铱迅入侵防御系统
管理员手册

南京铱迅信息技术股份有限公司

Nanjing YXLink Information Technology Co. Ltd.

- 未经南京铱迅信息技术股份有限公司（Nanjing YXLink Information Technology Co.,Ltd.，简称：铱迅信息）的事先书面许可，对本产品附属的相关手册之所有内容，不得以任何方式进行翻版、传播、转录或存储在可检索系统内，或者翻译成其他语言。
- 本手册没有任何形式的担保、立场表达或其他暗示。若有任何因本手册或其所提到之产品信息，所引起直接或间接的数据流失、利益损失或事业终止，铱迅信息不承担任何责任。
- 铱迅信息保留可随时更改手册内所记载之硬件及软件规格的权利，而无须事先通知。
- 本手册描述的“铱迅入侵防御系统”之功能，并非所有型号都支持，对于每个型号拥有的功能模块，请咨询供货商或联系铱迅客服人员。
- 本公司已竭尽全力来确保手册内载信息的准确性和完善性。如果您发现任何错误或遗漏，请向铱迅信息反映。对此，我们深表感谢。

商标信息

铱迅信息、铱迅信息的标志、铱迅入侵防御系统标志为南京铱迅信息技术股份有限公司的商标或注册商标。本手册或随铱迅信息产品所附的其他文件中所提及的所有其他商标名称，分别为其相关所有者所持有的商标或注册商标。

版本历史

版本	发布时间	说明
0.9	2010 年 3 月 12 日	初稿
…		
6.1	2019 年 12 月 26 号	更换产品 logo 和截图

阅读指导

如果您是第一次使用铱迅入侵防御系统，建议首先阅读如下章节：

3.安装部署

4.安装及初始化

5.快速使用指南

6.开始使用

如果您做日常入侵告警的查看和分析，建议阅读如下章节：

7.系统监控

8.数据中心

如果您是高级用户，建议重点阅读如下章节：

9.策略配置

10.网络配置

11.系统管理

12.用户管理

13.Console 功能

14.复位与还原

如果您想了解产品特点及规格，建议阅读如下章节：

1. 简介

2. 产品规格

如果您有问题需要寻求答案，建议阅读如下章节：

1.常见问题与解答

目 录

前言：

文档范围

本文将覆盖铱迅入侵防御系统的硬件产品规格和 Web 管理界面的所有功能特点，并详细介绍该系统的具体使用方法。

期望读者

期望了解本产品主要技术特性和使用方法的系统管理员、网络管理员、网络安全专家等。本文假设您对下面的知识有一定的了解：

- 1. 系统管理
- 2. TCP/IP 协议
- 3. HTTP 协议
- 4. FTP 服务
- 5. ， DNS 服务
- 6. 邮件服务
- 7. 虚拟化
- 8. Windows 或 Linux 操作系统
-

内容简介

1. 简介：介绍铱迅入侵防御系统的产品功能
2. 产品规格：介绍本产品的硬件规格和电气特性
3. 安装部署：简明介绍本产品的安装和部署方式
4. 安装及初始化：介绍本产品的安装的一般过程
5. 快速使用指南：介绍设备的基本使用方法
6. 开始使用：介绍 Web 管理页面的内容组织和使用指南
7. 系统监控：介绍 Web 管理界面中的设备监控信息的查看

8. 数据中心：介绍 Web 管理界面中的设备数据的监视

9. 策略配置：介绍 Web 管理界面中策略的管理及配置

10. 网络配置：介绍 Web 管理界面中的网络配置

11. 系统配置：介绍 Web 管理界面中的系统配置

12. 用户管理：介绍 Web 管理界面中的用户管理配置

13. Console 功能：介绍 Console 功能的配置

14. 系统复位与还原：系统的复位与还原的方法

15. 常见问题与解答：用户常见的问题与解答

附录 A：出厂默认设置

获得帮助

获取网络安全相关资料，请访问铱迅信息网站：http://www.yxlink.com/

如需获取更详尽的网络安全专业服务信息、商务信息，您可通过如下方式和我们取得联系：

地址：江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

邮编：210012

服务热线：400-097-5557

电话：025-83235296，025-83235396，025-58722055

传真：025-83235296，025-83235396 转 601

网站：http://www.yxlink.com/

Email：info@yxlink.com

格式与名词约定

设备、产品、系统——除非特指，本手册中均表示铱迅入侵防御系统

防火墙、应用防火墙——除非特指，本手册中均表示铱迅入侵防御系统

【A】 —— 菜单名称和按钮名称的表示方式

【A】→【B】—— 菜单项选择的表示方式

—— 使用技巧、建议和引用信息等

—— 重要注意信息

1. 简介

1.1 产品介绍

铱迅入侵防御系统（英文：YXLink Network Intrusion Prevention System，简称：YXLink IPS）是铱迅信息结合多年在应用安全理论与应急响应实践经验积累的基础上，自主研发的一款防护系统。铱迅入侵防护系统提供了实时、主动的防护能力，通过新一代的入侵防护技术，能够有效的阻断攻击，保证合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。该产品致力于解决应用及业务逻辑层面的安全问题，广泛适用于“政府、金融、运营商、公安、能源、税务、工商、社保、交通、卫生、教育、电子商务”等各个行业。部署铱迅入侵防御系统，可以帮助用户解决目前所面临的各类应用安全问题。

1.2 技术特点

铱迅入侵防御系统支持多种灵活的部署方式，如透明网桥模式、混合部署模式、策略路由模式。

铱迅入侵防御系统工作在透明网桥模式下时，管理员可在不需要修改原网络拓扑结构的情况下进行部署，对于标准的 Web 应用，可以做到即插即用，无需对“YXLink IPS”进行任何配置。同时工作在透明网桥模式下时，设备具有软硬件 Bypass 功能（光口 Bypass 为选配件），具有较高的容错机制，相当于一根网线串入当前网络中，并对应用攻击进行防御。而混合部署模式更是在应对复杂的网络应用环境中，提供了更加人性化的均衡部署能力。铱迅入侵防御系统基于先进的技术架构和高效的检测引擎，其主要特点有：

防护能力：

- 支持 IP 碎片重组、TCP 流重组、协议分析高度自由的自定义规则系统， 轻松应对各种黑客攻击方式；
- 支持模式匹配、异常检测，统计分析；
- 可检测蠕虫、木马、缓冲区溢出、暴力破解、扫描、DDOS、SQL 注入、XSS 跨站脚本、ARP 欺骗攻击、CC 攻击等各种攻击行为，支持反垃圾邮件功能；
- 支持超长报文组包（最大 30M）；
- 基于应用端口的 ACL；
- 丢弃数据包、阻断 TCP 连接、禁止恶意 IP 的后续访问；

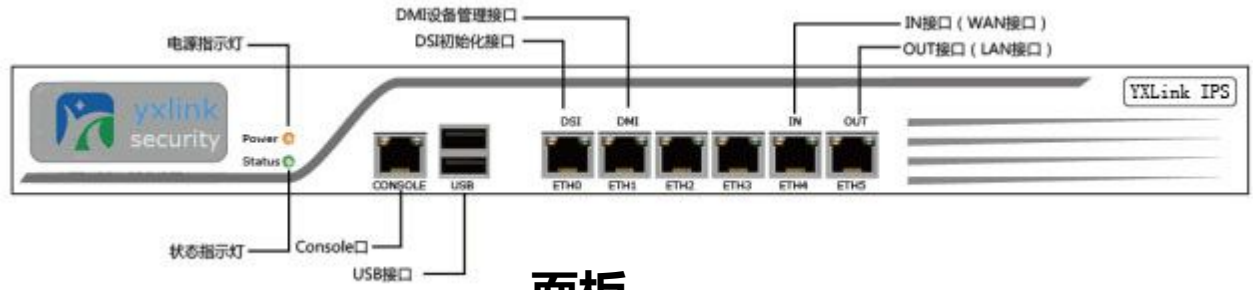
- 对内置规则能够进行任意组合成策略集，该策略集要求有图形界面，可以高度定制；
- 能针对不同的 IP 地址区域指定不同的防护策略集，最大程度避免误报；

性能及可靠性：

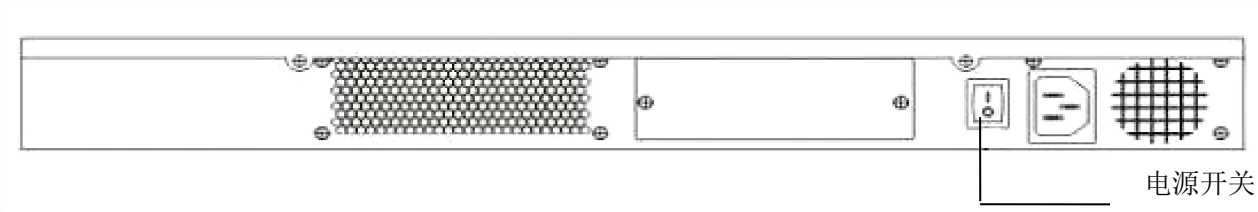
- 透明网桥模式，支持高并发连接数；
- 内置高性能解码、检测引擎；
- 支持复杂的网络环境：策略路由、VLAN 802.1Q、端口汇聚等；
- 具有硬件/软件 Bypass 功能，高可靠性 HA 架构（双机热备），保证业务稳定、长期运行；
- 完善的固件和规则升级功能，长期保证网络的安全；

2. 产品规格

2.1 面板说明



面板



背板

2.1.1 接口说明

⚠注意：

DSI 接口自带 DHCP 功能，仅供直接连接计算机时使用。

切勿将其接入内部管理网络，否则会造成 DHCP 冲突。

序号	名称	说明
1	DSI 接口	设备初始化管理接口(Device Setting Interface),直接连接计算机，供本设备初次启动时配置 DMI 接口的 IP 地址使用。在正常情况下，此接口无需连接任何网络。
2	Console 口	Console 口，连接 PC 机的串口，提供命令行进行设备维护。
3	WAN 接口	外部网络流量流入接口(WAN Interface)，也称 IN 接口。
4	LAN 接口	内部网络流量流出接口(LAN Interface)，也称 OUT 接口，连接内部设备。根据部署方式的不同，可以连接内部的服务器或交换机、路由器等网络设备。
5	DMI 接口	设备管理接口(Device Management Interface)， 连接内部管理网络，管理员通过此接口登录本设备的 Web 管理页面进行日常管理工作。
6	电源指示灯	指示设备的电源状态，熄灭表示断电状态。
7	状态指示灯	指示设备的磁盘读写状态，闪烁时表示正在读写磁盘。
8	USB 接口	USB 接口，厂家检修专用。
9	电源开关	设备的电源开关。

3. 安装部署

3.1 透明网桥模式

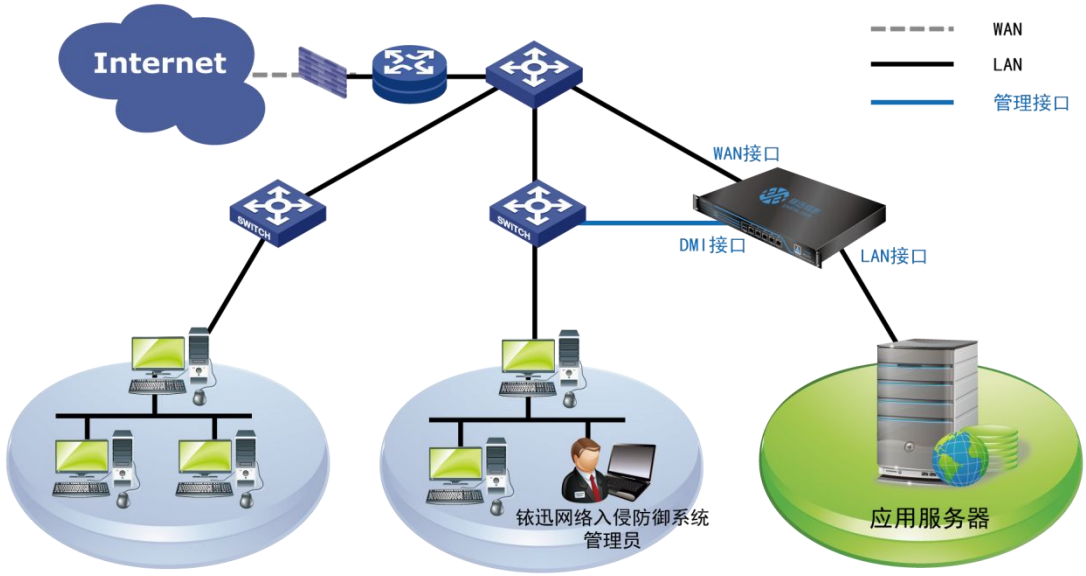
透明网桥模式指在两台运行的网络设备中间插入“铱迅入侵防御系统（也称：铱迅 WEB 服务入侵防护系统）”，但是对流量并不产生影响。在透明网桥模式下，“铱迅入侵防御系统”可以阻断、拦截来自 Web 应用层攻击，而让其他正常的流量通过。透明网桥部署模式的最大特点是快速、简便，做到即插即用，先部署后配置。

采用“铱迅入侵防御系统（也称：铱迅 WEB 服务入侵防护系统）”透明网桥部署模式主要应用于如下五种场景：

1. 单一混合型应用服务（应用服务、数据库服务(以下简称 DB)在同一台服务器上）
2. 单一分离式应用服务（应用服务、DB 采用不同的服务器部署，但应用服务器只有一台）
3. 集群式/集中式应用服务（采用集群方式的应用服务系统，或者多台应用服务器，但网络拓扑分布较为集中）
4. 半分散式应用服务（应用服务器分布在局域网的部分子网中）
5. 全分散式应用服务（应用服务器几乎分布在局域网的任何子网中）

3.1.1 单一混合型 Web 服务部署模式

单一混合型应用服务：采用一台服务器提供应用服务，并且该服务器同时提供数据库服务(DB)，这种情况主要适用于中小型企业的应用服务器模式。在这种网络拓扑结构下，可直接将“YXLink IPS”串接在服务器的前端，如下图显示：



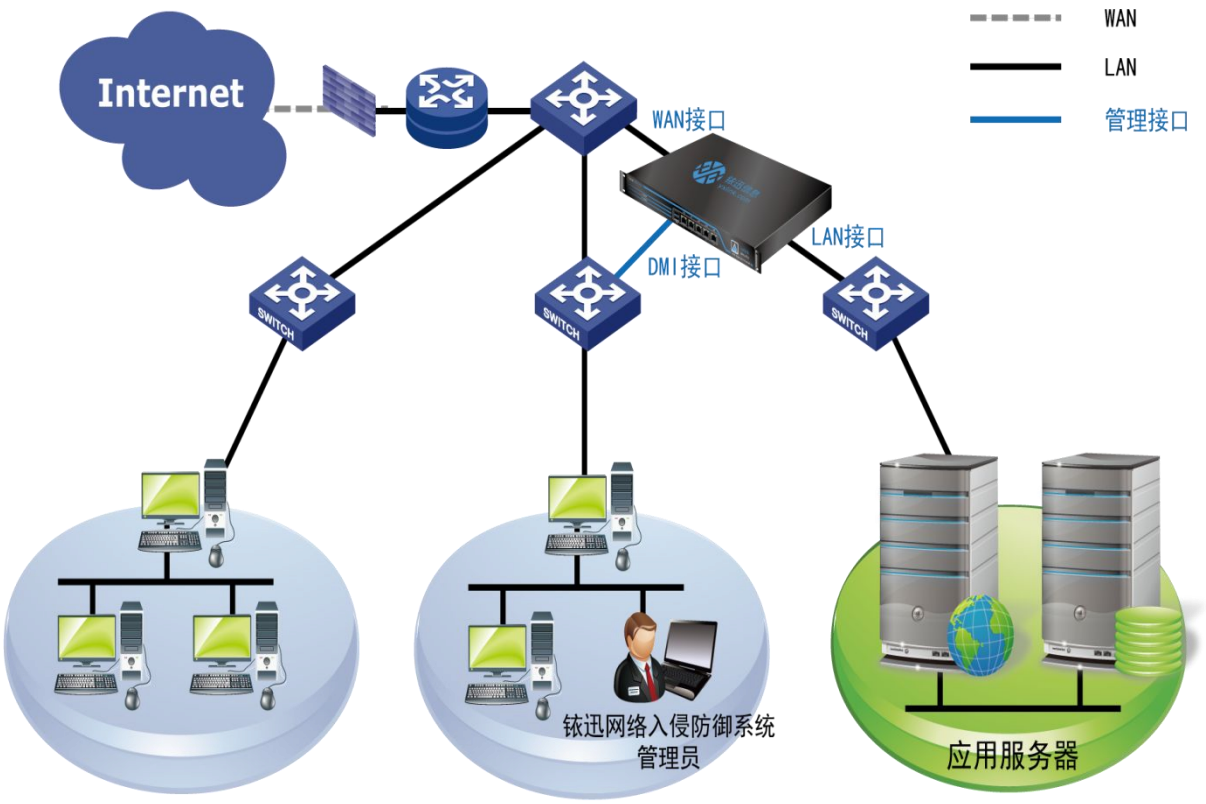
部署步骤如下：

6. 1.在机架上选择合适的位置正确安装设备；
7. 2.确认设备处于断电状态；
8. 3.确认应用服务器处于正常工作状态（局域网内的其他机器可正常访问应用服务），如工作异常，请与应用服务器管理员联系，工作正常后，继续下一步；
9. 4.将原来接在应用服务器上的网线 A 从应用服务器上拔下；
10. 5.将拔下的网线 A 连接在“YXLink IPS”的 IPS 接口；
11. 6.用网线连接“YXLink IPS”的 LAN 接口和应用服务器原网线 A 接插的网口上；
12. 7.此时，设备在硬件 Bypass 状态，再次确认应用服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；
13. 8.打开设备电源，等待约 120 秒；
14. 9.再次确认应用服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
15. 10.用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
16. 11.上述所有步骤完成后，请用网线将‘YXLink IPS’的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.1.2 单一分离式应用服务部署模式

单一分离式应用服务：采用一台服务器提供应用服务，同时采用另一台服务器提供数据库服务，网站的应用服务和相关的数据库服务分布在不同的服务器上。这种情况主要适用于中小型企业的应用服务器模式。在这种网络拓扑结构下，可直接将“YXLink IPS”串接在应用服务器和 DB 服务器所在的交换机前端，如下图显示：



部署步骤如下：

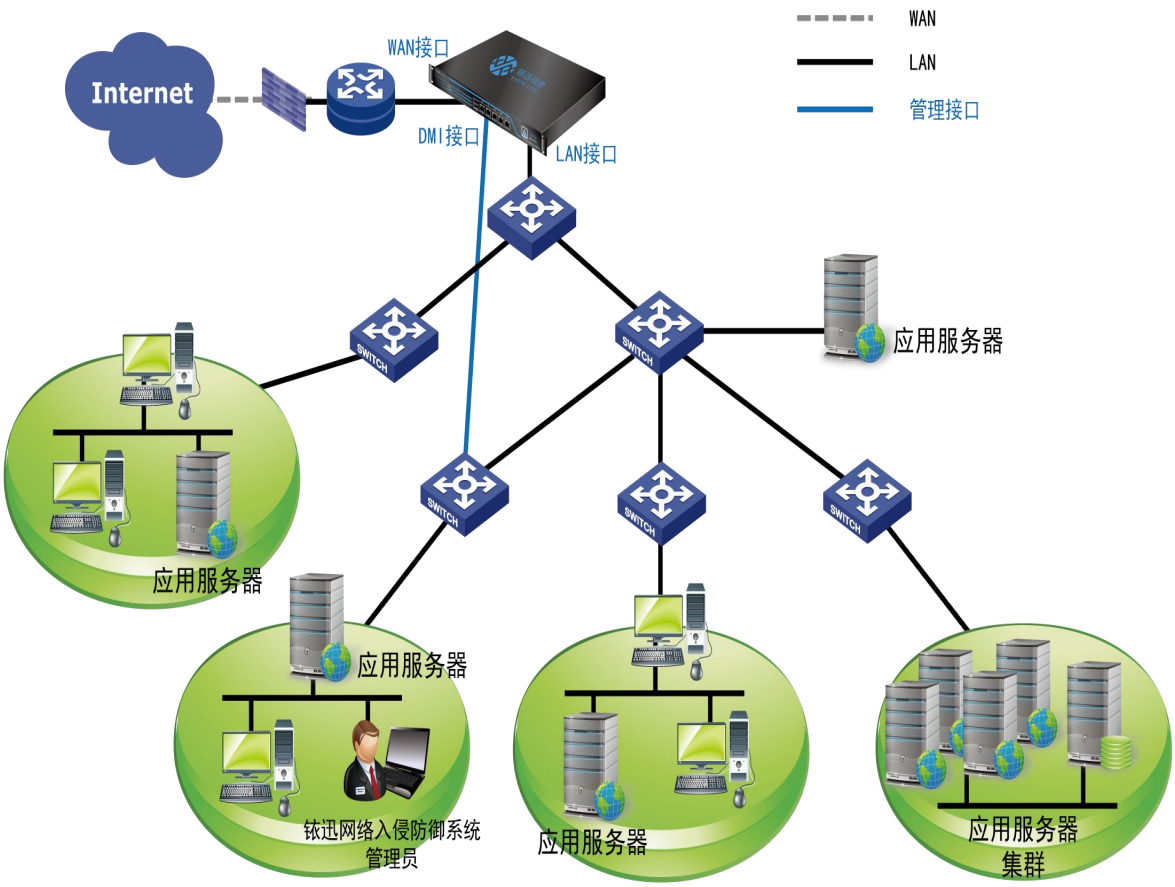
1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认应用服务器处于正常工作状态（局域网内的其他机器可正常访问应用服务），如工作异常，请与应用服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
5. 将拔下的网线连接在“YXLink IPS”的 WAN 接口；
6. 用网线连接“YXLink IPS”的 LAN 接口和交换机 B 的 UPLINK 网口；

7. 此时，设备在硬件 Bypass 状态，再次确认应用服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；
8. 打开设备电源，等待约 120 秒；
9. 再次确认应用服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
11. 上述所有步骤完成后，请用网线将“YXLink IPS”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.1.3 集群式/集中式应用服务部署模式

集群式/集中式应用服务：集群式应用服务采用多台应用服务器负荷分担提供同一应用服务；集中式应用服务主要体现在不同的应用服务器放置在同一网段或者相邻的网段内，但不同的应用服务器可能提供多样的应用服务。这种情况多数应用于大中型企业的应用服务器模式，或者是 IDC 机房。在这种网络结构下，可直接将“YXLink IPS”串接在应用服务器群所在子网交换机前端，如下图显示：



部署步骤如下：

1.在机架上选择合适的位置正确安装设备；

2.确认设备处于断电状态；2.确认设备处于断电状态；

3.确认应用服务器处于正常工作状态（局域网内的其他机器可正常访问应用服务），如工作异常，请与应用服务器管理员联系，工作正常后，继续下一步；

4.将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；

5.将拔下的网线连接在“YXLink IPS”的 WAN 接口；

6.用网线连接“YXLink IPS”的 LAN 接口和交换机 B 的 UPLINK 网口；

7.此时，设备在硬件 Bypass 状态，再次确认应用服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；

8.打开设备电源，等待约 120 秒；

9.再次确认应用服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；

10.用网线将设备的 DMI 接口同管理员所在网段的交换机连接；

11.上述所有步骤完成后，请用网线将“YXLink IPS”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

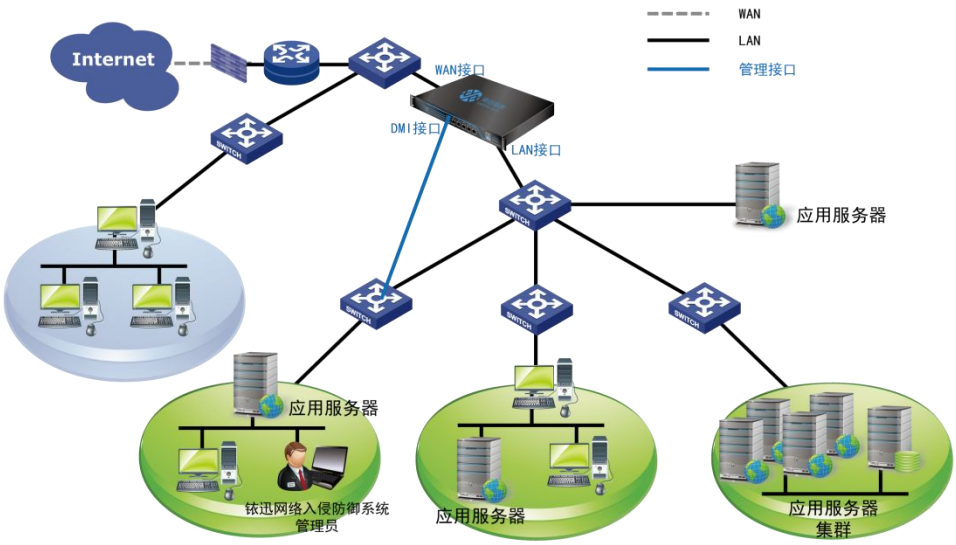
请参考后续章节继续配置设备。

0. 确认设备处于断电状态；
1. 确认应用服务器处于正常工作状态（局域网内的其他机器可正常访问应用服务），如工作异常，请与应用服务器管理员联系，工作正常后，继续下一步；
2. 将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；
3. 将拔下的网线连接在“YXLink IPS”的 WAN 接口；
4. 用网线连接“YXLink IPS”的 LAN 接口和交换机 B 的 UPLINK 网口；
5. 此时，设备在硬件 Bypass 状态，再次确认应用服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；
6. 打开设备电源，等待约 120 秒；
7. 再次确认应用服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
8. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
9. 上述所有步骤完成后，请用网线将“YXLink IPS”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

请参考后续章节继续配置设备。

3.1.4 半分散式应用服务部署模式

半分散式应用服务：在局域网中存在各种不同的应用应用服务，并且这些应用应用服务器分散在不同的子网中。比如：公司有整体的应用服务集群，同时，各个部门还有各自的应用服务器，而这些服务器分布在不同的子网中，如果需要对这些应用服务器进行保护，需要将“YXLink IPS”部署在这些应用服务器所在网络的边缘，如下图显示：



部署步骤如下：

1.在机架上选择合适的位置正确安装设备；

2.确认设备处于断电状态；

3.确认应用服务器处于正常工作状态（局域网内的其他机器可正常访问应用服务），如工作异常，请与应用服务器管理员联系，工作正常后，继续下一步；

4.将原来连接在交换机 A 和交换机 B 的网线从交换机 B 上拔下；

5.将拔下的网线连接在“YXLink IPS”的 WAN 接口；

6.用网线连接“YXLink IPS”的 LAN 接口和交换机 B 的 UPLINK 网口；

7.此时，设备在硬件 Bypass 状态，再次确认应用服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；

8.打开设备电源，等待约 120 秒；

9.再次确认应用服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；

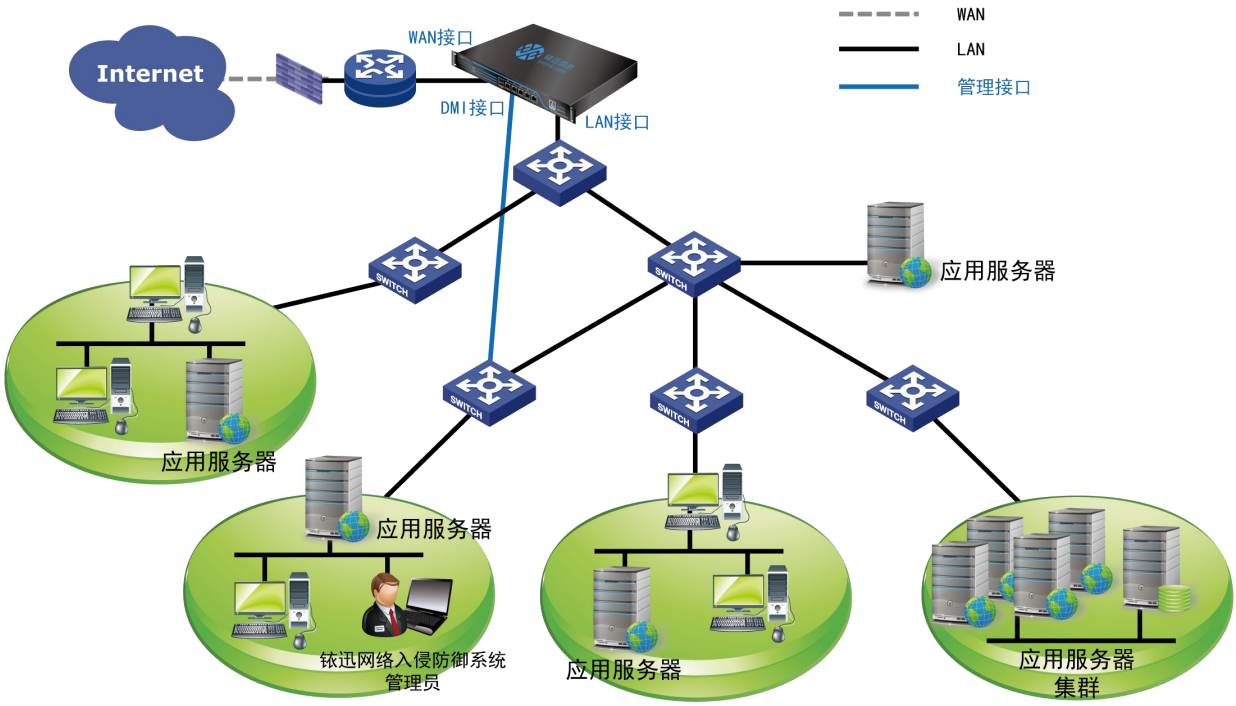
10.用网线将设备的 DMI 接口同管理员所在网段的交换机连接；

11.上述所有步骤完成后，请用网线将“YXLink IPS”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

12.请参考后续章节继续配置设备。

3.1.5 全分散式应用服务部署模

全分散式应用服务：在局域网中存在各种不同的应用应用服务，并且这些应用应用服务器分散在几乎全部的子网中，比较常见的案例：IDC 机房。此时，需要将“YXLink IPS”部署在局域网边缘，一般部署在主交换机同主路由器之间，如下图显示：



部署步骤如下：

1. 在机架上选择合适的位置正确安装设备；
2. 确认设备处于断电状态；
3. 确认应用服务器处于正常工作状态（从 Internet 可正常访问应用服务），如工作异常，请与应用服务器管理员联系，工作正常后，继续下一步；
4. 将原来连接在主路由器和主交换机的网线从交换机上拔下；
5. 将拔下的网线连接在“YXLink IPS”的 WAN 接口；
6. 用网线连接“YXLink IPS”的 LAN 接口和主交换机的 UPLINK 网口；

7. 此时，设备在硬件 Bypass 状态，再次确认应用服务器是否能够正常访问，如工作状态异常，请检查前面步骤插接的网线是否接触良好；
8. 打开设备电源，等待约 120 秒；
9. 再次确认应用服务器是否能够正常访问，如工作状态异常，请同技术服务人员联系；
10. 用网线将设备的 DMI 接口同管理员所在网段的交换机连接；
11. 上述所有步骤完成后，请用网线将“YXLink IPS”的 DSI 接口同一台普通的台式机网口直接连接（请勿通过局域网进行连接，DSI 带有 DHCP 功能，可能会同您的网络环境中的其他 DHCP 设备产生冲突，导致部分网络不可用）；

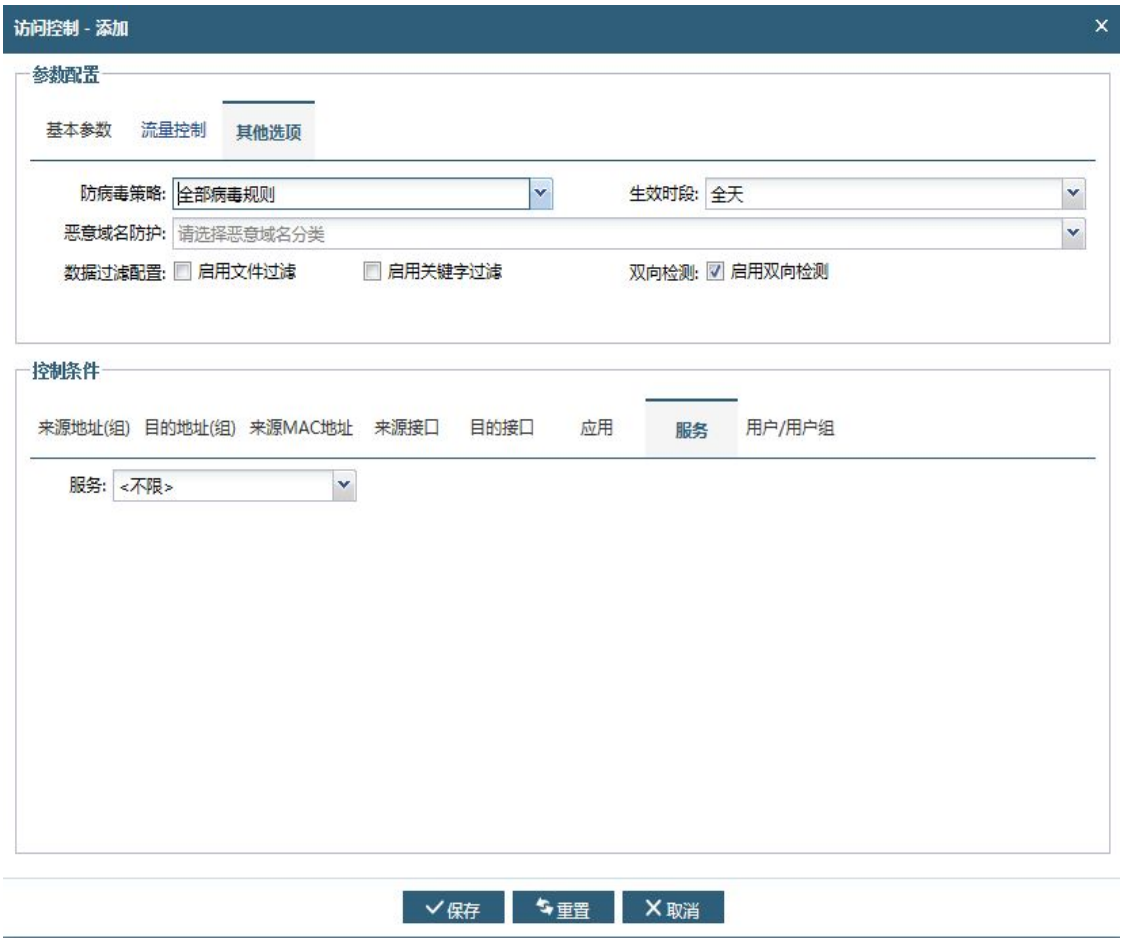
请参考后续章节继续配置设备。

3.1.6 部署环境举例

IPS 配置：

访问控制配置：

动作：继续检测；规则防护策略：默认防护策略；防病毒策略：全部病毒规则。双向检测默认勾选；点击【保存】，再点击【应用】即可。



虚拟网桥配置：

虚拟网桥添加一个网桥 bridge0。

网络接口配置：

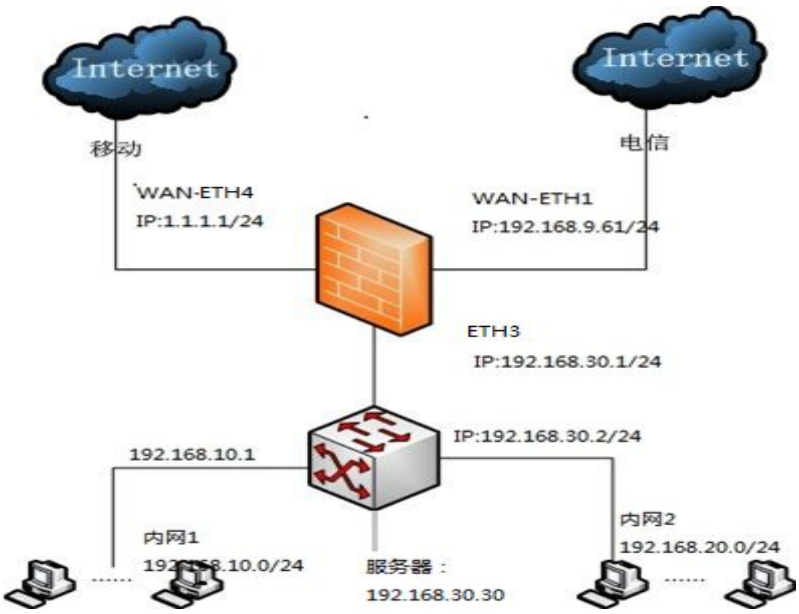
网络接口中添加 ETH2，透明，WAN，网桥 bridge0；

ETH3，透明，LAN，网桥 bridge0。

测试环境：

WAN 口接交换机，LAN 口接服务器即可。

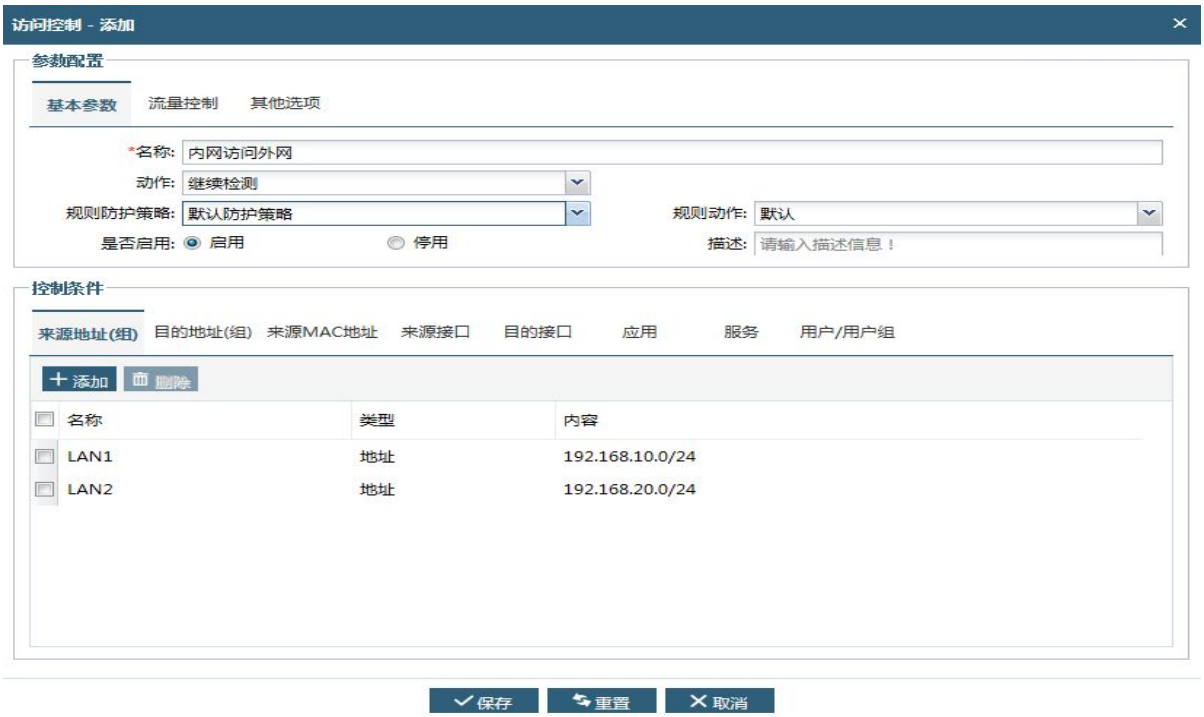
3.2 网关模式

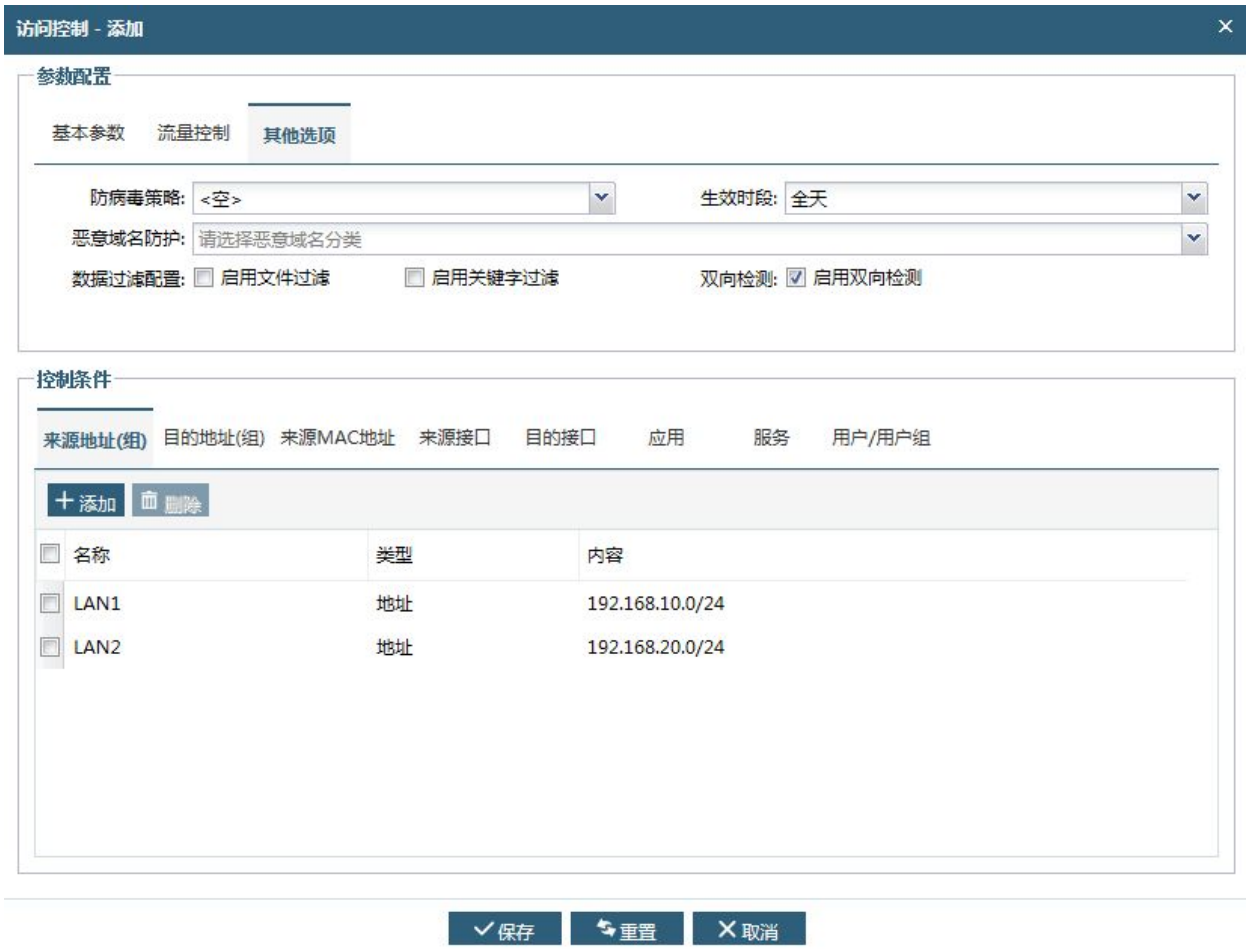


IPS 配置：

访问控制配置：

动作：继续检测；规则防护策略：默认防护策略；防病毒策略：全部病毒规则。来源地址添加 192.168.10.0/24,192.168.20.0/24。双向检测：默认勾选。点击【保存】，再点击【应用】即可。


