SANGFOR_GAP 安全隔离与信息交换系统_v3.0_用户手册

深信服智安全
SANGFOR SECURITY

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

目录

声明

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深信服科技股份有限公司客户服务部。

深信服科技股份有限公司（以下简称为深信服科技、SANGFOR）。

前言

手册内容

本手册以深信服安全隔离与信息交换系统 v3.0 正式版本为例进行配置说明。

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	[ ]	菜单项“系统设置”可简化为[系统设置]
连续选择菜单项及子菜单项	→	选择[系统设置]→[接口配置]
下拉框、单选框、复选框选项	[ ]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【 】	如点击弹出【新增用户】窗口
提示信息	“”	提示框中显示“保存配置成功，配置已修改，需要重启 DLAN 服务才能生效，是否立即重启该服务?”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

小心、注意：提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

警告：该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

说明、提示、窍门：对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服社区：bbs.sangfor.com.cn

深信服服务商及服务有效期查询：

http://bbs.sangfor.com.cn/plugin.php?id=service:query

公司网址：www.sangfor.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

第 1 章 深信服安全隔离与信息交换系统系列硬件设备的安装

本部分主要介绍了 SANGFOR GAP 深信服安全隔离与信息交换系统（简称网闸）系列产品的硬件安装。硬件安装正确之后，您可以进行配置和调试。

1.1. 环境要求

深信服安全隔离与信息交换系统系列硬件设备可在如下的环境下使用：

输入电压：110-230V

温度：0～45℃

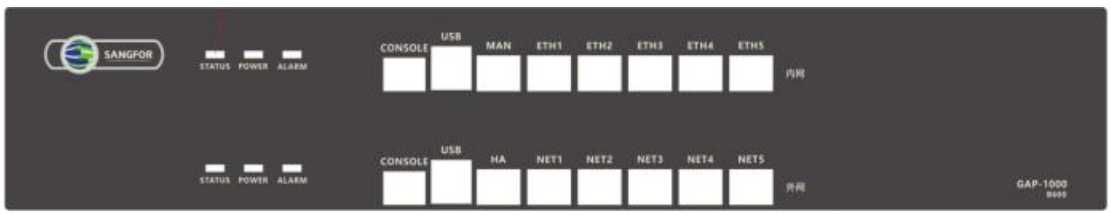
湿度：最大相对湿度 5%-95%，不结露

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.2. 电源

SANGFOR 深信服安全隔离与信息交换系统系列硬件设备使用交流 220V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3. 产品接口说明



图(1)　GAP 前面板图（以 GAP1000 为例）

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

网闸有两块主板 1.CONSOLE(控制)口　　2. MAN 口（管理口）、HA 口（热备心跳口）

3.内网口 ETH1-ETH5　　4.外网口 NET1-NET5

1.图片仅供参考，不同型号的产品外观请以实物为准。

2. 设备内端与外端接口的序号对应并不是指一对一的通道，只是内外端机自身的多个网络接口而已，自身的各个接口采用逻辑隔离，与内外端主机之间的隔离效果不同。

在接插光纤模块时要注意防尘，否则会影响通信效率。

1.4.配置与管理

深信服安全隔离与信息交换系统安装在两个不同业务网络之间或者安装在重要服务器之前，实现网络之间的数据安全交互。

1.5.开始使用

1.5.1 设备启动

打开深信服安全隔离与信息交换系统背板上的电源开关，设备随即启动，并加载上次关闭时的安全策略。

1.5.2 设备关闭

关闭深信服安全隔离与信息交换系统背板上的电源开关，设备随即停止运行。

1.5.3 WEB 管理

深信服安全隔离与信息交换系统的所有管理、配置、监控工作均在 WEB 管理平台完成。

1.5.3.1 登录

深信服安全隔离与信息交换系统是多用户系统，用户在对设备进行操作之前，必须使用正确的用户凭据（[用户]、[口令]、证书）登录。登录界面如下图：

图(2)　登录系统

[用户名]：本系统用于区分用户身份的唯一标识，由具备用户管理权限的用户（如sysuser、secuser、loguser 等）创建并维护。

[密码]：系统用户的访问密码，用户在正确登录之后可修改自身用户的密码。

证书：sysuser、secuser、loguser 用户登录 WEB 管理平台时的凭据。

1、系统出厂默认的 IP 地址、用户名、密码如下：

- **管理口 IP：10.251.251.11**
- **系统管理员用户名：sysuser**
- **系统管理员密码：admin**
- **安全保密员用户名：secuser**
- **安全保密员密码：admin**
- **日志管理员用户名：loguser**
- **日志管理员密码：admin**

2、管理员在第一次登录系统成功后，请及时修改系统默认的密码。

1.5.3.2 退出

用户在完成管理工作后，点击管理界面右上方的  按钮，可以退出登录。通过此方式退出登录，比直接关闭浏览器页面更安全。

1.5.3.3 修改密码

用户可维护自己的登录密码。系统内置了三个默认的管理账户，并为它们设置了初始密码，点击管理界面右上部分的修改密码，可修改当前用户的登录密码。界面示例如下图：

图(3)　修改密码

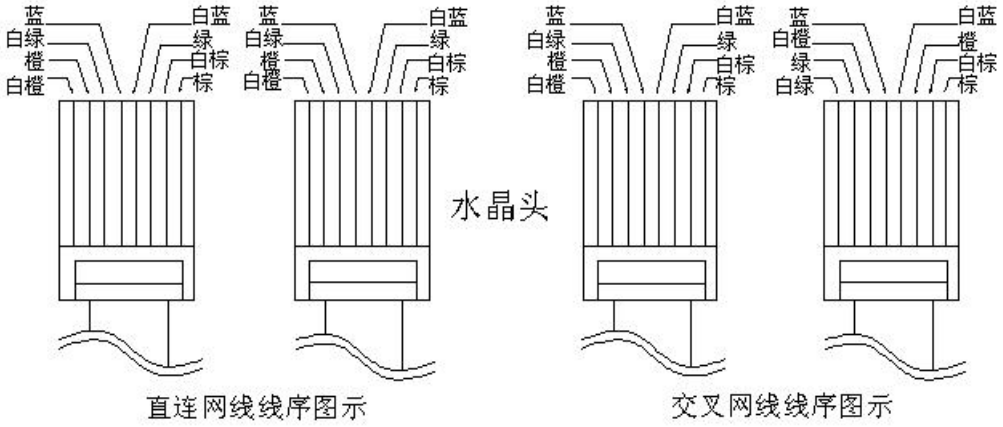
1.6. 设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 ETH1 口与内部局域网连接，对设备进行配置。

设备正常工作时 POWER 灯常亮，接线的数据接口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不能熄灭，请与我们联系。

网口直接连接交换机应使用直连线、连接路由器和电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：



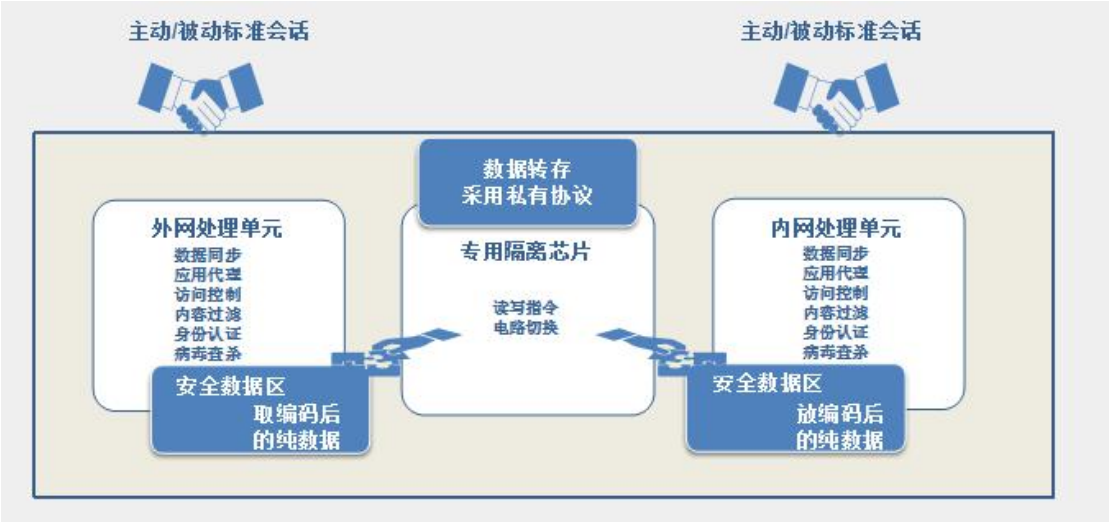
图(4)　直连线、交叉线 线序

第 2 章 深信服安全隔离与信息交换系统系列硬件设备的部署

图(5)　典型部署拓扑图

如图所示，网闸部署在不同的安全域之间。可以在网闸上设置源与目的的 IP 地址和访问的端口。网闸分为三种工作模式：**透明（无需改变网络环境）、代理（需修改访问 IP 和端口为网闸接口地址加端口）、路由（需改写路由下一跳为网闸接口地址）端口根据实际应用进行确认。**

