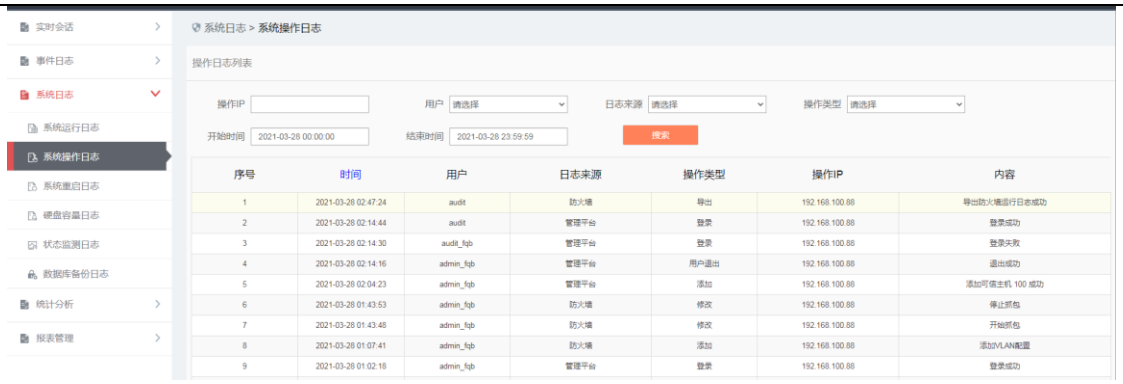


图 **错误!文档中没有指定样式的文字。**-186 系统操作日志列表页

表 **错误!文档中没有指定样式的文字。**-65 系统操作日志各项说明

项目名称	说明
用户	操作的用户
日志来源	业务程序/web 管理程序
操作类型	具体的操作类型，如登录、增加
操作 IP	操作的 IP 地址
内容	操作的具体内容描述
时间	日志产生时的时间

22.3.2.3 检索日志

请参考其它日志处理方式。

22.3.3 系统重启日志

22.3.3.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统日志/系统重启日志]，点击菜单进入页面，如图所示：

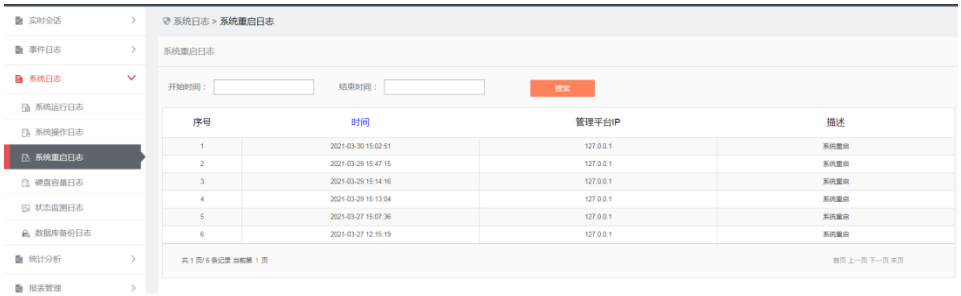


图 **错误!文档中没有指定样式的文字。**-187 系统重启日志列表页

表 **错误!文档中没有指定样式的文字。**-66 系统重启日志各项说明

项目名称	说明
描述	系统重启
时间	日志产生时的时间

22.3.3.2 检索日志

请参考其它日志处理方式。

22.3.4 硬盘容量日志

硬盘的容量达到设定的阈值时将进行日志记录。

22.3.4.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统日志/硬盘容量日志]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-188 硬盘容量日志

表 **错误!文档中没有指定样式的文字。**-67 硬盘容量日志各项说明

项目名称	说明
描述	硬盘容量的的具体内容描述
时间	日志产生时的时间

22.3.4.2 检索日志

请参考其它日志处理方式。

22.3.5 状态监测日志

相关操作可以参考 022.3.1 系统运行日志的介绍。

22.3.6 数据库备份日志

22.3.6.1 日志列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[系统日志/数据库备份日志]，点击菜单进入页面，如图所示：

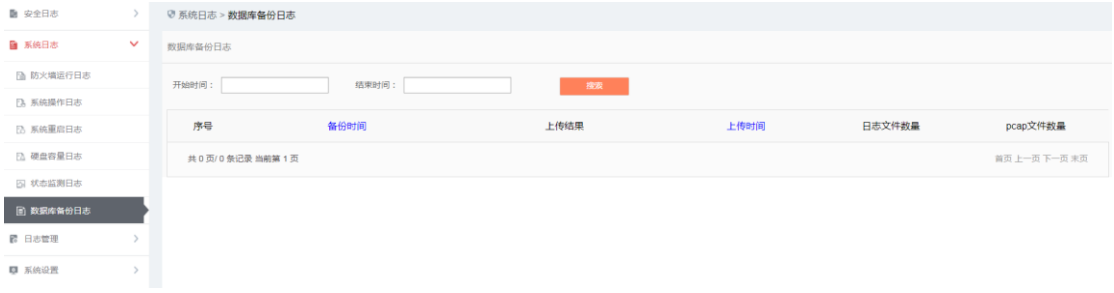


图 **错误!文档中没有指定样式的文字。**-189 数据库备份日志

22.3.6.2 检索日志

请参考其它日志处理方式。

22.4 统计分析

22.4.1 事件分析

22.4.1.1 页面导航

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[统计分析/事件分析]，点击菜单进入页面，如图所示，该界面以饼图的方式展示了告警总数，未处理告警数，已处理告警数，以折线图的方式展示各个告警的趋势。如图所示：

图 **错误!文档中没有指定样式的文字。**-190 事件分析

22.5 报表管理

22.5.1 日志导出下载

22.5.1.1 日志导出列表

审计用户 audit 登录防火墙的 Web 管理界面后，在左侧导航栏找到[报表管理/日志导出下载]，点击菜单进入页面，如图所示：

图 **错误!文档中没有指定样式的文字。**-191 日志导出下载

22.5.1.2 日志导出下载

点击日志后面的<下载>按钮可以下载该日志文件。

22.5.1.3 日志导出检索

在[日志导出下载]的列表页面中，可以根据条件对日志导出进行检索。如图所示：

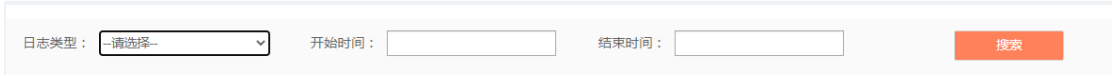


图 **错误!文档中没有指定样式的文字。**-192 日志导出检索

22.6 修改密码

参考配置管理修改密码部分。

23. 系统操作员

23.1 用户管理

用户管理，用于展示、修改设备创建的用户信息，可以通过[修改密码]、[修改备注]、[删除]等操作对存在的账户进行相应的修改，可以通过[添加]按钮进行新用户的添加操作，表如下图：

图 **错误!文档中没有指定样式的文字。**-193 用户管理页面

通过[添加]按钮，可以创建一个新用户。输入用户名、用户密码、确认密码、用户权限和备注（可以选填）通过[保存]按钮重建一个新用户，其中，用户密码和确认密码必须一致，用户权限可以选择配置管理员、审计管理员、网络管理员三种用户权限。通过[返回]按钮返回到上一级菜单，如下图：

图 **错误!文档中没有指定样式的文字。**-194 用户添加

23.2 修改密码

参考配置管理修改密码部分。