访问控制 - 添加
参数配置
基本参数
流量控制
其他选项
*名称: 内网访问外网
动作: 继续检测
规则防护策略: 默认防护策略
规则动作: 默认
是否启用: 启用 停用
描述: 请输入描述信息！
控制条件
来源地址(组)
目的地址(组)
来源MAC地址
来源接口
目的接口
应用
服务
用户/用户组
添加
删除
名称
类型
内容
LAN1
地址
192.168.10.0/24
LAN2
地址
192.168.20.0/24
保存
重置
取消


访问控制 - 添加
参数配置
基本参数
流量控制
其他选项
防病毒策略: <空>
生效时段: 全天
恶意域名防护: 请选择恶意域名分类
数据过滤配置: 启用文件过滤
启用关键字过滤
双向检测: 启用双向检测
控制条件
来源地址(组)
目的地址(组)
来源MAC地址
来源接口
目的接口
应用
服务
用户/用户组
添加
删除
名称
类型
内容
LAN1
地址
192.168.10.0/24
LAN2
地址
192.168.20.0/24
保存
重置
取消

网络接口配置：

ETH4：1.1.1.1,255.255.255.0,1.1.1.1，WAN 属性。

ETH1：192.168.9.61,255.255.255.0,192.168.9.1，WAN 属性。

NAT 配置：

源 NAT 出接口-ETH4，来源 IP 192.168.10.0/24，目的任意，转换 IP 1.1.1.1。

源 NAT 出接口-ETH4，来源 IP 192.168.20.0/24，目的任意，转换 IP 1.1.1.1。

源 NAT 出接口-ETH1，来源 IP 192.168.10.0/24，目的任意，转换 IP 192.168.9.61。

源 NAT 出接口-ETH1，来源 IP 192.168.20.0/24，目的任意，转换 IP 192.168.9.61。

目的 NAT 入接口-ETH4，来源 IP 任意，目的 1.1.1.1，转换 IP192.168.30.30。

目的 NAT 入接口-ETH1，来源 IP 任意，目的 192.168.9.61，转换 IP192.168.30.30。

静态路由配置：

任意到任意，网关 1.1.1.2，优先走移动口。

链路负载均衡配置:

修改智能负载均衡,如下图所示：

添加策略选路：

选择某个 IP 从哪个口出去，比如访问服务器从移动口进来，需要从移动口出去，即添加一条 192.168.30.30，并从 ETH1 出去的策略。

4. 安装及初始化

4.1 打开安装箱

对照物品清单检查物品，如果发现有所损坏或者任何配件短缺的情况，请及时和供货商联系。

4.2 安装设备

请使用附件箱中的耳片和螺钉将设备固定在机架上。

4.3 选择部署方案

参考安装部署，选择适合自己网络拓扑结构的部署方式。

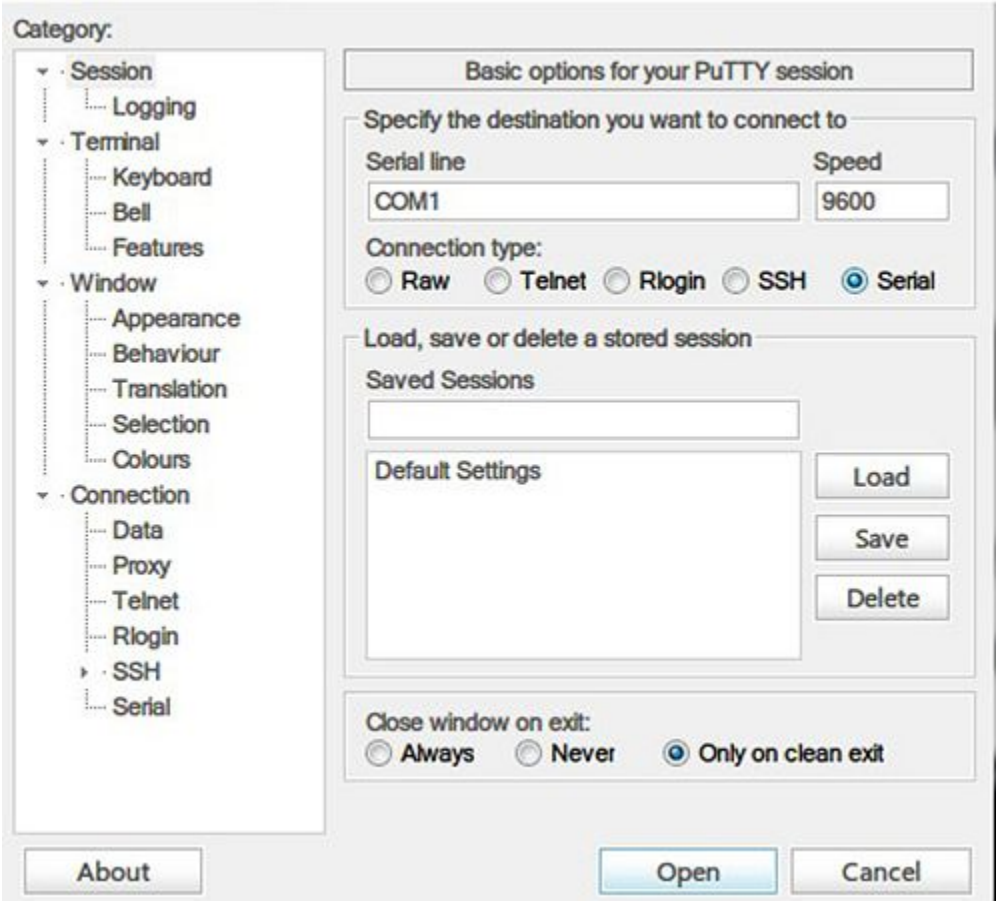
4.4 初始化设备

4.4.1 连接设备的 Console 口

1.用 Console 线连接 PC 机和防火墙;

2.onsole 线串口一端连接 PC 机串口，另一端连接设备的 Console 口;

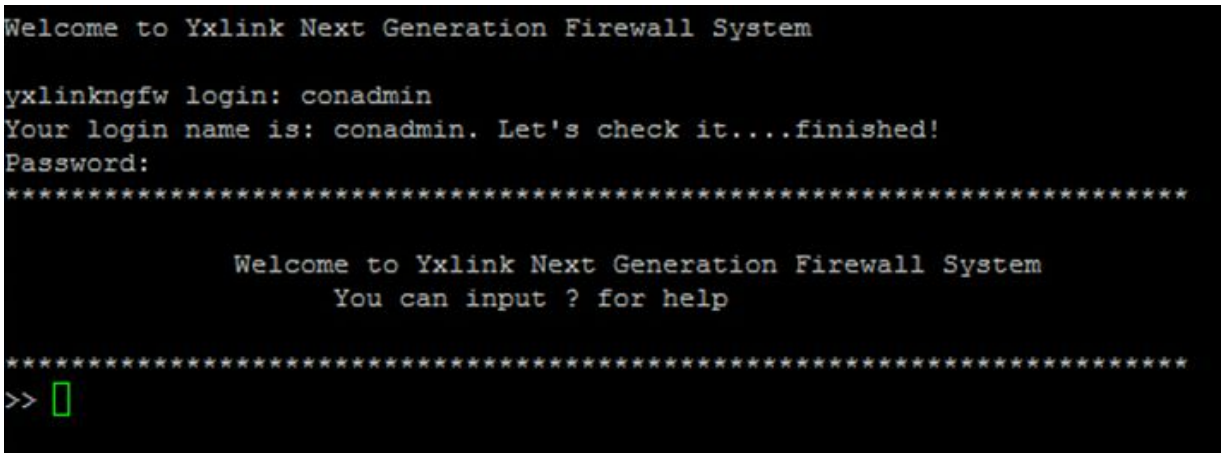
3.运行支持 COM 口通讯的软件（如 PUTTY、超级终端等）连接设备，连接状态选择“串口”，波特率设置为 9600;



⚠注意:

每台 PC 机的 COM 口设备编号可能不一样，请选择正确的 COM 口设备编号进行连接。

设置好参数，点击【Open】按钮连接，输入用户名 conadmin，密码 conadmin 登陆系统，进入欢迎界面;



4.4.2 连接设备的 DSI 接口

使用网线将一台计算机直接连接至本设备的 DSI 接口，（请参考面板说明）将该计算机设置为“自动获得 IP 地址”，而不要设置静态 IP 地址。

在 Microsoft Windows XP 下设置“自动获得 IP 地址”的方法如下：

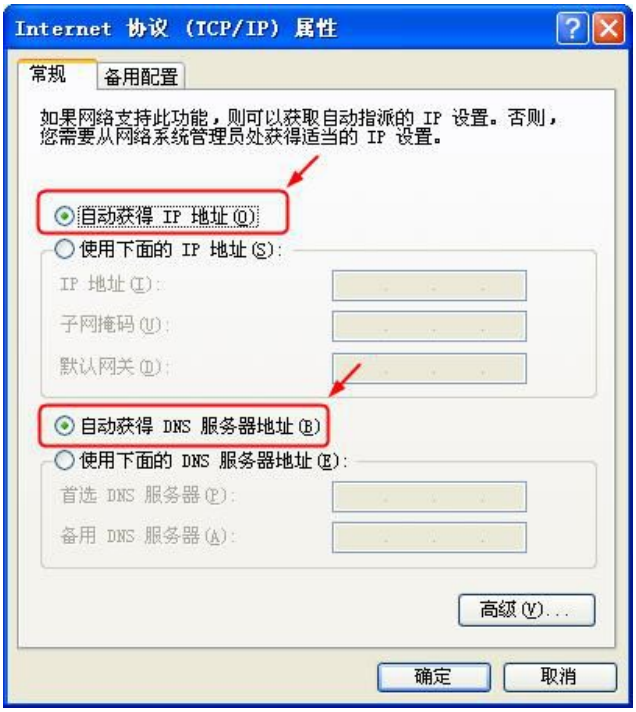
（1）【开始】→【控制面板】→【网络连接】；

（2）在“本地连接”图标上点击右键，然后点击弹出的“本地连接 属性”。如图；

（3）在弹出的“本地连接 属性”对话框中选中“Internet 协议（TCP/IP）”，然后点击【属性】；

（4）在弹出的“Internet 协议（TCP/IP）属性”对话框中，选择“自动获得 IP 地址”和“自动获得 DNS

服务器地址”，然后点击【确定】；

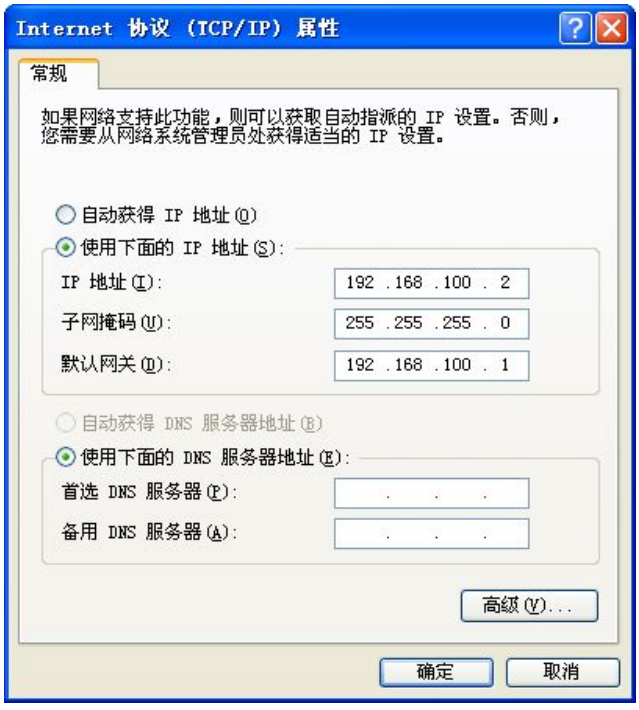


（5）等待并确认您的计算机通过 DHCP 获得了真实有效的 IP 地址，IP 地址应为 192.168.100.xx。

提示:

如果通过步骤（4）“自动获得 IP 地址”无法自动获得有效的 IP 地址，您也可以手工指定计算机的静 态 IP 地址。

静态 IP 地址的设置参数如下:

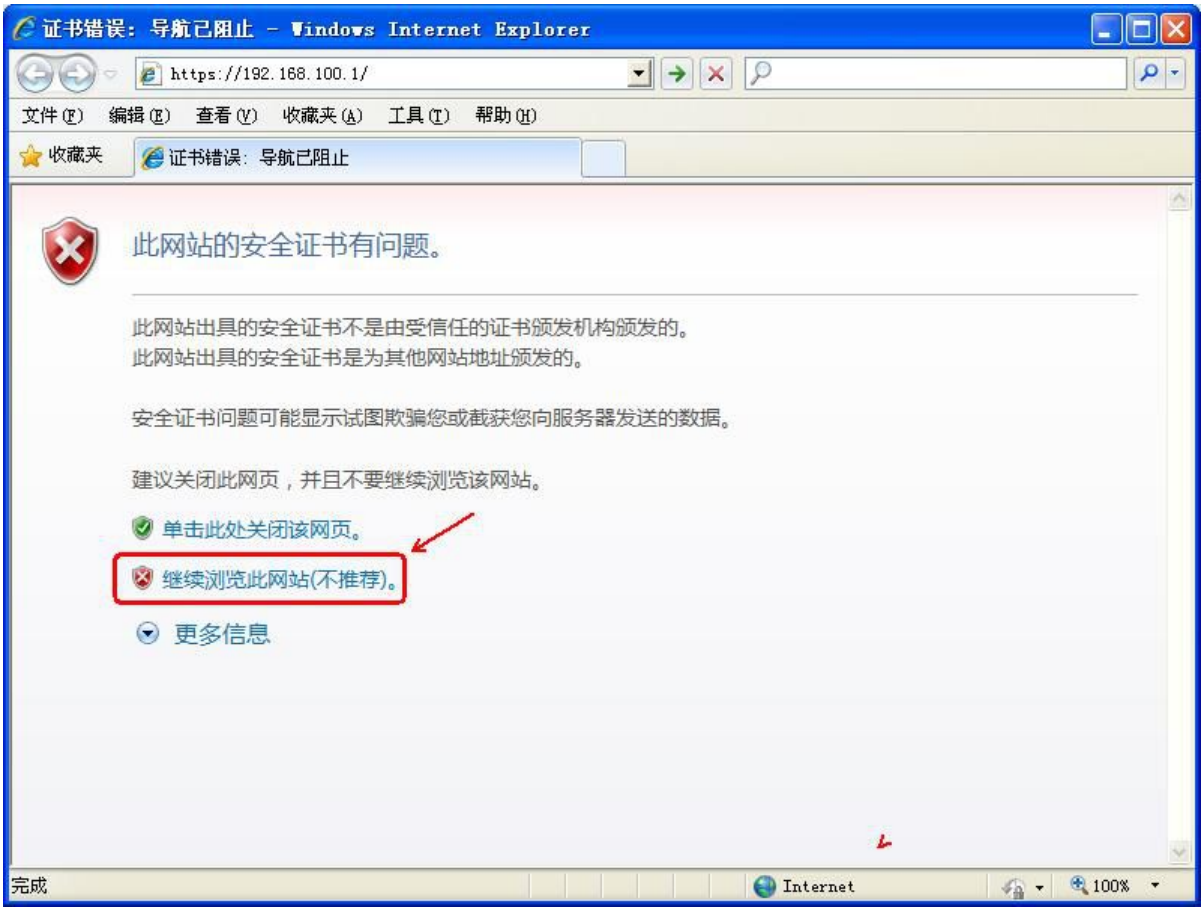


4.4.3 配置 DMI 接口网络参数

假设您已经将计算机连接至本设备的 DSI 接口，并且通过 DSI 接口使您的计算机自动获得了 IP 地址。

下面介绍配置 DMI 接口网络参数的操作方法：

（1）使用浏览器访问 https://192.168.100.1，浏览器可能会提示“此网站的安全证书有问题”，如图：



提示：

如果无法访问该网址，请检查计算机的防火墙设置，需要打开 443 端口才能访问此网址。

（2）点击“继续浏览此网站（不推荐）”，然后显示系统登录页面，如图：

（3）输入用户名和密码（设备初始用户名和密码请参看附录 A），点击【登录】按钮，进入“铱迅入侵防御系统”强制修改密码页面。

⚠注意：

1、必须同时修改 webadmin、sysadmin、auditor 三个用户的密码，以增强系统安全性。

2、如果登录失败，请检查是否为以下原因引起：

1） 用户名输入错误；

2） 密码输入错误；

3） 没区分大小写。

3、如果某用户连续登录失败超过设定的次数（缺省为 3 次），则该用户将被锁定 15 分钟，15 分钟后该用户自动解锁。

建议使用 Microsoft Internet Explorer 7.0 及以上版本的浏览器，屏幕分辨率最好设置为 1024×768 及以上。

4、点击【网络配置】→【接口】→【网络接口】，然后双击接口属性为“DMI”的网络接口进行配置（以下简称为 DMI 接口，即设备管理接口），具体参数请根据内部管理网络的实际情况设置，配置完成后需要在“静态路由”配置相对应的默认网关地址。（配置方式详见修改默认路由）

⚠注意：

请联系网络管理员，以便获取正确的网络设置参数。

提示：

如果网络配置失败（包括 IP 地址填写错误，网关、DNS 配置错误等），从而无法访问设置好的网络接口的 IP 地址，请重新配置或者执行产品复位。

提示：

如果 DMI 接口的 IP 地址无法访问，请检查：

确认部署环境中是否有防火墙，该防火墙中是否针对该 IP 地址进行了一些访问控制的限制；（比如：设置了 MAC 地址绑定。）

确认该 IP 地址是否已经被别的主机占用。

5. 快速使用指南

5.1 修改密码

系统管理员登录“铱迅入侵防御系统”后，选择 webadmin 用户，点击 webadmin，重新设置密码。密码长度应该大于或等于设定的长度，且至少包含数字、大小写字母等字符。

系统管理员可以修改所有安全管理员和用户的密码；

安全审计员可以修改安全审计员的密码；

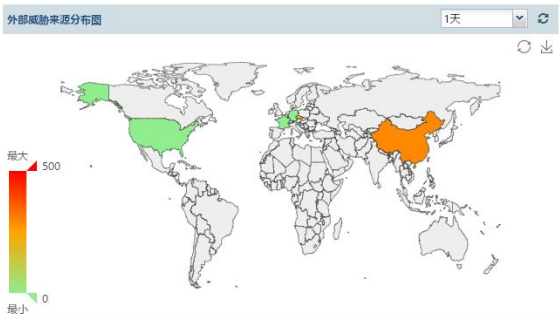
每个用户都可以修改自己的密码。点击右上角“欢迎您：某用户”，系统弹出该用户的密码修改对话框，如下图所示：

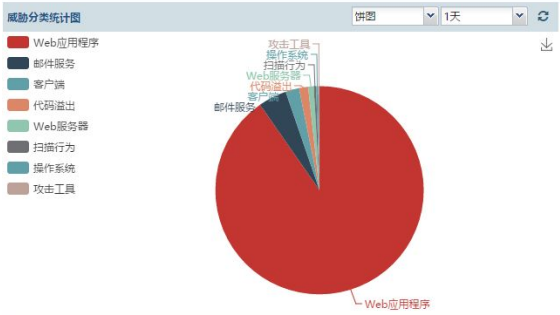
5.2 查看系统状态

点击【系统监控】，可以看到当日入侵记录，入侵记录，入侵类别统计，拦截原因统计，实时流量监测，流量统计，攻击 IP 统计，被攻击 IP 统计，风险等级，系统状态，授权信息，设备信息，cpu，内存，硬盘等信息。具体详见下面各小节。

5.2.1 系统监控

用于显示设备的当前系统状态，如图:





接口名称	接口描述	连接状态	IPv4地址	子网掩码	网关/下一跳...	属性
ETH0(默认出...	电信20兆		218.	255.255.255.0	218.94.	WAN,DFLT
ETH1	移动30兆		221.	255.255.255....	221.	WAN
ETH2			100.	255.255.255....	100.	PPPoE(PPP0...
ETH3	1网段		192.168.	255.255.255.0	*	LAN
ETH4	8网段		192.168.	255.255.255.0	*	LAN
ETH5			192.168.	255.255.255.0	*	LAN
ETH6			192.168	255.255.255.0	*	DMI,LAN
ETH7			192.168.	255.255.255.0	*	DSI

操作时间	日志内容
2016-10-27 09:08:13	检测引擎启动
2016-10-25 18:50:18	检测引擎停止
2016-10-25 09:02:34	检测引擎重启
2016-10-25 09:02:32	许可证书导入成功
2016-10-24 16:12:46	检测引擎重启
2016-10-24 16:12:45	许可证书导入成功
2016-10-24 15:51:30	许可证书已过期，设备已工作于无防护模式（检测模式），请尽快联系供货商或厂家!
2016-10-24 15:51:28	检测引擎重启
2016-10-24 15:26:07	许可证书已过期，设备已工作于无防护模式（检测模式），请尽快联系供货商或厂家!
2016-10-24 15:26:04	检测引擎重启

- 快捷方式： 可以在单击对应图标后快速进入对应的功能模块。
- 风险等级： 显示当前设备检测拦截到的威胁等级分布情况。
- 系统状态： 显示设备当前 CPU，内存，磁盘等关键部分的运行状态。
- 外部威胁来源分布图：显示当前设备检测拦截到攻击的地理位置分布情况。
- 威胁 IP Top10 视图：显示在当前攻击威胁中占据前 10 位的 IP。
- 威胁 Top 10 视图：显示当前最具威胁力的 10 种攻击类型。
- 接口流量：显示当前设备对应接口的实时流量。
- 网络接口：显示当前设备的网络接口信息。
- 系统运行日志：显示当前设备的关键运行日志。
- 设备信息：显示当前设备的详细关键信息，比如产品型号，序列号，版本号等等。
- 威胁分类统计图：显示当前攻击威胁的分类情况。
- 布局换肤：可以根据个人需要进行页面板块布局修改与换肤。
- 流量统计-应用分类：用于显示一段时间内，基于应用分类的流量统计。
- 流量统计-应用：用于显示一段时间内，基于应用的流量统计。
- 流量统计-IP：用于显示一段时间内，基于 IP 的流量统计。
- 实时流量-应用分类：实时显示各个应用分类的流量状况。
- 实时流量-应用：实时显示各个应用的流量状况。
- 实时流量-IP：实时显示各个 IP 的流量状况。
- 新建连接数：实时显示本设备，新建连接数状况。
- 并发连接数：实时显示本设备，并发连接数状况。

ⓘ提示：

本设备会尽可能多的使用内存以便提高性能，因此内存占用较大(超过 80%)是正常现象。

5.2.2 设备信息

用于显示本设备的硬件版本、固件版本、系统版本、规则版本、产品型号和产品序列号。

5.2.3 授权信息

用于显示本设备的授权信息。每一台铱迅入侵防御系统都有唯一的许可证书，该许可证文件只能导入一次，重复导入相同证书无效。同时，许可证书不能在不同型号、同型号不同设备之间混用。当设备没有许可证或者许可证已经过期的情况下，使用安全管理员账号登录时就会出现如下页面。

当本设备许可证是有效期授权类型的，使用安全管理员账号登录时，可以看到当前的许可证状态如下。

当本设备许可证是终身授权类型的，使用安全管理员账号登录时，可以看到当前许可证状态如下。

⚠注意：

当设备没有许可证或者许可证已经过期，铱迅入侵防御系统将在一小时之内关机。如果遇到上述情况，请及时联系供货商或者铱迅信息以便获取有效许可证书。

5.2.4 查看入侵记录

【数据中心】->【入侵事件】->【入侵记录】，可以查看入侵的记录。您可以选择日期查看某天的入侵记录，也可以选择左边菜单栏的【入侵统计】查看入侵记录的统计信息。详细操作请参考《铱迅入侵防御系统管理员手册》。

序号	最后攻击时间	规则编号	规则名称	规则分类	动作...	危害...	来源IP	地理位置	目的IP	协议	来源...	目的...	攻...	操作
198	2016-03-04 1...	1650418	Checkpoint Firewall-1 HTTP解析格...	WEB应用	检测	中	5.9.63.149	德国	192.168.1.70	TCP	58870	80	2	
196	2016-03-04 1...	2510217	Microsoft OLE复合文件Flowbit魔法...	其它客户端	检测	低	192.168.	LAN	123.150.241....	TCP	80	9257	2	
194	2016-03-04 1...	1080325	Microsoft Internet Explorer HP Ph...	Activex攻...	检测	低	192.168	LAN	69.30.214.42	TCP	80	41121	11	
183	2016-03-04 1...	1080397	疑似LEADTOOLS ActiveX Raster T...	Activex攻...	检测	中	192.168.	LAN	69.30.214.42	TCP	80	35845	6	
177	2016-03-04 1...	1670046	快速IMAPS连接 - 疑似暴力破解攻击	IMAP服务	检测	高	223.104.15.1...	内蒙古呼和浩...	192.168	TCP	38164	993	16	
176	2016-03-04 1...	1670046	快速IMAPS连接 - 疑似暴力破解攻击	IMAP服务	检测	高	223.104.4.52	江苏省南京市...	192.16	TCP	43266	993	1	
174	2016-03-04 1...	1650418	Checkpoint Firewall-1 HTTP解析格...	WEB应用	检测	中	91.121.221.15	法国	192.168.	TCP	59164	80	4	
170	2016-03-04 1...	1650870	ASP/JSP源码泄露输出	WEB应用	检测	中	106.39	北京市 电信	192.168	TCP	80	57835	1	
169	2016-03-04 1...	1650891	SQL信息泄露 v6	WEB应用	检测	中	221.10.66.56	四川省巴中市...	192.168	TCP	80	43698	2	
168	2016-03-04 1...	1650896	IIS信息泄漏 v2	WEB应用	检测	中	221.10.66.56	四川省巴中市...	192.168	TCP	80	43698	2	
165	2016-03-04 1...	1650870	ASP/JSP源码泄露输出	WEB应用	检测	中	219.136.245....	广东省广州市...	192.168	TCP	80	53805	1	

5.2.5 查看网络流量

【数据中心】->【监视】->【接口历史流量】，可以按天或者按月以折线图的形式显示某块网卡的网络流量变化趋势。

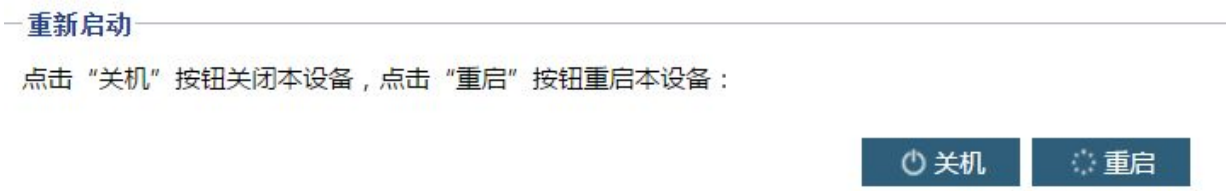
【数据中心】->【监视】->【接口实时流量】，可以显示所有网口的实时流量变化。

刷新

网络接口	模式	速率	连接状态	收到的数据包	发送的数据包	收到的字节	发送的字节	收到的错误包	丢失接收的包	接收速率	发送速率
ETH0	全双工	100 Mbps		278710297	637865462	236.45 GB	167.88 GB	0	442148	18.99 Kbps	43.3 Kbps
ETH1	全双工	100 Mbps		244882221	302827531	244.66 GB	112.38 GB	0	0	229.14 Kbps	107.59 Kbps
ETH2	全双工	1000 Mbps		179505277	197014500	138.23 GB	143.81 GB	1	17458	2.51 Mbps	4.82 Mbps
ETH3	全双工	1000 Mbps		42697761	33103946	36.07 GB	9.01 GB	0	0	204.95 Kbps	167.61 Kbps
ETH4	全双工	100 Mbps		212910070	187033348	160.36 GB	150.05 GB	0	0	4.15 Mbps	359.52 Kbps
ETH5	全双工	1000 Mbps		2107924621	604773629	376.43 GB	376.07 GB	58	251331	159.63 Kbps	258.73 Kbps
ETH6	全双工	1000 Mbps		248623851	301231527	113.62 GB	263.57 GB	827	0	920.48 Kbps	2.43 Mbps
ETH7		自动		0	0	0	0	0	0	0	0

5.2.6 关机和重启

【系统配置】->【高级配置】->【重新启动】页面中可以选择【关机】和【重启】。



⚠注意：

请您尽量避免在本设备运行的时候直接切断电源，这样可能造成数据的丢失或影响设备的使用寿命。

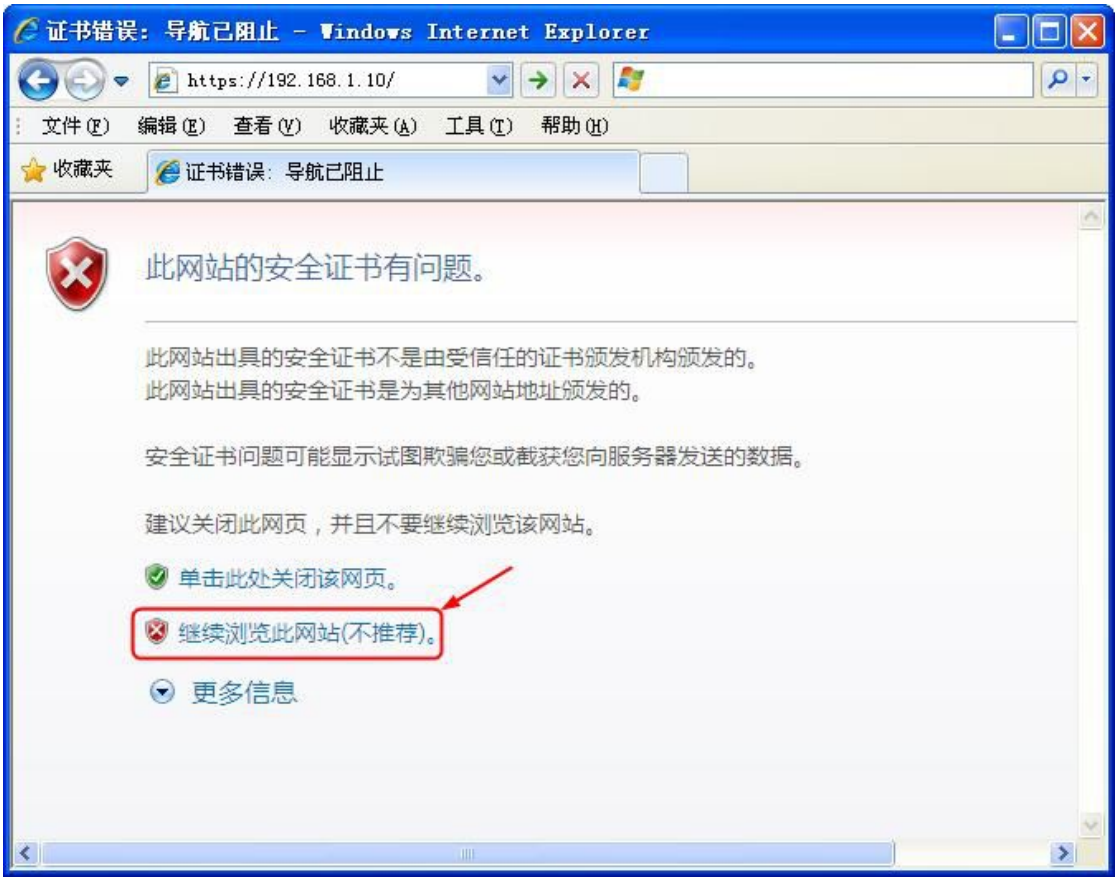
在您点击【关机】按钮，或者直接按下设备上的电源按钮后，请等待设备电源指示灯熄灭后再切断电源。设备安全关闭需要一定时间。

6. 开始使用

6.1 登录

6.1.1 登录系统

在浏览器中输入您已经配置好的本设备 DMI 接口的访问地址（如： https://192.168.1.10） 后按回车（Enter）键，浏览器可能会提示“此网站的安全证书有问题”，如图：



点击“继续浏览此网站（不推荐）”，然后显示系统登录界面，如图。输入正确的用户名和密码，点击【登录】按钮即可登录到本设备进行操作。

提示：

如果是首次安装并使用本设备，请先仔细阅读设备安装及初始化相关章节。

关于如何配置本设备 DMI 接口的 IP 地址，具体请参考设备安装及初始化的相关章节。

出厂的默认用户名和密码请参考附录 A。

提示：

为了获得最佳的页面浏览效果，建议您使用 Microsoft Internet Explorer 7.0 及以上版本的浏览器，推荐显示分辨率 1024×768 以上。

注意：

如果连续登录失败的次数超过设定值（缺省为 3 次），则该用户将被锁定 15 分钟。15 分钟内不允许该用户登录。

6.1.2 系统管理员登录

系统管理员为系统内置账号，可创建并管理安全管理员、普通用户的账号，除此之外无其它权限。系统管理员的所有操作行为都被记录到审计日志。内置的系统管理员账户 sysadmin 不可删除。

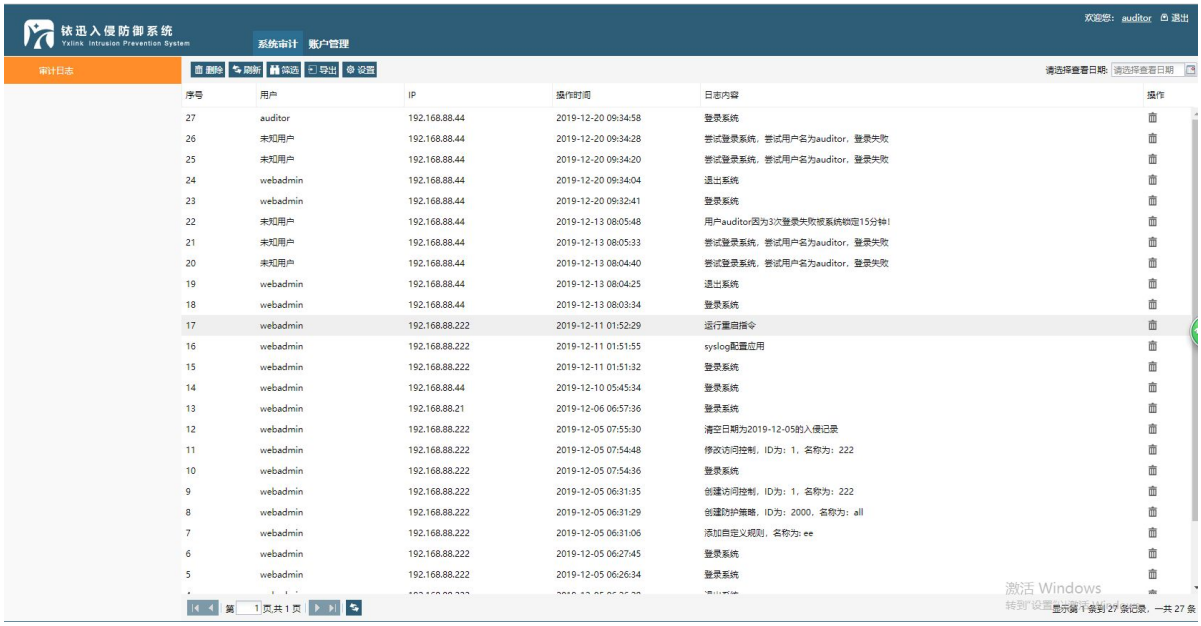
系统管理员可以使用内置的 sysadmin 账号登录界面，如下图所示：

使用系统管理员账号登录成功后的欢迎界面，如下图所示。具体功能的介绍，请参见用户设置（系统管理员适用）。

6.1.3 安全审计员登录

安全审计员只负责对系统管理员和安全管理员的操作日志进行查看和管理，还负责管理安全审计员类型的账号。安全审计员可以使用内置的 auditor 账号登录界面，如下图所示：

使用安全审计员账号登录成功后的欢迎界面，如下图所示。具体功能的介绍请参见用户设置（安全审计员适用）与审计日志(仅限于安全审计员)。



6.1.4 安全管理员登录

安全管理员负责产品安全策略制定、产品配置以及日常维护等管理，不能进行审计日志的查看和管理，不能创建系统管理员、普通用户、安全审计员账号。

安全管理员可以使用内置的 webadmin 账号登录界面，如下图所示：

使用安全管理员账号登录成功后的欢迎界面，如下图所示（具体功能介绍请参见后面的各个章节）。

6.2 密码修改

密码修改有三种方式：

系统管理员可以修改所有安全管理员和普通用户类型账号的密码；

安全审计员可以修改安全审计员类型账号的密码；

每个用户都可以修改自己的密码。

（点击右上角“欢迎您：某用户”，系统弹出该用户的密码修改对话框，如下图所示）。

6.3 欢迎页面

安全管理员在登录界面输入用户名和密码并通过验证后，将看到如图所示的首页。

功能菜单列表：所有的操作管理页面都可以通过上方的 tab 窗口点击进入。

1、在【首页】页面中显示了本产品的当日入侵记录，实时流量以及设备信息等。

2、 2、在首页页面的右上角，您可以点击【帮助】获取系统的帮助信息。

3、 3、您可以点击【退出】按钮，以便安全退出 Web 管理页面。

ⓘ提示：

按 F11 键可以让浏览器进入全屏浏览模式，提供更大的操作界面。

6.4 功能菜单

功能菜单包括以下主菜单，数据中心，策略配置，网络配置，系统配置，用户管理，每一个主菜单下面包含若干功能，具体功能如下：

6.4.1 数据中心

数据中心包括入侵事件，监视，报表，日志菜单。

入侵事件

- 【入侵记录】：查看本设备记录的入侵事件。可以进行查看历史入侵记录、筛选记录、导出入侵记录到文件等操作。
- 【入侵查询】：提供对入侵记录的查询，筛选，以及对查询结果生成报表，日志导出的功能。
- 【入侵统计】：查看当月和历史月份的入侵统计图，以便快速掌握不同日期遭受攻击的状况，判断攻 击变化的趋势。
- 【防病毒记录】：查看本设备防病毒入侵事件，可以进行查看历史入侵记录、筛选记录、导出入侵记录到文件等操作。
- 【DDOS 记录】：记录 DDOS 攻击日志。
- 【关键字过滤日志】：记录关键字过滤和文件类型过滤日志。

监视

- 【IP 地址流量统计】：统计各个 IP 地址在每一个时间段的流量。
- 【应用流量统计】：统计各个应用在每一个时间段的流量。
- 【接口历史流量】：统计每一个网口在每一个时间段的流量。
- 【IP 地址实时流量监测】：实时显示 IP 地址上下行流量及总流量。
- 【应用实时流量监测】：实时显示应用上下行流量及总流量。
- 【接口实时流量】：显示每一个接口的实时流量，发送，接受速率以及丢包率。

报表

- 【报表管理】：查看和导出系统生成的报表。
- 【即时报表】：即时导出报表。
- 【定期报表】：提供按照设定的时间自动生成报表的功能。

日志

- 【系统日志】：记录系统的每一个操作的信息，包括登陆，退出，升级，配置等等。
- 【PPPoE 日志】：记录 PPPoE 的连接情况。

6.4.2 策略配置

策略配置包括策略配置，规则配置，对象配置，每一个菜单下包括若干二级菜单，具体功能使用如下所示。

策略配置

- 【访问控制】：针对来源 IP，目的 IP，来源接口，目的接口，服务设置访问控制。
- 【NAT 配置】：设置源 NAT，以及目的 NAT，保证外网可以访问内网，内网可以上外网。
- 【DDOS 防护】：防止主机遭受 DDOS 攻击，可针对某一个 IP 对其设置禁止和放行。

⚠注意：

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。

规则配置

- 【防护策略配置】：通过选择不同的规则可配置不同的策略，为访问控制选用。
- 【防病毒策略配置】：配置防病毒策略，为访问控制选用。
- 【自定义规则】：可根据环境需要自定义。
- 【内置规则】：里面包含了下一代防火墙所有的规则。
- 【内置防病毒规则】：里面包含了下一代防火墙所有的防病毒规则。
- 【内置应用列表】：里面包含了下一代防火墙所有的应用规则。

对象配置

- 【地址】： 可添加多个地址，地址段，为访问控制使用。
- 【地址组】：可选择多个地址，地址段，为访问控制使用。
- 【服务】： 里面包含了各种内置服务，可自己添加，为访问控制使用。
- 【计划任务】：用户自定义防护生效时间。
- 【蜘蛛设置】：提供对搜索引擎蜘蛛 IP 的白名单功能。
- 【运营商地址】：包含了移动，电信，联通，教育网的所有地址。
- 【内网地址配置】：系统将不检测属于内网地址范围内的 IP 地址间的数据报文。

6.4.3 网络配置

网络配置包含了网络接口，路由，高级网络应用，每一个模块下包含若干二级菜单，具体功能如下：

接口

- 【网络接口】：查看设备包含的所有网络接口，可为每一个接口配置地址，以及各种接口属性。

路由

- 【静态路由】：配置本设备的静态路由，但是默认路由只能有一个。
- 【路由信息】：用于展示系统当前的路由信息。

高级网络应用

- 【本地 DNS 配置】：配置本设备的 DNS。
- 【DNS 代理】：实现 DNS 代理，DNS 缓存以及域名代理的功能 。
- 【动态 DNS】：DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上。
- 【UPNP 服务】：遵循此协议的不同厂商的各种设备可以自动发现对方并进行连接。
- 【HTTP 缓存加速】：可针对某一个接口实现缓存加速。
- 【DHCP 服务】：配置本设备的网口使其具有 DHCP 功能。
- 【镜像流量检测】：为镜像端口上的数据报文进行检测。

- 【BYPASS 设置】：开启 BYPASS 后，每对 WAN/LAN 接口在物理上直接连通，流量不经过设备，一般用于网络故障排除。

OSPF 路由

- 【OSPF 接口】：用于配置系统当前的 OSPF 接口属性。
- 【使能网段】：用于配置系统当前的 OSPF 使能网段，添加该网段之后，该接口网段即加入 OSPF 属性。
- 【全局配置】：用于配置系统当前的 OSPF 参数。
- 【OSPF 信息】：显示 OSPF 的接口信息，链路信息，邻居信息及路由信息。

RIP 路由

- 【RIP 接口】：用于配置系统当前的 RIP 接口属性。
- 【使能网段】：用于配置系统当前的 RIP 使能网段，添加该网段之后，该接口网段即加入 RIP 属性。
- 【邻居配置】：配置 RIP 邻居的 IP 地址，这样可以保证被动接口只给对应的邻居发送 RIP 的更新数据包。
- 【全局配置】：用于配置系统当前的 RIP 参数。
- 【RIP 信息】：用于显示 RIP 的路由信息和路由状态。

6.4.4 系统配置

系统配置包括基本配置和高级配置，每个配置下包括若干功能，具体功能如下：

基本配置

- 【时间配置】：设置系统时间等。
- 【产品授权】：给设备导入授权。
- 【配置管理】：导入和导出系统的配置参数或恢复出厂时的默认配置。
- 【告警管理】：配置设备的邮箱，当开启报警管理时，发现高危入侵记录时，立即发送 Email 报警。
- 【磁盘清理】：设置磁盘使用上限，达到上限会发送报警邮件，可导出入侵记录等日志，可针对某一时间段的日志进行清理。
- 【升级配置】：升级本设备中的软件和安全补丁。
- 【版本管理】：显示设备的固件版本，防护规则版本等各种版本信息。

高级配置

- 【SNMP Trap】：对本设备的 SNMP Trap 功能进行配置
- 【SNMP】：对本设备的 SNMP 功能进行相关配置。

- 【syslog】：对本设备的 syslog 功能进行相关配置。
- 【抓包工具】：提供对本设备接口进行数据抓包的功能。
- 【网络工具】：提供常用的网络命令。
- 【重新启动】：关闭或重启本设备。
- 【高可用性】：可实现主备部署和主主部署。