2.1 工作原理



地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

图(6)　产品原理图

- 深信服网闸是边界安全隔离设备，连接两个网络，两网通信的唯一关卡。
- 主要用来解决不同安全域之间的数据交换问题，如数据库同步、文件传输、跨域访问等。
- 采用 SOCKET 代理机制，管理对象为会话，数据包有去有回，往返即为会话，与防火墙包过滤工作机制不同。
- 白名单工作机制，策略中需明确允许，数据才可通过深信服网闸访问.除此之外的信息，无论是有害还是无害，全部会被丢弃。

2.2 工作模式

为了适应客户不同的网络应用环境要求，深信服网闸提供了三种工作模式：代理、路由、透明。（安全防护效果与工作模式无关）

图(7)　工作模式选择

- 代理模式：代理模式适用于在两端网络在不同的网段，并且不允许访问对方的真实 IP。代理模式使用最多，部署方便，两侧主机分别通过本端网络与用户主机通信。客户端只需访问深信服网闸 IP，后续通信由深信服网闸完成。**如下图所示，内网客户访问外网 FTP 服务器，只需访问深信服网闸 IP192.168.11.253，深信服网闸将会代理客户端访问 192.168.10.254，并将返回数据回传给客户端。如图所示**

图(8)　代理模式部署示意图

◆ 路由代理：客户端与服务器不在同一个网段，但是必须访问对方的真实 IP 才能通信。客户端需要把去往目标服务器的下一跳路由指向深信服网闸本端的 IP，目标服务器也需要将去往客户端的下一跳路由指向网闸的 IP。如果目标服务器不设置回指路由的话，需要在深信服网闸的连接目标服务端这一端的网络接口处勾选隐藏源地址(**该功能选项仅在设备工作在路由模式时出现**)。

图(9)　隐藏源地址

当网闸的内外网地址与目标服务器或客户端不在同一子网时，需要添加去往目标的路由，路由写法：route add -net 192.168.11.0 netmask 255.255.255.0 gw 192.168.11.253

图(10)　路由模式部署示意图

◆ 透明代理：客户端与服务器之间本身可建立通信，加入深信服网闸后不希望改变现有网络拓扑。

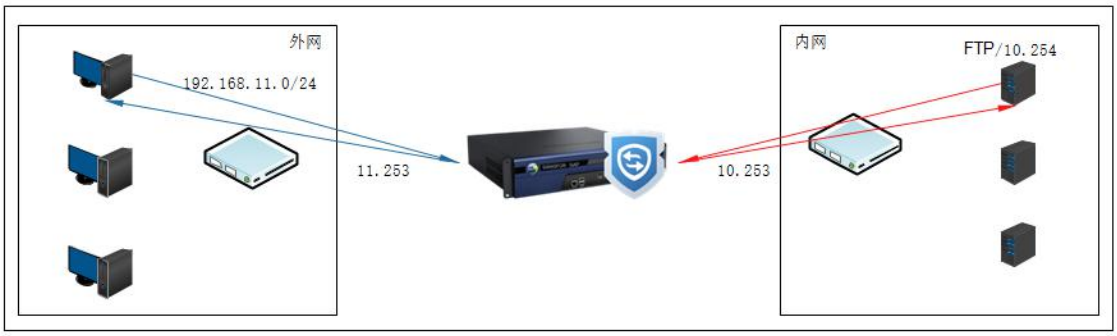
图(11)　透明模式部署示意图

类比网桥/交换机，客户端与服务端自身在跳开深信服网闸的情况下，可直接通信。

2.3 调试前需要了解的信息

首先，要了解用户网络情况、用户需求。确定深信服网闸使用什么工作模式，需要通过深信服网闸访问**什么业务系统、服务器 IP、客户端 IP**、深信服网闸**内外网接口的 IP 等信息**。

在安全设备中，策略里要定义通讯的整个过程，数据才可通过。



图(12)　代理业务流程示意图

以上图为例，确定客户端 IP 为内网，服务器 IP 为 192.168.10.254、要访问的服务为 FTP（端口 TCP 21）、深信服网闸内网接口 IP（192.168.10.253）、深信服网闸外网 IP（192.168.11.253）。

了解了以上信息后才可以进行策略配置。

2.4 基本设置

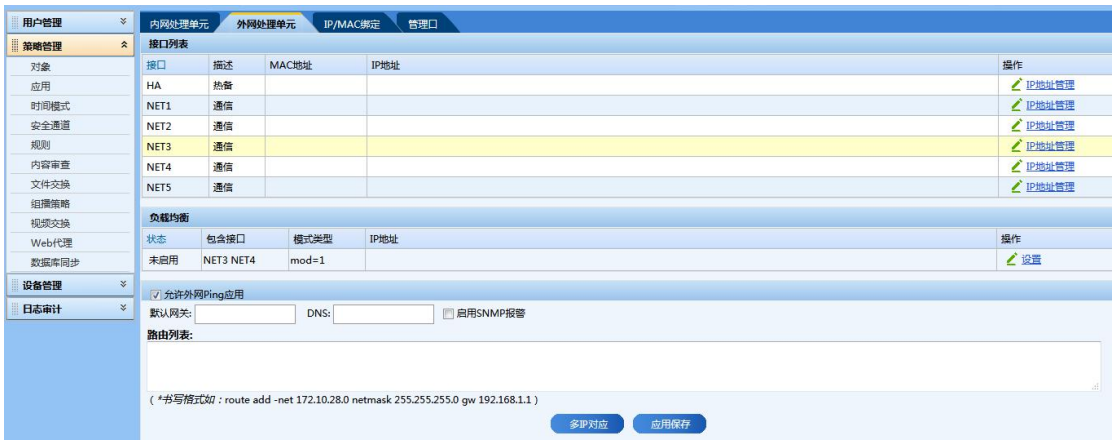
使用系统管理员账户登录系统，在 「 设备管理→基本设置 」处更改当前工作模式，点击应用保存。（开启策略日志记录有助于排错，如需通过深信服网闸传输 VLAN、OSPF 登协议，请勾选开启其它协议支持。）

图(13)　设备基本设置示意图

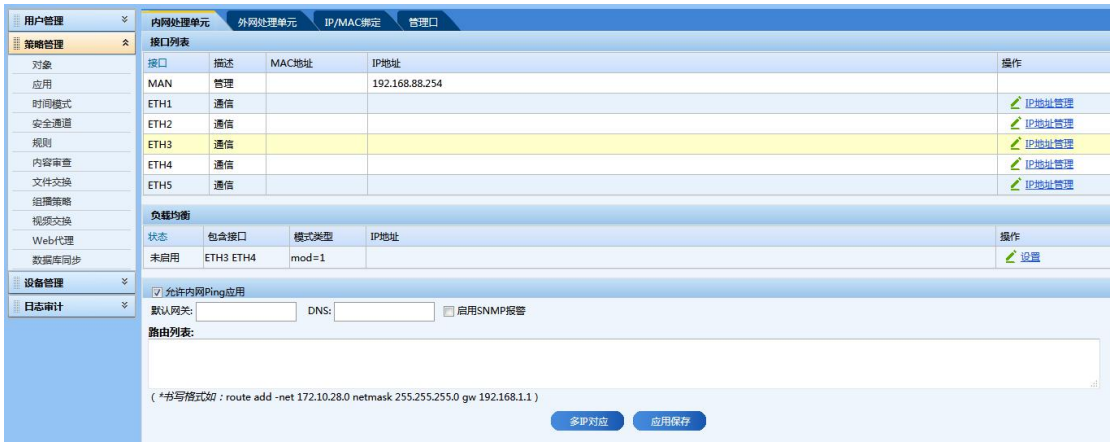
2.5 设备 IP 设置

在 「 设备管理→ 网络接口 」处分别为设备内外网接口设置 IP。点击右侧 IP 地址管理，然后输入 IP、掩码，点击应用保存按钮使配置生效。

注意：**同一个网络接口上可以设置一个或多个同网段或不同网段的 IP 地址，但是不同的网络接口上绝对不可以设置同一网段的 IP 地址。**



图(14)　外网接口示意图



图(15)　内网接口示意图

负载均衡是指接口的负载均衡，其有 7 种工作模式，具体参见界面里的说明。勾选“允许内网 PING 应用”是指允许 PING 到网闸内网接口 IP。启用 SNMP 是指启用 SNMP 服务，接受来自 SNMP 客户端的请求服务。共同体名称和 SNMP 客户端 IP 均可通过界面