6.5 通用菜单、按钮介绍

6.5.1 保存和应用功能

如图，在许多页面中都有【保存】和【应用】按钮。

【保存】按钮的含义是保存当前的设置更改但并不立即生效。

【应用】按钮的含义是保存当前的设置更改并立即生效。

⚠注意：

建议在每次设置更改后点击【保存】按钮。将所有设置全部配置完成以后，再点击【应用】按钮让所有设置更改生效。频繁点击【应用】按钮会降低系统的工作效率。

6.5.2 重置和取消功能

重置与取消功能如图所示：

【重置】按钮的含义是清空当前窗口中用户已经输入的内容以便用户重新输入。

【取消】按钮的含义是不保存当前的用户输入并关闭窗口。

6.5.3 刷新功能

如图，【刷新】按钮的含义是从设备数据库中获取最新的数据到用户界面。当您觉得当前 Web 页面显示的信息已经过期的情况下可使用此按钮强制刷新。

网络接口	模式	速率	连接状态	收到的数据包	发送的数据包	收到的字节	发送的字节	收到的错误包	丢失接收的包	接收速率	发送速率
ETH0	全双工	100 Mbps		278710297	637865462	236.45 GB	167.88 GB	0	442148	18.99 Kbps	43.3 Kbps
ETH1	全双工	100 Mbps		244882221	302827531	244.66 GB	112.38 GB	0	0	229.14 Kbps	107.59 Kbps
ETH2	全双工	1000 Mbps		179505277	197014500	138.23 GB	143.81 GB	1	17458	2.51 Mbps	4.82 Mbps
ETH3	全双工	1000 Mbps		42697761	33103946	36.07 GB	9.01 GB	0	0	204.95 Kbps	167.61 Kbps
ETH4	全双工	100 Mbps		212910070	187033348	160.36 GB	150.05 GB	0	0	4.15 Mbps	359.52 Kbps
ETH5	全双工	1000 Mbps		2107924621	604773629	376.43 GB	376.07 GB	58	251331	159.63 Kbps	258.73 Kbps
ETH6	全双工	1000 Mbps		248623851	301231527	113.62 GB	263.57 GB	827	0	920.48 Kbps	2.43 Mbps
ETH7		自动		0	0	0	0	0	0	0	0

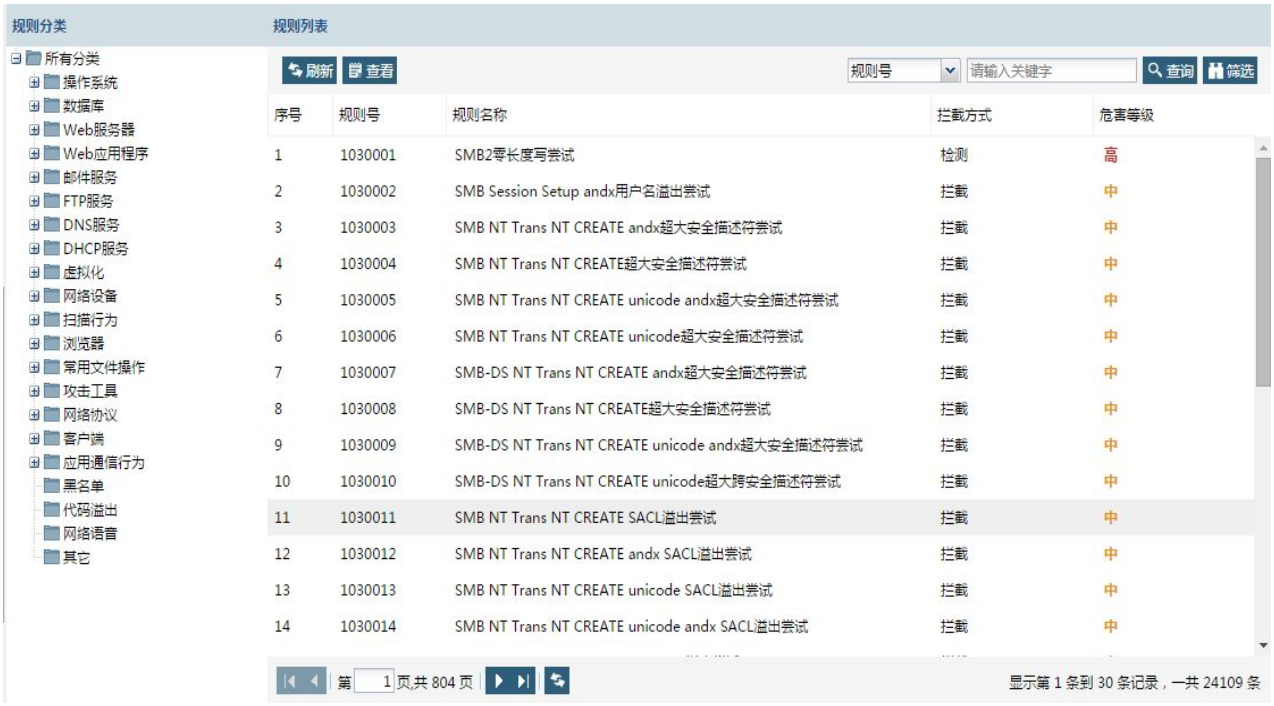
6.5.4 多选功能

如图，在大多数支持列表操作的页面中，您都可以通过按住 Ctrl 键点击以选择多条记录，或者通过按住 Shift 键选择开始记录和结尾记录以便选择一个记录范围。您也可以两种方法配合使用。

序号	名称	是否启用	动作	生效时段	描述	操作
1	test用户可以上网	已启用	继续检测	全天		
2	any	已启用	继续检测	全天		

6.5.5 双击功能

在大多数支持列表操作的页面中，您可以通过双击某条记录，以便快速地进行相应的操作。如图，例如您在自定义规则页面双击一条记录时，系统会自动打开该条规则的编辑页面。



6.5.6 翻页功能

如图，在以列表显示的页面中，您可以通过左下角的翻页按钮来翻页：

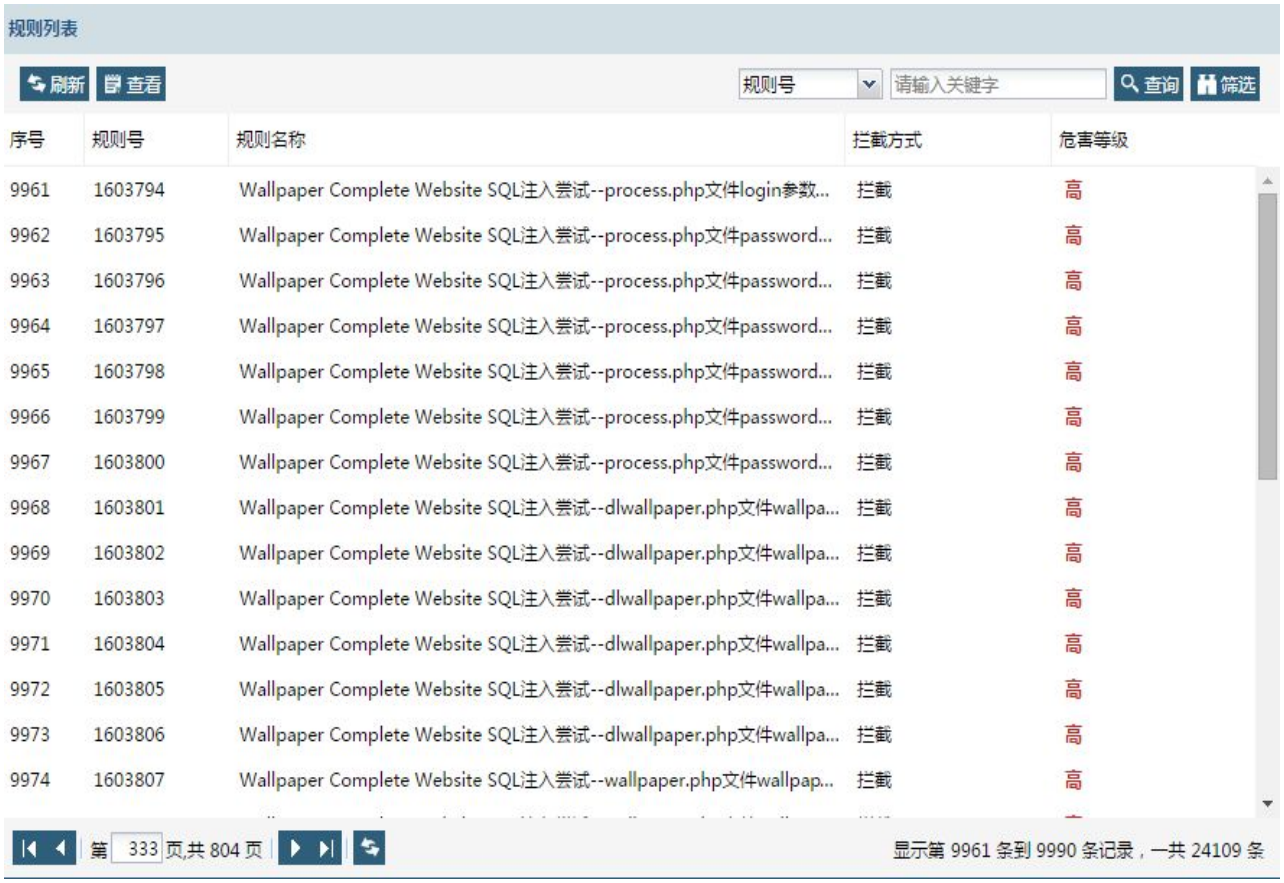
 表示跳到首页

 表示上一页

 表示跳到末页

 表示下一页

您也可以直接在编辑框中输入页码并按回车（Enter）键来进行跳转。



6.5.7 排序功能

在大多数支持列表操作的页面中，当把鼠标箭头放在列名称上时，例如：规则编号，右侧会出现一个向上或者向下箭头，点击此箭头，点击此箭头，在出现的菜单中选择正序或者倒序，如图。

6.5.8 选择列功能

在大多数支持列表操作的页面中，当把鼠标箭头放在列名称上时，例如：拦截原因，右侧会出现一个向上或者向下箭头，在出现的菜单中的“列”子菜单下，可以根据需要选择只显示某些列，如图。

序号	最后攻击时间	规则编号	规则名称	规则分类	动作...	危害...	来源IP	地理位置	目的IP	协议	来源...	目的...	攻...	操作
559	2016-03-07 1...	1060582	ColdFusion管理员访问		检测	低	192.168.88.19	LAN	202.	TCP	1346	80	1	
558	2016-03-07 1...	1650898	目录遍历		检测	中	210.29.144.53	江苏省南京市...	192.	TCP	80	57181	8	
550	2016-03-07 1...	1060582	ColdFusion管理员访问				192.168.88.19	LAN	210.	TCP	56636	80	1	
549	2016-03-07 1...	1650870	ASP/JSP源码泄露输出	WEB应用			180.97.66.49	江苏省苏州市...	192.168	TCP	80	51491	1	
548	2016-03-07 1...	1570031	SQL注入(AND/OR/XOR/HAVING) v1	通用SQL.			61.142.75.39	广东省中山市...	192.168	TCP	56823	80	2	
547	2016-03-07 1...	1570032	SQL注入单引号	通用SQL.			61.142.75.39	广东省中山市...	192.168.	TCP	56823	80	2	
546	2016-03-07 1...	1570039	SQL注入(AND/OR/XOR) v2	通用SQL.			61.142.75.39	广东省中山市...	192.168	TCP	56823	80	2	
545	2016-03-07 1...	1570043	SQL注入(AND/OR/XOR) v3	通用SQL.			61.142.75.39	广东省中山市...	192.168.	TCP	56823	80	5	
544	2016-03-07 1...	1570066	SQL注入字符型	通用SQL.			61.142.75.39	广东省中山市...	192.168	TCP	56823	80	2	
543	2016-03-07 1...	1570067	SQL注入数字型	通用SQL.			61.142.75.39	广东省中山市...	192.168.	TCP	56823	80	2	
542	2016-03-07 1...	1570031	SQL注入(AND/OR/XOR/HAVING) v1	通用SQL.			61.142.75.38	广东省中山市...	192.168.	TCP	3504	80	4	
541	2016-03-07 1...	1570032	SQL注入单引号	通用SQL...	检测	中	61.142.75.38	广东省中山市...	192.168.	TCP	3504	80	4	

7. 系统监控

7.1 快捷方式

点击快捷方式上的按钮可以快速进入对应的功能页面。

7.2 风险等级

显示主机处于何种安全状态中。

7.3 系统状态

用于显示设备的当前系统状态，如图：

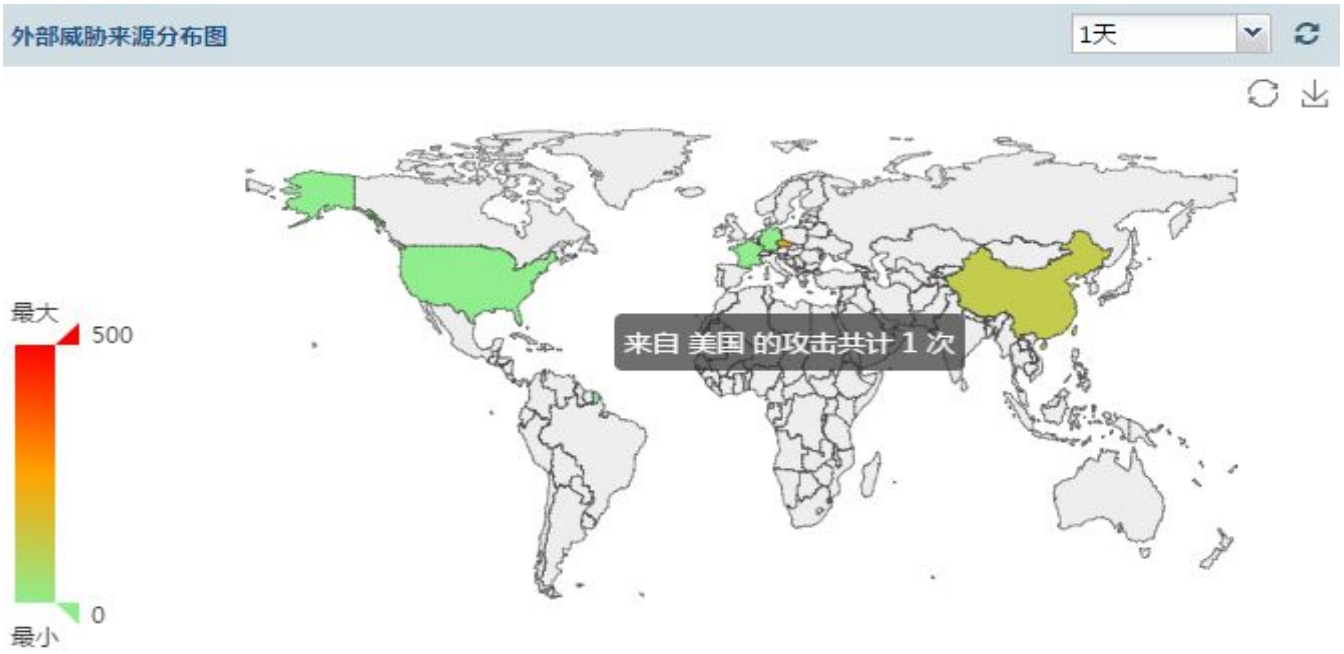
- CPU： 显示当前设备的 CPU 使用情况。
- 内存： 显示当前设备的内存使用情况。
- 磁盘： 显示当前设备的磁盘使用情况，当磁盘空间不足时，会向管理员发送邮件提醒，并且会自动清理磁盘。如果需要手动清理磁盘，请参考磁盘日志清理。

提示：

本设备会尽可能多的使用内存以便提高性能，因此内存占用较大（超过 80%）是正常现象。

7.4 外部威胁来源分布图

显示本设备每天所受到的外部威胁来源分布，以便快速定位所遭受的网络攻击来源状况。

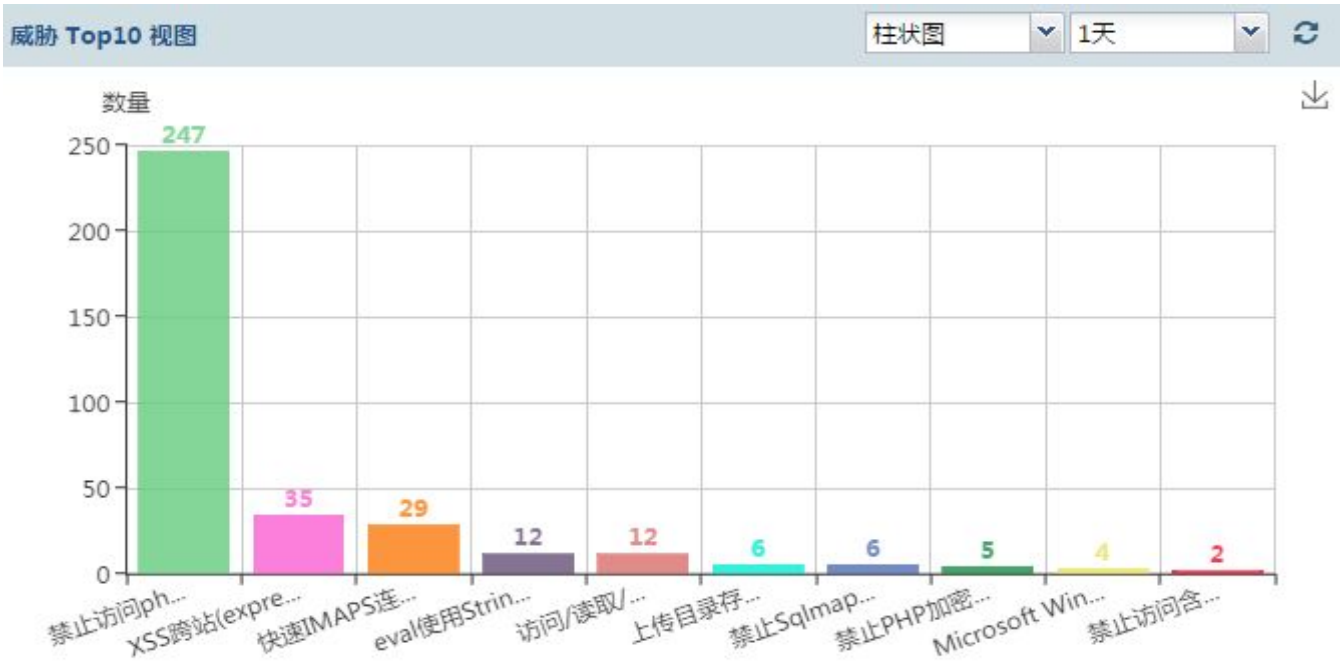


7.5 威胁 IP Top10 视图

显示入侵的地址以及地址的位置和数量，快速显示受哪些地址的影响最大。

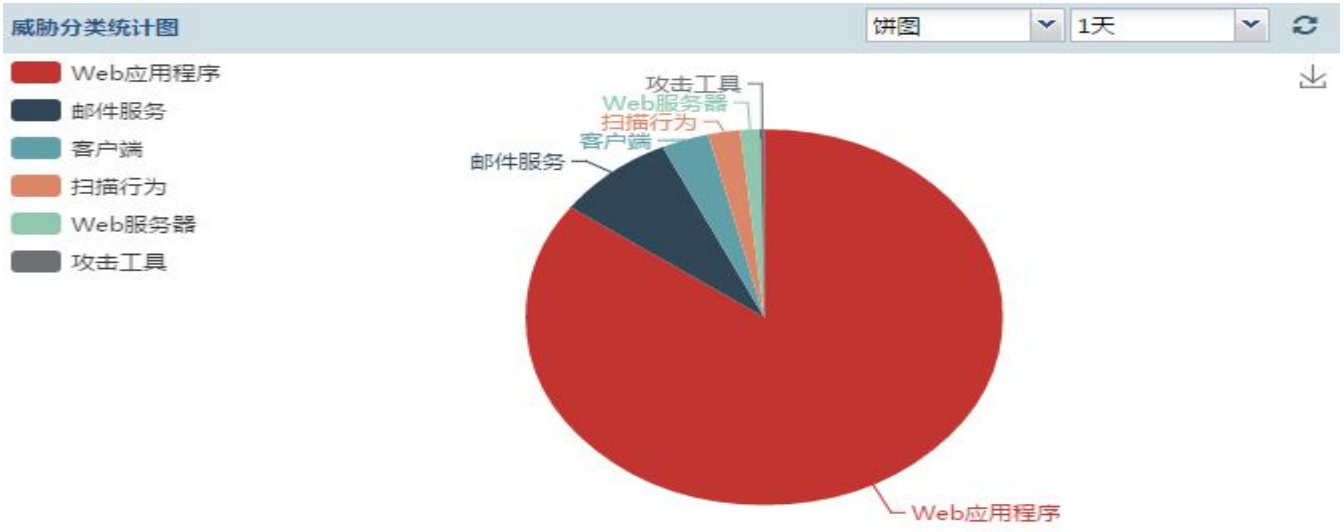
7.6 威胁 Top 10 视图

显示总攻击中占比最高的前 10 类以及次数。



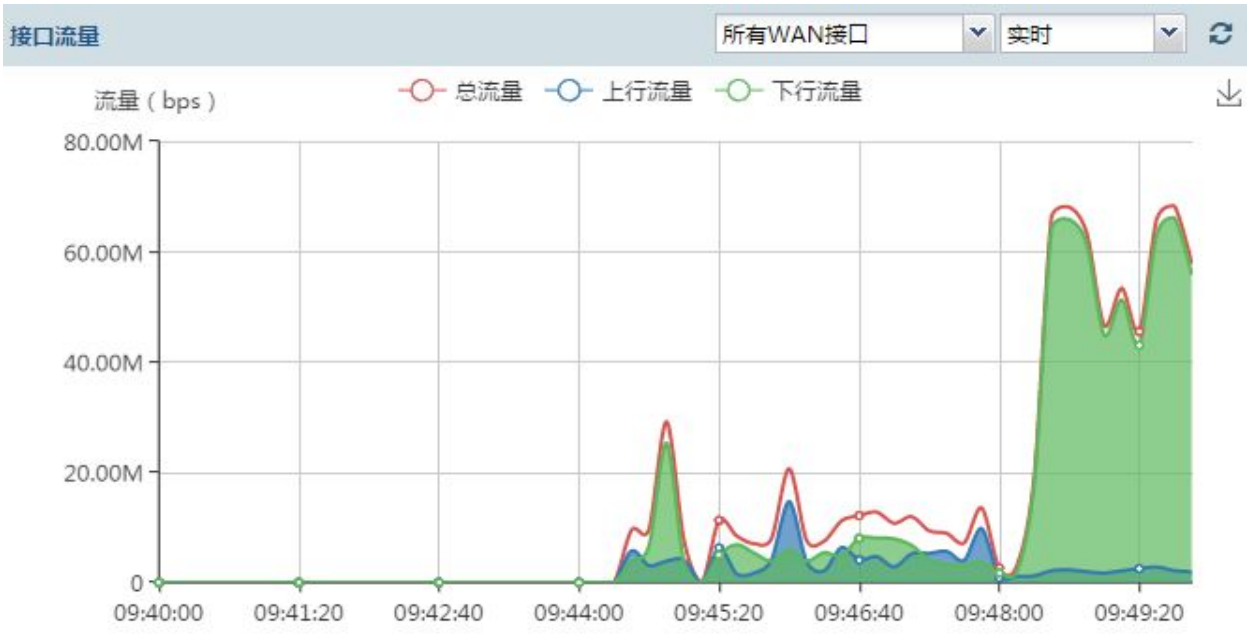
7.7 威胁分类统计图

显示本设备入侵触发的规则类别与数量，以便快速掌握系统遭受的网络攻击并判断网络攻击状况。



7.8 接口流量

监测每一个网口的实时流量。



7.9 网络接口

用于显示设备当前的网络接口。

网络接口

接口名称	接口描述	连接状态	IPv4地址	子网掩码	网关/下一跳地...	属性
ETH0(默认出口)	电信20兆		218	255.255.255.0	218	WAN,DFLT
ETH1	移动30兆		221.	255.255.255....	221.	WAN
ETH2			100	255.255.255....	100	PPPoE(PPP0),...
ETH3	1网段		192.168.	255.255.255.0	*	LAN
ETH4	8网段		192.168	255.255.255.0	*	LAN
ETH5			192.168	255.255.255.0	*	LAN
ETH6			192.168	255.255.255.0	*	DMI,LAN
ETH7			192.168	255.255.255.0	*	DSI

7.10 系统运行日志

用于显示设备运行过程的重要系统日志。

序号	操作时间	日志内容	操作
15	2016-03-01 11:15:19	防火墙引擎启动	
14	2016-03-01 11:14:34	防火墙引擎停止	
13	2016-03-01 10:47:25	防火墙引擎重启	
12	2016-03-01 09:52:27	防火墙引擎重启	
11	2016-03-01 01:00:16	发送Email，名称：Auto Report,2016-03-01 01:00:02	
10	2016-02-29 14:54:29	防火墙引擎重启	
9	2016-02-29 14:54:07	防火墙引擎重启	

7.11 设备信息

用于显示本设备的硬件版本、固件版本、系统版本、规则版本、产品型号和产品序列号。

⚠注意：

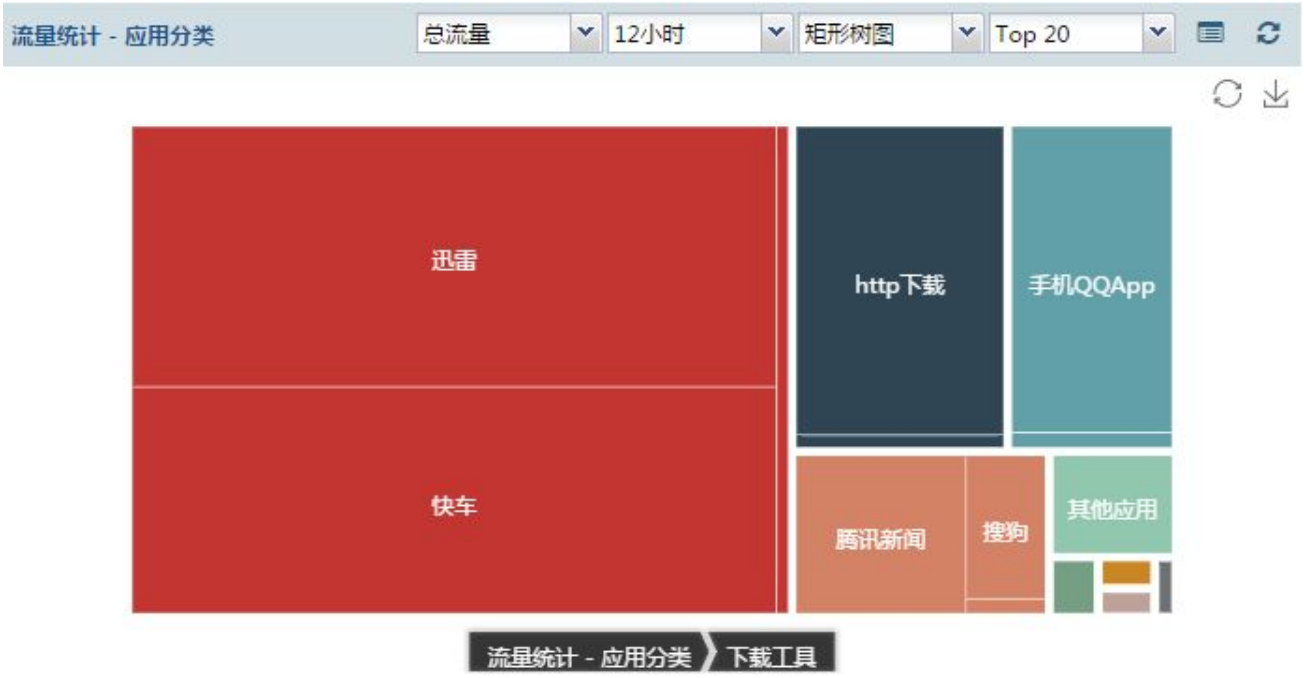
请记录下您使用产品的“产品序列号”等重要信息，以便在设备升级或出现故障的情况下，快速向铱迅客服人员请求帮助

7.12 布局换肤

用于显示监控页面的板块布局与颜色，可以根据个人需要进行设置。

7.13 流量统计-应用分类

用于显示一段时间内，基于应用分类的流量统计。



7.14 流量统计-应用

用于显示一段时间内，基于应用的流量统计。

7.15 流量统计-IP

用于显示一段时间内，基于应用 IP 的流量统计。

7.16 实时流量-应用分类

实时显示各个应用分类的流量状况。

实时流量 - 应用分类

应用分类	上行流量	下行流量	总流量
下载工具	200B	56B	256B
未知应用分类	60B	116B	176B

7.17 实时流量-应用

实时显示各个应用的流量状况。

实时流量 - 应用

应用	上行流量	下行流量	总流量
迅雷	591B	342B	933B
未知应用	140B	154B	294B
QQ	82B	64B	146B
腾讯新闻	40B	40B	80B

7.18 实时流量-IP

实时显示各个 IP 的流量状况。

实时流量 - IP

IP地址	备注	上行流量	下行流量	总流量
19 18		90B	170B	260B
11 57		58B	30B	88B
24 24		56B	30B	86B
20 7		56B	30B	86B

7.19 新建连接数

实时显示本设备，新建连接数状况。

7.20 并发连接数

实时显示本设备，并发连接数状况。

8. 数据中心

8.1 入侵事件

8.1.1 入侵记录

用于显示被本设备拦截的入侵记录，显示的具体内容包括：序号、攻击时间、规则编号、规则分类、动作类型、危害等级、来源 IP、地理位置、目的 IP、协议、来源端口、目的端口、操作，具体如下图所示。入侵记录列表中不同的颜色代表了不同优先级，红色代表该条入侵记录的优先级最高，黄色代表该条入侵记录的优先级是中等，白色代表该条入侵记录的优先级是轻微。

序号	最后攻击时间	规则编号	规则名称	规则分类	动作...	危害...	来源IP	地理位置	目的IP	协议	来源...	目的...	攻...	操作
198	2016-03-04 1...	1650418	Checkpoint Firewall-1 HTTP解析格...	WEB应用	检测	中	5.9.63.149	德国	192.168.1.70	TCP	58870	80	2	
196	2016-03-04 1...	2510217	Microsoft OLE复合文件Flowbit魔法...	其它客户端	检测	低	192.168.	LAN	123.150.241....	TCP	80	9257	2	
194	2016-03-04 1...	1080325	Microsoft Internet Explorer HP Ph...	Activex攻...	检测	低	192.168	LAN	69.30.214.42	TCP	80	41121	11	
183	2016-03-04 1...	1080397	疑似LEADTOOLS ActiveX Raster T...	Activex攻...	检测	中	192.168.	LAN	69.30.214.42	TCP	80	35845	6	
177	2016-03-04 1...	1670046	快速IMAPS连接 - 疑似暴力破解攻击	IMAP服务	检测	高	223.104.15.1...	内蒙古呼和浩...	192.168	TCP	38164	993	16	
176	2016-03-04 1...	1670046	快速IMAPS连接 - 疑似暴力破解攻击	IMAP服务	检测	高	223.104.4.52	江苏省南京市...	192.16	TCP	43266	993	1	
174	2016-03-04 1...	1650418	Checkpoint Firewall-1 HTTP解析格...	WEB应用	检测	中	91.121.221.15	法国	192.168.	TCP	59164	80	4	
170	2016-03-04 1...	1650870	ASP/JSP源码泄露输出	WEB应用	检测	中	106.39	北京市 电信	192.168	TCP	80	57835	1	
169	2016-03-04 1...	1650891	SQL信息泄露 v6	WEB应用	检测	中	221.10.66.56	四川省巴中市...	192.168	TCP	80	43698	2	
168	2016-03-04 1...	1650896	IIS信息泄漏 v2	WEB应用	检测	中	221.10.66.56	四川省巴中市...	192.168	TCP	80	43698	2	
165	2016-03-04 1...	1650870	ASP/JSP源码泄露输出	WEB应用	检测	中	219.136.245....	广东省广州市...	192.168	TCP	80	53805	1	

- 选择查看日期： 您可以在“请选择查看日期”右侧点击日历图标，如图，在弹出的日历窗口中选择某一个日期。或者您也可以手工输入需要查看记录的日期，请注意输入日期的格式，例如：2015-03-03。

- 查询记录： 在选定某个日期后，可以快速查看指定日期的所有入侵记录。如果当天记录超过 30 条，会以多页的形式显示出来，可以通过翻页功能来查看指定日期的所有记录。
- 删除入侵记录： 选择一条或者多条记录后，点击【删除】按钮可以将所选择的记录删除掉。如需删除多日的入侵记录，请参考磁盘日志清理。
- 刷新： 如果需要从数据库中重新获取指定日期的入侵记录，请点击【刷新】按钮。
- 入侵记录排序：当把鼠标箭头放在列名上时，例如：规则编号，右侧会出现一个向下箭头，点击此向下箭头，在出现的菜单中可以对当前列表进行正序或逆序排序，还可以选择只显示某些列，如图。

- 查看入侵记录的详细信息： 当您双击一条记录时，会显示该记录的详细信息，如图：

- 入侵记录中对规则停用功能添加：在一条入侵记录上点击右键，会弹出对话框，可选择禁用此条规则，如图。：

- 攻击时间：记录入侵的开始时间。
- 源 IP 地址：记录入侵的来源 IP 地址。
- 目的 IP 地址：记录入侵要到达的目的 IP 地址。
- 危害等级：描述入侵记录的危害程度。
- 参考信息：针对此类攻击的参考信息。

提示：

本设备会尽可能的保存所有的历史日志，但如果保存的历史日志达到了磁盘空间的设置上限 5000 条，本设备会自动执行磁盘清理，删除过期的日志。

筛选入侵记录

在入侵记录数量特别大的时候，可能需要在入侵记录中筛选出符合条件的记录，以便于进一步的分析。

在【入侵记录】页面上点击【筛选】按钮，弹出“入侵记录-筛选”对话框。在此对话框中输入需要筛

选的条件，点击【开始筛选】按钮后，【入侵记录】页面中将只显示符合条件的入侵记录。

如果某项内容不填写，则表示忽略该项的筛选条件。用户可以在【入侵记录】页面上点击【取消筛选】按钮以恢复筛选之前的列表。

提示:

选择某条记录后点击【筛选】按钮，系统会自动将该条入侵记录的内容填充至筛选对话框中。

导出入侵记录

在【入侵记录】页面上点击【导出日志】按钮，将指定日期的入侵记录导出并以 csv 文件格式保存，如图。用户可以用 Microsoft Excel 等工具查看。如需导出多日的入侵记录，请参考磁盘清理。

入侵记录的右击菜单

在【入侵记录】页面右击某条入侵记录，出现如下图的右击菜单，提供各种快捷操作。针对该条入侵记录，可以进行例如：设置此规则为检测，设置此规则为拦截等操作。

该菜单提供的功能具体说明如下：

- 设置来源 IP 为“检测”：使用后会将此规则设置为“检测”模式，您可以进入【策略配置】-【规则配置】中得【内置规则】或者【自定义规则】选择此规则，查看规则属性。
- 设置来源 IP 为“丢弃”：使用后会将规则设置为“丢弃”模式。【策略配置】-【规则配置】中得【内置规则】或者【自定义规则】选择此规则，查看规则属性。
- 设置目的 IP 为“拦截”：使用后会将规则设置为“拦截”模式。【策略配置】-【规则配置】中得【内置规则】或者【自定义规则】选择此规则，查看规则属性。
- 禁用此条规则：使用后会将规则设置为“停用”模式，不再对该条规则进行检测。您可以进入【策略配置】-【规则配置】中的【禁用规则列表】查看所有被禁用的规则。

ⓘ提示：

本设备会尽可能的保存所有的历史日志， 但如果保存的历史日志达到了磁盘空间的设置上限，本设备会自动执行磁盘清理，删除过期的日志。

8.1.2 入侵查询

该页面提供对入侵记录根据时间、动作类型、来源 IP、目的 IP、规则编号、规则分类、来源端口、目的端口、危害等级、协议进行条件组合查询的功能，同时对查询的结果，提供报表生成和日志导出的功能。

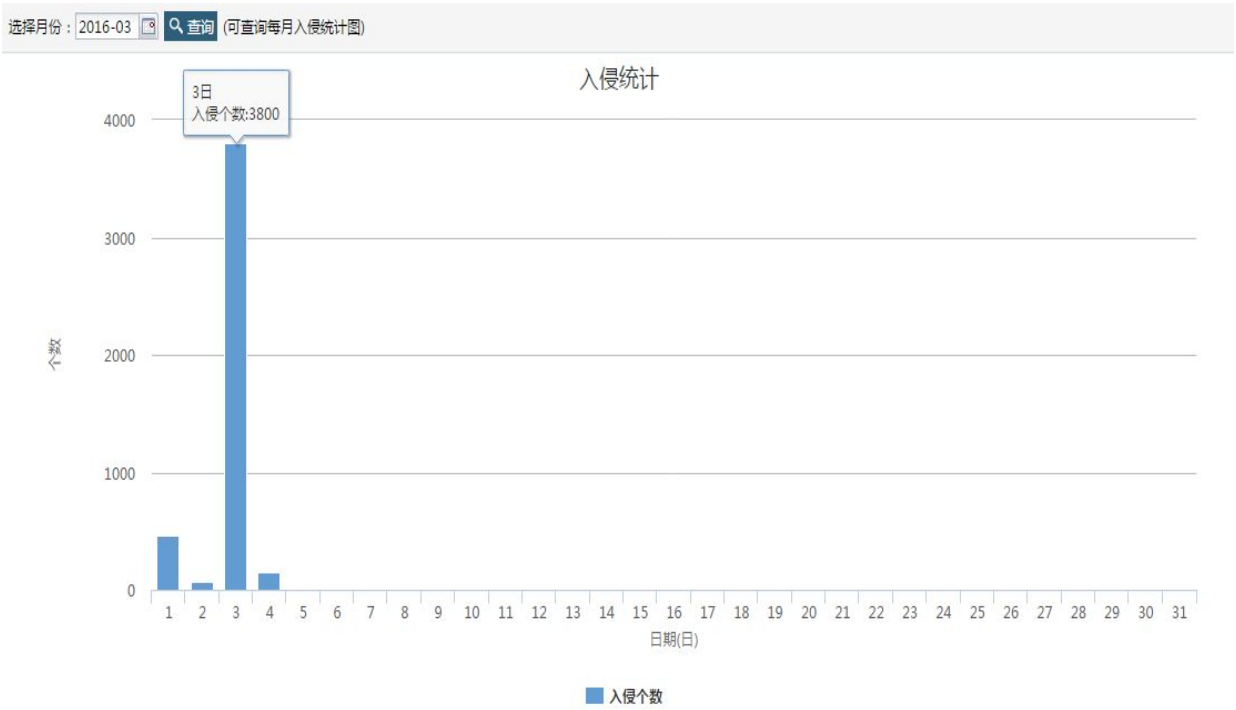
- 根据时间查询入侵记录：设置“开始时间”和“结束时间”，点击【开始查询】，即可查询出该日期范围内的所有入侵记录。
- 根据规则编号查询入侵记录：填写拦截原因例如“2450017”，点击【开始查询】，即可查询出该日期范围内的所有拦截原因为“2450017”的入侵记录。
- 根据来源 IP 查询入侵记录：在文本框中写入来源 IP 例如“192.168.1.14”，点击【开始查询】，即可查询出该日期范围内的所有来源 IP 为“192.168.1.14”的入侵记录。
- 根据目的 IP 查询入侵记录：在文本框中写入目的 IP 例如“192.168.1.15”，点击【开始查询】，即可查询出该日期范围内的所有目的 IP 为“192.168.1.15”的入侵记录。
- 根据规则类别查询入侵记录：在下拉菜单中选择规则类别例如“操作系统”，点击【开始查询】，即可查询出该日期范围内的所有规则类别为“操作系统”的入侵记录。
- 根据源端口查询入侵记录：在文本框中写入源端口号，例如“5326”，点击【开始查询】，即可查询出该日期范围内的所有源端口号为“5326”的入侵记录。
- 根据目的端口查询入侵记录：在文本框中写入目的端口号，例如“80”，点击【开始查询】，即可查询出该日期范围内的所有目的端口号为“80”的入侵记录。
- 根据拦截方式查询入侵记录：在下拉框中选择拦截方式例如“拦截”，点击【开始查询】，即可查询出该日期范围内的所有拦截方式为“拦截”的入侵记录。
- 根据协议查询入侵记录：在下拉菜单中选择协议例如“TCP”，点击【开始查询】，即可查询出该日期范围内的所有协议为“TCP”的入侵记录。
- 对查询的结果使用右键加强功能：具体参考 入侵记录的右击菜单。将查询后的结果生成报表：查询出所需要的入侵记录，在下拉菜单中选择“HTML 格式”或者“DOC 格式”，点击【生成报表】出现以下提示：

HTML 格式直接点击生成的链接就可以在浏览器中查看。DOC 格式的请点击生成的链接下载到本机后，再使用“Microsoft Office Word”工具打开即可查看。

将查询后的结果导出：查询出所需要的入侵记录，点击【导出日志】，在弹出的下载框中点击保存，下载完成后使用“Microsoft Office Excel”等工具打开即可。

8.1.3 入侵统计

该页面以柱状图的形式显示指定月份内所发生的所有入侵事件。您可以输入或者选择月份来查询历史月份的入侵统计，了解本设备在该月份每天所检测到的入侵事件数目，以便快速掌握不同日期遭受网络攻击的状况，判断网络攻击变化的趋势。



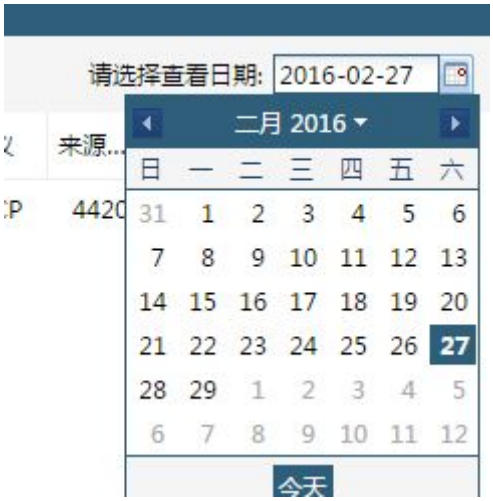
8.1.4 防病毒记录

防病毒记录：记录病毒攻击的时间、病毒名称、源 IP 地址、地理位置、目的 IP 地址等详细信息。并支持快速查询和导出日志功能。

查看防病毒记录

用于显示被本设备拦截的防病毒记录，显示的具体内容包括：序号、最后攻击时间、病毒名称、来源 IP、地理位置、目的 IP、协议、来源端口、目的端口、攻击次数，具体如下图所示。

- 选择查看日期： 您可以在“请选择查看日期”右侧点击日历图标，如图，在弹出的日历窗口中选择某一个日期。或者您也可以手工输入需要查看记录的日期，请注意输入日期的格式，例如：2015-03-10。



- 查询记录： 在选定某个日期后，可以快速查看指定日期的所有防病毒记录。如果当天记录超过 30 条，会以多页的形式显示出来，可以通过翻页功能来查看指定日期的所有记录。
- 删除防病毒记录： 选择一条或者多条记录后，点击【删除】按钮可以将所选择的记录删除掉。如需删除多日的入侵记录，请参考磁盘日志清理。
- 刷新： 如果需要从数据库中重新获取指定日期的防病毒记录记录，请点击【刷新】按钮。

- 入侵记录排序：当把鼠标箭头放在列名上时，例如：协议，右侧会出现一个向下箭头，点击此向下箭头，在出现的菜单中可以对当前列表进行正序或逆序排序，还可以选择只显示某些列，如图。

- 查看入侵记录的详细信息： 当您双击一条记录时，会显示该记录的详细信息。

提示：

本设备会尽可能的保存所有的历史日志，但如果保存的历史日志达到了磁盘空间的设置上限，本设备会自动执行磁盘清理，删除过期的日志。

8.1.5 DDOS 记录

该页面记录了所有的 DDOS 攻击事件，您可以通过本页面了解所有发生的 DDOS 攻击事件，可以实时的看到被加入黑名单中的 IP。

- 删除：选中某条记录，点击【删除】即可删除该条记录。

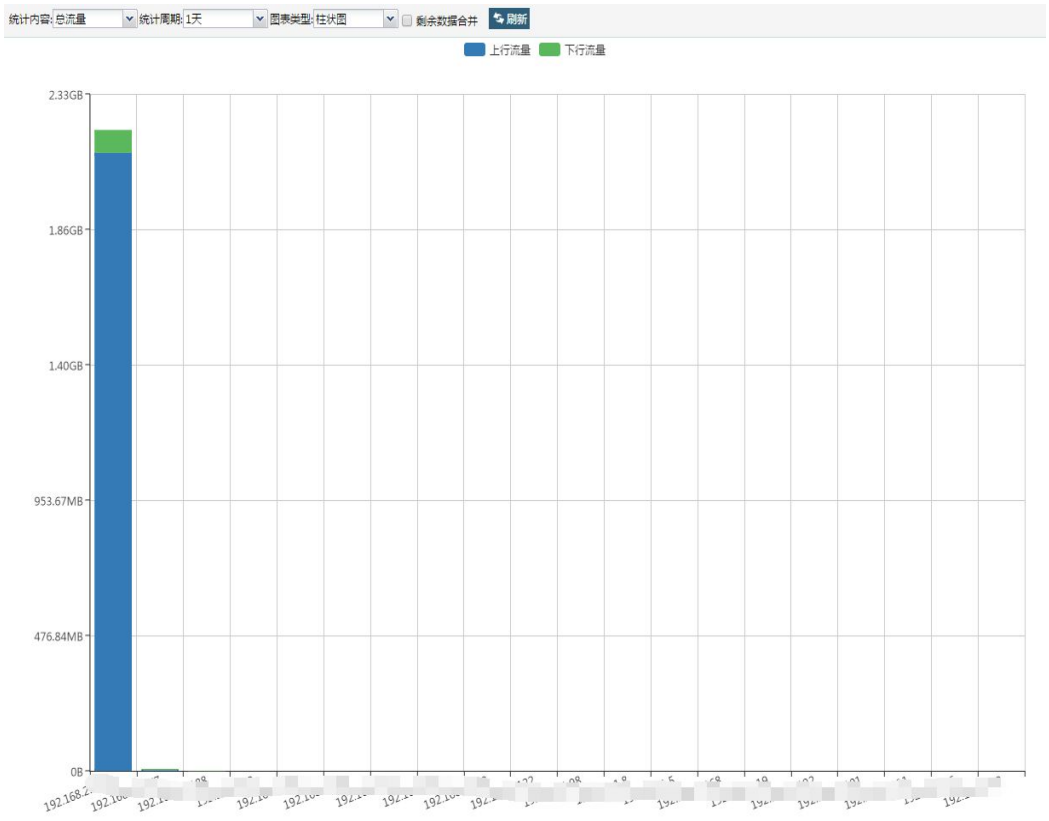
- 筛选：根据日志内容和时间进行筛选。例如查找所有 192.168.11.17 在 2015 年 3 月 10 日的相关的 DDOS 日志，点击【筛选】就可以筛选出所有的符合条件的 DDOS 日志。
- 清空：将现有的 DDOS 记录清除。
- 刷新：将对应的 DDOS 记录进行刷新。

8.2 监视

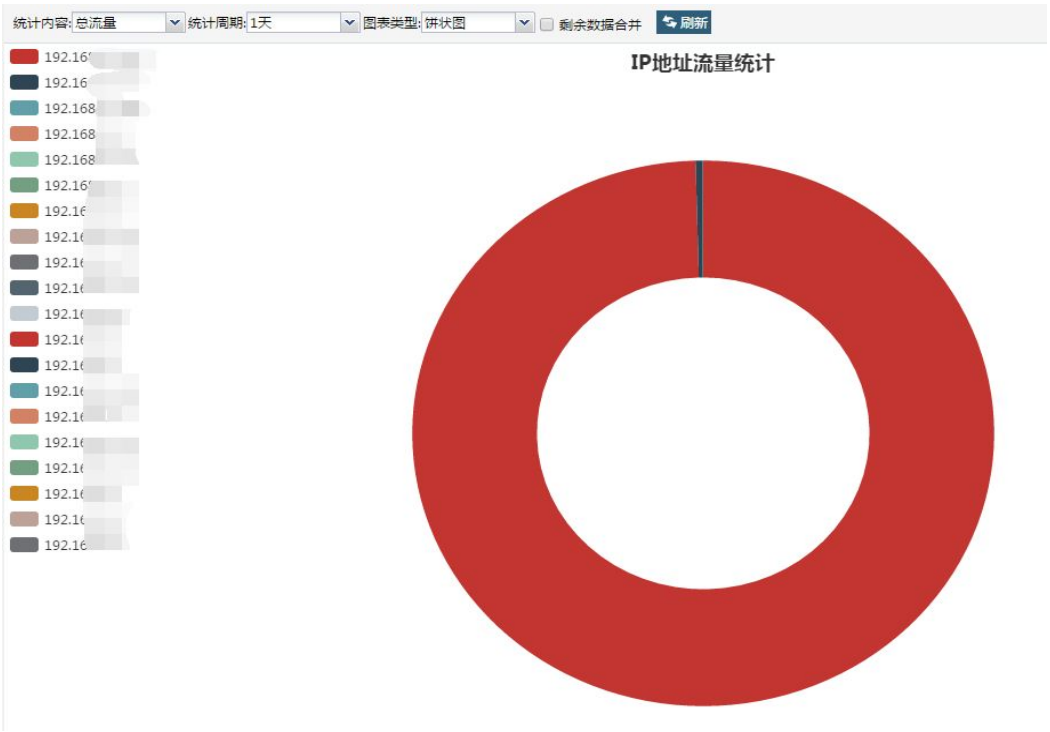
8.2.1 IP 地址流量统计

该页面统计并显示各个 IP 地址的网络流量，可以以柱状图、饼状图、表格、矩形树图的形式显示出来。您可以选择时间段，了解本设备在该时间段内的网络流量，流量以字节（bytes）为单位。

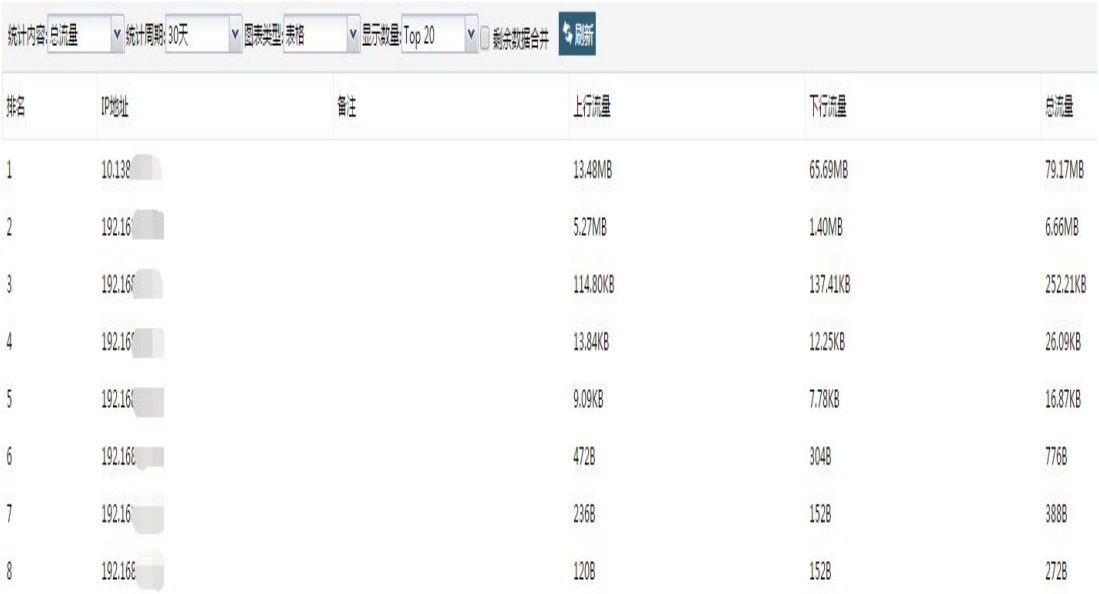
柱状图：



饼状图：



表格：



排名	IP地址	备注	上行流量	下行流量	总流量
1	10.138		13.48MB	65.69MB	79.17MB
2	192.16		5.27MB	1.40MB	6.66MB
3	192.16		114.80KB	137.41KB	252.21KB
4	192.16		13.84KB	12.25KB	26.09KB
5	192.16		9.09KB	7.78KB	16.87KB
6	192.16		472B	304B	776B
7	192.16		236B	152B	388B
8	192.16		120B	152B	272B

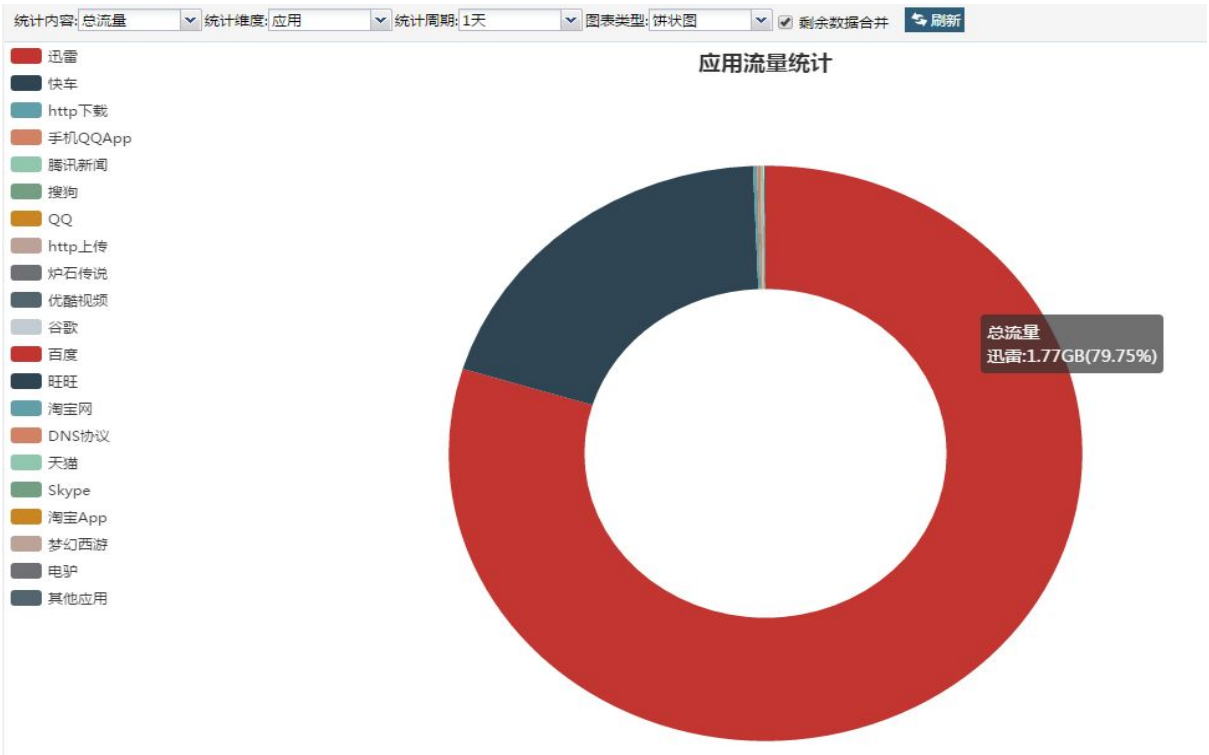
8.2.2 应用流量统计

该页面统计并显示各个应用、应用分类的网络流量，可以以柱状图、饼状图、表格、矩形树图的形式显示出来。您可以选择时间段，了解本设备在该时间段内的网络流量，流量以字节（bytes）为单位。

柱状图：


统计内容: 总流量
统计维度: 应用
统计周期: 1天
图表类型: 柱状图
剔余数据合并
刷新
上行流量
下行流量
1.96GB
1.68GB
1.40GB
1.12GB
858.31MB
572.20MB
286.10MB
0B
旺旺
总流量: 71.85KB
上行流量: 2.77KB
下行流量: 69.08KB
迅雷
快车
http下载
手机QQApp
腾讯新闻
搜狗
QQ
http上传
炉石传说
优酷视频
谷歌
百度
旺旺
淘宝网
DNS协议
天猫
Skype
淘宝App
梦幻西游
电驴

饼状图:

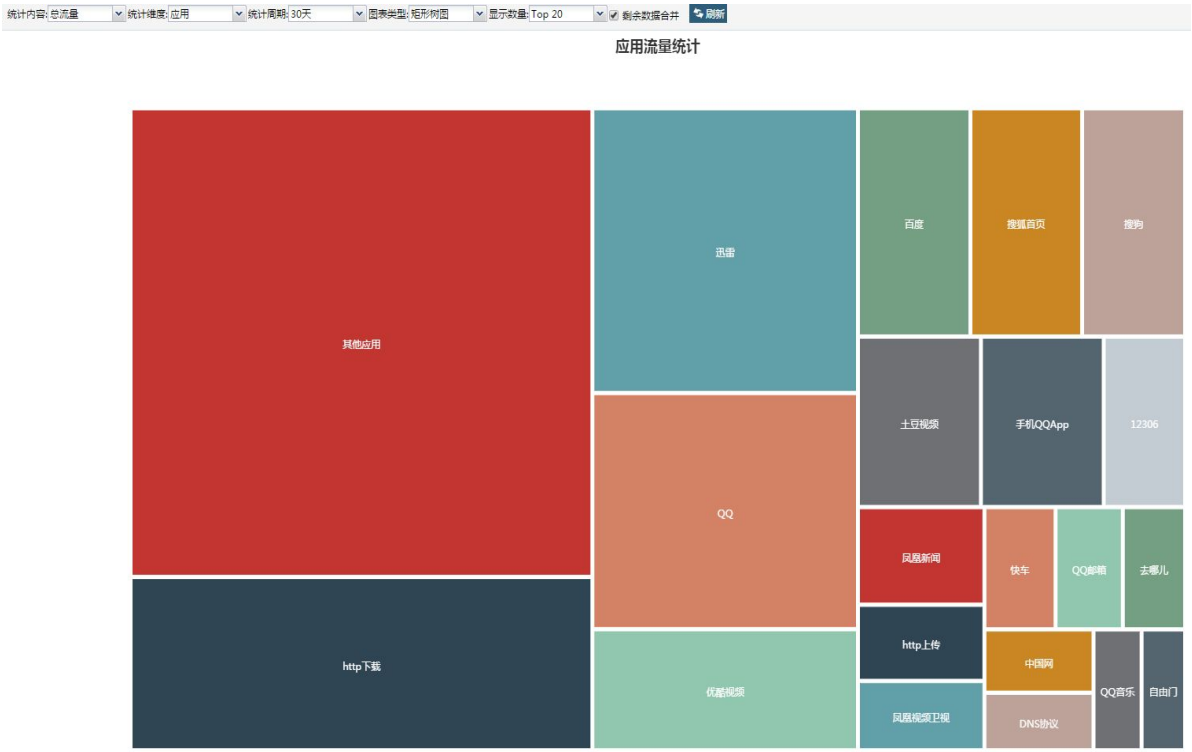

统计内容: 总流量
统计维度: 应用
统计周期: 1天
图表类型: 饼状图
剔余数据合并
刷新
应用流量统计
迅雷
快车
http下载
手机QQApp
腾讯新闻
搜狗
QQ
http上传
炉石传说
优酷视频
谷歌
百度
旺旺
淘宝网
DNS协议
天猫
Skype
淘宝App
梦幻西游
电驴
其他应用
总流量
迅雷:1.77GB(79.75%)

表格:

统计内容: 总流量 统计维度: 应用 统计周期: 30天 图表类型: 表格 显示数量: Top 20 剩余数据合并 刷新

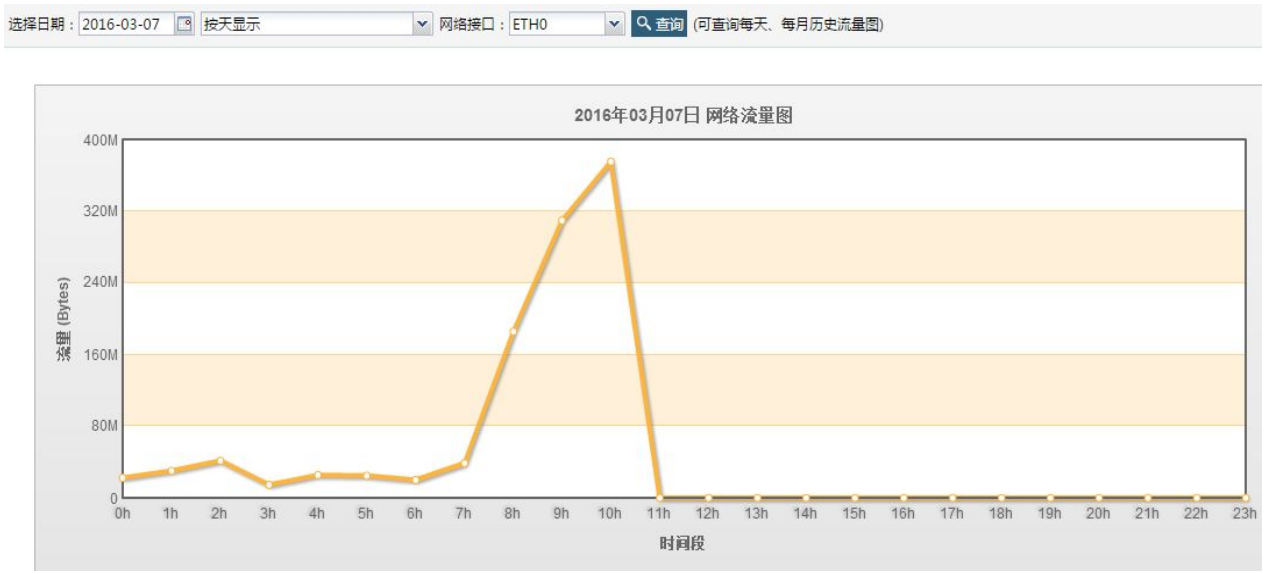
排名	应用	上行流量	下行流量	总流量
1	http下载	1.77MB	8.42MB	10.19MB
2	迅雷	659.00KB	8.98MB	9.62MB
3	QQ	529.31KB	7.46MB	7.98MB
4	优酷视频	90.06KB	4.01MB	4.09MB
5	百度	772.33KB	2.51MB	3.26MB
6	搜狐首页	884.86KB	2.38MB	3.24MB
7	搜狗	669.83KB	2.34MB	2.99MB
8	土豆视频	49.77KB	2.62MB	2.67MB
9	手机QQApp	86.03KB	2.58MB	2.66MB
10	12306	209.90KB	1.56MB	1.76MB
11	凤凰新闻	419.28KB	1.16MB	1.57MB
12	http上传	366.58KB	888.80KB	1.23MB
13	凤凰视频卫视	152.59KB	990.53KB	1.12MB
14	快车	122.42KB	1010.63KB	1.11MB
15	QQ邮箱	352.73KB	718.78KB	1.05MB
16	去哪儿	28.68KB	963.52KB	992.20KB
17	中国网	57.62KB	842.42KB	900.04KB
18	DNS协议	233.44KB	585.51KB	818.95KB
19	QQ音乐	34.68KB	722.80KB	757.48KB
20	自由门	178.00KB	507.40KB	685.40KB
21	其他应用	11.35MB	16.18MB	27.53MB

矩形树图：



8.2.3 接口历史流量

该页面统计并显示 WAN 接口的网络流量，可以按天或者按月以折线图的形式显示出来。您可以输入或者选择日期，了解本设备在该时间段内的网络流量，流量以字节（bytes）为单位。



8.2.4 IP 地址实时流量

该页面实时显示各个 IP 地址的网络流量，按表格的形式显示出来。您可以选择 Top 20、Top 50、Top 100，了解本设备在实时的网络流量，流量以字节（bytes）为单位。


显示数量: Top 50 自动刷新: 5秒 刷新

排名	IP地址	备注	上行流量	下行流量	总流量
1	192.16		5.94KB	5.04KB	10.98KB
2	111.13.		660B	2.80KB	3.44KB
3	119.188.1		1.94KB	690B	2.62KB
4	122.193.4		392B	1000B	1.36KB
5	114.114.1		777B	388B	1.14KB
6	106.120.1		456B	472B	928B
7	123.125.1		456B	120B	576B
8	182.118.12		196B	228B	424B
9	121.10.12		48B	209B	257B
10	120.210.1		136B	80B	216B
11	221.222.2		56B	30B	86B

8.2.5 应用实时流量

该页面实时显示各个应用的网络流量，按表格的形式显示出来。您可以选择 Top 20、Top 50、Top 100，了解本设备在实时的网络流量，流量以字节（bytes）为单位。

统计标准: 应用 Top 20 自动刷新: 5秒 刷新

排名	应用	上行流量	下行流量	总流量
1	迅雷	505.85KB	11.24MB	11.73MB
2	快车	617.38KB	51.91KB	669.30KB
3	http下载	109.61KB	547.27KB	656.89KB
4	未知应用	46.56KB	357.41KB	403.97KB
5	优酷视频	22.83KB	263.33KB	286.16KB
6	QQ	9.41KB	232.41KB	241.82KB
7	同花顺App	11.28KB	164.44KB	175.73KB
8	http上传	20.98KB	43.71KB	64.70KB
9	SSH协议	12.97KB	42.00KB	54.97KB
10	QQ音乐	4.63KB	47.42KB	52.05KB
11	58同城	20.86KB	24.24KB	45.10KB
12	中国政府网	28.28KB	9.60KB	37.89KB
13	淘宝网	4.90KB	10.83KB	15.72KB
14	QQ游戏	400B	11.72KB	12.11KB
15	淘宝App	2.32KB	8.75KB	11.07KB
16	六间房	3.59KB	4.01KB	7.60KB
17	谷歌	2.90KB	4.11KB	7.01KB
18	新浪首页	2.84KB	3.66KB	6.50KB
19	自由门	1.38KB	4.20KB	5.58KB
20	DNS协议	1.76KB	3.71KB	5.48KB

8.2.6 接口实时流量

用于显示各个网络接口的实时流量信息，如图。

刷新

网络接口	模式	速率	连接状态	收到的数据包	发送的数据包	收到的字节	发送的字节	收到的错误包	丢失接收的包	接收速率	发送速率
ETH0	全双工	100 Mbps		278778951	637934139	236.48 GB	167.93 GB	0	442148	14.42 Kbps	14.57 Kbps
ETH1	全双工	100 Mbps		246166172	303764200	246.28 GB	112.45 GB	0	0	29.27 Mbps	1.54 Mbps
ETH2	全双工	1000 Mbps		181269287	198468910	140.09 GB	144.38 GB	1	17458	20.94 Mbps	2.23 Mbps
ETH3	全双工	1000 Mbps		42926884	33254657	36.31 GB	9.06 GB	0	0	263.71 Kbps	25.08 Kbps
ETH4	全双工	100 Mbps		213743129	187909692	160.82 GB	150.87 GB	0	0	1.55 Mbps	20.18 Mbps
ETH5	全双工	1000 Mbps		2109533356	606589846	377.25 GB	378.05 GB	58	251331	93.07 Mbps	30.21 Mbps
ETH6	全双工	1000 Mbps		249922769	302990647	114.12 GB	265.55 GB	827	0	1.61 Mbps	92.43 Mbps
ETH7		自动		0	0	0	0	0	0	0	0

8.3 报表

该模块提供按指定日期生成 HTML、DOC、DOCX 和 PDF 格式报表的功能。可以对生成的报表进行管理，能够按照设置自动生成报表并且发送至管理员邮箱。

8.3.1 报表管理

该页面提供了对已经生成的报表进行管理和导出的功能。

- 删除：选择某条记录，点击【删除】，在弹出的对话框点击【确定】即可删除此条报表。
- 刷新：点击【刷新】按钮，即可刷新该页面。
- 导出：选择某条记录，点击【导出】，即可导出该条记录所对应的报表。双击选中的记录，也能够导出该条记录所对应的报表。
- 快速查询：可以输入任意字符，对报表名称进行匹配查询操作。

8.3.2 即时报表

该页面能够按照选择的报表类型、日期范围、输入格式立刻生成对应的报表。

- 攻击报表：针对入侵记录生成的攻击行为分析报表。
- 流量报表：针对系统端口的流量生成的流量报表。
- 日期范围：可以选择最近一个月，最近一周，当天，或者自定义统计范围。
- 输入格式：可以选择 HTML、DOC、PDF 的格式。
- 说明：可以为生成的报表填写相关说明信息。

⚠注意：

点击【生成报表】，会在该表单下方显示出该报表的链接，点击即可进行打开操作，报表也会自动保存至“报表管理”页面，可以进入“报表管理”页面进行导出操作。

8.3.3 定期报表

该页面提供了对定期报表进行配置的功能。设置自动生成报表的类型、时间、格式、是否邮件发送等配置信息。

- 报表包含的日志类型：可以根据需要选择不同的报表类型。
- 选择日期：每天（默认在每天的一点钟生成），每周（默认在每个星期日的一点钟生成），每月（默认在每月的第一天的一点钟生成）。
- 选择邮件发送：如果开启将会自动将报表发送至管理员邮箱。
- 输出格式：可以选择 PDF，DOC，HTML。
- 说明：可以填写定期报表的说明。

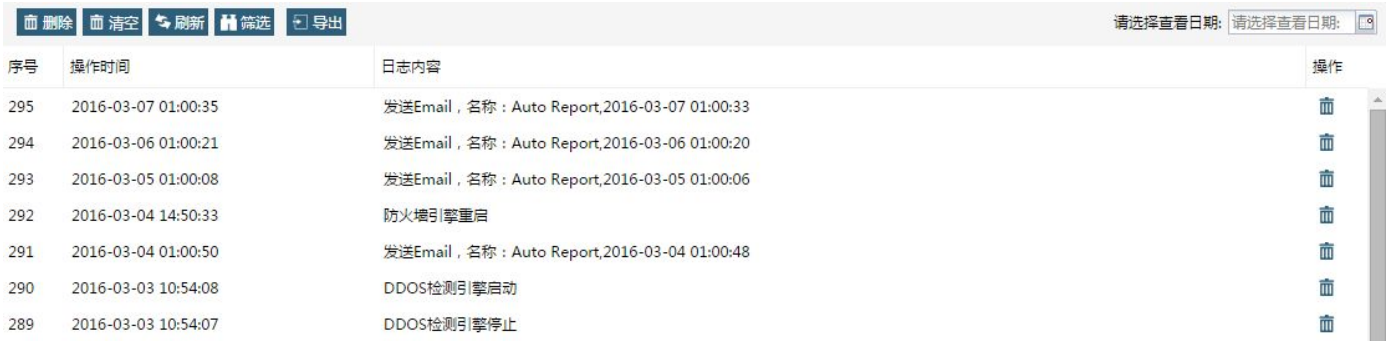
⚠注意：

如果需要开启邮件发送的功能，请先配置好邮件通知，具体请参照：通知设置。

8.4 日志

8.4.1 系统日志

系统日志页面显示了本设备上的系统事件如图，您可以通过查询日志了解本设备上所发生的所有系统事件。



- 快速查询： 在右上侧选择或者输入指定日期，点击【快速查询】按钮，可以查询指定日期的系统日志。
- 导出日志： 选择某个日期，点击【导出日志】按钮，导出指定日期的日志信息，以 csv 文件形式保存，您可以选择用 Microsoft Excel 等工具查看导出的系统日志文件。
- 日志筛选：点击【筛选】按钮，弹出“系统日志-筛选“对话框，如下图。您可以组合日期和日志包含内容条件，筛选出需要查看的系统日志。

- 取消筛选：点击【取消筛选】按钮，可以取消已经筛选出的日志列表，恢复到正常状态。
- 清空：点击【清空】按钮，即可删除所有系统日志。
- 删除：选择一条或者多条系统日志，点击【删除】按钮，这些系统日志将被从系统中删除。

⚠注意：

系统会根据当前的磁盘空间上限设置，自动定期执行日志清理工作。如果需要保留日志，请参见磁盘日志清理。

8.4.2 PPPoE 日志

PPPoE 日志记录了 PPPoE 拨号上网的所有记录,您可以查阅 PPPoE 日志来判断 PPPoE 不能成功拨号的原因。

9. 策略配置

9.1 9.1 策略配置

9.1.1 访问控制

访问控制是指按用户及其所属于的策略条件来控制其访问权限，即当匹配策略的所有控制条件时，允许或阻塞对网络的访问。安全策略提供记录日志功能及日志转发功能，当安全策略为允许时，可以设定防病毒策略、规则防护策略功能。界面如下图所示：

1. 添加：点击“添加”，弹出”访问控制-添加”窗口，输入名称、描述，配置生效时间、规则防护策略、防病毒策略、控制条件和策略动作，新建访问控制。
2. 删除：选择策略后，该按钮呈可选择状态；点击“删除”可以删除所选择的策略。
3. 启用：选择策略后，该按钮呈可选择状态；点击“启用”可以启用所选择的策略。

4. 停用：选择策略后，该按钮呈可选择状态；点击“ 停用”可以禁用所选择的策略。

5. 置顶：配置多条策略，选择一条排在后面的策略，该按钮呈可选择状态；点击“ ”可以将所选策略的优先级置为同级策略中最高。

6. 上移：选择一条策略后，点击“ 上移”，该策略的位置上升一位，即优先级提升一级。

7. 下移：选择一条策略后，点击“ 下移”，该策略的位置下移一位，即优先级下降一级。

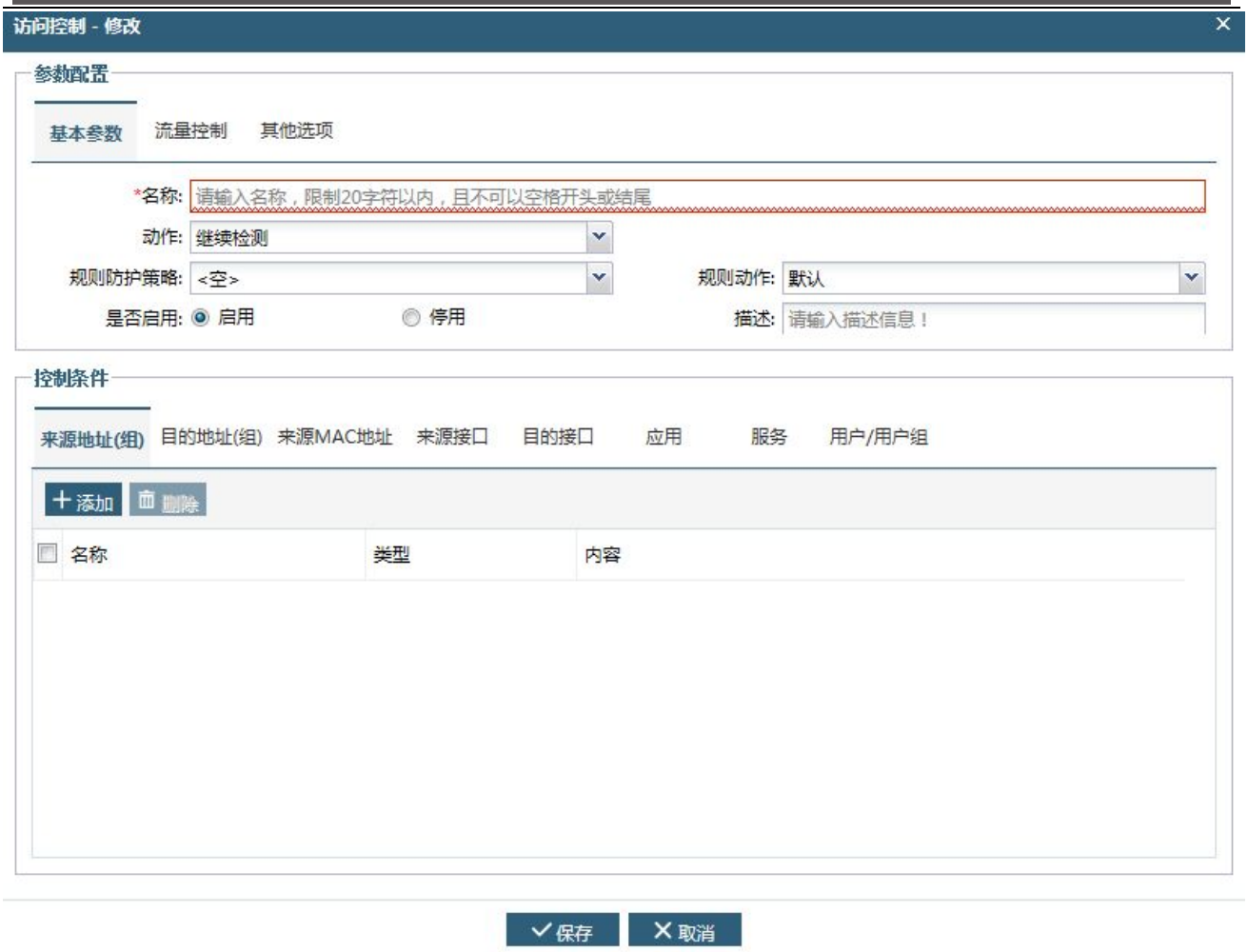
8. 置底：配置多条策略，选择一条排在前面的策略，该按钮呈可选择状态；点击“ ”可以将所选策略的优先级置为策略中最低。

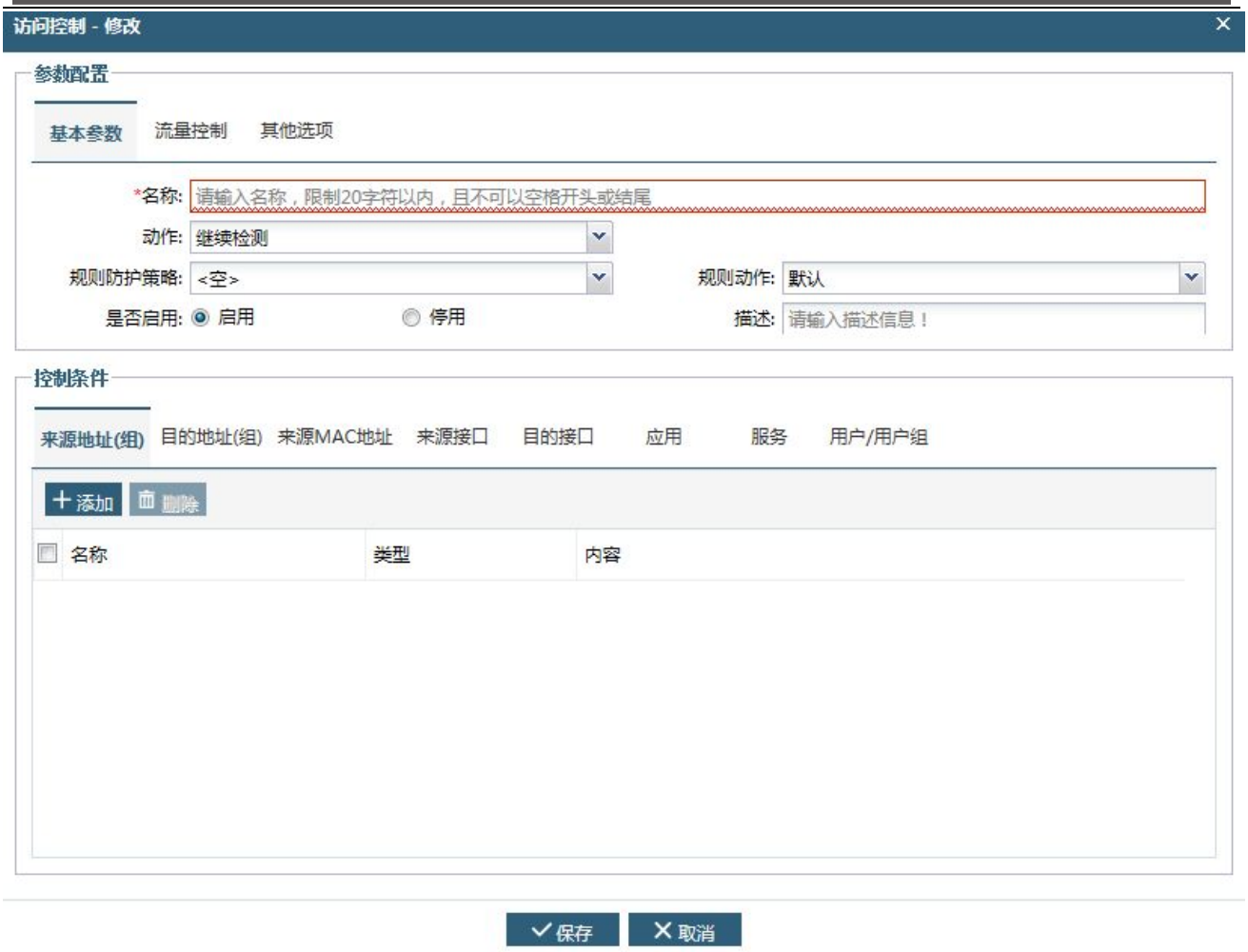
9. 应用：添加或修改策略后，应点击页面右上角“应用”按钮使策略真正生效。

10. 选中所有未提交的策略：勾选该项，会同步勾选策略列表中未提交的策略。

11. 点击 冲突检测，会检测访问控制是否冲突

12. 点击【添加】，弹出“访问控制-添加”；


访问控制 - 修改
参数配置
基本参数
流量控制
其他选项
*名称:
请输入名称，限制20字符以内，且不可以空格开头或结尾
动作:
继续检测
规则防护策略:
<空>
规则动作:
默认
是否启用:
启用
停用
描述:
请输入描述信息！
控制条件
来源地址(组)
目的地址(组)
来源MAC地址
来源接口
目的接口
应用
服务
用户/用户组
添加
删除
名称
类型
内容
保存
取消



1. 名称（必填项）：输入所要创建的安全策略的名称；

2. 选择“是否启用”：是否启用此条规则；

3. 生效时间：选择策略的生效时间，默认为所有时间，可通过以下方式进行选择

   方式一：请从【策略配置】→【对象配置】→【计划任务】已配置的应用对象中选择。

   方式二：通过选择窗口的快捷方式 – 新建按钮来添加时间调度对象。

4. 动作：设置策略的动作，包括允许该请求和阻塞该请求，还可以配置日志转发策略。选择允许时，可同时进行防病毒策略、防护规则策略配置（具体配置请参考动作配置部分）；选择阻塞时，只能配置是否记录流量日志。

5. 描述：可以追加一些描述信息，便于识别；

6. 来源地址/地址段：选择策略生效的内部地址，可通过以下方式选择

方式一：请从【策略配置】→【对象配置】→【地址】/【地址组】已配置的地址（组）对象和用户对象中选择。

方式二：通过选择窗口的快捷方式 – 新建按钮来添加地址（组）对象。

7. 源接口：选择策略的生效源接口，可通过以下方式选择：

方式一：通过【网络配置】→【网络接口】标签页已配置的接口。

方式二：通过选择源接口窗口快捷创建接口。

8. 目的地址/地址段：选择策略生效的外部地址，可通过以下方式选择

方式一：请从【策略配置】→【对象配置】→【地址对象】/【地址组对象】已配置的地址（组）对象和用户对象中选择。

方式二：通过选择窗口的快捷方式 – 新建按钮来添加地址（组）对象。

9. 服务：选择策略对哪些服务生效，可通过以下方式进行选择

方式一：请从【策略配置】→【对象配置】→【服务对象】选择已配置的服务对象。

方式二：通过选择窗口的快捷方式 – 新建按钮来添加服务对象。

10. 来源 MAC 地址：选择策略生效的来源 MAC 地址，可通过以下方式选择

方式一：请从【策略配置】→【对象配置】→【MAC 地址】已配置的 MAC 地址对象中选择。

方式二：通过选择窗口的快捷方式 – 新建按钮来添加 MAC 地址对象。

- 选择“动作”：即匹配到此条策略所做的操作，例如“继续检测”；

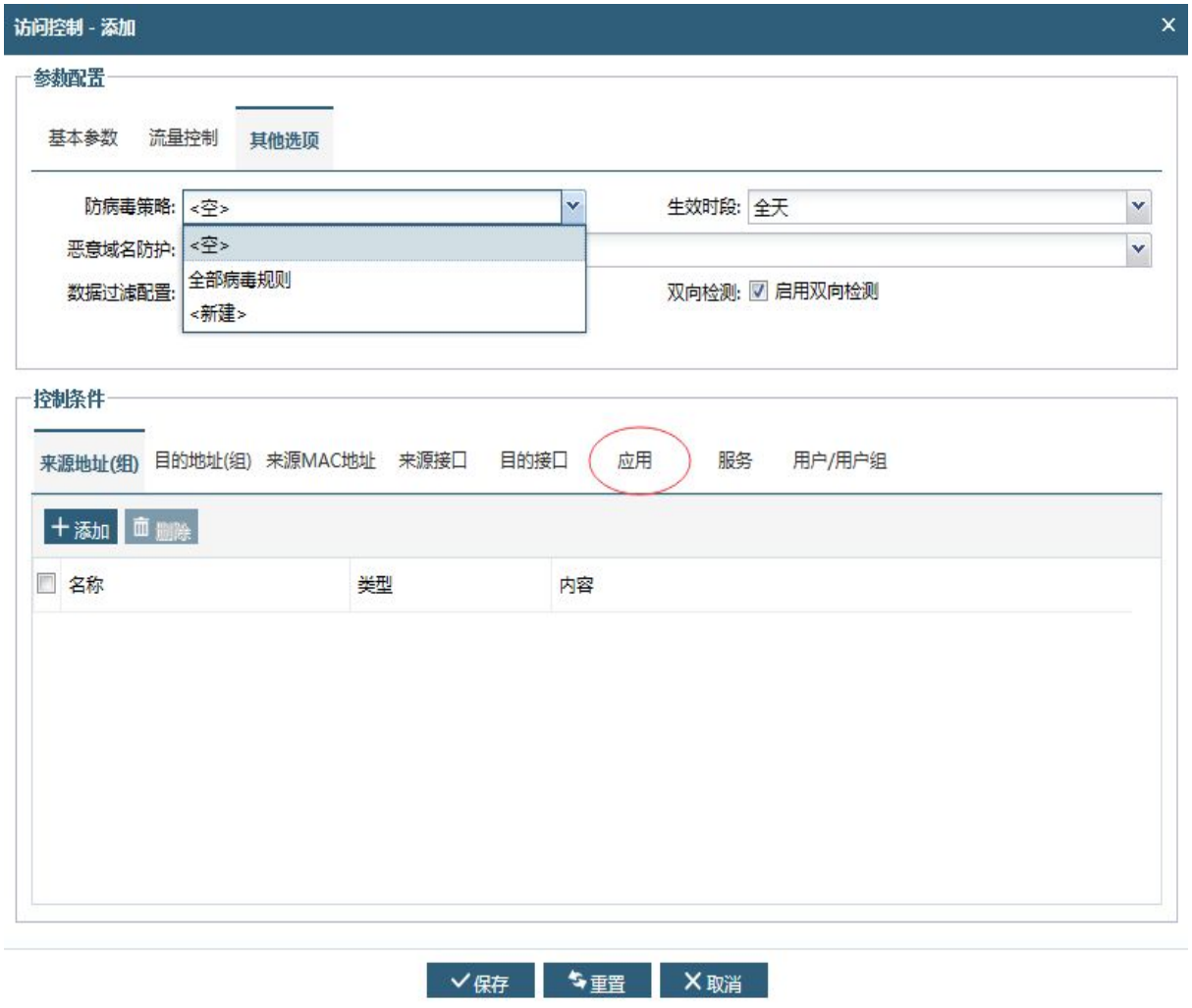
- 填写“描述”：对此条规则的说明；

- 选择“规则防护策略”：即匹配到此条策略所做的操作，例如“默认防护策略”；（添加详细步骤请参考：【策略配置】-【规则配置】-【防护策略配置】）

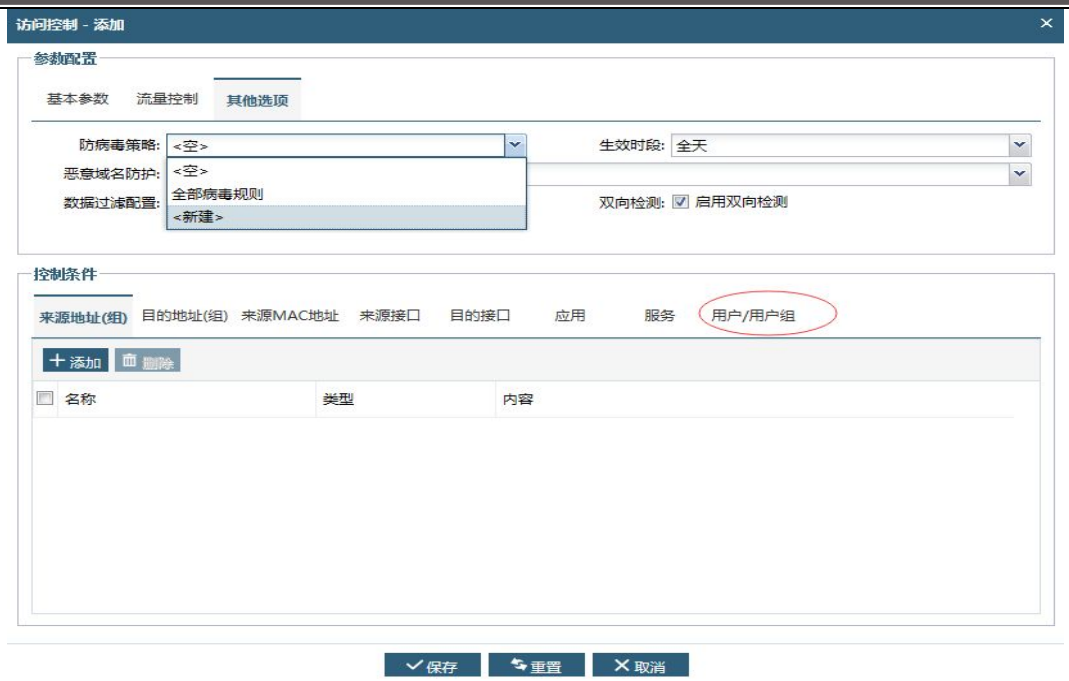
- 选择“生效时间”：即匹配到此条策略所做的操作，例如“全天“；（添加详细步骤请参考：【策略配置】-【对象配置】-【计划任务】）