进行设置。管理员可为网闸的内外端机分别设置默认网关和 DNS。

第 3 章 深信服安全隔离与信息交换系统系列硬件设备的配置

3.1 用户管理

3.1 管理员账户

具备相应权限的用户可完成[管理员账户]的维护工作。

3.2 权限分立

系统采用三权分立的用户组织方法，用户分为三种角色（即类型），分别为：系统管理员、安全保密员、安全审计员。每种角色都包含一个内置的默认用户，系统管理员默认用户为 sysuser，安全保密员默认用户为 secuser，安全审计员默认用户为 loguser。[管理员账户]界面示例如下图：

图(16) 管理员设置

生成证书：会使上次的证书失效，使本次生成的证书有效，请根据需要操作。每种类型的默认用户只能维护同类型的用户，并且内置默认用户不能被删除。

3.3 登录限制

内置安全保密员默认用户，可以设置[界面超时退出时间]、[最大尝试登录次数]、[账户锁定等待解锁时间]、[密码更换周期]、[密码最小长度]。

[自动超时退出]：超过设置的时间界面无任何操作，管理界面自动退出。

[最大尝试次数]：同一账户，连续鉴别失败超过限制就被锁定。

[账户锁定等待解锁时间]：锁定账号的时长。

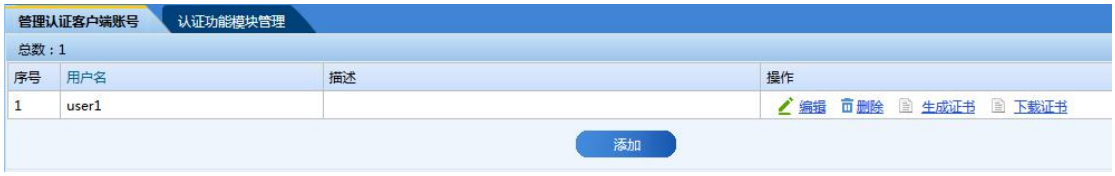
[密码更换周期]：超过规定天数，提示用户更新密码。

[密码最小长度]：新增或更新后的密码位数。

3.4 认证账号

系统启用身份认证功能之后，只有通过身份认证的计算机才能使用深信服安全隔离与信息交换系统通信，从而提供更多一层的安全防护。

认证账号的添加、编辑、删除、生成证书、下载证书等操作可通过[管理认证客户端账号]界面完成。



图(17)　认证用户管理

[认证功能模块管理]界面见上图：

图(18)　启用认证功能设置用户

[认证功能模块当前状态]：查看认证功能是否启用。

1、工作模式为透明代理时，无法启用认证功能。

2、认证账号只在系统启用了身份认证功能之后有效。

3、开启认证功能时，一定要配合认证账号使用。

4、开启认证功能后，客户端需要先主动访问 https://网闸 IP:59876，通过认证后才能访问网闸代理的业务。

3.2 策略管理

[策略管理]是管理软件的重要使用部分。系统策略采用五元组的形式组合定制。定制好的元素，在定制策略时可以直接引用。

3.2.1 对象

系统采用通信[对象]的方法进行通信控制。具备[对象]管理权限的用户可通过管理界面进行[对象]的维护工作。

3.2.1.1 对象

通过[对象]管理界面，可以添加、编辑、删除对象，[对象]管理界面如下图：

图(19)　对象管理

点击添加，在[添加对象]的操作区，正确填写[名称]、[IP 地址]、[掩码地址]、[Mac 地址]各项内容，选择填写[描述]，点击确定即完成添加对象操作。

IP 地址唯单一地址时，界面示例如下图：

图(20)　对象 IP 地址设置

IP 地址为范围地址时，界面示例如下图：

图(21)　范围地址对象

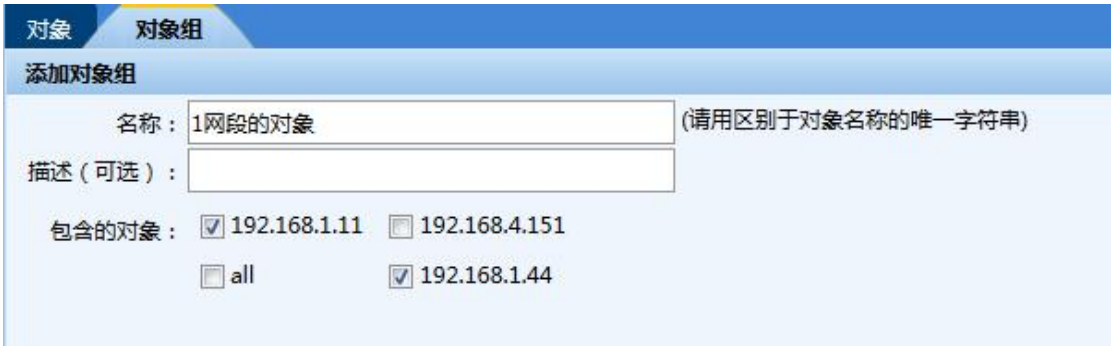
对象可以是单 IP 对象，也可以是某个 IP 段的范围 IP 对象。对于单 IP 对象，Mac 地址可以使用默认的全 0，也可以写成真实 Mac 地址。当 Mac 地址不为全 0 时，系统会尝试为该 IP 绑定 Mac 地址；对于范围 IP 对象，IP 地址的填写格式为 ip1-ip2。系统会忽略 Mac 地址，即不会尝试绑定 Mac，请使用默认的全 0。

3.2.1.2 对象组

通过[对象组]管理界面，可以添加、编辑、删除对象，[对象组]管理界面如下图：

图(22)　添加对象组

点击添加，在[添加对象组]的操作区，正确填写[名称]、选择填写[描述]，选择[包含的对象]，点击确定即完成添加对象组操作。[添加对象组]界面示例如下图：



图(23)　对象组设置

当一个规则中，源对象或目标对象，是一个或多个不连续的对象时，可以把这些零散的对象放在一个组里，方便策略的定制。定制策略时可以使用对象组，也可以直接使用对象。

3.2.2 应用

系统采用层次化的应用组织方法，准确表述客户网络中发生的各种网络通信，以供定制访问策略之用。

3.2.2.1 应用

通过[应用]管理界面，可以添加、编辑、删除应用，[应用]管理界面如下图：

图(24)　添加应用

点击添加，在[添加新应用]的操作区，正确填写[名称]、[目的端口]、[源端口]、[代理端口]各项内容，选择[协议]、[所属模块]、[未定义的命令]、[日志开关]，点击确定即完成添加新应用操作。

[代理端口]为单个端口的应用界面示例如下图：

图(25)　定制应用内容

[所属模块]、[协议]：所属模块及协议具体含义见附录一。

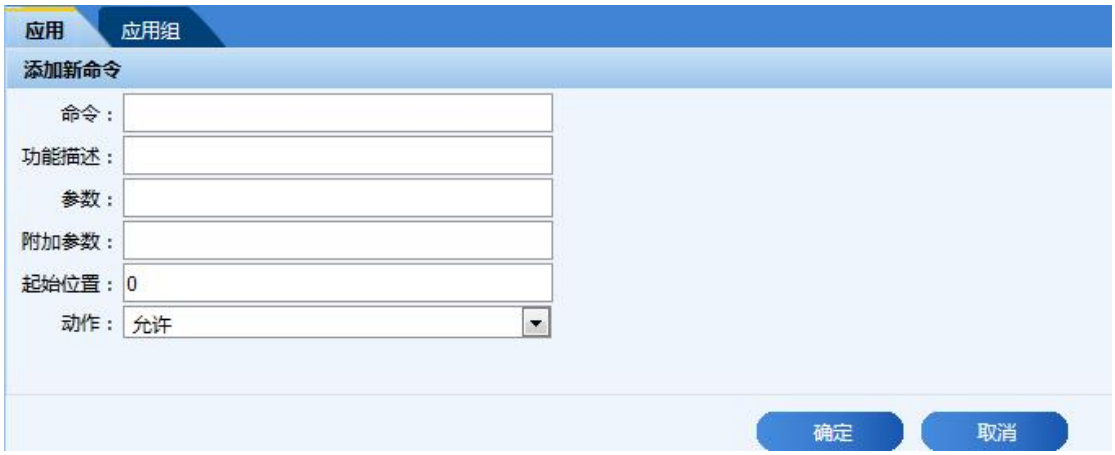
[代理端口]为范围端口的应用界面示例如下图：

图(26)　范围端口定义

已经添加的[应用]，通过编辑可以[添加新命令]信息。如下图：

图(27)　添加应用命令

点击添加新命令，在[添加新命令]的操作区，正确填写[命令]、[功能描述]、[参数]、[附加参数]、[起始位置]各项内容，选择[动作]，点击确定即完成添加新命令操作。如下图：