- 选择“防病毒策略”：即匹配到此条策略所做的操作，例如“全部病毒规则”；（添加详细步骤请参考：【策略配置】-【规则配置】-【防病毒策略配置】）

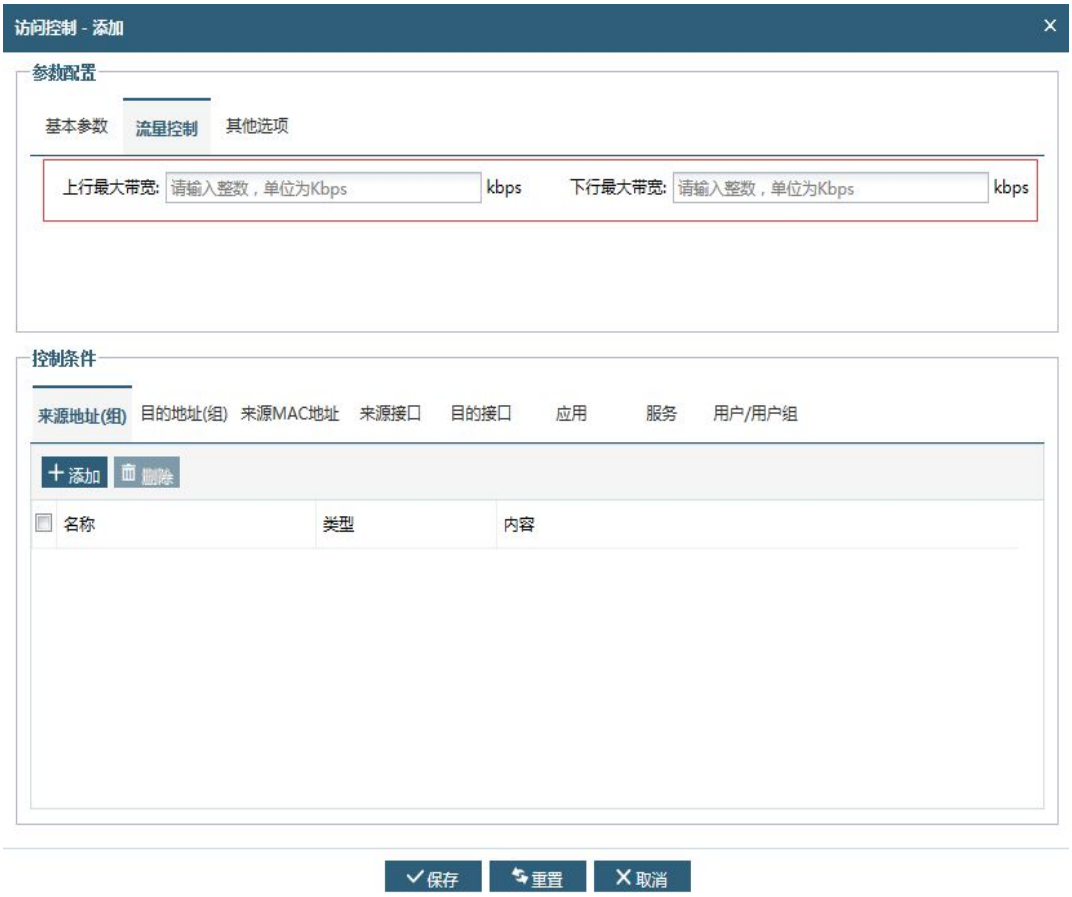
- “应用”：提供对应用的设置，您可以根据您的需求自行选择添加；



- “用户/用户组”：提供对用户/用户组的设置，您可以根据您的需求自行选择添加；（添加详细步骤请参考：【用户管理】）



- 选择“流量控制”设置流量控制被限制 IP，针对被限制的 IP 的上下行宽带进行流量控制；



- 上行最大带宽：上行宽带最大值；
- 下行最大带宽：下行宽带最大值；
- 来源地址、地址段：添加来源地址/来源地址段，限制源地址/来源地址段的上行、下行带宽；

- “恶意域名防护”：即匹配到此条策略所做的操作；

- “来源地址/地址段”：提供对来源 IP 的设置，您可以根据您的需求自行选择添加（添加详细步骤请参考：【策略配置】-【对象配置】-【IP 地址组】）

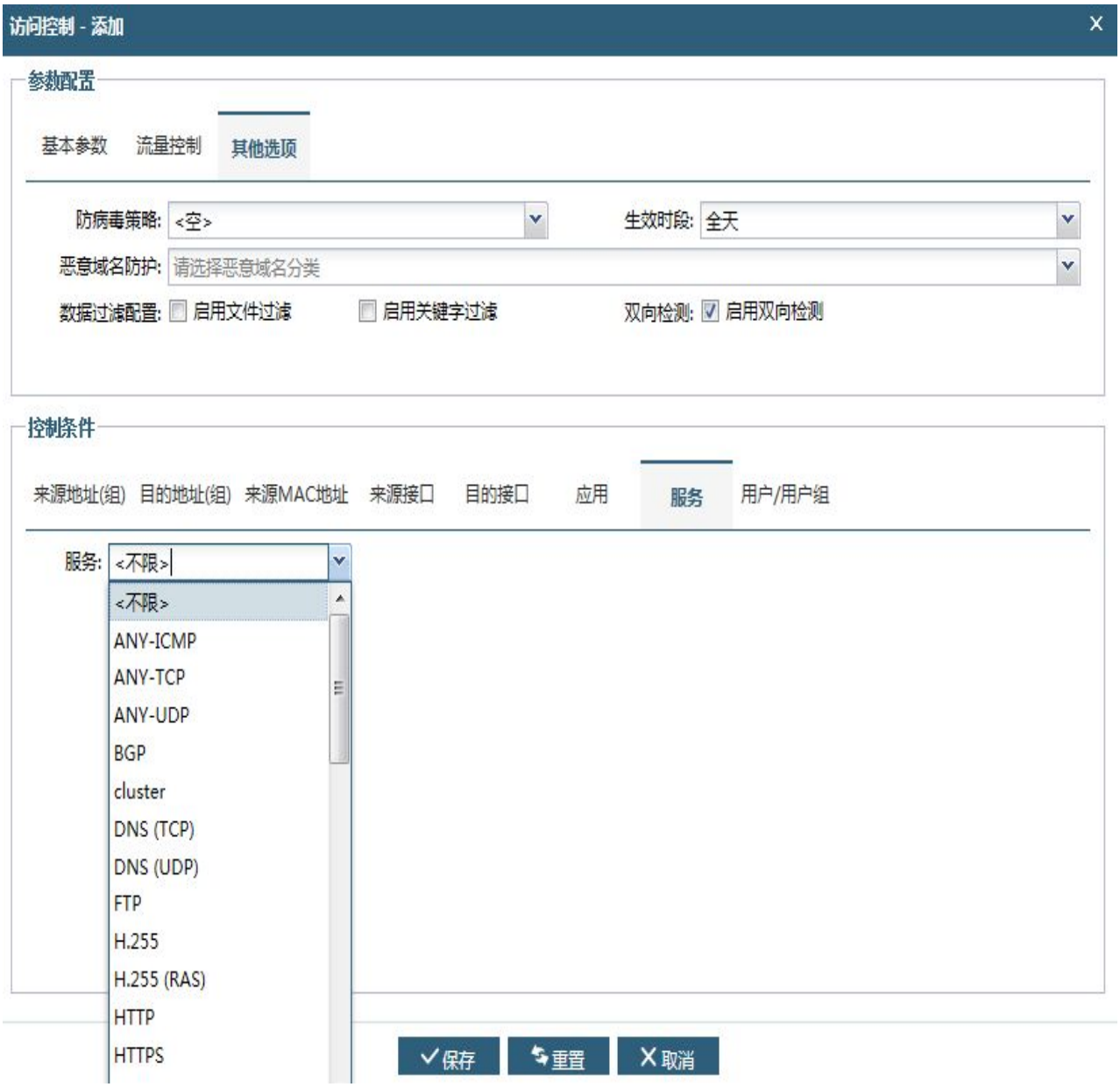
- “来源 MAC 地址”：提供对来源 MAC 地址设置，您可以根据您的需求自行选择；（添加详细步骤请参考：【策略配置】-【对象配置】-【MAC 地址】）

- “来源接口”：提供对来源接口设置，您可以根据您的需求自行选择；（添加详细步骤请参考：【网络配置】-【接口】-【网络接口】）

- “目的接口”：提供对目的接口设置，您可以根据您的需求自行添加；（添加详细步骤请参考：【网络配置】-【接口】-【网络接口】“）

- “目的地址/地址段”：提供对目的 IP 的设置，您可以根据您的需求自行选择添加；（添加详细步骤请参考：【策略配置】-【对象配置】-【地址】/【IP 地址组】“）

- “服务”：选择策略对哪些服务生效设置，您可以根据您的需求自行选择；（添加详细步骤请参考：【策略配置】-【对象配置】-【服务】“）



⚠注意：

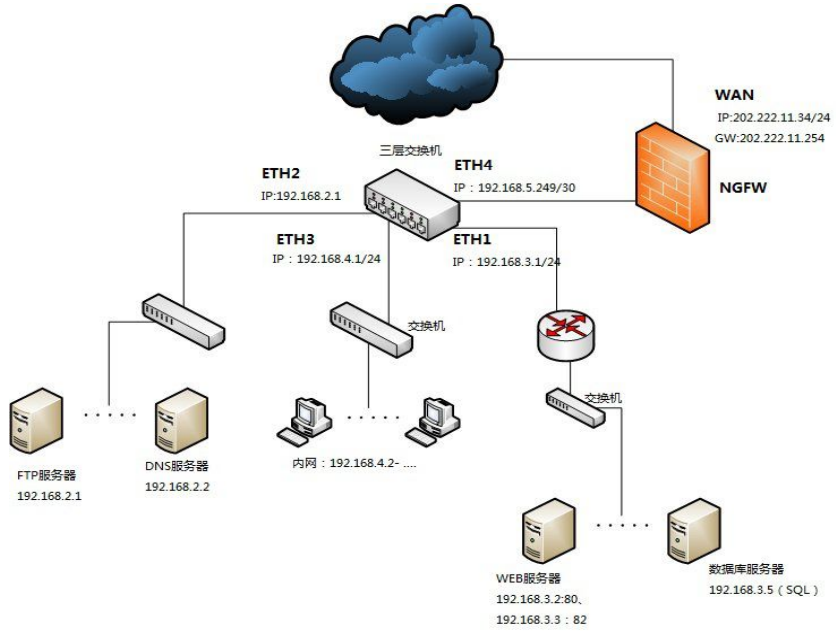
1、当各选项默认为空或未设置时、表示规则策略中各条件没有任何限制。

2、访问控制包含一条默认的不显示的安全策略，策略动作是阻塞任意流量，因此，IPS 管理员需配置好允许通过的流量的策略，否则会导致网络不通。

3、安全策略的优先级由策略在界面的排列顺序决定，按照由上到下的顺序优先级由高到低，最上方的策略优先级最高。

9.1.2 访问控制基本环境举例：

客户环境模拟 1：



模拟客户需求：

一、所有内网用户可以访问外网。

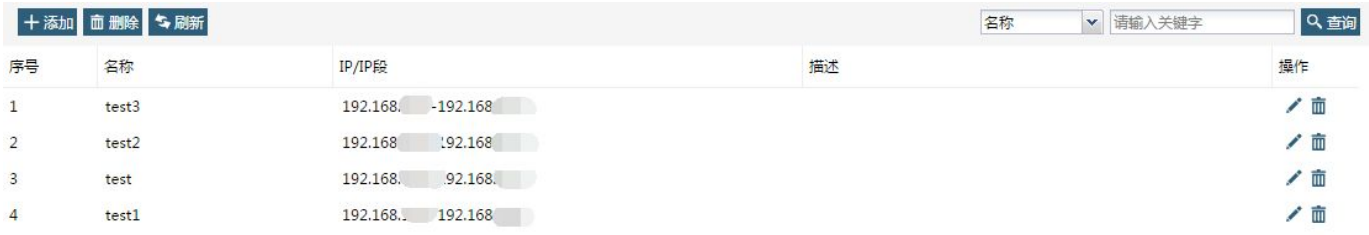
二、允许 192.168.4.1-192.168.4.200 内网用户可以上外网。

三、将 web 服务器映射出去。

详细步骤如下图：

一、所有内网用户可以访问外网。

1、添加内网地址。



2、针对内网做源 NAT、使内网用户可以访问外网。

⚠注意：

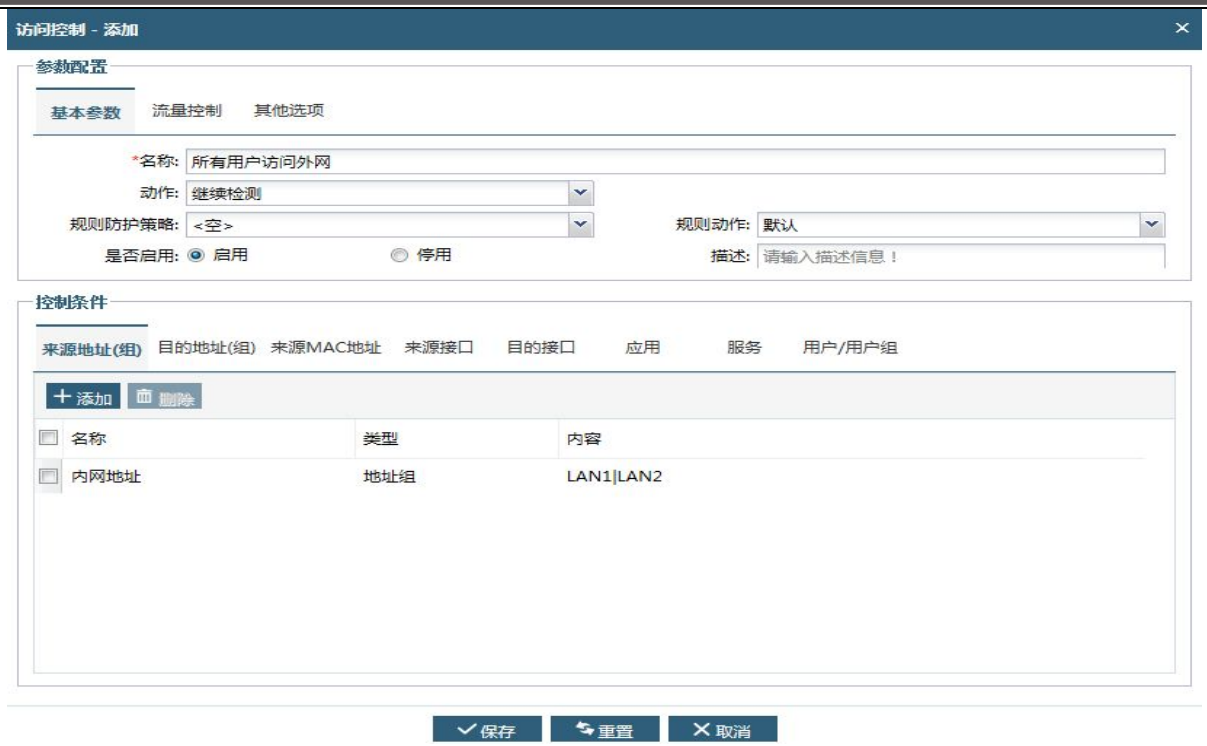
接口 ETH1 是对外的公网地址、转换后的地址即公网地址。（例如：公网地址：202.222.11.34，则设置 ETH1 接口属性为 WAN 口地址为 202.222.11.34、转换后 IP 为 202.222.11.34）

3、添加一条默认路由与静态路由（数据返回时直接将数据送到与设备连接的三层交换机/路由接口、网关为该接口地址）。

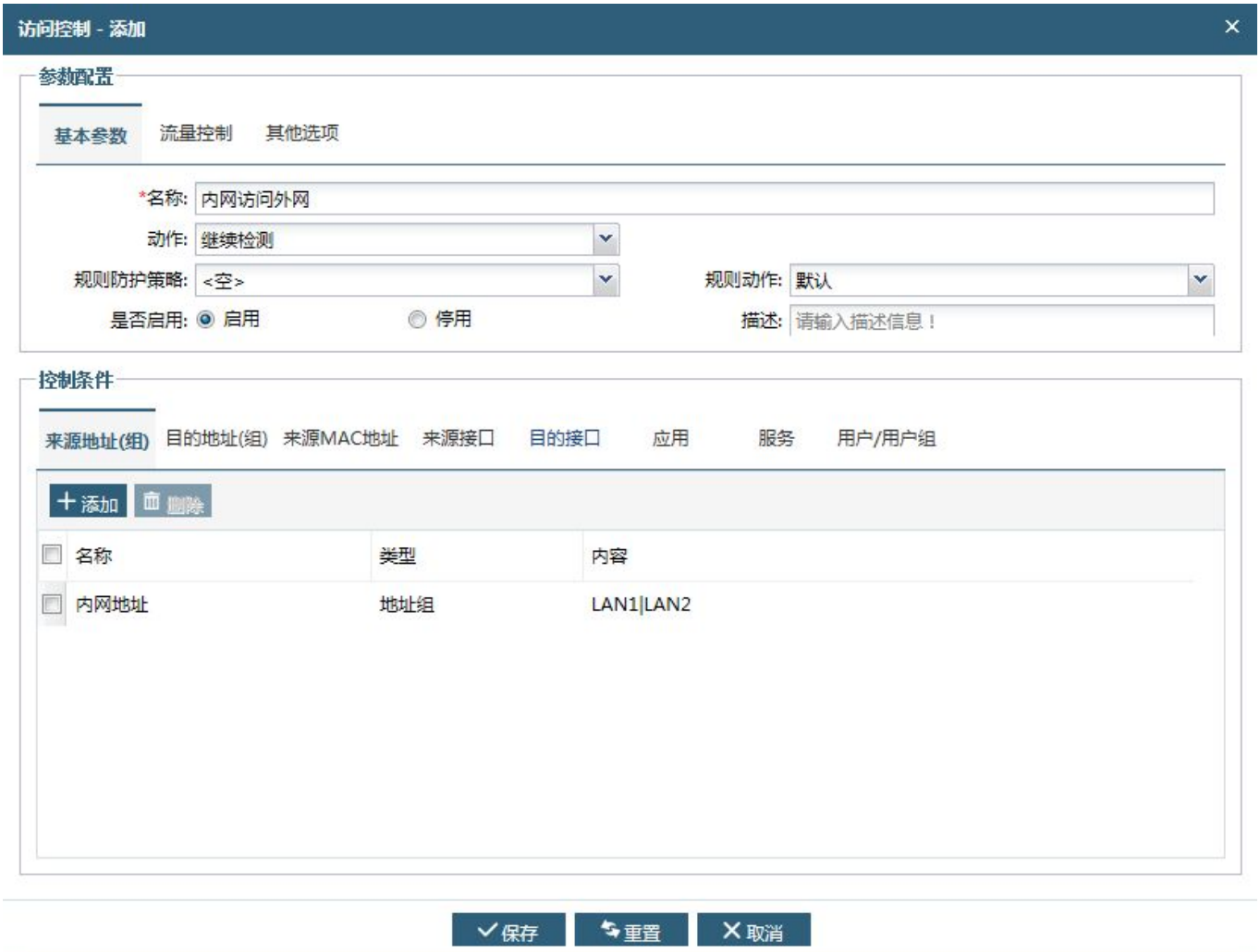
⚠注意：

三层交换机或路由需保证内网所有的数据可以直接到达设备的接口。（如上所述举例：需要在三层交换机/路由上设置一条默认路由、网关为三层交换机/路由与设备连接的设备接口地址）

4、添加一条访问控制，源地址/地址段为内网地址,目的为任意,动作为继续检测。



5、添加一条回流，目的地址/地址段为内网地址目的为任意、动作为默认。



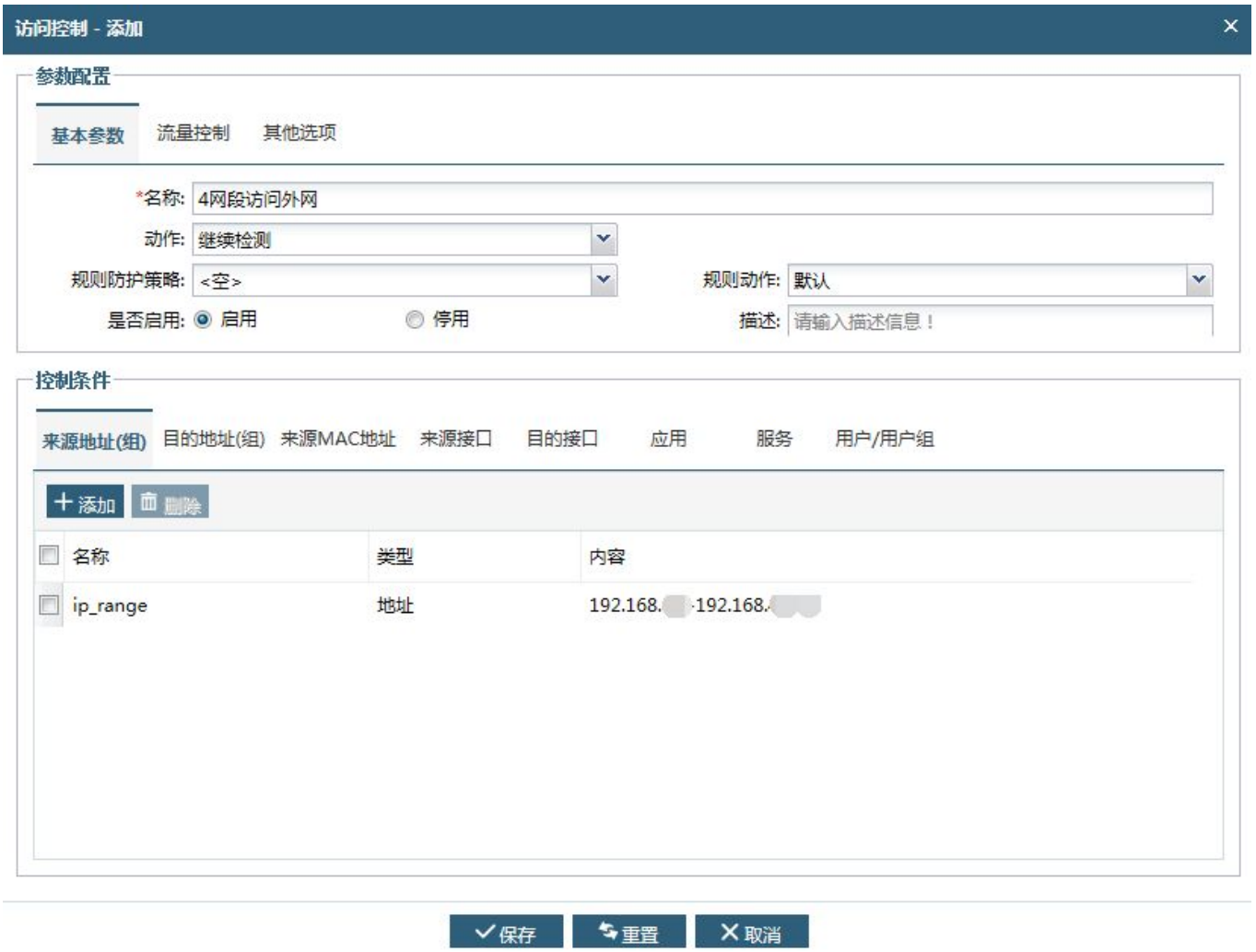
6、点击【保存】后，如下图：

7、内网用户 ping www.baidu.com，或者访问网页可以成功。

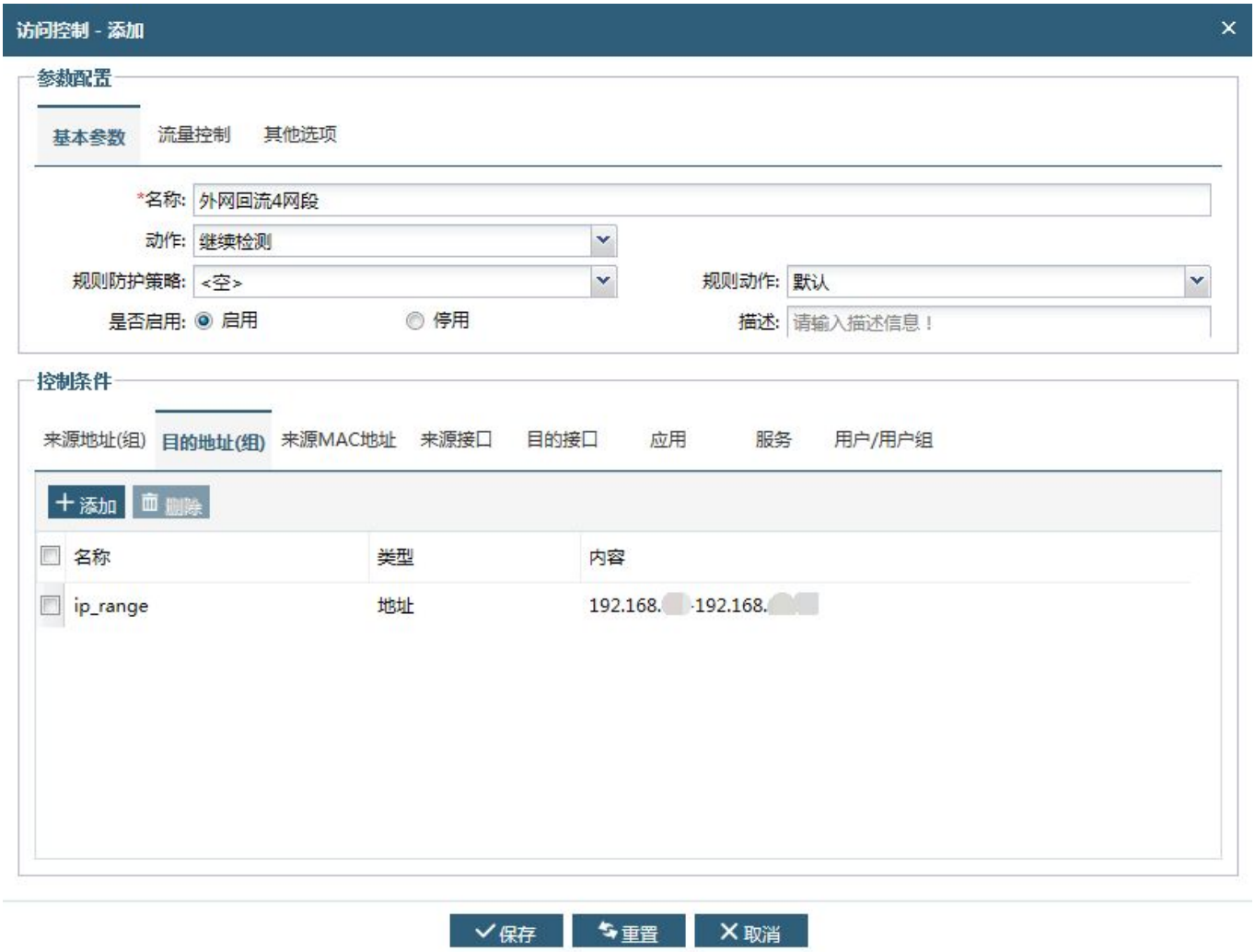
二、允许 192.168.4.1-192.168.4.255 内网用户可以上外网。

1、添加内网地址。

2、添加一条访问控制，源地址/地址段为内网地址目的为任意、动作为默认。



3、添加一条回流，目的地址/地址段为内网地址目的为任意、动作为默认。



4、针对内网做源 NAT、使内网用户可以访问外网。

5、添加一条默认路由与静态路由（数据返回时直接将数据送到三层交换机/路由与设备连接的三层交换机/

路由接口、网关为该接口地址）。

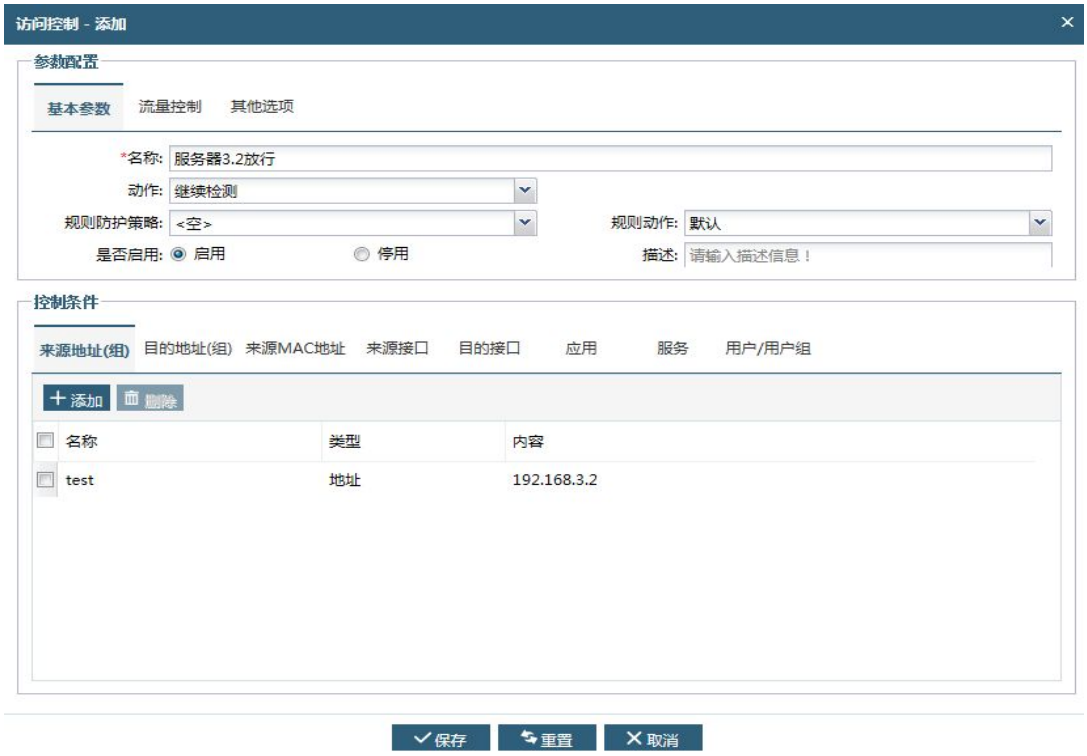
6、内网用户 ping www.baidu.com、或者访问网页，成功。

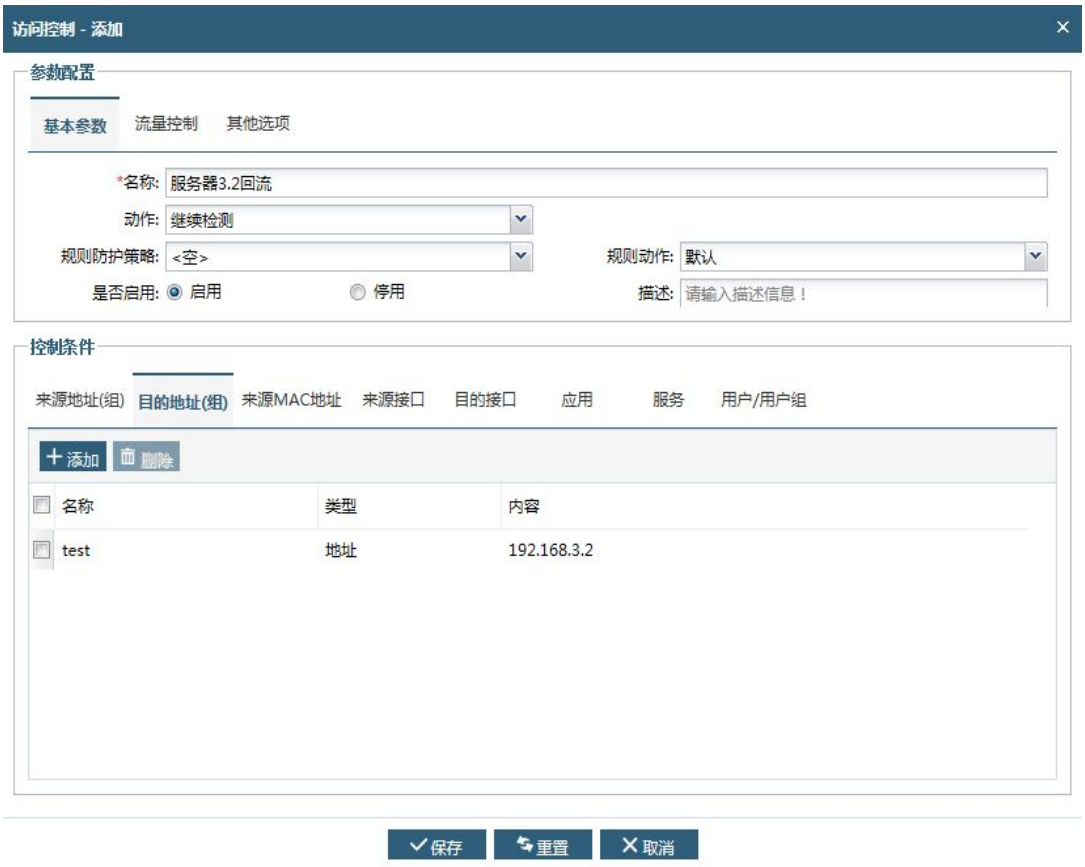
三、将 web 服务器映射出去

1、添加 web 服务器地址。

2、添加两条目的 NAT、将 192.168.3.2 的 80 端口，和 192.168.3.3 的 82 端口映射出去。

3、添加访问控制。





Web 服务器 192.168.3.3 添加访问控制方法同上。

4、静态路由：

5、外网访问公网地址的 443 端口（或其他端口）、将跳转到 web 服务器指定端口。

四、不允许访问“博彩赌球”类网站。

1、添加内网地址。

2、针对内网做源 NAT、使内网用户可以访问外网。

⚠注意：

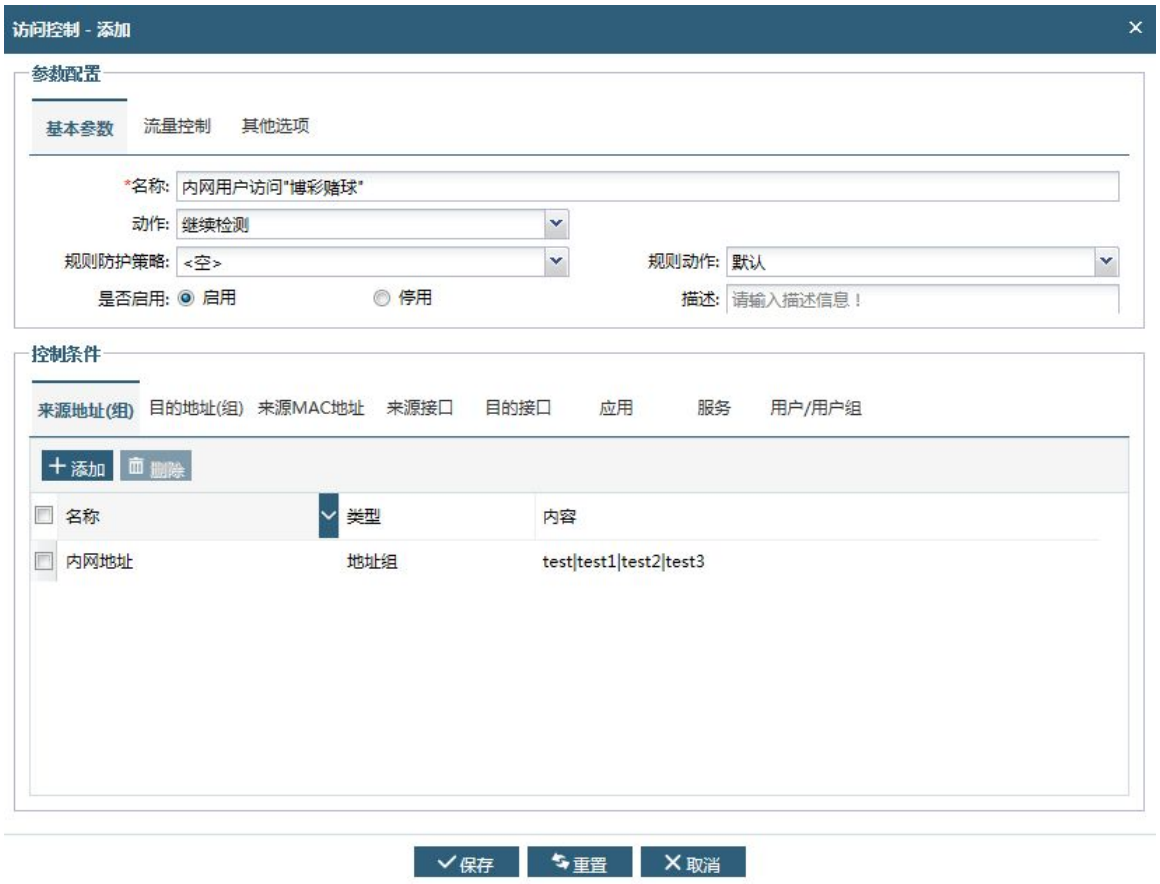
接口 ETH1 是对外的公网地址、转换后的地址即公网地址。（例如：公网地址：202.222.11.34，则设置 ETH1 接口属性为 WAN 口地址为 202.222.11.34、转换后 IP 为 202.222.11.34）

3、添加一条默认路由与静态路由（数据返回时直接将数据送到三层交换机/路由与设备连接的三层交换机/路由接口、网关为该接口地址）。

⚠注意：

三层接换机或路由、需保证内网所有的数据可以直接到达设备的接口。（如上所述举例：需要在三层交换机/路由上设置一条默认路由、网关为三层交换机/路由与设备连接的设备接口地址）

4、添加一条访问控制，源地址/地址段为内网地址目的为任意、动作为默认、选择“恶意域名防护”选项为“博彩赌球”。



5、点击【保存】后，如下图：

6、内网用户 ping www.baidu.com、或者访问网页，成功。

7、内网用户访问“博彩赌博”相关网站（例如：www.sb5206.com）、无法访问。

五、不允许用户访问“爱奇艺视频”。

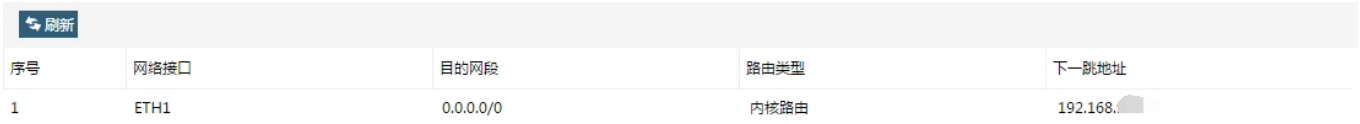
1、 添加内网地址。

2、针对内网做源 NAT、使内网用户可以访问外网。

⚠注意：

接口 ETH1 是对外的公网地址、转换后的地址即公网地址。（例如：公网地址：202.222.11.34，则设置 ETH1 接口属性为 WAN 口地址为 202.222.11.34、转换后 IP 为 202.222.11.34）

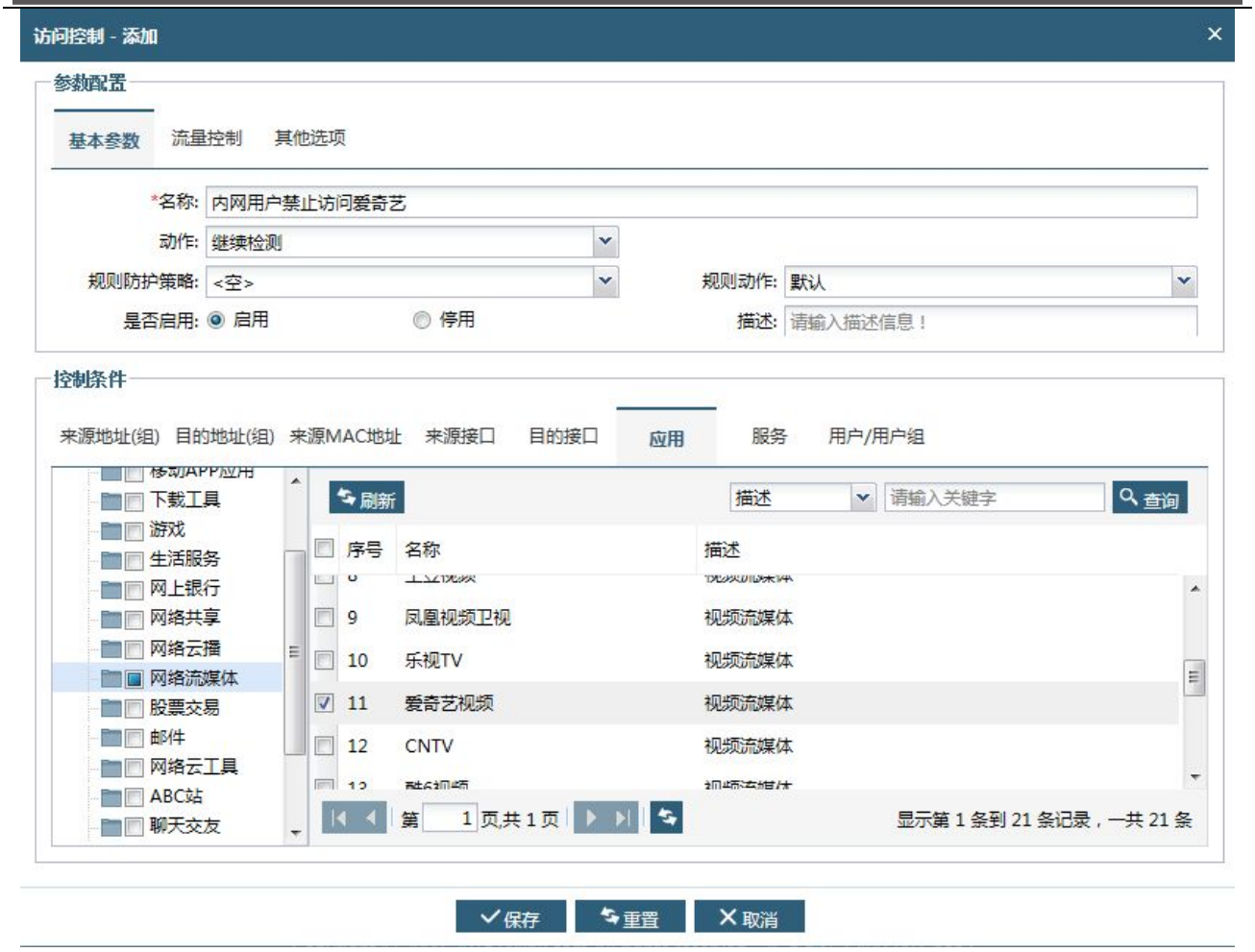
3、添加一条默认路由与静态路由（数据返回时直接将数据送到三层交换机/路由与设备连接的三层交换机/路由接口、网关为该接口地址）。



⚠注意：

三层接换机或路由、需保证内网所有的数据可以直接到达设备的接口。（如上所述举例：需要在三层交换机/路由上设置一条默认路由、网关为三层交换机/路由与设备连接的设备接口地址）

4、添加一条访问控制，源地址/地址段为内网地址目的为任意、动作为默认、选择“应用”选项为“爱奇艺视频”。



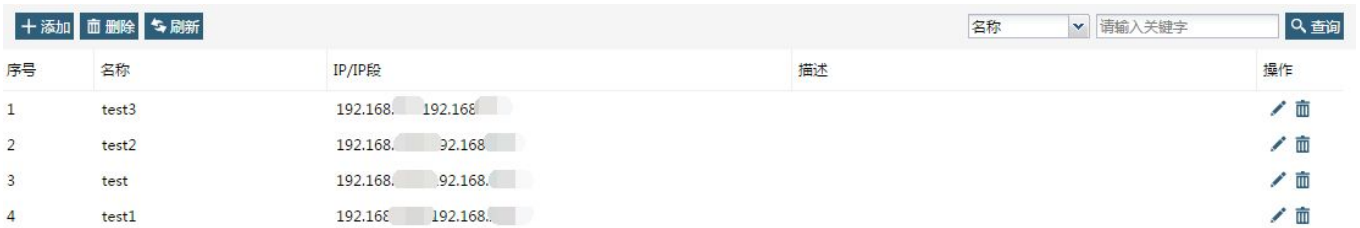
5、 点击【保存】后，如下图:

6、 内网用户 ping www.baidu.com、或者访问网页，成功。

7、 内网用户访问“爱奇艺视频”相关网站（例如：www.iqiyi.com 或者爱奇艺 APP 等）、无法访问。

8、 只允许 test 用户可以上网。

9、 添加内网地址。



10、针对内网做源 NAT、使内网用户可以访问外网。

⚠注意：

接口 ETH1 是对外的公网地址、转换后的地址即公网地址。（例如：公网地址：202.222.11.34，则设置 ETH1 接口属性为 WAN 口地址为 202.222.11.34、转换后 IP 为 202.222.11.34）

11、添加一条默认路由与静态路由（数据返回时直接将数据送到三层交换机/路由与设备连接的三层交换机/路由接口、网关为该接口地址）。

⚠注意：

三层接换机或路由、需保证内网所有的数据可以直接到达设备的接口。（如上所述举例：需要在三层交换机/路由上设置一条默认路由、网关为三层交换机/路由与设备连接的设备接口地址）

12、添加一条访问控制，源地址/地址段为内网地址目的为任意、动作为放行、选择“用户/用户组”为“test”。

13、点击【保存】后，如下图：

14、内网用户直接 ping www.baidu.com、或者访问网页，无法访问。

15、test 用户登录后（用户登录详细步骤请参考：【用户管理】-【用户管理】-【自定义用户组】“）、再次 ping www.baidu.com、或者访问网页，成功访问。

9.1.3 NAT 配置

NAT 配置用于将经过本设备的流量且符合条件的数据进行 IP 地址转换的功能。常用的情景主要是进行源 NAT 的配置，代理内网用户上网；进行目的 NAT 配置，用于外部用户访问内部服务器时，需要将目

的地址转换为内网服务器地址，实现“端口转发”功能；进行静态地址配置，将所有外部的流量都重定向到内网地址。

添加源 NAT 点击【添加】按钮，弹出“NAT 配置-添加”对话框，如下图所示。

- 类型：选择需要添加的 NAT 类型，源 NAT，目的 NAT，静态地址。
- 出接口名称：选择流量的出接口，均为设备上的接口。
- 是否启用：选择这条策略是否启用。
- 来源设置：设置来源 IP，包括任意 IP、单 IP、IP 段。
- 目的设置：设置目的 IP，包括任意 IP、单 IP、IP 段。
- 转换后地址设置：设置转换后的地址，包括单 IP、IP 段。可以使用出接口的 IP 或者手动配置。在“转换后 IP”项中可同时配置多个转换后的地址，支持多对多。
- 其他设置：选择适合网络环境的协议，默认是“任意”协议。

源 NAT 环境举例

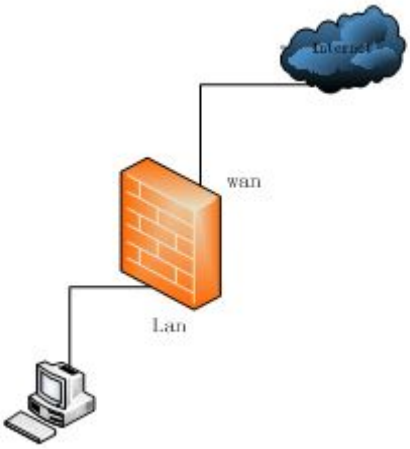
示例一：内网用户通过 IPS 设备访问外网

环境搭建：

1.网络接口中配置一个 WAN 口，ETH1:10.0.0.1（公网 IP）；

2.网络接口中配置一个 LAN 口，ETH2:192.168.0.1（内网 IP）；

3.pc 接 LAN 口，WAN 口连接交换机。



类型：选择源 NAT。

出接口名称：ETH1。

是否启用：选择启用。

来源设置：选择任意 IP。

目的设置：选择任意 IP。

转换后地址设置：手动输入 10.0.0.1。

其他设置：默认“任意”协议。

PC 设置 192.168.0.123，网关为 192.168.0.1，接 ETH2 口，访问外面的网站，可以上网。

目的 NAT 环境举例

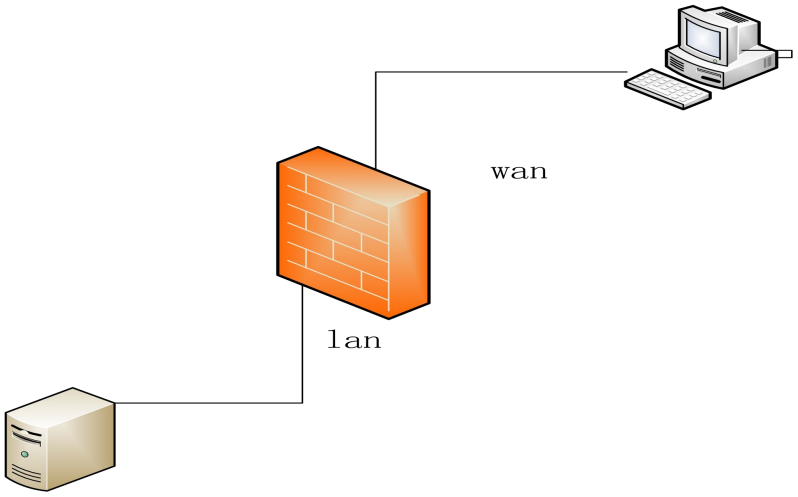
示例一：外网用户通过 IPS 设备访问内网服务器

环境搭建：

1.网络接口中配置一个 WAN 口，ETH1:10.0.0.1（公网 IP）；

2.网络接口中配置一个 LAN 口，ETH2:192.168.0.1，网关:192.168.0.29（内网网页服务器）；

3.pc 接 WAN 口，LAN 口连接设备。



类型：选择目的 NAT。

入接口名称：ETH1。

是否启用：选择启用。

来源设置：选择任意 IP。

目的设置：单 IP：10.0.01。

转换后地址设置：单 IP：192.168.0.29。

其他设置：默认“TCP”协议，来源端口：80，目的端口：80。

PC 设置 10.0.0.123，网关为 10.0.0.1，接 ETH1 口；服务器 IP192.168.0.29，接 ETH2 口，PC 直接访问

10.0.0.1，将转换到到内网的服务器地址。

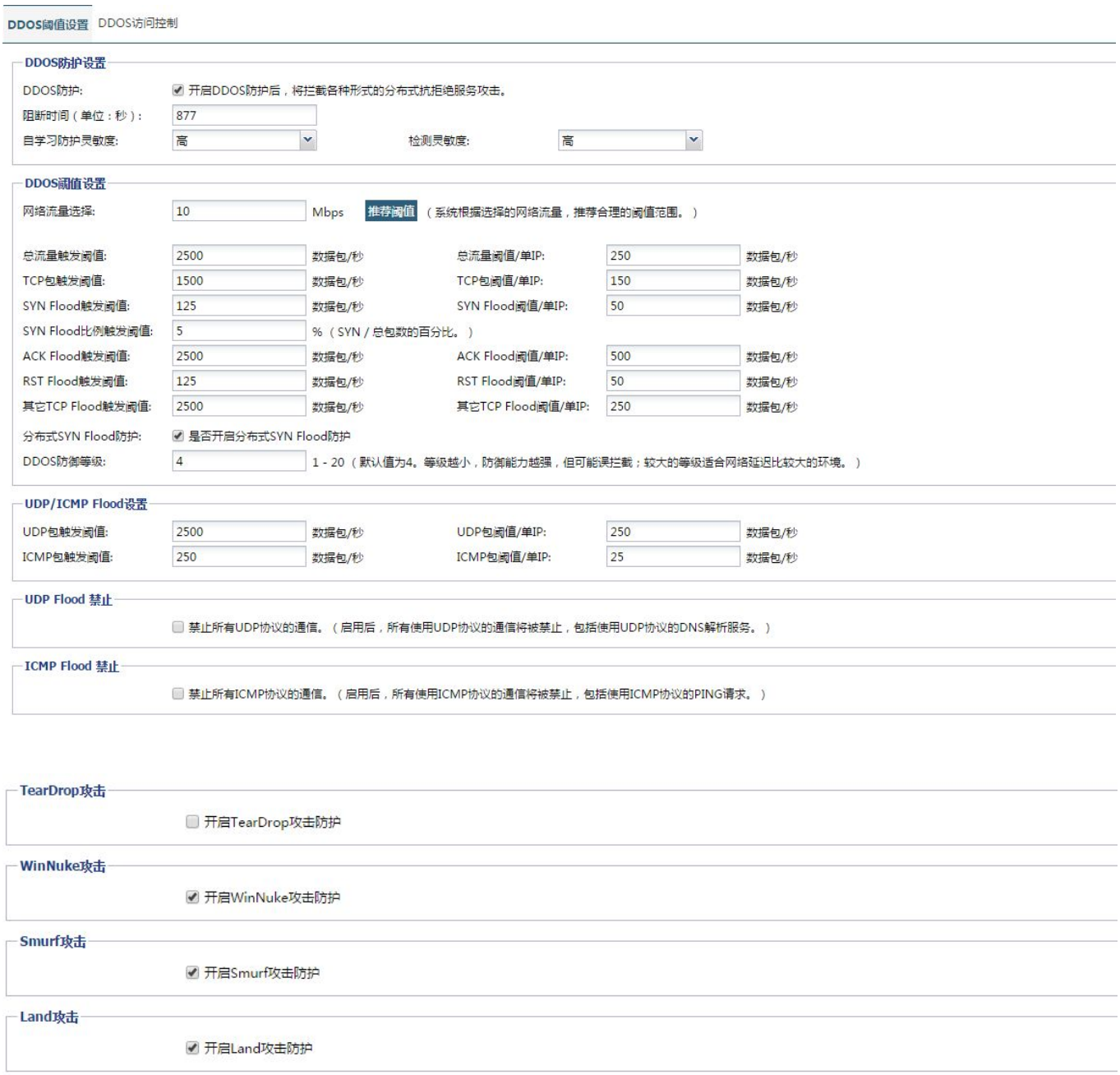
提示：

静态地址，与目的 NAT 类似，本手册不在示例。不同之处是所有访问 10.0.0.1 不同端口内容将被重定向到 192.168.0.29 上的相应端口。如非必要，请谨慎使用该功能。

9.1.4 DDOS 防护

DDOS 阈值设置

本页面设置与 DDOS 防护相关的网络流量参数，如图：



- 选择阈值集：选择需要进行参数配置的阈值集。
- 网络流量选择：可以根据您的网络环境流量大小来进行设定，默认阈值设置为 100Mbps。您只需要在网络流量选择中输入当前网络流量的大小（可以输入 1--10000Mbps），再点击【推荐阀值】，系统会根据您设定的网络流量数值自动生成最适合您网络环境的的阀值信息，当然您也可以对每一个阀值进行单独设定。

- 勾选【禁止所有 UDP 协议的通信】后，所有经过本设备的 UDP 协议的网络数据将会不允许通过。
- 勾选【禁止所有 ICMP 协议的通信】后，所有经过本设备的 ICMP 协议的网络数据将会不允许通过。
- 勾选【禁止大于 1024 字节的 ICMP 报文】后，所有经本设备的大于 1024 字节的 ICMP 报文将会不允许通过。
- 勾选【TearDrop 攻击】后，可以进行 TearDrop 攻击防护
- 勾选【WinNuke 攻击】后，可以进行 WinNuke 攻击防护
- 勾选【Smurf 攻击】后，可以进行 Smurf 攻击防护
- 勾选【Land 攻击】后，可以进行 Land 攻击防护

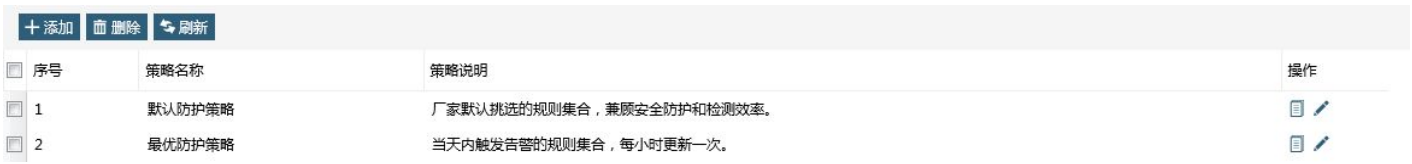
DDOS 访问控制

对防 DDOS 功能进行细粒度的控制，设置允许和禁止的 IP，如图：

9.2 9. 2 规则配置

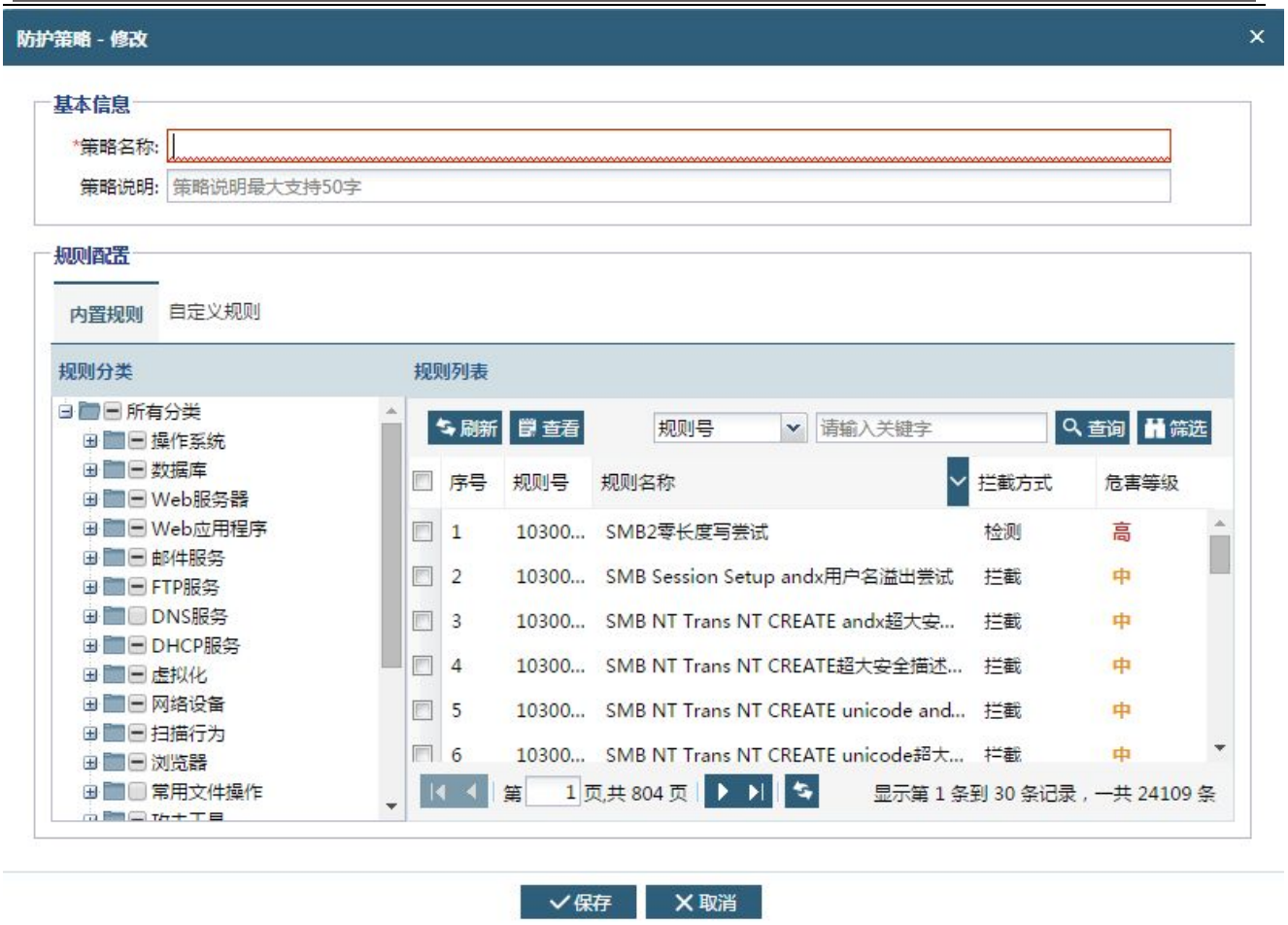
9.2.1 防护策略配置

防护策略中带有两个内置策略集，一个是默认防护策略，另一个是最优防护策略。



添加策略集

点击【添加】按钮，弹出“防护策略-添加”对话框，如下图：



- 策略名称：输入策略名称，支持 3 至 20 个说明，且不能以空格开始和结尾。
- 策略说明：输入关于该策略的说明，最大支持 50 个字符。
- 内置规则：选择需要添加的内置规则，内置规则为默认规则，不能修改和删除。
- 自定义规则：选择需要添加的自定义规则。
- 保存：内容填写完成后点击【保存】按钮，将保存更改到当前数据库。
- 重置：点击【重置】按钮以清空当前窗口中用户已经输入的内容以便用户重新输入。
- 取消：点击【取消】按钮不保存当前的用户输入并关闭窗口。

操作策略集

可以针对某一策略进行复制、修改和删除的操作。

- 复制：点击【复制】按钮，即可复制一条相同的策略集。
- 修改：选中所需要修改的策略集，点击【修改】按钮，修改之后点击【保存】，即可保存此操作。
- 删除：选中所需要修改的策略集，点击【删除】按钮，即可成功删除。

删除策略集

您可以在序号前面的白色方框内勾选多条一次性删除，也可以选中某条策略集，点击【删除】按钮，即可删除所选择的策略集。

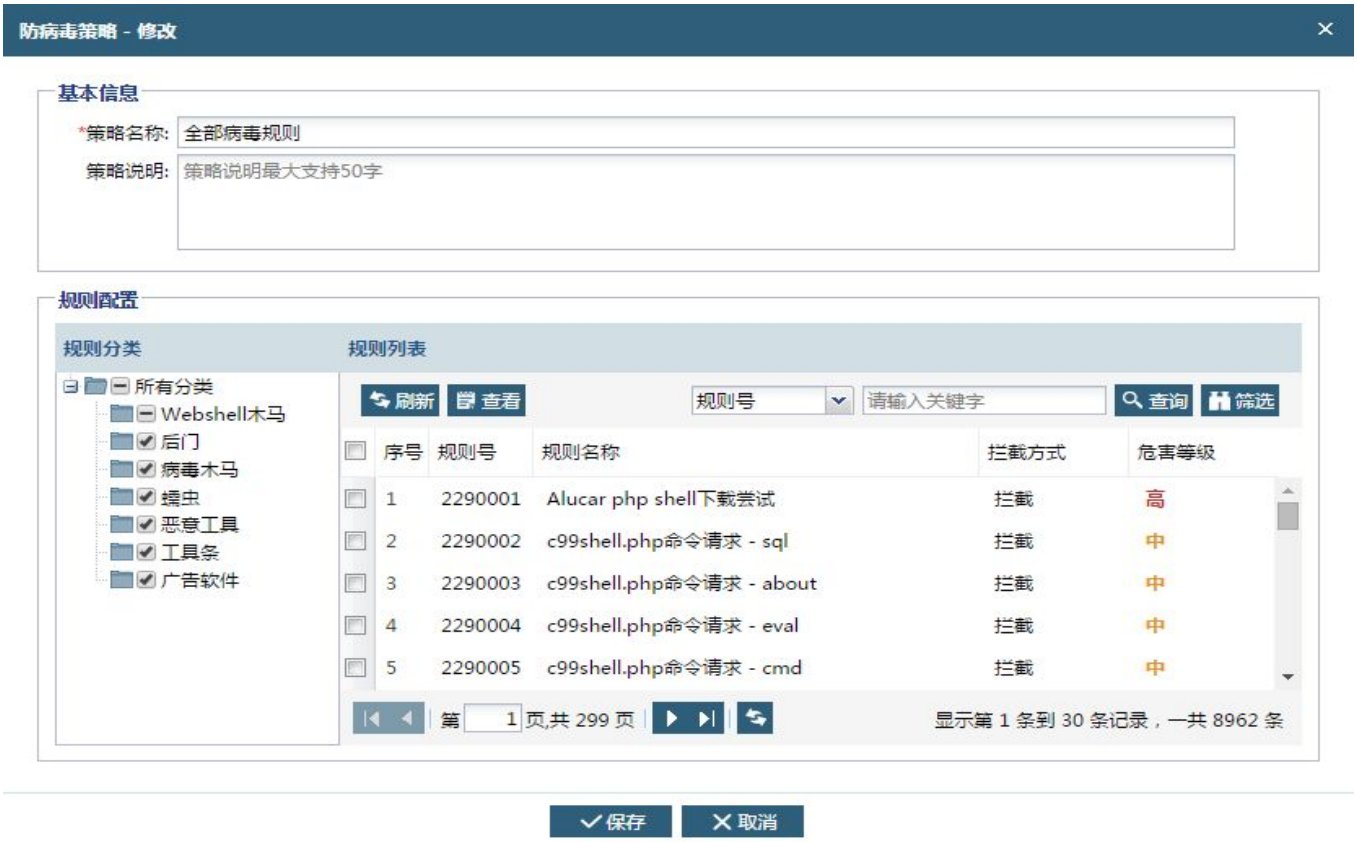
刷新策略集

点击【刷新】按钮，刷新该页面。

9.2.2 防病毒策略配置

添加防病毒策略集

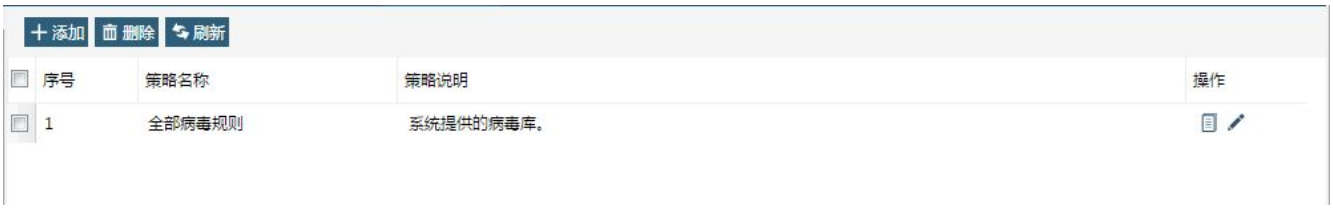
点击【添加】按钮，弹出“防病毒策略-添加”对话框，如下图。



- 策略名称：输入策略名称，支持 3 至 20 个说明，且不能以空格开始和结尾。
- 策略说明：输入关于该策略的说明，最大支持 50 个字符。
- 保存：选择好需要添加的规则后点击【保存】按钮，将保存更改到当前数据库。
- 重置：点击【重置】按钮以清空当前窗口中用户已经输入的内容以便用户重新输入。
- 取消：点击【取消】按钮不保存当前的用户输入并关闭窗口。

操作防病毒策略集

可以针对此策略进行复制、修改和删除的操作。



- 复制：点击【复制】按钮，即可复制一条相同的防病毒策略集。
- 修改：选中所需要修改的防病毒策略集，点击【修改】按钮，修改之后点击【保存】，即可保存此操作。
- 删除：选中所需要修改的防病毒策略集，点击【删除】按钮，即可成功删除。

删除防病毒策略集

您可以在序号前面的白色方框内勾选多条一次性删除，也可以选中某条策略集，点击【删除】按钮，即可删除所选择的防病毒策略集。

刷新防病毒策略集

点击【刷新】按钮，刷新该页面。

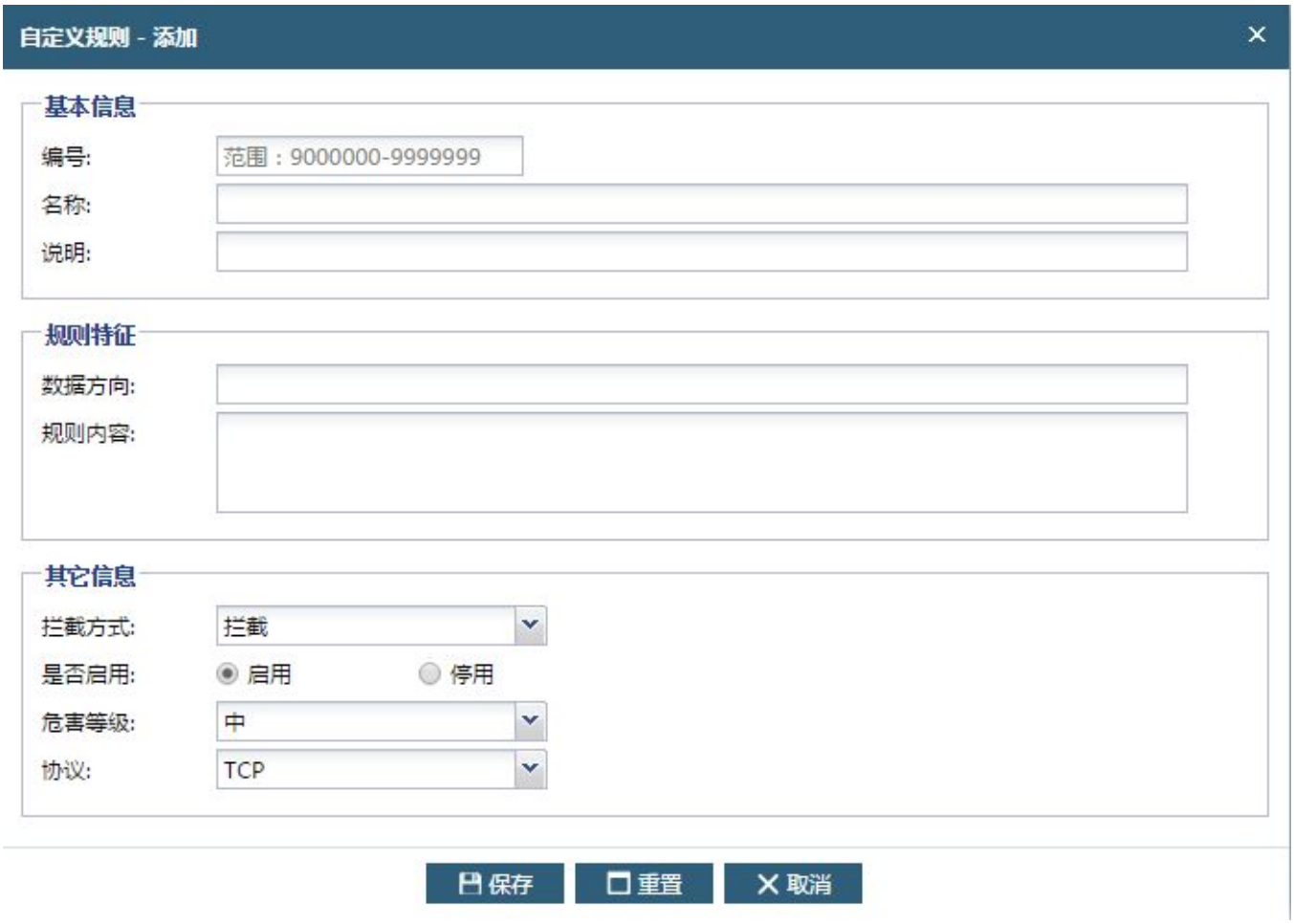
9.2.3 自定义规则

本页面设置用户自定义的规则，适合高级用户使用。通过完全自由的自定义规则框架，您可以根据实际的网络攻击情况对规则进行最大限度的定制。

- 添加自定义规则： 点击【添加】按钮，出现【自定义规则-添加】对话框。具体操作请参见下一节自定义规则的添加和修改。
- 修改自定义规则： 选择一条规则然后点击【修改】按钮，出现【自定义规则-修改】对话框。双击某条规则也可以直接打开【自定义规则-修改】对话框。具体操作请参见下一节自定义规则的添加和修改。
- 删除自定义规则： 选择一条或者多条自定义规则，然后点击【删除】按钮，则删除所选自定义规则。
- 刷新自定义规则：点击【刷新】按钮，实时刷新页面。
- 应用自定义规则：点击【应用】按钮后当前更改立即生效，建议在所有设置全部配置完成以后，点击【应用】按钮。
- 查询自定义规则： 当用户自定义规则比较多时，输入名称并点击【快速查询】按钮，可以根据名称快速筛选出包含输入名称的自定义规则。

自定义规则的添加和修改

自定义规则的添加和修改界面如图所示。



- 编号： 自定义规则的用户指定编号。此编号应该介于 9000000 和 9999999 之间，并且不允许重复。如果您输入的编号不在允许范围内，系统会提示您重新输入编号。
- 名称： 自定义规则的中文或者英文名称。建议名称尽量简洁并能反映该条规则的真实含义。

- 说明： 关于该条规则的备注信息，您可以在此处添加说明性的文字。
- 数据方向： 数据的来源方向。
- 规则内容： 规则需要匹配的内容。
- 拦截方式： 匹配到选择该条规则所执行的动作。
- 是否启用： 规则是否启用。
- 优先级： 该条规则的优先级。
- 协议： 该条规则检测的协议。

自定义规则举例

示例（字符串匹配）：

某高校网站后台有一个管理页面（URL：http://www.test.cn/admini/login.php），管理员想禁止所有用户访问此页面，我们可以做如下策略。

操作步骤:

“编号”填写“9000001”；

“名称”填写“后台管理页面”；

“说明”填写“禁止所有用户登录后台管理页面”；

“数据方向”填写“any any -> any any”；

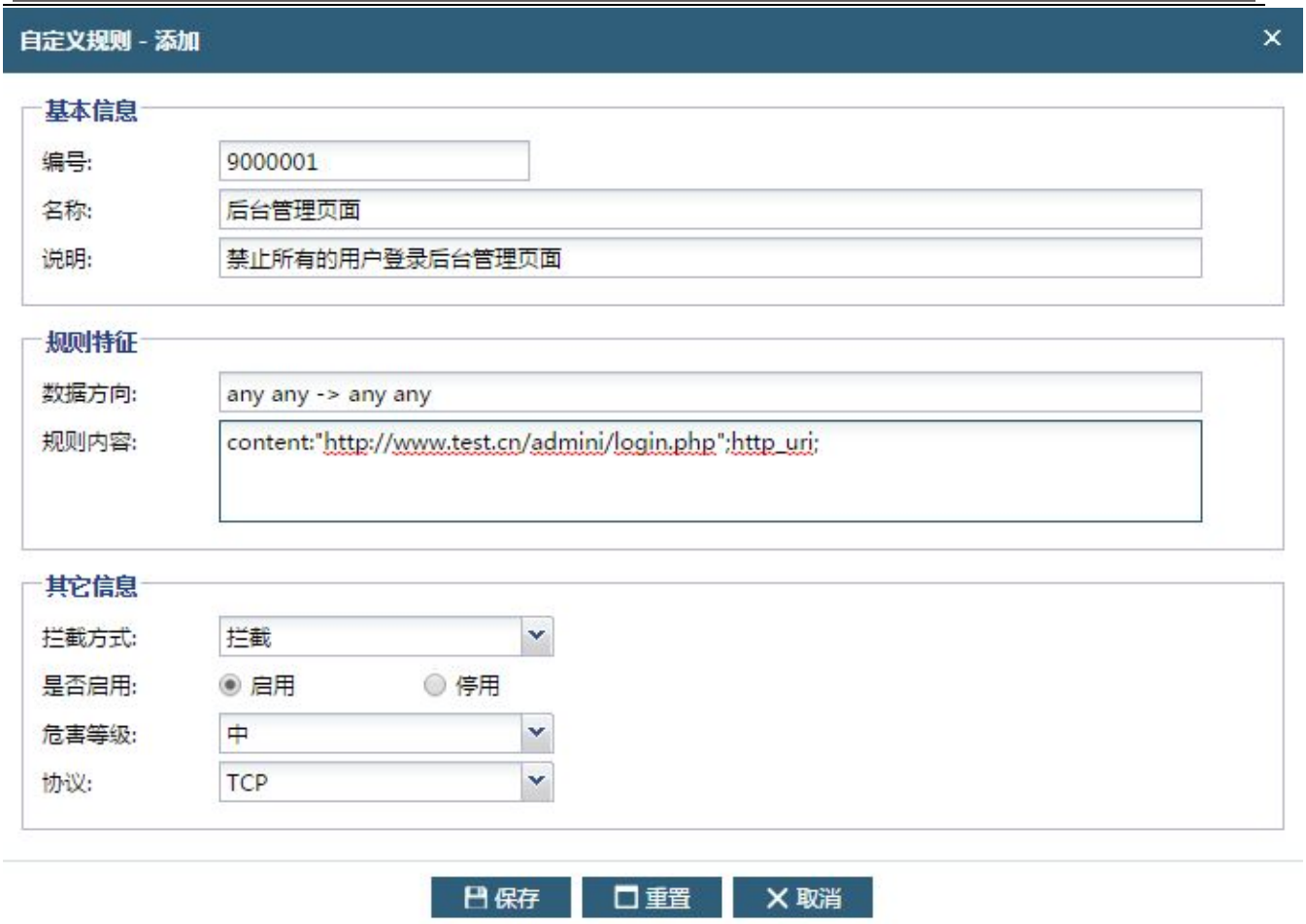
“规则内容”输入“content:"http://www.test.cn/admini/login.php";http_uri;”；

“是否启用”选择“启用”；

“优先级”选择“高”；

“协议”选择“TCP”；

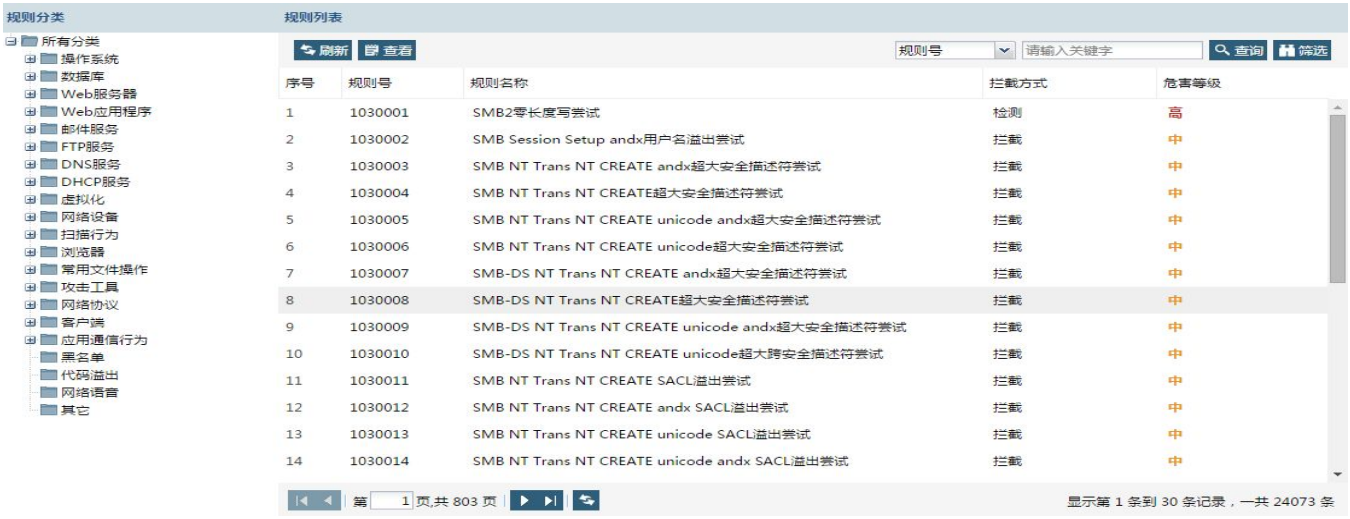
到这一步，规则生成初步完成，生成后的规则如图所示；



点击【保存】按钮，保存该条自定义规则。

9.2.4 内置规则

本页面显示铱迅入侵防御系统在出厂时已经内置好的防护规则集。页面具体如图所示，显示的详细内容包括：规则号、规则名称、拦截方式。



- 查询规则： 在右边的输入名称框中输入需要查询的规则名称，点击【查询】按钮，系统查询出所有规则名称中包含该文字的内置规则；

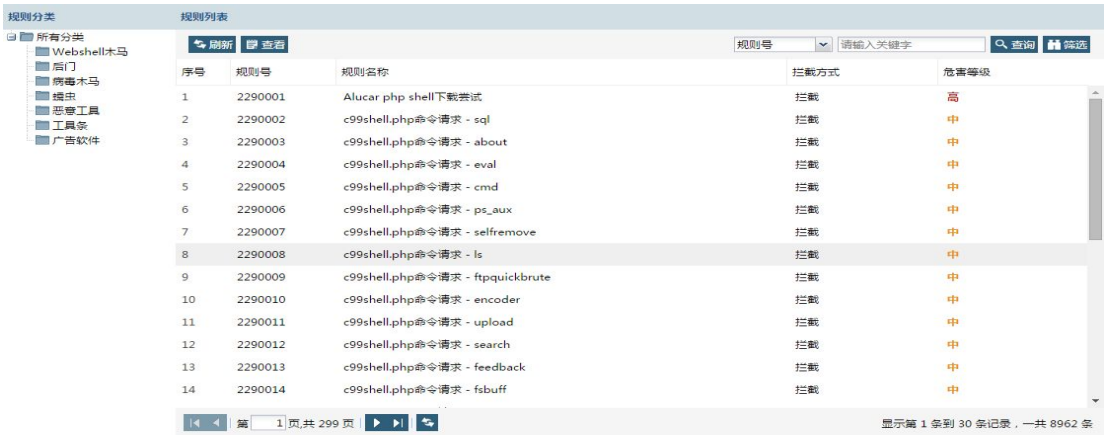
- 查看规则： 双击或选中需要查看规则点击【查看】，可查看规则的详细信息。如下图，查看规则号为“1030002”

注意：

所有内置规则集都经过厂家的严格测试，保证最小程度的误拦截。除非您完全清楚正在进行的操作，否则不要停用任何内置规则集。

9.2.5 内置防病毒规则

本页面显示铱迅入侵防御系统在出厂时已经内置好的防病毒规则集。页面具体如图所示，显示的详细内容包括：规则号、规则名称、拦截方式、危害等级。



- 查询规则： 在右边的输入名称框中输入需要查询的规则名称，点击【查询】按钮，系统查询出所有规则名称中包含该文字的内置规则；

- 查看规则： 双击或选中需要查看规则点击【查看】，可查看规则的详细信息。如下图，查看规则号为“2290001”。

注意：

所有内置防病毒规则集都经过厂家的严格测试，保证最小程度的误拦截。除非您完全清楚正在进行的

操作，否则不要停用任何内置防病毒规则集。

9.2.6 内置应用列表

本页面显示铱迅入侵防御系统在出厂时已经内置好的应用列表。页面具体如图所示，显示的详细内容包括：应用名称、描述。

- 查询规则： 在右边的输入名称框中输入需要查询的应用名称，点击【查询】按钮，系统查询出所有应用名称中包含该文字的内置应用；

9.2.7 禁用列表

本页面显示被用户禁用的规则的信息，用户添加禁用规则的步骤为：在“数据中心” -> “入侵记录”或者“防病毒记录”页面，右键点击某一条想要禁用的规则记录，选择“禁用此条规则”，将该规则加入到”禁用列表“。界面详细信息如图所示，内容包括：规则编号，规则名称，用户禁用该条规则的时间，