图(28)　定制自定义命令格式

1、对于标准协议，用户可以选择内置的标准模块，如 HTTP、FTP 等；对于私有协议，可以选择 TCP 自定义模块（NULL_TCP）和 UDP 自定义模块(NULL_UDP)。源端口、目的端口、代理端口可以是单个端口，也可以是范围端口。

2、有些应用模块提供了批量导入命令功能，用户可以逐个添加命令，也可以批量导入。

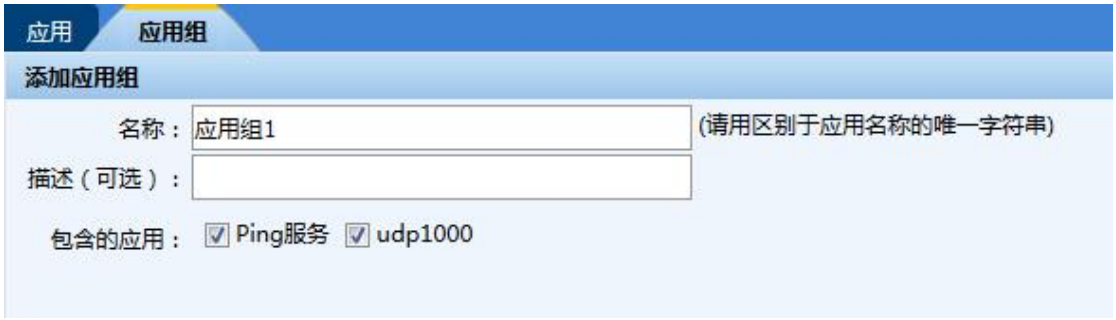
3、应用为某种特定形式的网络通信，当前系统提供的应用及应用信息详细说明见附录二。

3.2.2.2 应用组

通过[应用组]管理界面，可以添加、编辑、删除应用组，[应用组]管理界面如下图：

图(29)　添加应用分组

点击添加，在[添加应用组]的操作区，正确填写[名称]、选择填写[描述]，选择[包含的应用]，点击确定即完成添加应用组操作。[添加应用组]界面如下图：



图(30)　应用分组定制

当一个规则中，包含一个或多个应用时，可以把这些应用放在一个组里，方便策略的定制。定制策略时可以使用应用组，也可以直接使用应用。

3.2.3 时间模式

系统定制的访问策略，依据[时间模式]，可以自动加载或停用规则。[时间模式]提供三种调度类型：[每天循环]、[指定星期循环]、[指定日期区间]。用户可以根据自己的需求，选择不同的调度类型。

通过[时间模式]管理界面，可以添加、编辑、删除时间模式，[时间模式]管理界面如下图：

图(31)　添加时间模式

点击添加，在[添加时间模式]的操作区，正确填写[名称]、[开始时间、[结束时间]、选择填写[描述]，选择[调度类型]、[指定星期]，点击确定即完成添加时间模式操作。[添加时间模式]界面如下图：

图(32)　时间模式定义

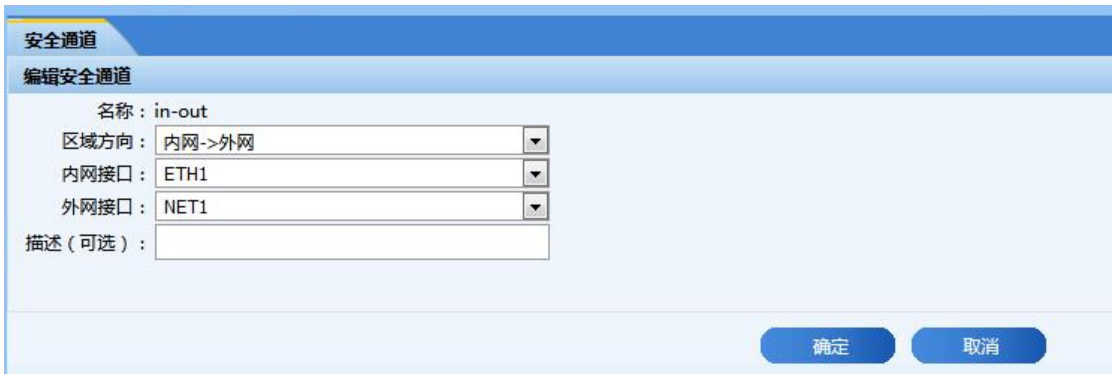
3.2.4 安全通道

[安全通道]用来设置进行数据交换的两个网络区域。[内网处理单元]和[外网处理单元]的任意两个[网络接口]都可组成一个[安全通道]。[安全通道]界面如下图：

图(33)　添加安全通道

点击添加，在[添加安全通道]的操作区，正确填写[名称]、选择填写[描述]，选择[区

域方向]、[内网接口]、[外网接口]，点击确定即完成添加安全通道操作。[添加安全通道]界面如下图：



图(34)　定义安全通道

[区域方向]：内到外/外到内。

[内网接口]：通道的内网端口，一般情况下为内网用户所在的网络区域，接口为该通道的内网通信接口。

[外网接口]：通道的外网端口，一般情况下为外网用户所在的网络区域，接口为该通道的外网通信接口。

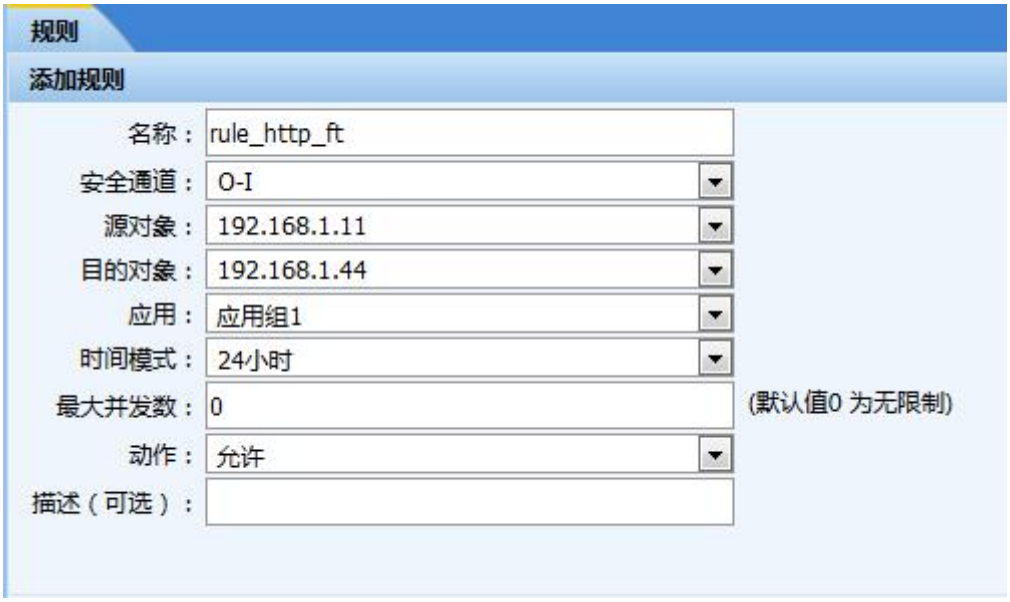
3.2.5 规则

用户可通过[策略管理]界面定制符合实际需求的[安全策略]。[安全策略]包含[名称]、[安全通道]、[源对象]、[目的对象]、[应用]、[时间模式]、[最大并发数]、[动作]、[描述]等元素。如下图：

图(35)　添加规则

点击添加，在[添加规则]的操作区，正确填写[名称]、[最大并发数]、选择填写[描述]，选择[安全通道]、[源对象]、[目的对象]，[应用]、[时间模式]、[动作]，点击确定即完