以及该条规则包含在哪些策略集里。

- 查询规则： 在右边的输入名称框中根据查询条件输入关键字，点击【查询】按钮，系统查询出相对应的禁用规则；

注意：

对所要禁用的规则，用户要慎重，否则有可能造成威胁漏报。

9.3 9.3 对象配置

9.3.1 IP 地址

该功能可以根据自己需要定义一些地址对象。在地址对象中建立的地址可以被访问控制重复调用。

添加地址

点击【添加】按钮，弹出“地址-添加”对话框，如下图：

- 名称：输入该地址的名称，支持 3 至 20 字符，且不可以以空格开头或结尾。
- IP/IP 段：请输入有效的单 IP 或者 IP 段，支持短横线分割或者掩码的形式。比如 192.168.50.5，192.168.50.50-192.168.50.80，或者 192.168.50.0/24。
- 描述：可以填写关于该 IP 的说明。
- 保存：内容填写完成后点击【保存】按钮，将保存更改到当前数据库。
- 重置：点击【重置】按钮以清空当前窗口中用户已经输入的内容以便用户重新输入。
- 取消：点击【取消】按钮不保存当前的用户输入并关闭窗口。

删除地址

未选中记录，点击【删除】按钮，弹出“系统提示”对话框，如下图：

选择记录，点击【删除】按钮，弹出“系统提示”对话框，如下图，点击【是】删除该条地址对象。

提示：

正在被访问控制使用的地址对象是不允许被删除的，执行删除操作时，系统会给出警告。

刷新地址

点击【刷新】按钮，刷新该页面。

查询地址

点击右上角下拉框，弹出“ 名称-描述“对话框。可以选择查询的条件，比如查询“名称”，选择“名称”，在“输入关键字”一栏，输入已经存在的“123”或者“3”，点击【查询】按钮即可查出。

9.3.2 IP 地址组

该功能可以把已经添加的地址对象组合成地址组对象。在地址组添加的地址组对象可以被任何访问控制策略调用。

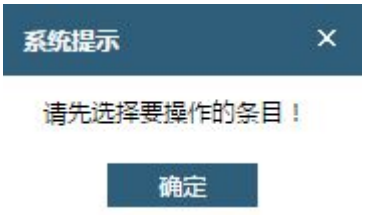
添加地址组

点击【添加】按钮，弹出“地址组-添加”对话框，如下图：

- 名称：输入该地址的名称，支持 3 至 20 字符，且不可以以空格开头或结尾。
- 添加：选择需要添加的 IP 或者 IP 组，也可以在该页面中直接添加地址对象，添加过程请参考“地址-添加地址”目录。
- 删除：选中记录，点击【删除】按钮，即可从列表中删除。
- 保存：内容填写完成后点击【保存】按钮，将保存更改到当前数据库。
- 重置：点击【重置】按钮以清空当前窗口中用户已经输入的内容以便用户重新输入。
- 取消：点击【取消】按钮不保存当前的用户输入并关闭窗口。

删除地址组

未选中记录，点击【删除】按钮，弹出“系统提示”对话框，如下图：



选择记录，点击【删除】按钮，弹出“系统提示”对话框，如下图，点击【是】删除该条地址对象。

提示：

正在被访问控制使用的地址组对象是不允许被删除的，执行删除操作时，系统会给出警告。

刷新地址组

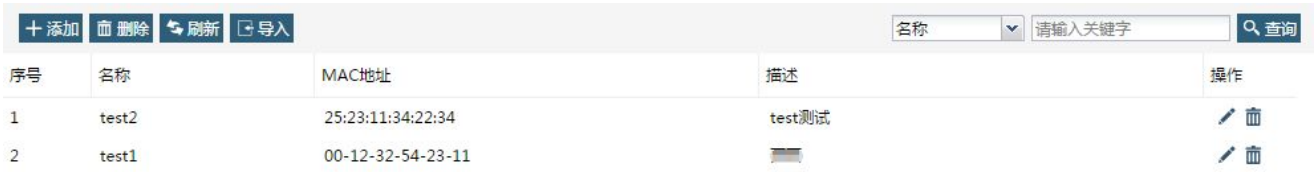
点击【刷新】按钮，刷新该页面。

查询地址组

点击右上角下拉框，比如选择“名称”，在“输入关键字”一栏，输入已经存在的“123”或者“3”，点击【查询】按钮即可查出。

9.3.3 MAC 地址

该功能可以根据自己需要定义一些 MAC 地址对象。在 MAC 地址对象中建立的 MAC 地址可以被访问控制重复调用。



添加 MAC 地址

点击【添加】按钮，弹出“MAC 地址-添加”对话框，如下图：

- 名称：输入该地址的名称，支持 3 至 20 字符，且不可以以空格开头或结尾。
- MAC 地址：请输入有效的 MAC 地址，支持冒号或者短横线分隔，如 12:DB:90:AB:7A:0B 或者 12-DB-90-AB-7A-0B。
- 描述：可以填写关于该 MAC 地址的说明。
- 保存：内容填写完成后点击【保存】按钮，将保存更改到当前数据库。
- 重置：点击【重置】按钮以清空当前窗口中用户已经输入的内容以便用户重新输入。
- 取消：点击【取消】按钮不保存当前的用户输入并关闭窗口。

删除地址组

未选中记录，点击【删除】按钮，弹出“系统提示”对话框，如下图：

选择记录，点击【删除】按钮，弹出“系统提示”对话框，如下图，点击【是】删除该条地址对象。

提示：

正在被访问控制使用的 MAC 地址对象是不允许被删除的，执行删除操作时，系统会给出警告。

刷新 MAC 地址

点击【刷新】按钮，刷新该页面。

导入 MAC 地址

支持纯文本文件导入，和直接输入的方式，可以批量生成 MAC 地址对象。

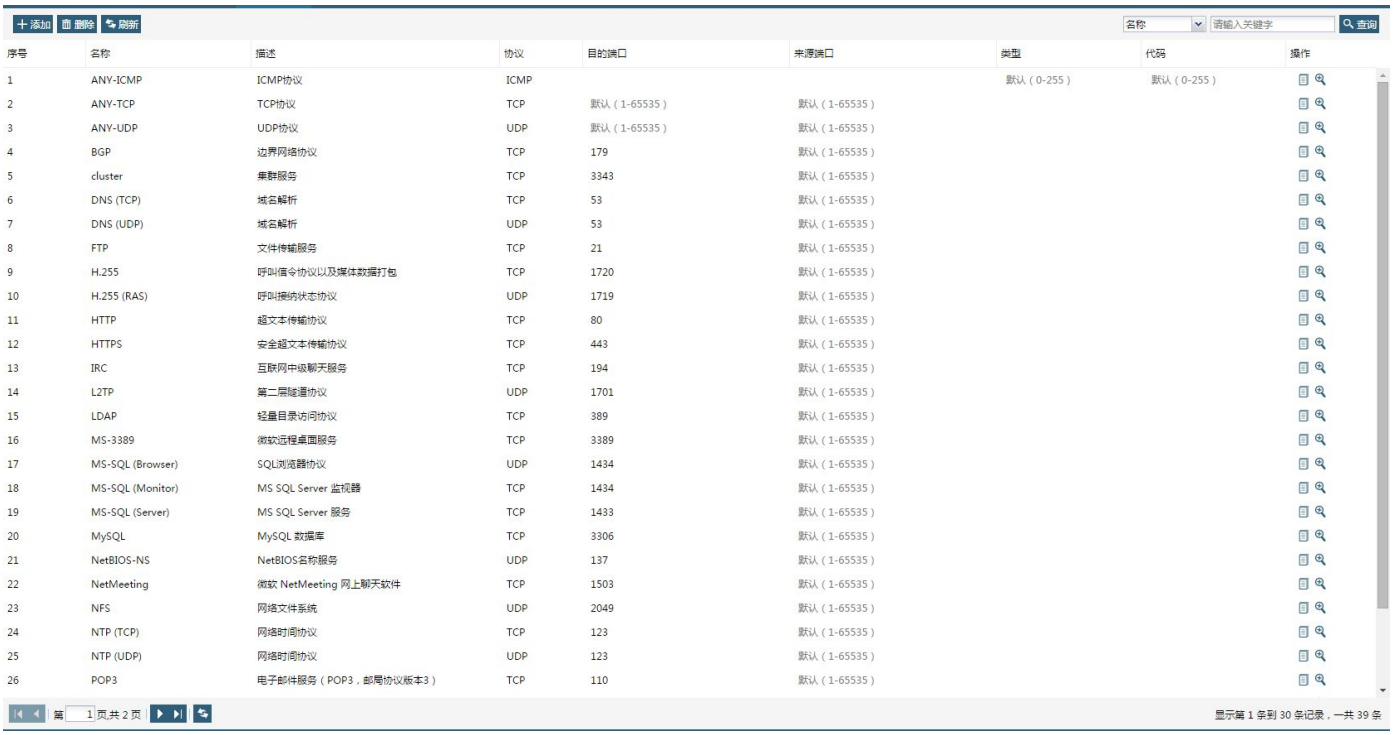
查询 MAC 地址

点击右上角下拉框，比如选择“名称”，在“输入关键字”一栏，输入已经存在的“123”或者“3”，点击【查询】按钮即可查出。

9.3.4 服务

该功能可以以协议加端口的形式定义一些服务对象，供构建策略时使用。在服务中添加的服务对象可

以被任何访问控制策略调用。设备中会默认保存一些常用的服务，只允许复制和查看，不允许修改和删除。



添加服务

点击【添加】按钮，弹出“服务列表-添加”对话框，如下图

- 名称：输入该地址的名称，支持 3 至 20 字符，且不可以以空格开头或结尾。
- 描述：可以填写关于该服务的说明。

- 协议：选择需要添加的协议，默认选择 TCP。
- 目的端口：对应服务的数据/连接的目的端口。不填写即默认所有端口，支持端口、端口段形式。
- 源端口：对应服务的数据/连接的源端口。一般无需填写，支持端口、端口段形式。
- 保存：内容填写完成后点击【保存】按钮，将保存更改到当前数据库。
- 重置：点击【重置】按钮以清空当前窗口中用户已经输入的内容以便用户重新输入。
- 取消：点击【取消】按钮不保存当前的用户输入并关闭窗口。

删除服务

未选中记录，点击【删除】按钮，弹出“系统提示”对话框，如下图

选择默认记录，点击【删除】按钮，弹出“系统提示”对话框，如下图，点击【是】，弹出“失败提示”对话框，如下图

选择自己添加的服务，选中，点击【删除】按钮，弹出“系统提示”对话框，点击【是】，成功删除该记录。

提示：

正在被访问控制使用的服务对象是不允许被删除的，执行删除操作时，系统会给出警告。

刷新服务

点击【刷新】按钮，刷新该页面。

查询服务

点击右上角下拉框，弹出“ 名称-描述“对话框。可以选择查询的条件，比如查询“名称”，选择“名称”，在“输入关键字”一栏，输入已经存在的“BGP”或者“G”，点击【查询】按钮即可查出。

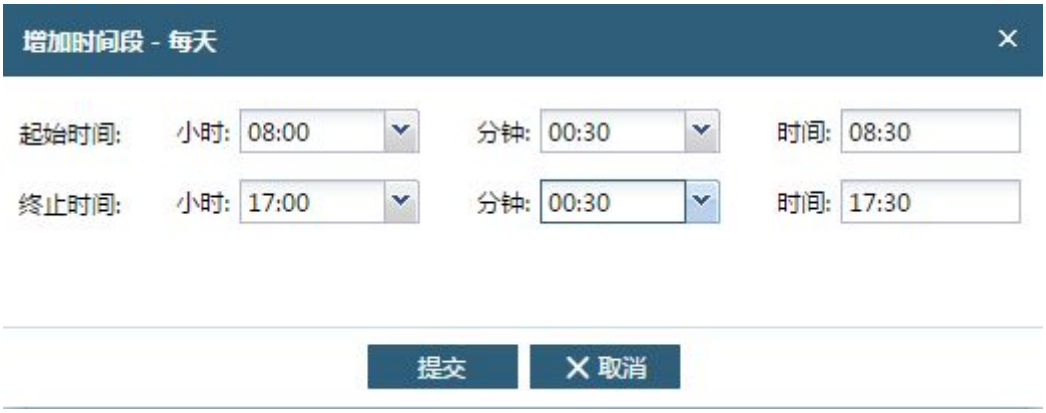
9.3.5 计划任务

本页面提供查看、添加和修改计划任务的功能。在防护策略、防病毒策略和访问控制功能中需要使用计划任务。

添加计划任务

点击【添加】，弹出“计划任务-添加”框，如下图；

输入“名称“和“说明”，点击【+】按钮；



选择起始时间和开始时间，点击【提交】；

点击【保存】，计划任务添加成功，您可以在防护策略、防病毒策略和访问控制的时候选择该计划任务。

修改计划任务

选中要修改的计划任务，点击【修改】；

修改完毕后点击【保存】。

删除计划任务

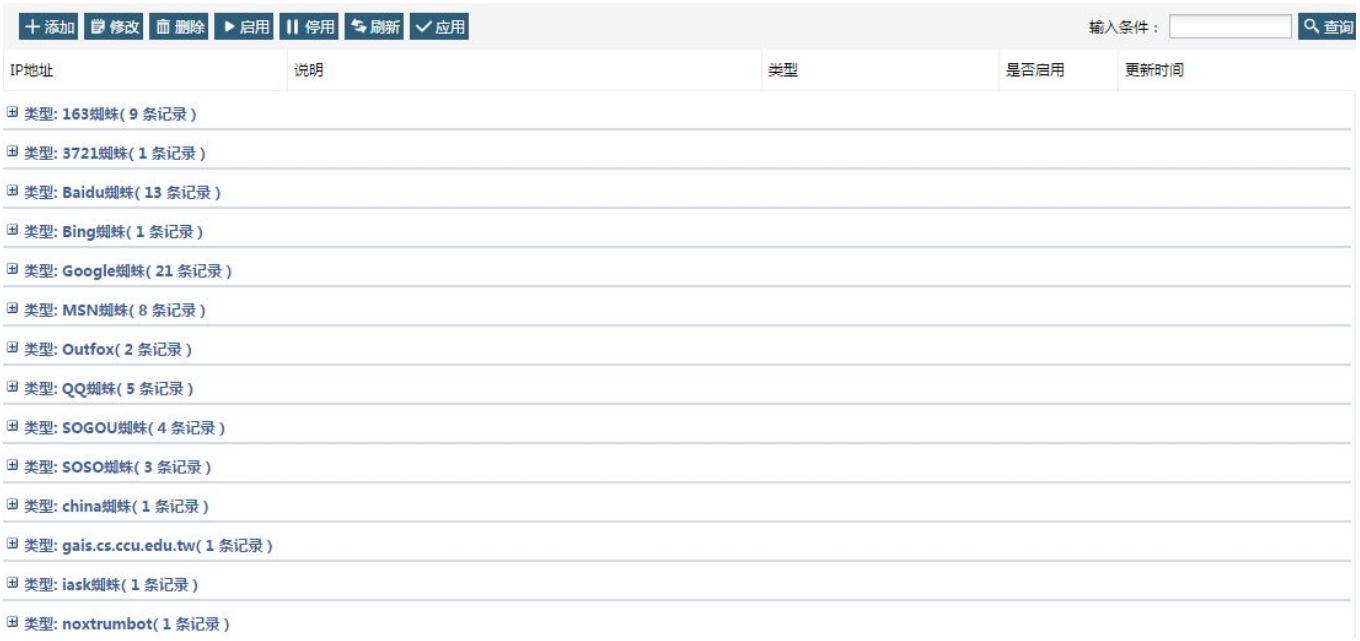
选中要删除的计划任务，点击【删除】，弹出确定对话框，点击【是】，成功删除计划任务。

提示:

系统提供 3 个默认的计划任务。名称为“全天”的计划任务是不可以删除的。时间段的添加支持多个时间段，例如：00:00-08:00,17:00-24:00。您可以根据您的需要自由添加。

9.3.6 蜘蛛设置

蜘蛛设置功能能够对搜索引擎的网页抓取行为进行“放行”操作，避免搜索引擎的蜘蛛被设备误拦截。设备中已经内置了一些常见的搜索引擎蜘蛛的 IP 地址。



【添加】：可以填写单独的 IP、IP 段、是否启用、蜘蛛类型、说明，来添加相关的蜘蛛信息。（注意：您可以在蜘蛛类型后直接输入新的蜘蛛类型以便添加一个新的蜘蛛类型。）

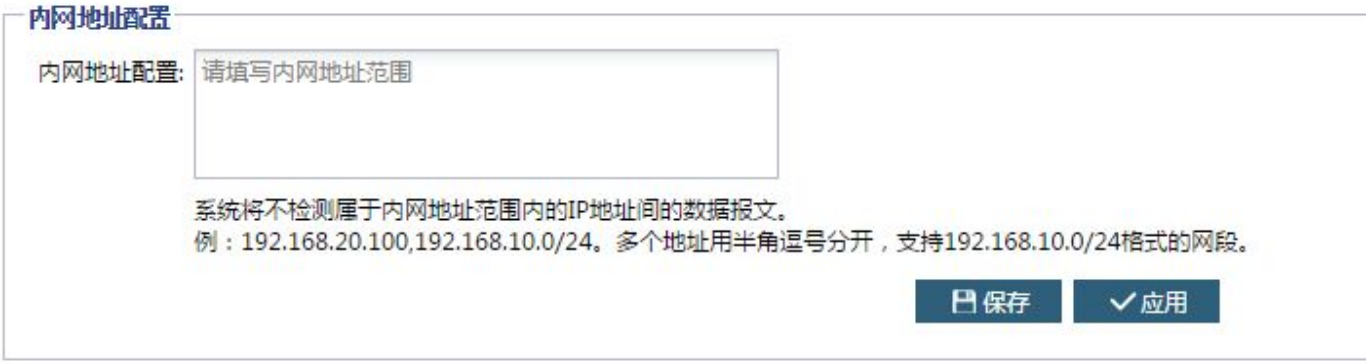
- 【修改】： 对已经添加的蜘蛛 IP 进行修改操作。
- 【删除】：删除已经添加的蜘蛛 IP。
- 【启用】：启用某条蜘蛛的 IP。
- 【停用】：停用某条蜘蛛的 IP。
- 【刷新】：刷新这个页面。
- 【应用】：当您修改了这个页面的内容后，可以点击【应用】以便使您的设置立即生效。

9.3.7 运营商地址

该功能预定义了四类运营商地址，分别为中国电信、中国移动、中国联通和教育网，供构建策略使用。

9.3.8 内网地址配置

系统将不检测属于内网地址范围内的 IP 地址间的数据报文。



10. 网络配置

10.1 接口

10.1.1 网络接口

该页面列出了设备所有网络接口的工作状态，包括接口名称、接口描述、设备类型、IP 地址、子网掩码、网关、连接状态、工作模式、接口属性等信息。

⚠注意：

DSI 是初始化接口，在设备初始配置时使用。如果一个网络接口的接口属性被配置为 DSI，通常简称为 DSI 接口，该接口的工作模式和接口属性都不能被修改。

DSI 接口提供 DHCP 服务，您可以在此设置 DHCP 服务分配的起始和结束 IP 地址。

如果您在【网络接口】页面修改了 DSI 接口 的 IP 地址，请相应地修改 DHCP 服务器的起始、结束地址，否则 DHCP 服务将无法正常工作。

配置网络接口为普通方式

1. 双击需要修改的网络接口，比如：ETH2，弹出“物理网口-修改”对话框；

2. 选择接口状态为“启用”；
3. 选择工作方式为“普通”选择网络类型“静态” “PPPOE” “DHCP”；
4. 填写“IP 地址”，“子网掩码”；
5. 如果该接口有相应的网关，请填写网关。如果没有，可以留空不填写；
6. 点击【保存】按钮，该设置生效并返回上一级页面。

配置网络接口为透明网桥方式

1. 双击需要修改的网络接口，比如：ETH2，弹出“物理网口-修改“对话框；

2. 选择“接口状态”为“启用”；
3. 选择“工作方式”为“透明网桥”；
4. 选择“选择网桥”，如果需要加入的网桥不存在，可以在【虚拟网桥】页面添加；
5. 点击【保存】按钮，该设置生效并返回上一级页面。

配置网络接口为策略路由方式

1. 双击需要修改的网络接口，比如：ETH2，弹出“物理网口-修改”对话框；

2. 选择接口状态为“启用”；
3. 选择工作方式为“策略路由”；
4. 选择接口属性为“WAN”或者“LAN”；
5. 填写“IPv4 地址”和“子网掩码”；
6. 点击【保存】按钮，该设置生效并返回上一级页面；

配置网络接口为端口汇聚方式

1. 双击需要修改的网络接口，比如：ETH2，弹出“物理网口-修改”对话框；

2. 选择“接口状态”为“启用”；
3. 选择“工作方式”为“端口汇聚”；
4. 选择对应的虚拟设备；（此虚拟设备需要在端口汇聚中添加，具体参照端口汇聚。）
5. 点击【保存】按钮，该设置生效并返回上一级页面。

⚠注意：

添加后的 combo 设备和普通网卡一样，可以配置为普通，透明，策略路由模式。

配置网络接口为 PPPOE 方式

1. 双击需要修改的网络接口，比如：ETH2，弹出“物理网口-修改”对话框；

2. 选择“接口状态”为“启用”；
3. 选择“网络类型”为“PPPOE”，选择 PPPOE 配置，点击立即连接将获取到 pppoe 地址。
4. PPPOE 配置页面：

配置网络接口为普通方式(IPV6)

1. 双击需要修改的网络接口，比如：ETH2，弹出“物理网口-修改”对话框；
2. 选择接口状态为“启用”；
3. 选择工作方式为“普通”，选择网络类型为“静态”；
4. 填写“IPv6 地址”，“IPv6 前缀”；
5. 如果该接口有相应的网关，请填写网关，如果没有，可以留空不填写；
6. 点击【保存】按钮，该设置生效并返回上一级页面。

IPV6 入侵记录识别

1. 内网地址配置为 IPV6 的地址；
2. 配置透明网桥使内网可以访问公网地址；

3. 在数据中心的入侵记录中可以查询到公网 IPV6 地址对内网产生的入侵。

10.1.2 虚拟网桥

工作于透明模式的网络接口必须从属于某个虚拟网桥，在本页面可以查看虚拟网桥的数量、名称、每个虚拟网桥拥有的网络接口，您也可以在此页面添加、删除、修改虚拟网桥。在配置高可用性功能时，根据您网络环境中的交换机配置，选择是否开启 STP，以及相关的 STP 参数的设置。

注意：

虚拟网桥所允许的最大数量与设备型号有关，具体请联系铱迅信息或者供货商。

10.1.3 PPPoE 设置

10.1.4 VLAN 网络设置

本设备支持 802.1Q Tag VLAN，如果您的网络环境配置了 VLAN 并且经过本设备的数据包带有 VLAN 的标记，您需要开启 VLAN 功能。

1. 开启 802.1Q VLAN 功能，勾选“开启 802.1Q VLAN 数据包检测”；
2. 点击【应用】按钮，则当前 VLAN 设置生效。

10.1.5 接口管理

配置设备管理接口（DMI）

DMI 是设备管理接口，通过该接口访问设备的管理页面。如果一个网络接口的接口属性被配置为 DMI，通常简称为 DMI 接口。

⚠注意：

只有工作模式为普通，且不是 DSI 接口的网络接口才能配置为管理接口。

系统允许配置多个设备管理接口。

10.1.6 端口汇聚算法

关于端口汇聚算法，需要配合已有环境进行选择，如果算法不对将造成端口汇聚效果降低或者无法工作。

10.2 路由

10.2.1 静态路由

用于配置系统当前的静态路由表，具体界面如下图。您可以添加、修改、删除静态路由。配置完成后，必须点击【应用】按钮以便使配置生效。

添加路由

您可以添加到主机或者某一网段的路由，请务必保证目的网段和下一跳地址的正确有效；根据需求设置合理的管理距离。

点击【添加】，弹出添加“静态路由-添加”对话框；

1) 填写“目的网段”；
2) 填写“下一跳地址”；
3) 填写“优先级”；

点击【保存】按钮，返回上一级页面。点击重置取消当前配置。点击取消不保存当前配置。

删除路由

您还可以在选择一行路由，点击删除按钮来删除一个路由。您还可以点击右侧的删除按钮来进行删除。

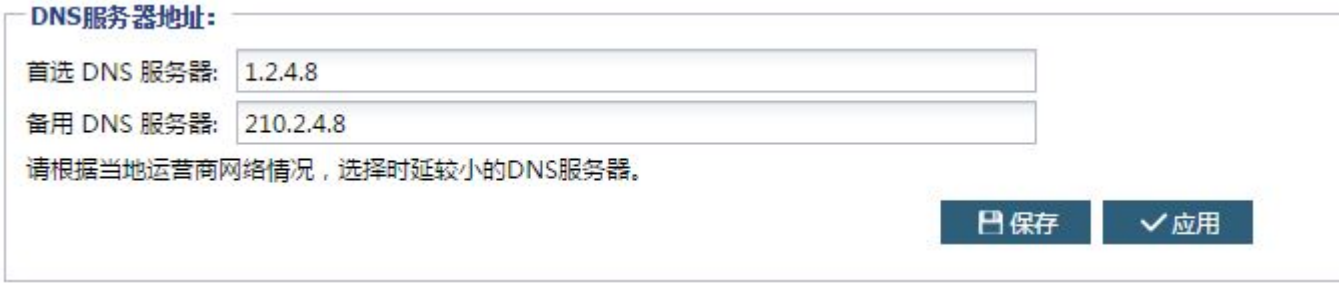
10.2.2 路由信息

用于展示系统当前的路由信息，具体界面如下图。

10.3 高级网络应用

10.3.1 本地 DNS 配置

设置 DNS 服务器地址，系统的邮件通知、漏洞扫描等功能依赖于 DNS 设置，因此建议您最好配置 DNS 服务器地址。



⚠注意：

如果您不清楚 DNS 服务器地址，请联系网络管理员获得。

10.3.2 DNS 代理

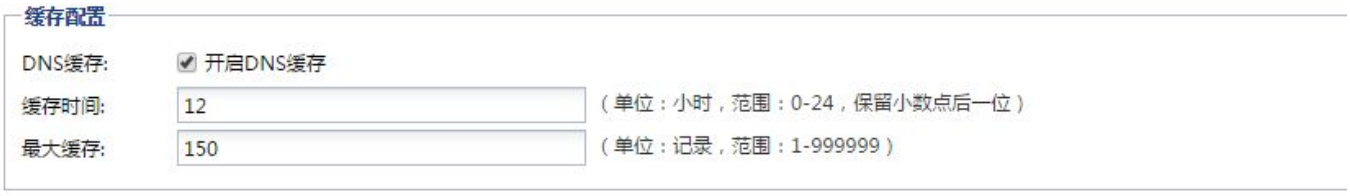
DNS 代理由 DNS 设置、DNS 缓存设置、域名代理设置、静态条目设置四部分组成。

DNS 地址设置

设置 DNS 服务器地址，在勾选上“开启 DNS 代理功能”选项后，内网用户可将自己电脑的 DNS 设置为此功能监听的接口 IP。内网的所有 DNS 解析请求指向页面“首选 DNS”或者“备选 DNS”所配置的 DNS 地址。

DNS 缓存设置

开启 DNS 缓存后、本设备相当于一台本地 DNS 服务器，内网用户可将自己电脑的 DNS 设置为此功能监听的接口 IP。内网的所有 DNS 解析请求，仅第一次需要向外网请求，以后的请求由 DNS 缓存功能通过查找其缓存完成。



- 缓存时间：缓存记录生效的时间，超过时间，缓存记录将失效
- 最大缓存：缓存记录的条数

域名代理设置

通过设置域名代理，在访问符合记录的域名时，DNS 请求就会指向记录所配置的 DNS 地址。入下图所示，访问以.com 结尾的域名，DNS 请求的 DNS 服务器地址为 218.9.2.3，而访问以.cn 结尾的域名时，DNS 请求的 DNS 服务器地址为 114.114.114.114。

- 名称：该条记录的名称
- 域名：需要特定 DNS 服务器的域名，或者某个域名集合

静态条目设置

设置静态条目后，访问配置的域名，直接指向所对应的 IP，类似于电脑里面 hosts 文件的作用，如图示，访问 www.baidu.com，实际就是访问 1.1.1.1 的 IP 地址。

⚠注意:

“开启 LAN 劫持功能”此功能在开启情况下， DNS 代理对设备上所有的 LAN 口流量生效。反之，如果不开启“DNS 劫持”，在 DNS 监控的接口后面接的客户机必须要把本机 DNS 设置成为 DNS 监控的接口 IP，否则 DNS 代理设置不生效

如果 4 个配置项都配置，其优先顺序为：静态条目->DNS 缓存->域名代理解析-> DNS 地址设置

10.3.3 动态 DNS

DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程

序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。

注册用户名

点击“注册用户名”按钮，链接到花生壳官网进行注册用户

添加

点击“添加”按钮，正确填写相关信息，如下图所示：

保存后，查看服务已连接，如下图：

DDNS 捕获用户每次变化的 IP 地址，然后将其与域名相对应，这样其他上网用户就可以通过域名来进行交流，而最终客户所要记忆的全部就是记住动态域名商给予的域名即可。

10.3.4 UPnP 服务

UPnP（Universal Plug and Play， 通用即插即用）协议，遵循此协议的不同厂商的各种设备可以自动发现对方并进行连接。

防火墙开启了 UPnP 服务后，局域网中的主机就可以根据软件的需要自动地在防火墙上打开相应的端口，使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源，这样原本受限于 NAT 的功能便可以正常使用。相对于转发规则而言，UPnP 的应用不需要用户手动设置任何规则，对于一些端口不固定的应用会更加方便。

功能设置：启用 UPnP 服务后，使用电驴，迅雷等支持 UPnP 的下载可看到打开的端口。

当该应用程序关掉之后，相应的 UPnP 服务打开的端口就会关掉，列表的内容将会被删掉。

注意:

一些木马、病毒可能会利用 UPnP 服务打开特定的端口，使局域网主机成为黑客的攻击目标，因此需谨慎应用 UPnP 服务。

10.3.5 HTTP 缓存加速

缓存加速主要用于 Web 服务器之间（1 个或多个，内容源服务器）和客户端之间（1 个或多个），缓存加速会根据进来的请求保存输出内容的副本，例如 html 页面， 图片，文件（统称为副本），然后，当下一个请求来到的时候，如果是相同的 URL，缓存直接使用副本响应访问请求，而不是向源服务器再次发

送请求。

缓存加速设置

⚠注意：

加速接口的选择，网关模式下选择连接内网接口，网桥模式下选择虚拟网桥接口，加速接口必须配置 IP。

10.3.6 DHCP 服务

设备为客户提供能够 DHCP 功能的地址，客户可以根据所需要对某个具体的网络接口配置成 DHCP 服务接口，并且可以配置租用期以及绑定地址。

1. 点击“添加”按钮

2. 点击“修改”按钮：当选中某条记录点击修改按钮时，你可以重新配置该条策略。
3. 点击“删除”按钮：当选中某条记录点击删除按钮时，你可以将该记录删除。
4. 点击“启/停用”按钮：当选中某条记录点击启/停用按钮，将改变此记录的工作状态。
5. 点击“应用”按钮：当选中某条记录点击应用按钮时意味着使用此记录。
6. 配置成功后页面显示如下：

10.3.7 镜像流量监测

支持端口镜像，端口镜像只能对镜像的流量进行检测，不能真正防护 Web 服务器，您可以参照以下方式进行部署。

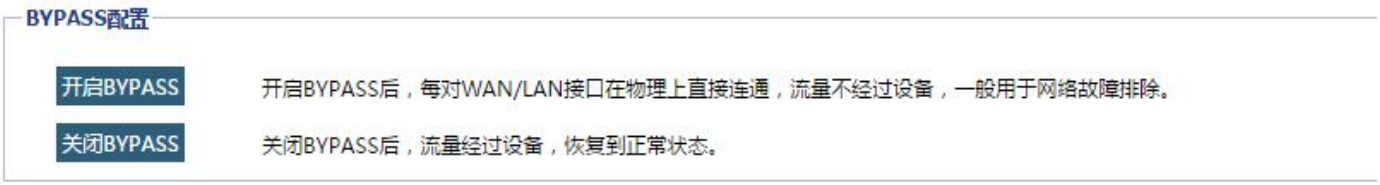
1. 勾选“是否开启端口镜像检测”，点击【保存】；

2. 将交换设备的镜像端口接到本设备的 WAN 接口，同时将 LAN 接口接到本设备的任意一个未使用的网络接口即可。

提示：

端口镜像功能只能对镜像端口的数据报文进行检测，不能进行拦截或者阻断。

10.3.8 BYPASS



- 【开启 BYPASS】:开启 BYPASS 后，设备不检测经过设备的流量。
- 【关闭 BYPASS】:关闭 BYPASS 后，设备检测经过设备的流量。

10.4 OSPF 路由

OSPF(Open Shortest Path First 开放式最短路径优先）是一个内部网关协议(Interior Gateway Protocol，简称 IGP），用于在单一自治系统（autonomous system,AS）内决策路由。是对链路状态路由协议的一种实现，隶属内部网关协议（IGP），故运作于自治系统内部。著名的迪克斯加算法(Dijkstra)被用来计算最短路径树。OSPF 分为 OSPFv2 和 OSPFv3 两个版本,其中 OSPFv2 用在 IPv4 网络，OSPFv3 用在 IPv6 网络。OSPFv2 是由 RFC 2328 定义的，OSPFv3 是由 RFC 5340 定义的。

10.4.1 OSPF 接口

用于配置系统当前的 OSPF 接口属性，具体界面如下图。

您可以修改 OSPF 路由接口属性，选择该接口属性是否为被动接口，认证方式为不认证、明文或者 MD5（明文的时候需要输入口令，MD5 的时候需要输入 key ID 以及口令，路由器之间必须配置相同的认证密码，如果密码不同，则无法形成邻居）。

接口开销，开销是用来衡量到达目标位置的代价，其值是两点之间某条路径上所有链路开销的总和。最小的路径开销是到达目标点的最佳路径。

hello 间隔时间，dead 时间，路由器之间的 Hello 时间和 Dead 时间必须一致，否则无法形成邻居。OSPF 接口发送 Hello 报文的时间间隔，即 Hello 报文发送计时器。这个值在 Hello 报文中被通告。这个 Hello 包发送间隔越小，则可以越快地检测到拓扑结构所发生的变化，但这样也会带来额外的路由通信负担。在一个指定的网络中的所有路由器和访问服务器中的这个值的设置必须相同。seconds 参数的取值范围为 1～65535 秒，以太网接口的默认值为 1 秒，非广播型接口的默认值为 30 秒。

接口优先级，接口设置路由器优先级，这样就可以帮助确定网络中的指定路由器，用于 DR 和 BDR 路由器选举。number-value 参数的取值范围为 0～255，默认优先级均为 1，值越大，优先级越高。优先级设置为 0 的路由器不能成为 DR 或者 BDR 路由器。路由器优先级仅需要在连接多路访问网络的接口配置，也就是说在连接点对点网络的接口上是不用设置优先级的。

当连接到同一个网络中的两个路由器都想成为 DR 或者 BDR 路由器时，具有本命令所设置的优先级越高的路由器，将优先成为 DR 或者 BDR 路由器。如果两个路由器的优先级设置一样，

则要看连接同一网络中的两路由器的路由器 ID 了，路由器 ID 值越小越优先。

配置重传时间间隔，在收不到对方报文回应的情况下，多长时间重新发送一次。

MTU 不匹配检测是否开启，开启之后会检查 MTU 值。两端路由器的 MTU 值应当一致，如果开启检测，MTU 值不一致，OSPF 不能正常建立邻居。

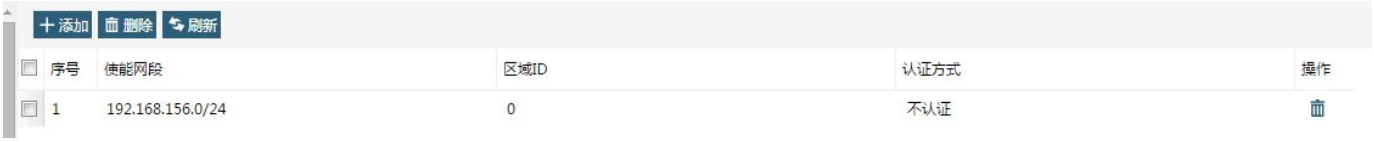
修改接口属性

可以点击右边的修改按钮来进行修改，或者双击该行进行修改。

配置完成之后，点击保存按钮进行保存，或者取消按钮不保存；您还可以选择恢复默认设置，所有的配置将恢复为默认值。

10.4.2 使能网段

用于配置系统当前的 OSPF 使能网段，添加该网段之后，该接口网段即加入 OSPF 属性，使能网段配置格式为 192.168.156.0/24.



添加使能网段

您可以点击添加按钮，添加一个您想使能的网段，使其加入 OSPF 路由，并配置该使能网段的区域 ID 以及认证方式，路由器之间必须配置在相同的 OSPF 区域，否则无法形成邻居，此外，认证方式以及口令

也必须保持一致，否则无法建立邻居。

删除使能网段

您还可以在选择一行使能网段，点击删除按钮来删除一个使能的网段。您还可以点击右侧的删除按钮来进行删除。

刷新使能网段

您还可以点击刷新按钮重新刷新页面。

10.4.3 全局配置

用于配置系统当前的 OSPF 参数，配置路由器 ID，一般配置为经常为 up 状态的接口 IP 地址，每一台 OSPF 路由器只有一个 Router-ID，Router-ID 使用 IP 地址的形式来表示。

配置域内优先级，域间优先级，外部优先级，这样就可以帮助确定网络中的指定路由器，用于 DR 和 BDR 路由器选举。number-value 参数的取值范围为 0～255，默认优先级均为 1，值越大，优先级越高。优先级设置为 0 的路由器不能成为 DR 或者 BDR 路由器。路由器优先级仅需要在连接多路访问网络的接口配置，也就是说在连接点对点网络的接口上是不用设置优先级的。当连接到同一个网络中的两个路由器都想成为 DR 或者 BDR 路由器时，具有本命令所设置的优先级越高的路由器，将优先成为 DR 或者 BDR 路由器。如果两个路由器的优先级设置一样，则要看连接同一网络中的两路由器的路由器 ID 了，路由器 ID 值越小越优先。

配置 SPF 计算间隔等参数，多长时间利用 SPF 算法计算一次 OSPF 路由开销值等，以便 OSPF 路由

可以很好的运行在当前网络。

此外您还可以进行路由重分布配置，选择在 OSPF 中是否引入其他路由协议，目前系统支持引入直连路由、RIP 路由、静态路由，您还可以配置引入路由的度量值。

配置完成之后点击确定保存，取消不保存。

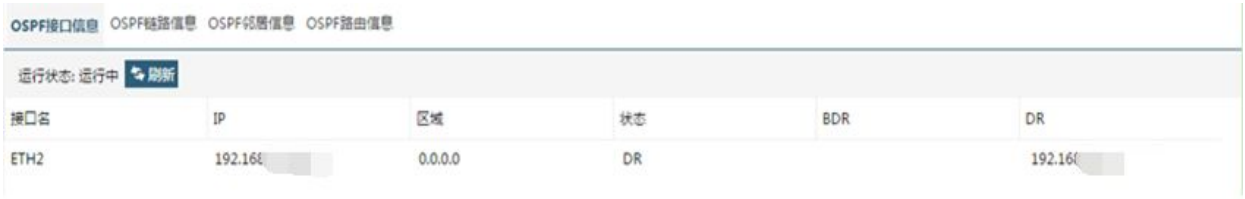
恢复默认设置

配置完成之后，您还可以选择恢复默认设置，所有的配置将恢复为默认值。

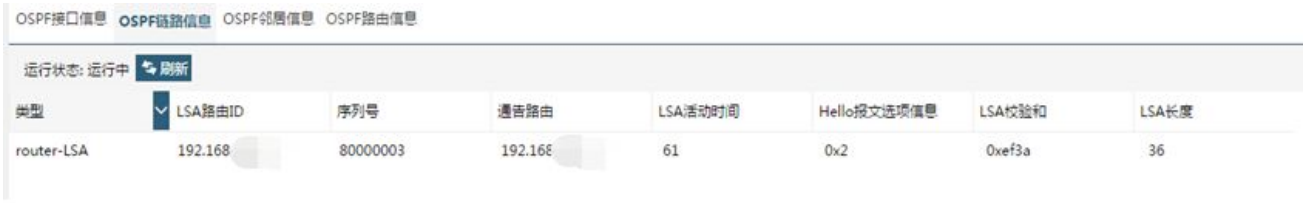
10.4.4 OSPF 信息

选举优先级最高的成为 DR，优先级数字越大，表示优先级越高，被选为 DR 的几率就越大，次优先

级的为 BDR，优先级范围是 0-255，默认为 1，优先级为 0 表示没有资格选举 DR 和 BDR。如果在优先级都相同的情况下，Route-Id 最大的成为 DR，其次是 BDR，数字越大，被选为 DR 的几率就越大。路由信息页面您可以查看配置 OSPF 的接口信息状态，如下图所示：

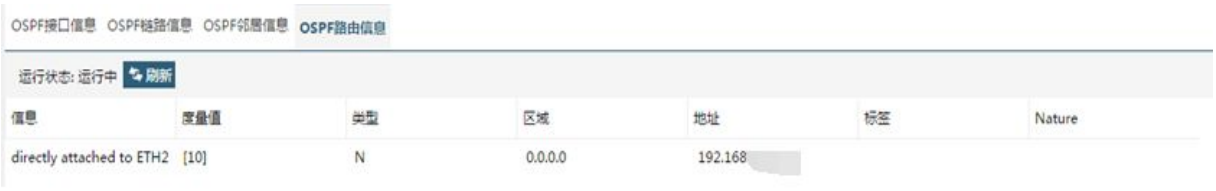


OSPF 链路状态信息，在配置完成 OSPF 之后，您需要在该页面点击开始按钮来启动 OSPF，启动之后可以查看 OSPF 是否建立起链路，链路状态（LSA）就是 OSPF 接口上的描述信息，例如接口上的 IP 地址，子网掩码，网络类型，Cost 值等等，OSPF 路由器之间交换的并不是路由表，而是链路状态（LSA），OSPF 通过获得网络中所有的链路状态信息，从而计算出到达每个目标精确的网络路径。如下图所示：



OSPF 只有邻接状态才会交换 LSA，路由器会将链路状态数据库中所有的内容毫不保留地发给所有邻居，要想在 OSPF 路由器之间交换 LSA，必须先形成 OSPF 邻居，OSPF 邻居靠发送 Hello 包来建立和维护，Hello 包会在启动了 OSPF 的接口上周期性发送，在不同的网络中，发送 Hello 包的间隔也会不同，当超过 4 倍的 Hello 时间，也就是 Dead 时间过后还没有收到邻居的 Hello 包，邻居关系将被断开。两台路由器之间如果 OSPF 建立成功，可以看到对端邻居的信息

通过查看 OSPF 路由信息页面，可以查看 OSPF 是否建立起路由，可以采用 ping 方式查看建立的路由是否正常：



10.5 RIP 路由

路由信息协议（RIP）是内部网关协议 IGP 中最先得到广泛使用的协议。RIP 是一种分布式的基于距离矢量的路由选择协议，是因特网的标准协议，其最大优点就是实现简单，开销较小。

RIP 协议的默认管理距离是 120，RIP 所接收的路由信息都被封装在 UDP 协议的数据报中，在 UDP 的 520 端口接收来自远程路由的信息。

RIP 使用 Hop Count（跳计数）作为路径选择的度量值。最大跳数是 15，如果最大跳数大于 15，则认为该网络失效。RIPv1 采用广播式更新，RIPv2 采用组播更新方式，RIP 默认每隔 30 秒周期性的发送整个路由表给邻路由。

10.5.1 RIP 接口

用于配置系统当前的 RIP 接口属性，具体界面如下图。

您可以修改 RIP 路由接口属性，选择该接口属性是否为被动接口，配置为被动接口之后，该接口不会主动发送 RIP 更新报文，但是可以接收 RIP 更新报文。

是否执行水平分割，从一个接口学习到的路由不会再广播回该接口。

认证方式为不认证、明文或者 MD5（明文或者 MD5 的时候需要输入钥匙链以及口令），目前支持接收版本为 RIP V1，RIP V2，发送版本支持 RIP V2。

刷新接口属性

您可以点击刷新按钮刷新页面。

修改接口属性

您还可以点击右侧的修改按钮来进行修改。

配置完成之后，点击保存按钮进行保存，取消按钮不保存。

恢复默认值

配置完成之后，您还可以选择恢复默认设置，所有的配置将恢复为默认值。

10.5.2 使能网段

用于配置系统当前的 RIP 使能网段，添加该网段之后，该接口网段即加入 RIP 属性，使能网段配置格式为 192.168.152.0/24.