成添加规则操作。如下图：



图(36)　用资源组合规则

[源对象]:使用客户端对象；[目的对象]:要访问的服务器对象，均在[网络接口]处添加。

[源对象]、[目的对象]这两项可以使用对象，也可以使用对象组。

[动作]：动作为允许，表示源对象是白名单，规则动作为拒绝，表示源对象是黑名单。

1、当有多个规则运行，客户端同时出现在白名单和黑名单中时，则按黑名单处理，即拒绝优先。

2、勾选[设备管理]→[基本设置]→[安全模块]→[启动抗 DDos 攻击]选项时，最大并发数表示该规则源对象中每个对象可以访问每个应用的最大连接数；不勾选[启动抗 DDos 攻击]选项时，最大并发数表示该规则所有源对象可以访问每个应用的最大连接数。

3.2.6 内容审查

系统能够对进出网络的通信进行深层的内容控制，包括[关键字过滤]、[文件类型过滤]、[防病毒]等。

3.2.6.1 关键字过滤

通过[关键字过滤]管理界面，可以添加、删除、导入关键字。还可以通过选择[启用关键字过滤]来控制是否开启关键字过滤功能。[关键字过滤]管理界面示例如下图：

图(37)　攻击者过滤

[启用关键字过滤]：系统会丢弃包含该关键字的数据包，并记录过滤日志。

导入关键字：导入的文件应是后缀为 txt 的文本文件，界面会把该文件的每一行当做一个关键字。

3.2.6.2 文件类型过滤

通过[文件类型过滤]管理界面，可以选择[不过滤]、[白名单过滤]、[黑名单过滤]。当启用了过滤时，系统会丢弃包含文件类型，而文件类型不符合该过滤条件的数据包，并记录过滤日志。[文件类型过滤]管理界面示例如下图：

图(38)　文件类型过滤

[文件类型列表]：填写需要过滤的后缀名。

3.2.6.3 防病毒

通过[防病毒]管理界面，可以查看[当前病毒库版本号]，可以导入文件升级病毒库。当[启用防病毒]时，系统会丢弃包含匹配病毒库特征码的数据包，并记录过滤日志。[防病毒]管理界面如下图：

图(39)　防病毒过滤

3.2.7 文件交换

通过[文件交换策略]管理界面，可以添加、启用、停用、编辑、删除文件交换策略，[文件交换策略]管理界面如下图：

图(40)　文件交换策略

点击添加，在[添加策略]的操作区，正确填写[策略名称]、[临时状态文件名]、[账户名]、[密码]、[目录路径]、[同步间隔时间]，选择[同步方向]、[交换策略类型]、[开启记录日志]，[文件类型过滤]、[网络协议]、[启用内网备份]、[开启目的端重名检查]、[开启同步完成后删除源]，点击确定即完成添加策略操作。如下图：

图(41)　文件交换定义

1、文件交换策略，可以运行在[代理模式]或[路由模式]，不可以运行在[透明代理]模式。

2、系统支持在网络隔离的情况下，两个或多个目录下文件的同步。需要同步的目录，通常为使用 SMB/CIFS 协议的共享目录。由于其特殊性，配置文件交换策略不使用之前定制的五元组策略信息。

3.2.8 组播策略

通过[组播策略]管理界面，可以添加、启用、停用、编辑、删除组播策略，[组播策略]管理界面如下图：

图(42)　组播策略

[组播策略]支持[透明代理]模式下启用，点击添加，在[添加组播策略]的操作区，正确填写[名称]、[源端组播 IP]、[源端组播端口]，选择[安全通道]，点击确定即完成添加组播策略操作。如下图：

图(43)　组播策略绑定通道

[组播策略]支持[代理模式]和[路由模式]下启用，点击添加，在[添加组播策略]的操作区，正确填写[名称]、[源端组播 IP]、[源端组播端口]、[目的组播 IP]、[目的组播端口]、[信源 IP 地址列表]，选择[安全通道]、[源接收 IP]、[目的发送 IP]、[组播类型]，点击确定即完成添加组播策略操作。[添加组播策略]界面，如下图：

图(44)　定义组播策略

1、组播地址的范围是 224.0.0.0—239.255.255.255。

2、支持 ASM（任意信源组播）、SSM（指定信源组播）、FSM（过滤信源组播）三种类型的组播。

3、使用透明代理模式，要求内外网网段相同，不需要给设备设置 IP，组播策略不能做组播地址和端口的转换，如：源组播地址为 224.0.0.1，源组播端口为 4000，则经过深信服安全隔离与信息交换系统之后，组播的地址仍然为 224.0.0.1，组播端口仍然为 4000。

代理模式和路由模式下组播策略使用方法相同。这两种模式下，可以实现组播地址和端口的转换，如：源组播地址为 224.0.0.1，源组播端口为 4000，则经过深信服安全隔离与信息交换系统之后，组播的地址可以转换为 224.0.0.2，组播端口可以转换为 8000。

4、系统支持代理组播信息的传输。由于组播代理的特殊性，配置组播策略不完全使用之前定制的五元组策略信息。

3.2.9 视频交换

系统支持使用 SIP 协议的视频信息的传输。[视频交换]，可以分为[平台级联]和[视频

代理]两种方式。用户可以根据需要，选择不同的方式。

视频交换，可以运行在代理模式或路由模式，不可以运行在透明代理模式。

3.2.9.1 平台级联

通过[平台级联]管理界面，可以添加、启用、停用、编辑、删除平台级联策略，[平台级联]管理界面如下图：

图(45)　平台级联策略

点击添加，在[添加策略]的操作区，正确填写[名称]、[上级平台 IP]、[上级服务端口]、[下级平台 IP]、[下级服务端口]，选择[安全通道]、[视频厂商]、[视频协议]，[网闸内网侧 IP]、[网闸外网侧 IP]、[未定义的信令]，点击确定即完成添加策略操作。如下图：

图(46)　定义平台级联策略

[安全通道]：在[安全通道]模块添加。

[网闸内网侧 IP]、[网闸外网侧 IP]：在[网络接口]模块添加。

编辑平台级联策略，在[编辑策略]的操作区，添加/导入内置信令，如下图：

图(47)　平台级联策略信令控制

3.2.9.2 视频代理

通过[视频代理]管理界面，可以添加、启用、停用、编辑、删除视频代理策略，[视频代理]管理界面如下图：

图(48)　视频代理策略

点击添加，在[添加策略]的操作区，正确填写[名称]、[客户端 IP]、[视频服务 IP]、[视频服务端口]，选择[安全通道]、[视频厂商]、[视频协议]、[网闸内网侧 IP]、[网闸外网侧 IP]、[未定义的信令]，点击确定即完成添加策略操作。如下图：

图(49)　视频点播

[安全通道]：在[安全通道]模块添加。

[网闸内网侧 IP]、[网闸外网侧 IP]：在[网络接口]模块添加。

[客户端 IP]：客户端的 IP，可以是单个 IP，也可以是范围 IP 段。

[视频服务 IP]、[视频服务端口]服务端的 IP 及端口号。

编辑视频代理策略，在[编辑策略]的操作区，添加/导入内置信令，如下图：

图(50)　视频代理应用信令控制

3.2.10 Web 代理

系统支持 HTTP/HTTPS 代理上网。通过[web 代理策略]管理界面，可以添加、删除、启用、停用平台级联策略，[web 代理策略]管理界面如下图：

图(51)　WEB 代理

点击添加，在[添加策略]的操作区，正确填写[名称]、[服务端口]、[URL 名称列表]，选择[方向]、[源对象]、[网闸服务 IP]，[时间模式]、[URL 过滤]，点击确定即完成添加策略操作。如下图：

图(52)　WEB 代理策略

[源对象]：在[对象]模块添加，可以是[对象]也可以是[对象组]。

[网闸服务 IP]：在[网络接口]模块添加。

[时间模式]：在[时间模式]模块添加。

[服务端口]：上网时需要使用的端口号。

3.2.11 数据库同步

通过[数据库同步策略]管理界面，可以添加、启用、停用、编辑、删除数据库同步策略，[数据库同步策略]管理界面示例如下图：

图(53)　数据库同步策略

[设置定时同步]：勾选开启定时同步功能可以自行设置[每天开始同步时间]，[持续同步时长]。

点击添加，在[添加策略]的操作区，正确填写[名称]、[内网数据库 IP]、[内网 DB 端口]、[内网 DB 名称]、[内网用户 ID]、[内网用户密码]、[字符集]、[外网数据库 IP]、[外网 DB 端口]、[外网 DB 名称]、[外网用户 ID]、[外网用户密码]、[对象别名前缀]，选择[内

网 DB 类型]、[同步数据方向]、[外网 DB 类型]，点击确定即完成添加策略操作。如下图：

图(54)　定义数据库同步策略

编辑数据库同步策略，在[添加同步表策略]的操作区，正确填写[内网表名称]、[内网表字段列表]、[内网表主键]、[同步过滤条件]、[外网表名称]、[外网表字段列表]、[外网表主键]，选择[同步动作]、[特殊选项]，如下图：

图(55)　定义数据库同步表

系统支持客户端软件部署和设备内置部署两种方式。该模块内置只是提供了部署简单的灵活性，同步性能会有所损失。

3.3 设备管理

在[设备管理]中管理员可读取、修改系统的各种设置信息及相关的设备操作，设备管理依据内容的不同分为[基本设置]、[网络接口]、[设备状态]、[诊断工具]、[备份升级]等部分。

3.3.1 基本设置

包含[基本设置]、[设备时间]、[双机热备]、[设备管理]四个标签页。

3.3.1.1 基本设置

主要有修改[设备工作模式、[日志设置]、[存储空间报警]、[通信口检查]、[实时报警设置]、[管理者 IP 设置]、[网络传输单元 MTU]、[最大流量设置]、[最大连接数设置]、[安全模块]和[扩展功能].

[设备工作模式]：设备支持三种工作模式[透明代理]、[代理模式]、[路由模式]。如下图：

图(56)　定义工作模式

[开启策略日志记录]：勾选此项时表示开启策略日志记录。记录日志可能对系统性能有一定的影响，请根据实际需要选择是否开启。

[开启 SYSLog 日志]：勾选此项系统会按一定周期把日志信息以 SYSLog 的形式，发送到远端服务器，以便管理人员查看设备[系统日志]。请确保设置的[接收日志服务器 IP]、[端口]的正确性。如下图：

图(57)　SYSLOG 发送

[通信口检查]：勾选此项表示开启通信口检查。此时设备会周期性扫描使用中的安全通道网口的网线连接状态，当发现有被拔网线的情况，就会把所有其他使用中的网卡 down 掉，设备处于业务停止状态，如果配置了备机，会要求备机启动。当所有安全通道网口的网线连接都恢复正常时，设备会把之前 down 掉的网卡都 up，设备处于业务运行状态，如果配置了备机，会要求备机停止。如此循环。

[实时报警设置]：勾选此项时，系统会把[访问日志]中拒绝通过的日志，以短信的形式实时发送给管理员。请确保短信平台服务器 IP 是设备内网路由可达的。如下图：

图(58)　短信报警

[管理者 IP 设置]：通过该项可以设置允许登录并管理设备的管理者的 IP。该 IP 可以是单个 IP，也可以是掩码形式的 IP 段。管理者 IP 无限制，请选用默认的 0.0.0.0/0。如下图：

图(59)　限定管理者 IP

[网络传输单元 MTU]，设置网络传输单元 MTU。

[安全模块]：设置是否开启入侵检测功能，抗 DDos 攻击功能等。

[通信口检查]：该项通常配合[双机热备]使用，不使用[双机热备]功能时，建议不要开启该选项。

[开启 STP 协议支持]:勾选该选项可以开启 STP 协议支持。

[开启其他协议支持]:勾选该选项时，TRUNK 包可以被正常识别和过滤，除了 TCP、UDP、ICMP 之外的其他基于 IP 协议可以通过。

[透明代理]：无任何 IP 地址，不改变用户的网络拓扑，设备透明接入。

[代理模式]：客户端可以通过访问隔离设备的代理 IP，和服务器通信。客户端不需要添加额外的路由信息。内外网网段可以相同，也可以不同。

[路由模式]：客户端添加正确的路由信息，就可以访问服务器的真实 IP 直接通信。如果策略配置了多 IP 对应，客户端也可以通过访问隔离设备的 IP 代理通信，即使用[路由模式]下的代理。内外网网段要求不同。

[开启 STP 协议支持]、[开启其他协议支持]：只在[透明代理]模式下生效。

管理者 IP 决定哪些 IP 设备可以管理安全隔离设备，修改时一定要确定好再填写。

3.3.1.2 设备时间

系统支持手动获取时间/设置时间

手动设置时间：选择要更改的时间，点击设置时间。

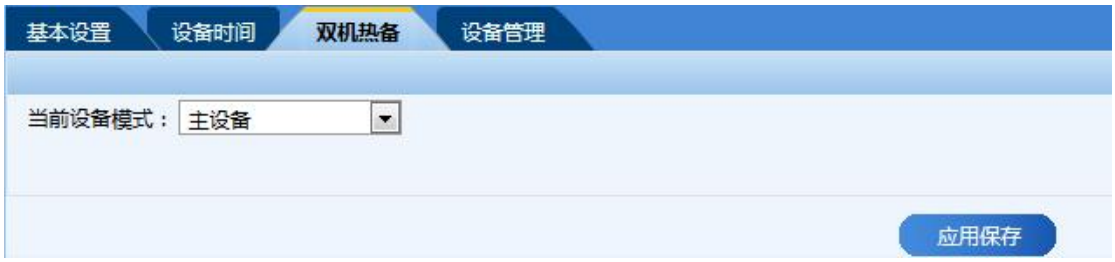
[启用时间服务器]：可以同步远程服务器时间，保证[远程时间服务器]填写正确，点击立刻同步，如下图：

图(60)　设备时间设置

3.3.1.3 双机热备

使用该功能时需两台设备，一台作为主设备，另一台作为从设备。主设备和从设备的热备口，通过网线直连，或者通过交换机相连。

［主设备］：采用主从模式，是主要的工作设备。如下图：



图(61)　双机热备设置

［从设备］：当主设备异常时，切换为工作状态；主设备恢复正常后，将停止工作。如下图：

图(62)　从设备设置

[主设备 ID 号]：从设备需要填写主设备的设备 ID，该 ID 号可以在主设备的[设备状态]查看。

[策略同步]：从设备可以选择是否开启自动主策略同步，以及设置同步的周期。开启自动主策略同步，则主设备可以按设定的周期把策略同步到从设备。

1、开启自动主策略同步时，从设备的策略会被同步过来的策略覆盖掉，但如下一些选项是不会被覆盖的。包括：管理口 IP，管理口端口，管理口掩码，允许的管理者 IP，当前是主设备还是从设备。

2、从设备运行的过程中，会继续探测主设备的状态，一旦发现主设备恢复正常了，从设备会自动切换为停止工作状态。

3、双机热备功能，支持宕机切换、拔线切换。

宕机切换指：当从设备探测到主设备工作异常时，可能是主设备断电、死机、程序崩溃等情况，从设备切机运行。

双机热备默认提供宕机切换功能，不需要通过管理界面设置。

拔线切换指：主设备策略中使用到的网口，有网线松动，或网口故障等情况时，主设备主动停止工作，从设备随即运行。可以在主设备管理界面设置拔线切换。

设置拔线切换界面示例如下图：

图(63)　通信口异常检查

3.3.1.4 设备管理

[设备管理]界面如下图：

图(64)　设备管理

重启设备操作：实现设备软重启。

设备初始化：设备会恢复到出厂设置。

[初始化操作同时清空数据库表]：初始化同时会重置数据库表。

导出设备信息：可以下载保存与设备有关的硬件 ID 信息文件。

导入授权：可以导入浏览选择的授权文件。

3.3.2 网络接口

包含[内网处理单元]、[外网处理单元]、[管理口]三个标签页。

3.3.2.1 内网处理单元

在接口列表部分，可以对设备的网络接口 IP 进行管理。同一个网络接口可以包含不同网段或者相同网段的多个 IP，但设备同一侧不同的网络接口，不要设置相同网段的 IP；也可以对添加的 IP 进行删除，点击删除。如添加 IP 需进入 IP 地址管理，在输入框输入要添加的[IP 地址]和[掩码]，点击添加完成添加。如下图：