1. **添加使能网段**

您可以点击添加按钮，添加一个您想使能的网段，使其加入 RIP 路由。

配置完成之后可以点击保存按钮进行保存，重置按钮清空数据，取消按钮不保存。

2. **删除使能网段**

选中您所配置的使能网段，点击删除按钮来删除所配置的使能网段。此外也可以点击右侧的删除按钮来删除。

3. **刷新使能网段**

您还可以点击刷新按钮刷新页面。

10.5.3 邻居配置

配置 RIP 邻居的 IP 地址，这样可以保证被动接口只给对应的邻居发送 RIP 的更新数据包。

添加邻居信息

您可以点击添加按钮，添加一个您想建立邻居的 IP，使其加入 RIP 路由。

配置完成之后可以点击保存按钮进行保存，重置按钮清空数据，取消按钮不保存。

删除邻居信息

您还可以选中您所配置的邻居信息，点击删除按钮来删除所配置的邻居 IP。此外也可以点击右侧的删除按钮来删除。

刷新邻居信息

您还可以点击刷新按钮刷新页面。

10.5.4 全局配置

在该界面服务开关，点击开始运行 RIP 服务，您还可以点击暂停按钮来暂停 RIP 服务。

您还可以配置系统当前的 RIP 参数，路由优先级，以确定 RIP 在网络系统中的优先级，路由器选择路由协议的依据就是路由优先级。给不同的路由协议赋予不同的路由优先级，数值小的优先级高。当有到达同一个目的地址的多条路由时，可以根据优先级的大小，选择其中一个优先级数值最小的作为最优路由，并将这条路由写进路由表中。

配置定时器，定时更新时间，超时定时器，垃圾收集时间等，垃圾收集时间一般要大于超时定时器，以便路由有足够的时间来老化；路由器以 30 秒一次地将整个路由表以应答消息地形式发送到邻居路由器。路由器收到新路由或者现有路由地更新信息时，会设置一个 180 秒地超时时间。如果 180 秒没有任何更新信息，路由的跳数设为 16。路由器以度量值 16 宣告该路由，直到刷新计时器从路由表中删除该路由。刷新计时器的时间设为 240 秒，或者比过期计时器时间多 60 秒。Cisco 还用了第三个计时器，称为抑制计时器。接收到一个度量更高的路由之后的 180 秒时间就是抑制计时器的时间，在此期间，路由器不会用它接收到的新信息对路由表进行更新，这样能够为网络的收敛提供一段额外的时间。

此外您还可以进行路由重分布配置，选择在 RIP 中是否引入其他路由协议，目前系统支持引入直连路由、OSPF 路由、静态路由，您还可以配置引入路由的度量值。

配置完成之后可以点击确定按钮保存数据或者取消按钮不保存。

恢复默认设置

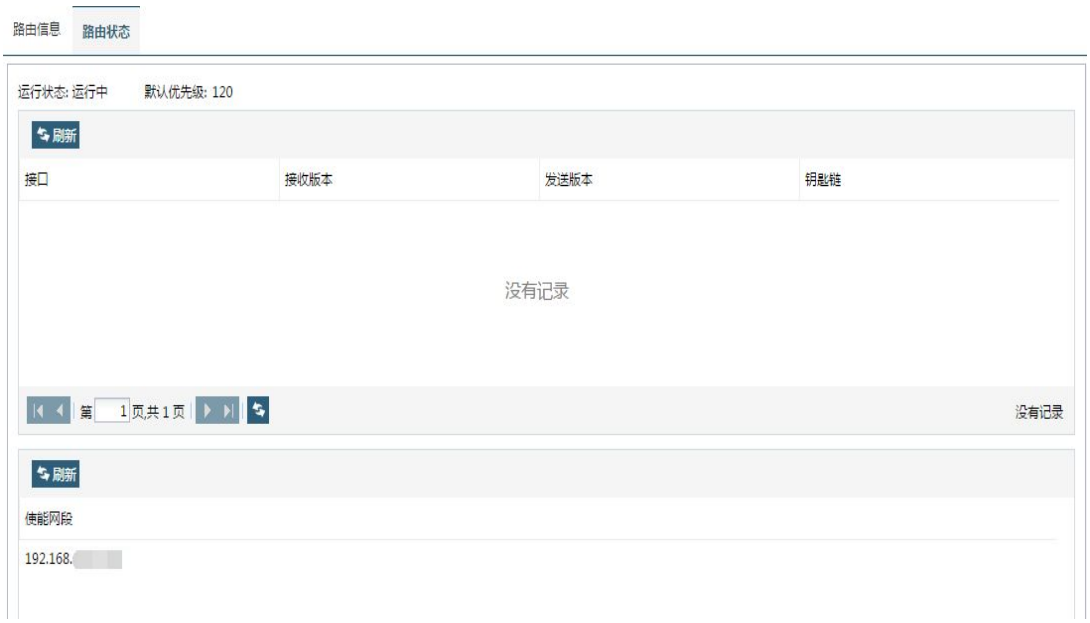
配置完成之后，您还可以选择恢复默认设置，所有的配置将恢复为默认值。

10.5.5 RIP 信息

路由信息页面您可以查看 RIP 路由信息表以及 RIP 路由状态表。

在 RIP 路由信息表您可以查看到使能 RIP 的接口配置信息，使能的网段以及配置的哪些接口类型为被动接口。

在 RIP 路由状态表您可以看到当前建立的 RIP 路由信息。



11. 系统配置

11.1 基本配置

11.1.1 时间设置

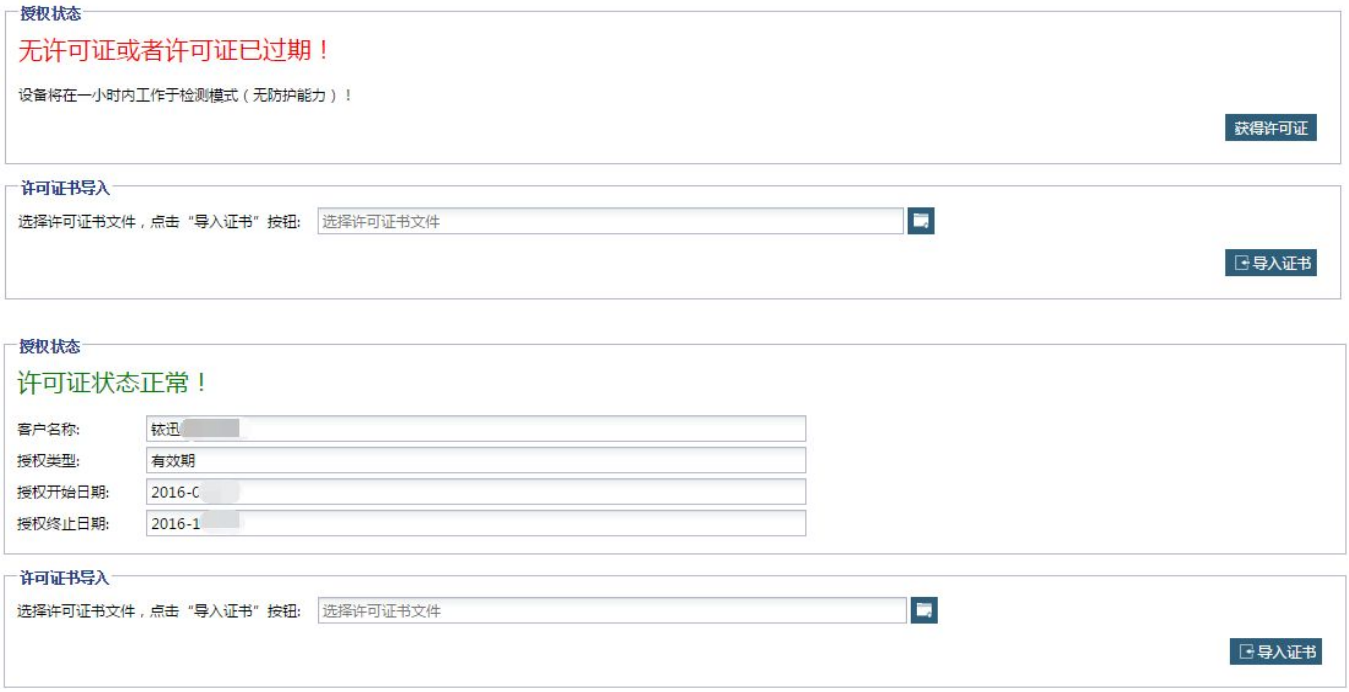
本页面设置设备的系统时间。设置好时间后，点击【应用】按钮，完成系统时间设定。您也可以设置时间同步服务，系统缺省的服务器地址 210.72.145.44 为中国国家授时中心的 NTP 服务器的 IP 地址。

11.1.2 产品授权

用于显示本设备的授权信息。每一台铱迅入侵防御系统都有唯一的许可证书，该许可证文件只能导入一次，重复导入相同证书无效。同时，许可证书不能在不同型号、同型号不同设备之间混用。

当设备没有许可证或者许可证已经过期的情况下，使用安全管理员账号登录时会显示如下页面。

当本设备许可证是有效期授权类型的，使用安全管理员账号登录时，可以看到当前的许可证状态如下。



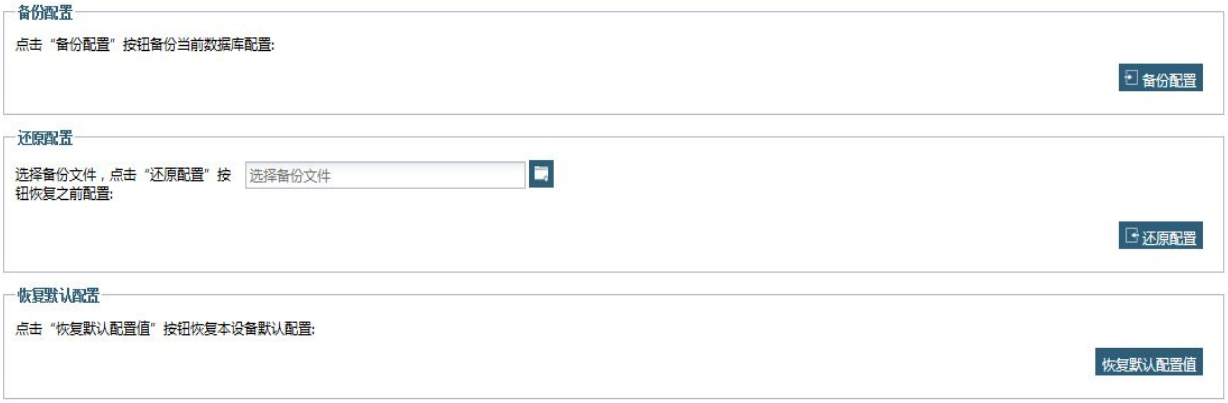
当本设备许可证是终身授权类型的，使用安全管理员账号登录时，可以看到当前许可证状态如下。

注意：

当设备没有许可证或者许可证已经过期时，铱迅入侵防御系统将在一小时之内关机。如果遇到上述情况，请及时联系供货商或者铱迅信息以便获取有效许可证书。

11.1.3 配置管理

用于备份和还原当前系统的设置，这些设置包括网络设置、基本参数设置、通知设置等。



- 【备份配置】： 点击【备份配置】按钮，按照提示将备份配置文件保存到计算机的指定目录中。
- 【还原配置】： 选择还原配置文件后，点击【还原配置】按钮，将备份文件导入到设备，恢复之前保存的配置。
- 【恢复默认配置值】： 点击【恢复默认配置值】按钮，则本设备的网络设置、基本参数设置、通知设置等将被恢复为默认值。

⚠注意：

1.只有从本设备导出的配置文件才可导入，系统不支持导入从其他设备导出的配置文件。

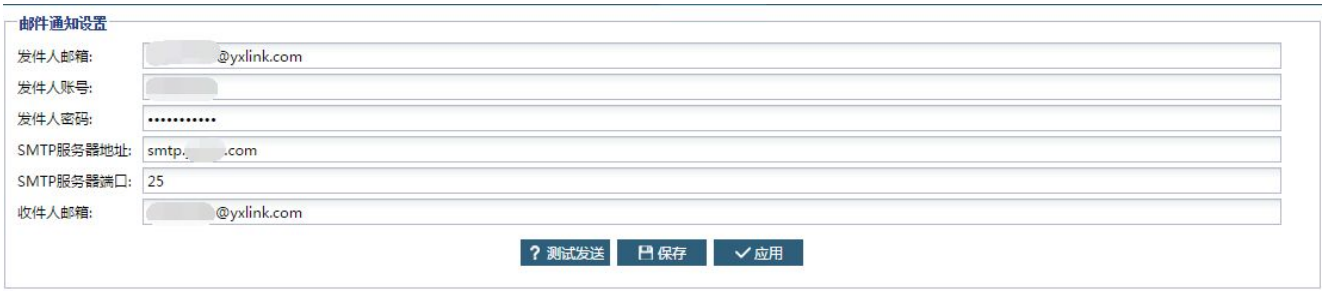
2.请不要手动修改导出的配置文件，以免造成无法导入。

3.建议您在配置好本设备后就导出一份配置文件并存放于安全的地方，以便日后需要时导入使用。

11.1.4 告警管理

邮件通知设置

本页面设置用于发送通知邮件的邮箱信息，包括发送邮件的 SMTP 服务器信息，以及接收通知的邮箱地址。



SMTP 设置：

“发件人邮箱”： 用于发送邮件的邮箱。

“发件人账号”： 用于发送邮件的账号名称。

“发件人密码”： 用于发送邮件的邮箱密码。

“SMTP 服务器地址”： 用于发送邮件的 SMTP 服务器地址。

“SMTP 服务器端口”： 用于发送邮件的 SMTP 服务器端口。

通知邮箱设置：

“收件人邮箱”：用于接收通知邮件的邮箱。

提示：

当本设备磁盘空间使用率接近设置上限的 90%的时候，本设备将自动发送邮件提醒管理员。

Email 报警

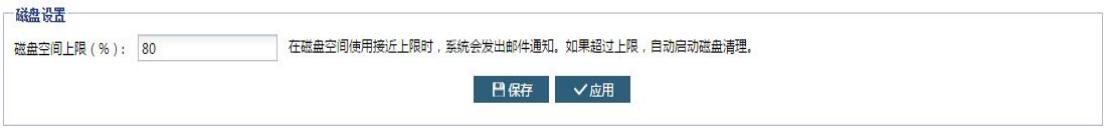
该功能可以在发现高危的入侵记录时立即给管理员发送 Email 报警，并且可以在指定的统计周期内当入侵记录达到阈值时，自动给管理员发送通知邮件。

- “入侵记录”：是否开启该功能的选项。
- “立即报警”：发现高危入侵时是否立即发送 Email 报警。
- “发送周期”：设置统计周期。
- “入侵记录阈值”：设置在该统计周期内入侵记录的阈值，达到该值发送 Email 报警。
- “计划任务”：设置该功能的生效时间。

- “系统资源告警”：是否开启该功能的选项。
- “检测周期”：设置统计周期
- “CPU 阀值”：设置在该统计周期内 CPU 使用率的阈值，达到该值发送 Email 报警。
- “内存阀值”：设置在该统计周期内内存使用率的阈值，达到该值发送 Email 报警。
- “流量阀值”：设置在该统计周期内流量的阈值，达到该值发送 Email 报警。
- “发送时段”：设置该功能的生效时间。

11.1.5 磁盘清理

系统会在磁盘空间使用率达到设置上限时自动执行磁盘清理工作。设备的“自动清理”会从最早的日志记录开始清理，直到磁盘空间的使用率低于设置值，所以请您记得定期备份日志。



除了系统自动清理功能，您还可以手动进行磁盘清理，在手动清理时，建议您先将日志导出后再删除。

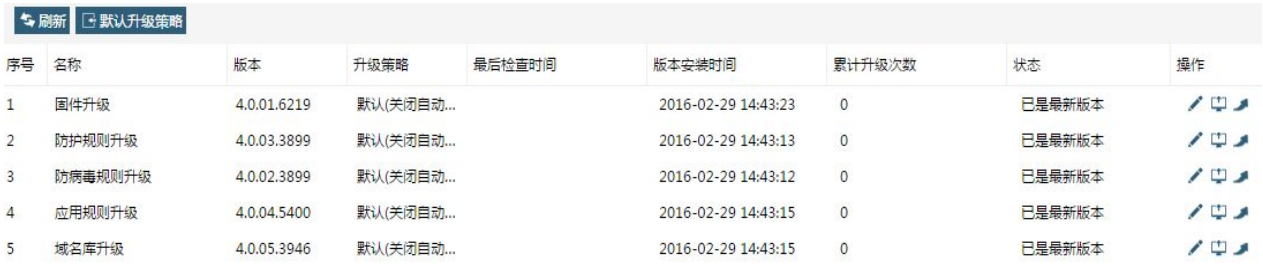
- “当前状态”： 显示磁盘当前的使用情况，用户可根据磁盘使用率来决定是否进行清理。
- “日志类型选择”： 选择要处理的日志类型，包括入侵记录、防病毒记录、系统日志等。
- “操作日期选择”： 可选择某个日期之前的所有记录或者选择一个日期的范围。
- 【导出】： 首先选择需要导出的日志类型和时间范围，点击【导出】按钮，导出的格式为 csv 文件。请用 Microsoft Excel 等软件查看。导出的日志将无法再导入到设备中。
- 【删除】： 首先选择需要删除的日志类型和时间范围，点击【删除】按钮，则指定的日志被直接删除。

⚠注意：

日志删除后不可以恢复，请您确认不再需要查看所选的日志后再决定将其删除。建议您在删除前将日志导出以便日后查看。

11.1.6 升级配置

通过升级配置，您可以获得最新的产品功能、规则、病毒库、网址库。



产品提供两种升级方式：

离线升级

点击 ，弹出升级界面，选择相应的文件点击【确定】即可升级。

离线升级请联系铱迅信息客服人员，然后提交产品序列号，根据您所购买的产品型号获取相应的升级文件，选择升级文件后，点击【升级】按钮，完成产品升级。

升级后，请进入【系统日志】页面查看相关系统日志。

在线升级

点击【默认升级策略】，如下图，按需制定升级策略，当触发升级条件并且有新版本的时候，会根据升级策略执行对应的动作。

也可点击，对固件或者规则制定单独的升级策略。

注意：

在线升级需设备能访问互联网。

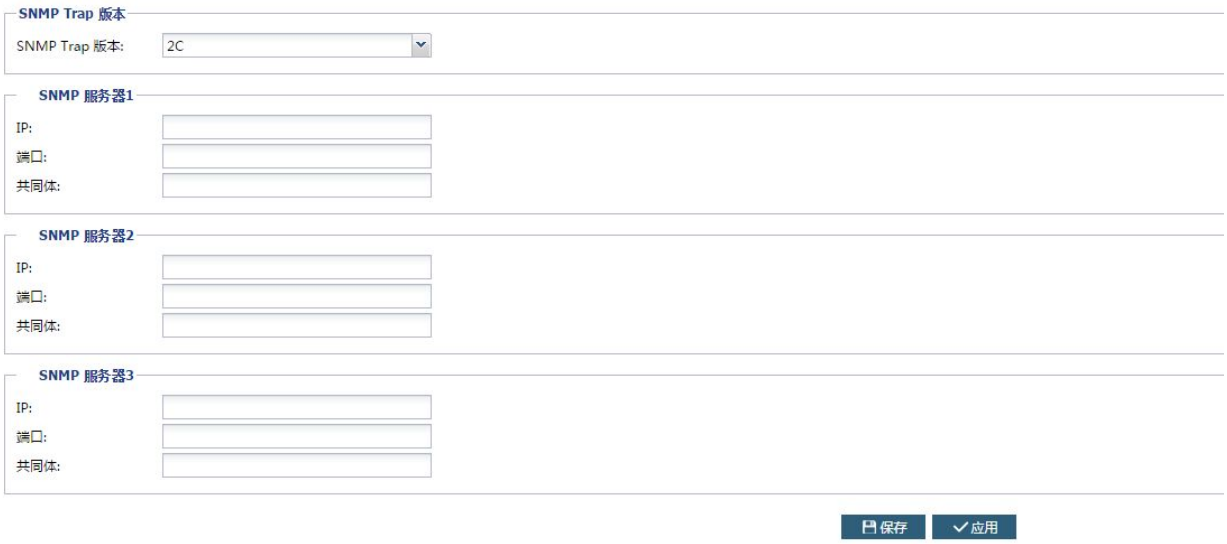
11.1.7 版本管理

通过版本管理，您可以查看固件版本，防护规则版本，防病毒规则版本，应用规则版本以及域名库版本的版本信息以及检查各个版本的更新。

11.2 高级配置

11.2.1 SNMP Trap

SNMP Trap：本设备可以通过 SNMP Trap 的方式发送系统日志。

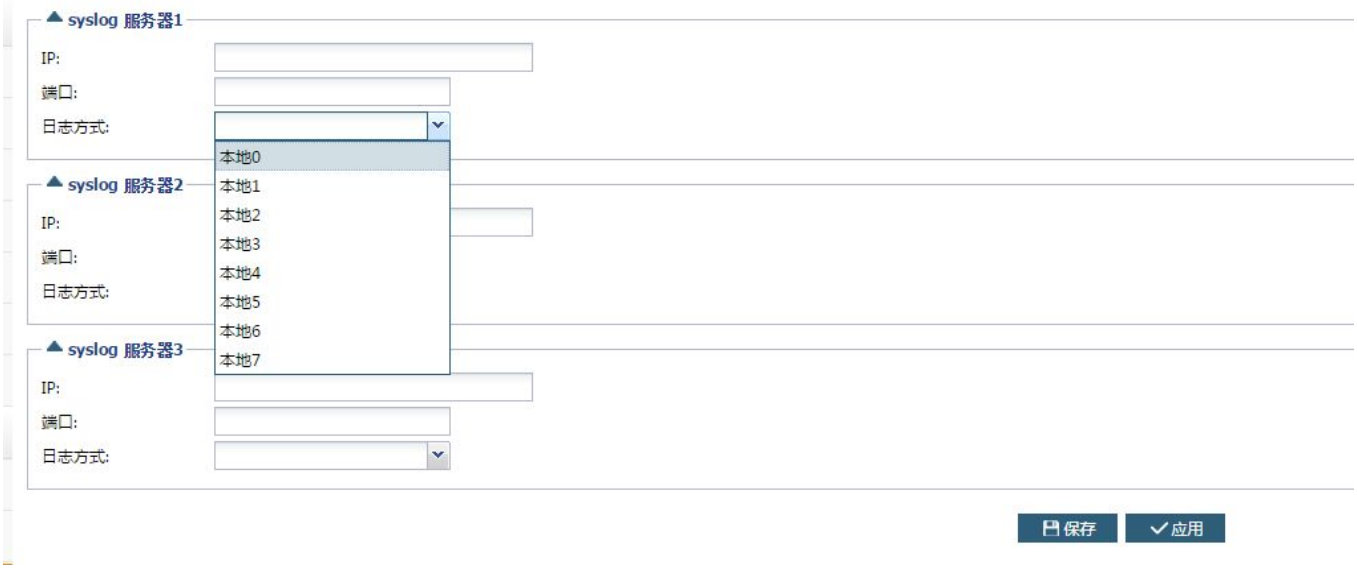


11.2.2 SNMP

简单网络管理协议（SNMP）是目前 TCP/IP 网络中应用最为广泛的网络管理协议。

11.2.3 SYSlog

syslog 常被称为系统日志或系统记录，是一种用来在互联网协议（TCP/IP）的网络中传递存档信息的标准。本系统支持 syslog 日志的发送。



11.2.4 抓包工具

该页面用于对本设备的各个接口进行数据抓包的操作。

对指定接口进行抓包：

1. 在抓包设置填写接口名称，比如：ETH2，抓包数目以及数据包长度等信息，点击【开始抓包】；

2. “抓包文件列表”出现抓包的文件名，抓包状态，操作的信息；

3. 您可以单击【刷新】按钮来查看当前抓包的最新状态，如果抓包时间过长，可以点击【停止抓包】按钮停止此次抓包；

当抓包状态为“完成”时，您可以点击“下载”操作来下载此次的抓包文件。下载后使用“wireshark”等分析软件打开此文件。

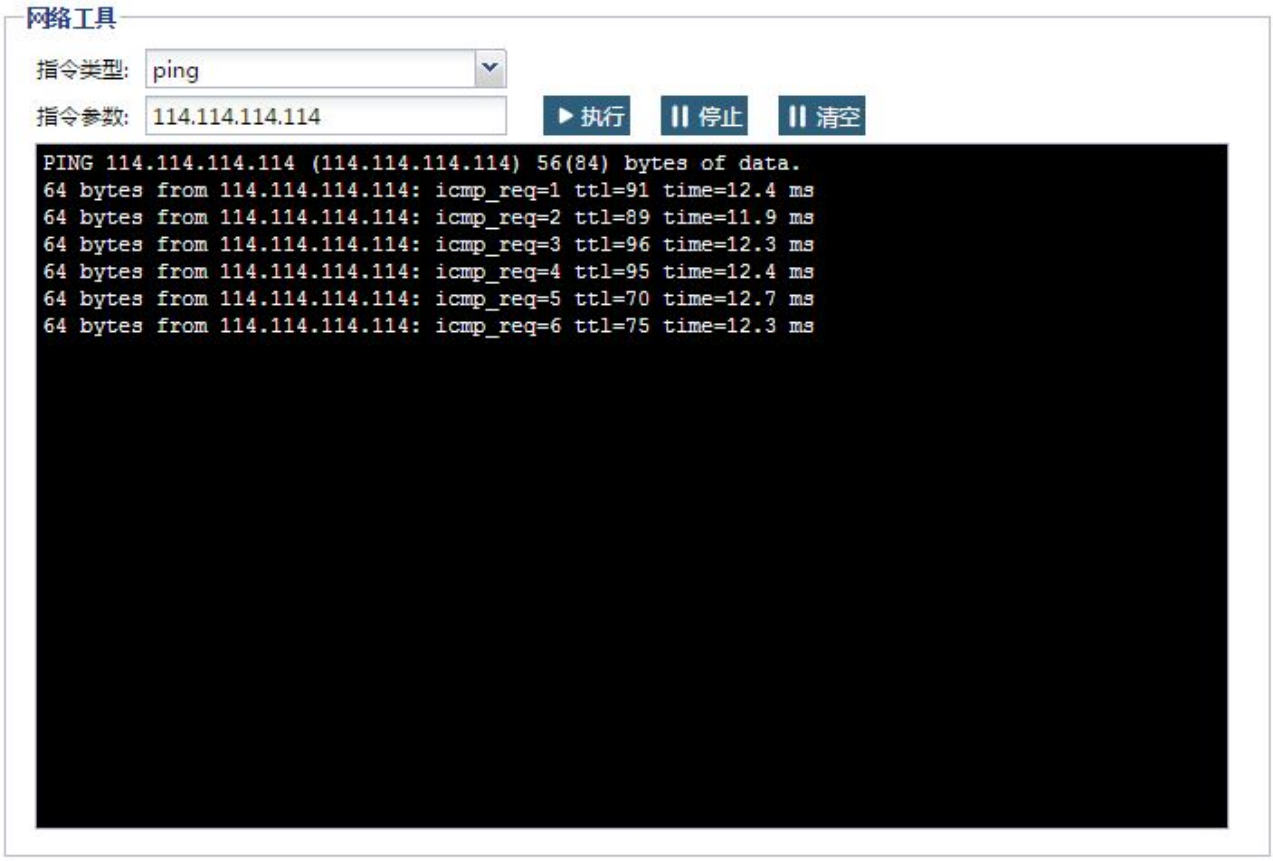
11.2.5 网络工具

本设备内部添加的一个包含有 ping、route、arp、traceroute 和 nslookup 的网络工具。

- “指令类型”：点击下拉菜单，可以选择 5 条常用指令中的一条。
- “指令参数”：相应指令所对应的参数，比如 ping 指令可以设定参数为域名或 IP 地址。
- 【执行】：执行选择的操作指令。
- 【停止】：一些操作指令需要手动停止，比如 ping。
- 【清空】：清除界面上显示的信息。

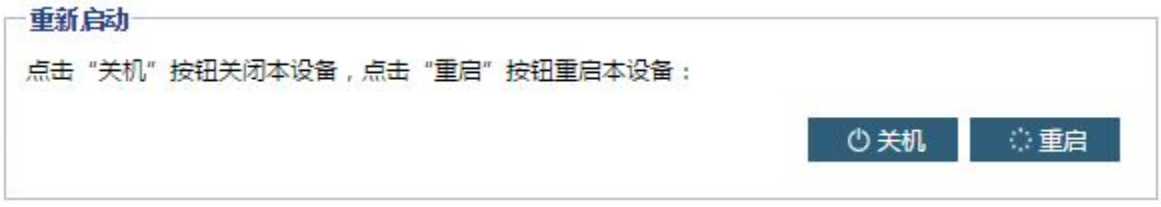
使用 ping 指令：可以检测本设备的网络连接状况。

选择指令类型为 ping，指令参数设定为 192.168.9.1，点击执行，出现如下信息。其他指令您可以参照 windows 下命令行的相对应指令信息使用。



11.2.6 重新启动

本页面用于对设备进行“关机”与“重启”操作。



【关机】： 点击【关机】按钮，稍后将会安全关闭设备。

【重启】： 点击【重启】按钮，将会重新启动设备。

⚠注意：

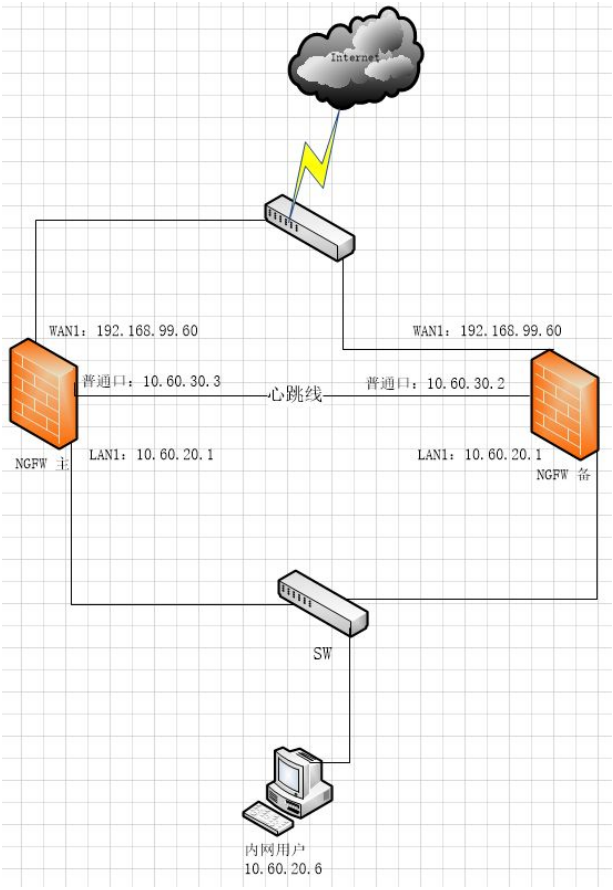
1. 请您尽量避免在本设备正常运行的时候直接切断电源。（这样可能造成数据的丢失或者影响设备的使用寿命）

2. 在您点击【关机】按钮，或者直接按下本设备上的电源按钮后，请等待电源指示灯熄灭后再切断电源，设备安全关闭需要一定时间。

11.2.7 高可用性

高可用性（HA）指双机状态备份，当两台防火墙，在确定主从防火墙后，由主防火墙进行业务的转发，而从防火墙处于监控状态，同时主防火墙会定时向从防火墙发送状态信息和需要备份的信息，当主防火墙出现故障后，从防火墙会及时接替主防火墙上的业务运行。

双机热备（主备部署）



1. 主设备

在 HA 设置填写本端心跳口和对端心跳口地址，比如：本端接口设为 ETH2（10.60.30.3），对端心跳口地址：10.60.30.2。

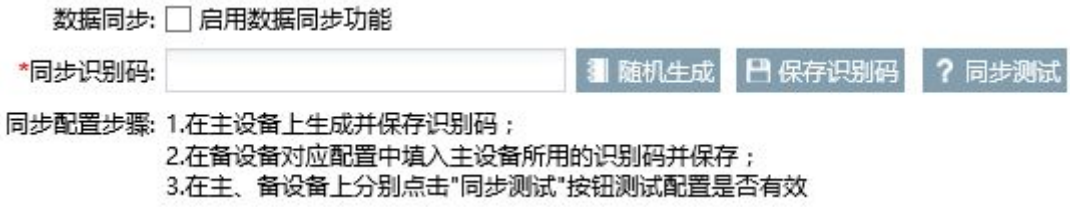
2. 备设备（DSI 口进入）

在 HA 设置填写本端心跳口和对端心跳口地址，比如：本端接口设为 ETH2（10.60.30.2），对端心跳口地址：10.60.30.3。

3. 网口列表：

网口列表是非 DSI、DMI、心跳口（物理口、和没有绑定任何接口或仅直接绑定物理口的端口汇聚和、网桥），设备将监控列表中的所有网口，当任意网口断开时，都将触发主从切换。

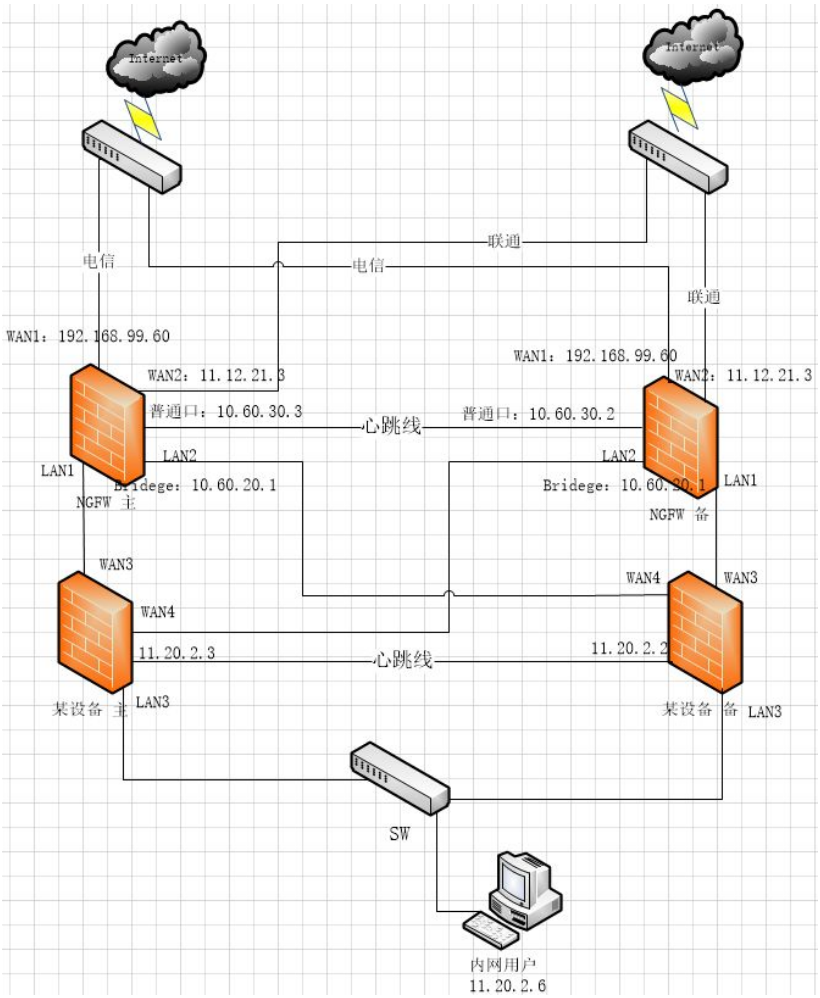
4. 点击数据同步，在主设备上生成并保存识别码，在备设备对应配置中填入主设备所用的识别码并保存，在主、备设备上分别点击"同步测试"按钮测试配置是否有效主设备的数据就和备设备同步了



5. 点击 

按钮，该设置生效。

多台设备联合部署



IPS 的 HA 功能也可以与其他设备联合摄制，将 LAN1 和 LAN2 口进行桥接，将 Bridege 设置为 LAN 属性，并分配地址。

⚠注意：

此产品仅支持主备模式；心跳口的 IP 不能以“.1”形式结尾；数据同步仅仅是同步一些日志；默认抢占模式。

12. Console 功能

12.1 主菜单

在主菜单界面输入“?”显示”主菜单目录”，主菜单提供常用的网络命令，ping，route，traceroute，

nslookup，查看设备信息以及关机重启等操作。

主菜单常用命令

显示接口信息：

>> show interface

显示设备信息：

显示网卡 MAC 地址：

>> show macaddress

显示 ARP 信息：

>>arp

重启：

>>reboot

关机：

>>shutdown

12.2 配置菜单（configure）

在主菜单输入：*configure* 进入*配置*菜单，在*配置*主菜单界面输入“?”显示*配置*菜单目录，*配置*菜单可以配置 DMI，DSI，DNS，DHCP，还原，复位等操作。

```
>> configure
(configure)#
(configure)#
system                          Set the system information
show                            Display some configuration
restore                         Restore the software
reset                           Reset the device
help                            List all available commands
exit                            Exit from configure mode
```

配置菜单常用命令：

参数说明：

netmask 子网掩码

gateway 网关

ip_beginDHCP 起始 IP

ip_end DHCP 结束 IP

配置 DMI：

IPS(configure)#system interface DMI ip 192.168.9.10 netmask 255.255.255.0 gateway192.168.9.1

配置 DSI：

IPS(configure)#system interface DMI ip 192.168.100.2 netmask 255.255.255.0 gateway192.168.100.1

配置系统时间：

IPS(configure)#system clock 2012-09-12

配置首选 DNS：

IPS(configure)#system dns1 8.8.8.8

配置备用 DNS：

IPS(configure)#system dns2 9.9.9.9

配置 DHCP：

IPS(configure)#system dchp ip_begin 192.168.9.10 ip_end 192.168.9.100

修改密码：

IPS(configure)#system passwd 123456789

显示系统时间：

IPS(configure)#show clock

显示 DMI：

IPS(configure)#show DMI

显示 DSI：

IPS(configure)#show DSI

显示 DHCP：

IPS(configure)#show dhcp

显示 DNS：

IPS(configure)#show dns

还原：

IPS(configure)#restore

复位：

IPS(configure)#reset

返回上级菜单：

IPS(configure)#exit

⚠注意：

所有的参数请根据实际情况输入。

13. 复位与还原

如需对设备复位，必须先断开 DMI 接口的网络连接，并通过 DSI 接口连接本设备。然后通过浏览器访问页面 https://192.168.100.1/product_reset.htm。此处的 192.168.100.1 可能根据您的具体设备有所不同，请参考附录 A.1. 设备设置接口(DSI 接口)初始设置。

点击【系统复位】将会使本设备的所有设置恢复到出厂值，所有的入侵记录和页面统计数据等日志数据将被清空，用户账户和密码将恢复到出厂值。

点击【系统还原】后，除了执行【系统复位】的操作外，还将会使设备固件恢复到出厂版本。只有在固

件升级失败和系统异常时才可以使用。

⚠注意：

请提前备份系统配置并且导出重要的日志数据。在设备复位或还原后，本设备的配置和运行数据将全部恢复到出厂状态。

14.常见问题与解答

问题：选择某个日期后，查看不到任何入侵记录?

解答：当天没有任何入侵事件产生，所以没有记录。如果您选择的是一个很早的日期，有可能这个日期的入侵记录日志已经被清理掉。

问题：修改某个设置后，好像没有生效?

解答： 请点击该页面的【应用】按钮后等待 1 分钟左右，设置生效需要一定时间。

问题：如何正常关闭设备?

解答：按下本设备背面的电源按钮或者进入【重新启动】页面后点击【关机】按钮。安全关闭设备需要一定时间，前面板的 Power 灯熄灭后，设备正常关闭。

问题：使用本设备后，部分网页访问不正常?

解答：

（1）请检查自定义规则，是否是由于您写的自定义规则导致数据包被误拦截。

（2）请检查关键字设置中是否包含了会造成大量数据包内容被替换的字符，如您将关键字设置为单个字符，系统点击保存时，系统将会，自动去除单个字符。

（3）如果仍然出现此问题，请检查是否由内置规则误拦截引起。如果是，请停用此内置规则。

问题：无法进入 Web 管理页面怎么办?

解答：

（1）请先确认计算机能和本设备进行正常通讯（如果计算机开启了防火墙，请将 443 端口打开）。

（2）如果仍然无法进入 Web 管理页面，请尝试从 DSI 接口连接。

问题：忘记管理员密码怎么办?

解答： 可以通过复位功能重置管理员密码。首先，拔下 DMI 接口的网线，从 DSI 接口用网线连接计算机，并参考《铱迅入侵防御系统安装部署手册》设置您的计算机网络参数。在浏览器中访问 https://192.168.100.1/product_reset.htm，根据提示进行产品复位。

问题：规则升级失败怎么办?

解答：如果规则升级失败，系统会自动进行规则回滚操作，因此您不用担心规则升级失败。在确认升级文件正确的情况下，如果再次升级失败，请联系铱迅客服人员。

问题：固件升级失败怎么办?

解答：如果升级失败，请首先检查设备是否工作正常。如果一切正常，请忽略此失败事件。如果不正常，请进行产品复位。如果仍然无法解决此问题，请联系铱迅客服人员。

附录 A. 出厂默认设置

设备设置接口(DSI 接口)初始设置

IP 地址	192.168.100.1
子网掩码	255.255.255.0

预置账号

系统管理员预置账号

用户名	sysadmin
密　码	sysadmin

安全审计员预置账号

用户名	auditor
密　码	auditor

安全管理员预置账号

用户名	webadmin
密　码	webadmin

Console 用户预置帐号

用户名	conadmin
密　码	conadmin

默认设置

设置项	值
磁盘空间上限	80%

定期报表	开启每月报表邮件发送
HTTP 返回报文检测	开启
Email 报警	开启入侵记录 Email 报警 开启高危入侵报警

铱迅信息(YXLink)

南京铱迅信息技术股份有限公司

江苏省南京市雨花台区宁双路 18 号沁恒科技园 D 幢 4 层

Nanjing YXLink Information Technology Co., Ltd.