图(65)　设置地址

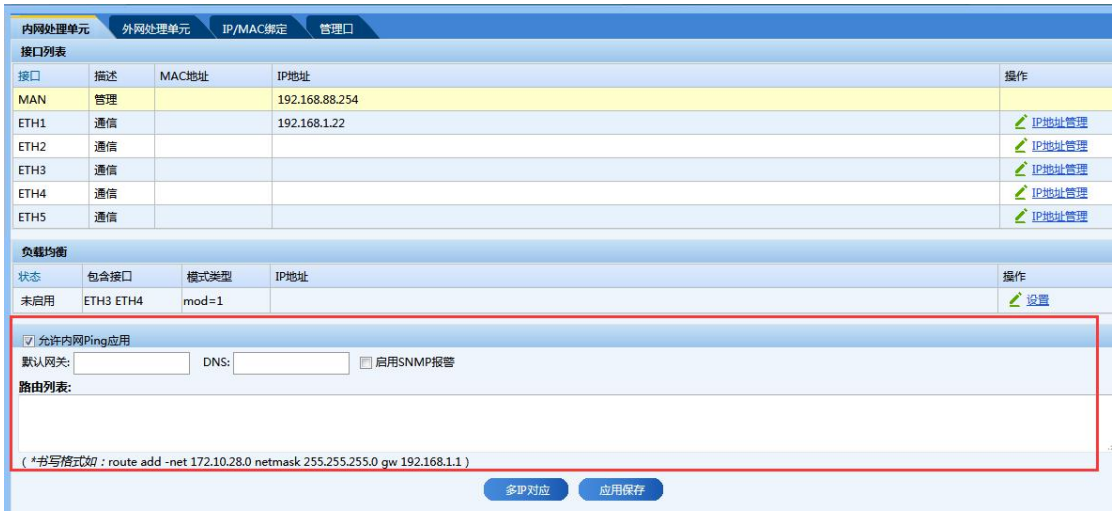
在负载均衡部分，可以启用和停用负载均衡，选择模式类型，并对负载均衡的 IP 进行管理。添加 IP 时同样要注意上面提到的问题。

图(66)　设置接口负载均衡

负载均衡模式类型，有七种可供选择，推荐使用主备模式：

图(67)　接口负载均衡模式

[允许内网 Ping 应用]界面如下图：



图(68)　接口地址、路由设置

[默认网关]：设置内网处理单元默认网关。

[DNS]：设置内网处理单元 DNS。

[启用 SNMP 报警]：设置内网处理单元 SNMP 告警。

[路由列表]：可以添加网络路由、也可以添加主机路由。

[允许 Ping 应用]：表示允许其他主机 Ping 隔离设备的网络接口。否则，其他主机 Ping 隔离设备网络接口时，设备是不会给回应的。

隐藏源地址:路由模式下用户可以选择是否开启此项，其他两种模式下不提供该选项。当勾选该项时，系统会自动获取当前网卡上的 IP 地址，用于替换从该网口出去的数据包中

IP 首部源 IP 地址。这样，服务器会以为是网闸在访问服务，客户端的真实 IP 被隐藏掉，服务器也就不用再添加去往该客户端真实 IP 的路由了。如果不勾选此项，服务器需要把去往该客户端 IP 的路由下一跳指向隔离设备的网口。

注意：应该在隔离设备靠近服务器的一端，选择是否开启此项，比如：规则方向是内到外，服务器在外网侧，则应该在隔离设备外网处理单元选择是否开启此项。

3.3.2.2 外网处理单元

和内网处理单元相似。

3.3.2.3 IP/MAC 绑定

[IP/MAC 绑定]管理界面示例如下：

图(69)　IP、MAC 绑定

在该界面可以启停[IP/MAC 绑定]功能，和管理要进行绑定的地址组。区域可以选择内网侧，外网侧或全区域。选择全区域表示同时在设备内外网主机进行绑定。

3.3.2.4 管理口

具有相应权限的用户，可通过[管理口]界面修改[管理口 IP]地址、[子网掩码]、[管理端口]等信息。[开启多口管理]为，允许通过管理口及内网通信口管理设备。请根据需要谨慎修改。

图(70)　管理口设置

管理 IP：MAN 口 IP 地址，需要连接此 IP 地址管理设备。

默认管理口 IP 为 10.251.251.11/24

子网掩码：根据实际网络环境配置

管理端口：如果业务中使用到了管理端口 443，则需要修改管理口端口为未使用的端口号，否则会产生歧义。

3.3.3 设备状态

设备状态界面，包含[设备状态]、[内网处理单元状态]、[外网处理单元状态]。分别可以查看设备整体状态，内网状态和外网状态。

3.3.3.1 设备状态

通过该界面，可以查看深信服安全隔离与信息交换系统整体运行状态，包括[设备 ID 号]、[设备类型]、[系统版本]、[权限许可]、[当前策略运行状态]等。设备状态界面示例如下图：

图(71)　设备状态

3.3.3.2 内网处理单元状态

通过该界面，用户可以了解设备内网单元资源（CPU/内存/存储/流量）的使用情况，隔离通道的状态等信息。隔离通道正常，表示设备内外网连接正常。

3.3.3.3 外网处理单元状态

和内网处理单元状态相似。

3.3.4 诊断工具

用户可以使用系统提供的多个[诊断工具]，了解网络的连通状况，进行系统异常排错。。

3.3.4.1 Ping 工具

在[Ping]的操作区，正确填写[目标主机]，选择[网络位置]，点击 Ping 测试即完成操作。如下图：

图(72)　PING 测试工具

目标主机是 IP 地址或域名（需设置 DNS）。

3.3.4.2 Traceroute 工具

在[Traceroute]的操作区，正确填写[目标主机]，选择[网络位置]，点击路由测试即完成操作。如下图：

图(73)　Traceroute 测试工具

3.3.4.3 TCP 服务检查工具

在[Tcp 服务]的操作区，正确填写[目标主机]、[服务端口]，选择[网络位置]，点击服务测试即完成操作。如下图：

图(74)　TCP 端口联通测试

3.3.4.4 抓包工具

在[抓包分析]的操作区，选择[网络位置]、[接口参数]、[协议类型]，点击启用抓包/停止抓包取数据即完成操作。如下图：

图(75)　抓包工具

3.3.5 备份升级

系统为用户提供了策略的备份与恢复功能，以及模块升级功能。

3.3.5.1 策略备份恢复

[备份恢复]区分为导入恢复、导出备份。

导出备份分为：手动备份、自动备份。

导入恢复：从文件恢复系统配置，选择浏览，然后选择以前备份的配置，点击导入恢复即完成恢复系统设置。

手动导出备份：点击导出备份，选择导出的路径，点击确定，完成导出备份。

自动导出备份：勾选[开启策略自动备份]，输入正确的参数，在设定的时间会发送备份到指定路径。如下图：

图(76)　策略自动备份

默认备份的策略上传到 FTP 服务器的根目录，上传路径填写的是子路径。

3.3.5.2 模块升级

在[模块升级]操作区，点击浏览，选择要升级的模块包，然后点击更新升级，完成升级模块操作。模块升级界面示例如下图：

图(77)　系统升级

3.4 审计

日志审计功能，可对设备的各项信息进行统计，包括管理信息、系统信息以及交换信息等。系统提供了日志的[排序]、[查询]、导出、删除等功能。

3.4.1 管理日志

管理日志记录所有管理员（审计管理员除外）通过 WEB 管理界面所做的操作信息。

记录ID	时间	用户	操作内容	结果
124	2018-10-17 03:17:02	admin	添加IP/MAC 绑定地址操作	成功
123	2018-10-17 03:16:44	admin	添加IP/MAC 绑定地址操作	成功
122	2018-10-17 03:16:35	admin	删除IP/MAC 绑定地址操作	成功
121	2018-10-17 03:16:18	admin	添加IP/MAC 绑定地址操作	成功
120	2018-10-17 03:16:02	admin	添加IP/MAC 绑定地址操作	成功
119	2018-10-17 03:15:54	admin	添加IP/MAC 绑定地址操作	失败
118	2018-10-17 03:15:45	admin	添加IP/MAC 绑定地址操作	失败
117	2018-10-17 03:15:42	admin	添加IP/MAC 绑定地址操作	失败
116	2018-10-17 03:15:22	admin	添加IP/MAC 绑定地址操作	失败
115	2018-10-17 03:12:02	admin	添加内网NET1 [新IP：10.73.88.2] [掩码：255.255.255.0]	成功

图(78)　管理日志

3.4.2 攻击防护日志

攻击防护日志是指系统内置的入侵检测监测到的攻击行为的记录。

图(79)　攻击防护日志

3.4.3 审计管理日志

管理日志是记录审计管理员通过 WEB 管理界面所做的操作信息。

图(80)　审计管理日志

3.4.4 系统日志

系统日志是记录系统运行中产生的状态信息。

图(81)　系统日志

3.4.5 访问日志

访问日志是通过深信服安全隔离与信息交换系统进行业务访问所产生的记录。

图(82)　访问日志

3.4.6 内容过滤日志

内容过滤日志是使用系统进行数据交换的过程中，经内容审查模块检查到的关键字、文件类型、病毒、木马等信息的记录。

图(83)　内容过滤日志

3.4.7 文件交换日志

文件交换日志是使用系统进行数据交换的过程中，文件交换策略部分记录的日志信息，详细记录了通过设备同步过去的文件名称、路径、区域等信息。

图(84)　文件交换日志

3.4.8 数据库同步日志

数据库同步日志是使用数据库同步模块的过程中，产生的信息记录。

图(85)　数据库同步日志

附录一 常用应用协议内部命令简介

FTP

内部指令	指令表现
PORT	PORT 模式传输数据
PASV	被动模式传输数据
PASS	密码
NLST	浏览 ls
LIST	浏览 ls
HELP	远程的帮助
DELE	删除
CWD	改变目录
APPE	上传并续传
REST	重置
XRMD	删除目录
XMKD	建立目录
XPWD	改变目录
USER	用户名
TYPE	传输文件的格式类型是二进制还是 ASCII
STOR	上传文件
RNTO	改写文件
RNFR	下载续传本地文件
OPTS	获取服务器信息
FEAT	提取文件
ACCT	帐号关联
CDUP	到上一级目录
MDTM	获得指定文件的修改时间
PWD	显示路径
SIZE	获取文件尺寸
SYST	获取操作系统类型
SITE	将参数作为 SITE 命令逐字发送至远程 ftp 主机
NOOP	保活指令
MODE	查看当前传输文件的模式
RETR	下载文件
AUTH	验证
QUIT	退出
SMTP	
内部指令	指令表现
DATA	邮件内容
EHLO	身份验证
ETRN	指定邮件系统队列中发给所设置的域名的邮件收取到本系统的邮件队列中
VRFY	校验用户
VERB	加密验证
REST	命令可以恢复被标记为删除的信件

RCPT	确认邮件是否收到
ONEX	加密 认证
NOOP	保活连接
MAIL	邮件信息
HELP	远程帮助
HELO	欢迎信息
EXPN	获取用户名列表
QUIT	退出
POP3	
内部指令	**指令表现**
USER	用户名
PASS	密码
AUTH	校验
APOP	密文认证口令
UIDL	提取邮件的标示
TOP	用来获取邮件头及被预定义的一块字符串
STLS	握手协议
STAT	获取你邮箱目前的状态，如邮件多少封、多大
RETR	提取某封邮件
REST	命令可以恢复被标记为删除的信件
QUIT	退出
NOOP	保活会话
LIST	列出邮件
DELE	删除邮件
CAPA	返回 POP3 服务器支持的功能列表
HTTP	
内部指令	**指令表现**
PROPFIND	查看属性
PROPPATCH	设置属性
LOCK	加锁
UNLOCK	解锁
SEARCH	搜索文件信息
PUT	上传文件
POST	提交数据（非文件）
COPY	拷贝信息
MOVE	移动文件
MKCOL	在服务器上创建目录
OPTIONS	询问可以执行哪些方法
TRACE	用于远程诊断服务器
HEAD	提取文件类似 GET,但是不返回 BODY 信息
GET	浏览或获取文件
DELETE	删除

SQLSERVER	
内部指令	**指令表现**
SELECT	查询数据
INSERT	插入数据
DELETE	删除记录
UPDATE	更新记录
CREATE	创建对象
DROP	删除对象
GRANT	赋予权限
ALTER	修改对象
REVOKE	废除权限
ORACLE	
内部指令	**指令表现**
SELECT	查询数据
INSERT	插入数据
DELETE	删除记录
UPDATE	更新记录
CREATE	创建对象
DROP	删除对象
GRANT	赋予权限
ALTER	修改对象
REVOKE	废除权限
COMMIT	提交数据
ROLLBACK	回滚操作

附录二 应用模块说明

应用模块	协议	说明
NULL_TCP	TCP	TCP 自定义模块，当不绑定标准协议模块时可以选用该模块
TCP_SINGLE	TCP	TCP 单向，指应用层的数据，只能从源对象到目的对象，一个方向传输。
HTTP	TCP	HTTP 模块
SSL	TCP	SSL 模块
POP3	TCP	POP3 模块
SMTP	TCP	SMTP 模块
FTP	TCP	FTP 模块，使用 FTP 协议时需要绑定该模块，不能用 NULL_TCP 代替

SMB	TCP	SMB 模块
MEDIA	TCP	MEDIA 模块，媒体流传输，如 RTSP 等
H323	TCP	H323 模块
1bit（旧版本叫做 4BYTES）	TCP	1bit 模块，要求目的对象发给源对象的响应信息，每个数据包的应用层数据长度不超过一个字节。
DBSYNC	TCP	数据库同步模块，配合“数据库同步”软件一起使用。“数据库同步”软件运行在设备两侧的计算机上。
FILEEXCHANGE	TCP	保留，暂未使用
CSM	TCP	信号集中监控模块,用于工业控制
SQLSERVER	TCP	SQLSERVER 数据库
ORACLE	TCP	ORACLE 数据库
DB2	TCP	DB2 数据库
SYBASE	TCP	SYBASE 数据库
MYSQL	TCP	MYSQL 数据库
DM	TCP	达梦数据库
OPC	TCP	OPC 模块
MODBUS	TCP	MODBUS 模块
S7	TCP	S7 模块
DNP3	TCP	DNP3 模块
IEC104	TCP	IEC104 模块
IEC61850_MMS	TCP	IEC61850_MMS 模块
WINCC	TCP	WINCC 模块
NULL_UDP	UDP	UDP 自定义模块，当不绑定标准协议模块时可以选用该模块
UDP_SINGLE	UDP	UDP 单向，指应用层的数据，只能从源对象到目的对象，一个方向传输。
DNS	UDP	DNS 模块
MODBUS_UDP	UDP	使用 UDP 协议的 MODBUS 模块

PING	ICMP	PING 模块

下表为应用信息说明：

属性	说明	
名称	某种网络通信在本系统中的标识，可由具备应用配置管理权限的用户命名（如 FTP、HTTP、TELNET 等）。	
协议	该网络通信使用的协议，可选择 TCP、UDP、ICMP 协议中的一种。	
所属模块	系统内置的通用服务处理单元，选中某处理模块代表该服务符合内置服务处理单元特性。	
源端口	该输入框仅在选择 TCP 或 UDP 协议后有效，表示该网络服务的源端口，源端口可是一个通信端口（如 1378），也可是一个端口范围（如 1024-65535）。通常使用默认的 1-65535。	
目的端口	该输入框仅在选择 TCP 或 UDP 协议后有效，表示该网络服务的目标端口，目标端口可是一个通信端口（如 80），也可是一个端口范围（如 20-40）。	
代理端口	该输入框仅在选择 TCP 或 UDP 协议后有效，表示向用户提供的服务端口的映射，可是一个通信端口（如 80），也可是一个端口范围（如 80-90），比如把服务器的 80 端口映射为 8080-8090 端口，用户访问 8080 到 8090 之间的任意端口都可以，代理端口是网闸开放的端口。 代理模式，以及路由模式下的代理（5.1.1 节有介绍），会用到该端口。当目的端口为单个端口时，代理端口可以是单个端口，也可以是范围端口；当目的端口为范围端口时，代理端口必须为范围端口，并且尽量使用相同的范围值。	
命令列表	用于定制该网络通信的数据内容控制。用户可添加一个或多个通信内容段的命令，并分别定制对该命令的处理方法。命令列表不是必填项，可以不添加命令。各个应用模块命令参数使用方法，详见附录四。 命令列表包含如下内容：	
	命令	用于定义该段内容的名称。例如：如果应用模块为 HTTP，则命令可以为 GET，POST 等等。
	功能描述	对该命令的注释信息

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn

	参数	用于定义该命令的参数。可以不填写，为空时匹配所有。
	附件参数	更深一层的参数，通过该参数，可以增强对协议更深一层的控制粒度。可以不填写，为空时匹配所有。
	起始位置	用于确定该命令在网络包中开始的位置。从通信协议包头结束开始计位。
	动作	用于定制对含有该命令的网络通信的处理方法，可选“允许”或“拒绝”。当选择“允许”时，设备分析出数据包符合该命令就按放行处理。当选择“拒绝”时，设备分析出数据包符合该命令就按丢弃处理。
未定义命令	定制的命令列表内容都不匹配时，按该选项处理。 可通过下拉框选择允许或拒绝	
描述	填写描述信息	
日志开关	该应用是否记录策略日志。跟[设备管理]->[基本设置]中“开启策略日志记录”选项组合使用，当它们全部勾选时，才记录该应用策略日志。	

地址:深圳市南山区学苑大道1001号南山智园A1栋
咨询热线：400-806-6868 | 服务热线：400-630-6430 | 邮箱: market@sangfor.com.cn | 网址：www.sangfor.com.cn