

# AF 8.0.6 用户手册



# 目录

声明.....	1
前言.....	2
手册内容.....	2
本书约定.....	2
图形界面格式约定.....	2
各类标志.....	3
技术支持.....	3
致谢.....	4
第 1 章 安装指南.....	5
1.1. 环境要求.....	5
1.2. 电源.....	5
1.3. 产品外观.....	6
1.4. 配置与管理.....	6
1.5. 设备接线方式.....	7
第 2 章 控制台的使用.....	9
2.1. 登录 WebUI 配置界面.....	9
2.2. 配置和使用.....	10
第 3 章 功能说明.....	13
3.1. 激活设备和技术社区导航.....	13
3.1.1. 进入技术社区.....	13
3.1.2. 安全助手.....	14
3.2. 运行状态.....	31
3.2.1. 总览.....	32
3.2.2. 安全运营中心.....	37
3.2.3. 业务安全.....	40
3.2.4. 用户安全.....	48
3.2.5. 流量会话.....	54

3.2.6. DHCP 运行状态.....	69
3.2.7. 在线用户管理.....	69
3.2.8. 封锁攻击者 IP.....	73
3.3. 网络.....	75
3.3.1. 接口/区域 .....	75
3.3.2. 路由.....	89
3.3.3. 虚拟网线.....	114
3.3.4. 高级网络配置.....	115
3.3.5. 光口 bypass 设置.....	125
3.3.6. SSL VPN.....	126
3.3.7. IPSec VPN .....	180
3.4. 对象.....	231
3.4.1. 网络对象.....	231
3.4.2. 服务.....	237
3.4.3. 安全策略模板.....	240
3.4.4. 安全防护规则库.....	275
3.4.5. 内容识别库.....	292
3.4.6. IP 地址库 .....	306
3.4.7. 时间计划.....	307
3.4.8. 信任的证书颁发机构.....	311
3.5. 策略.....	311
3.5.1. 地址转换.....	312
3.5.2. 访问控制.....	325
3.5.3. 安全策略.....	337
3.5.4. 解密.....	372
3.5.5. 流量管理.....	379
3.5.6. 配置向导.....	400
3.5.7. 黑白名单.....	411
3.5.8. 页面定制.....	412

3.6. 系统.....	413
3.6.1. 系统配置.....	413
3.6.2. 管理员账号.....	429
3.6.3. 系统维护.....	434
3.6.4. 排障.....	439
3.6.5. 高可用性.....	446
3.7. 用户认证.....	451
3.7.1. 用户管理.....	452
3.7.2. 用户认证.....	496
3.7.3. 服务器访问认证.....	559
3.8. 下一代安全防护体系.....	561
3.8.1. 体系总览.....	561
3.8.2. EDR.....	567
3.8.3. 云端增值服务.....	568
3.8.4. 安全防护能力.....	570
第 4 章 数据中心.....	572
4.1. 统计分析.....	572
4.1.1. 业务安全.....	573
4.1.2. 用户安全.....	575
4.1.3. 流量统计.....	577
4.1.4. 应用统计.....	580
4.1.5. 内容安全.....	583
4.1.6. 业务模型学习监督.....	584
4.2. 日志查询.....	586
4.2.1. DOS 攻击.....	587
4.2.2. WEB 应用防护.....	589
4.2.3. 漏洞攻击防护.....	592
4.2.4. 僵尸网络.....	596
4.2.5. 内容安全.....	597

4.2.6. 应用控制.....	601
4.2.7. SSL VPN 用户日志.....	603
4.2.8. 本机安全事件.....	604
4.2.9. 本机访问控制.....	604
4.2.10. 用户登录/注销 .....	606
4.2.11. 系统操作.....	607
4.3. 报表.....	609
4.3.1. 报表订阅.....	609
4.3.2. 自定义报表.....	615
4.3.3. 管理员操作报表.....	617
4.4. 系统.....	617
4.4.1. 系统设置.....	618
4.4.2. 日志库.....	619
第 5 章 案例集.....	620
5.1. 设备部署配置案例.....	620
5.1.1. 路由接口配置案例.....	620
5.1.2. 透明接口配置案例.....	626
5.1.3. 虚拟网线接口配置案例.....	634
5.1.4. 旁路镜像接口配置案例.....	638
5.1.5. 子接口配置案例.....	642
5.1.6. 混合部署配置案例.....	644
5.1.7. 二次穿透部署案例.....	650
5.2. 策略路由配置案例.....	651
5.2.1. 策略路由配置案例 1.....	651
5.2.2. 策略路由配置案例 2.....	654
5.3. ARP 代理配置案例.....	657
5.4. DHCP 配置案例 .....	659
5.4.1. 服务器配置案例.....	659
5.4.2. DHCP 中继配置案例 .....	661

5.5. Dos/DDos 防护配置案例.....	663
5.6. 应用控制策略配置案例.....	673
5.7. 内容安全策略配置案例.....	676
5.8. 漏洞攻击防护典型配置案例.....	681
5.9. WEB 应用防护配置案例.....	687
5.9.1. WEB 应用防护配置案例一 WAF.....	687
5.9.2. WEB 应用防护配置案例二 数据防泄密.....	693
5.10. 网站篡改防护 2.0 应用案例.....	699
5.11. 双机热备案例.....	708
5.12. SSL VPN 配置案例.....	715
5.12.1. 新建用户配置案例.....	715
5.12.2. TCP 应用配置案例 .....	716
附录 SANGFOR 设备升级系统的使用 .....	720

# 声明

Copyright ©2000- 2018 深信服科技股份有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

深信服科技股份有限公司（以下简称为深信服科技、SANGFOR）。

SANGFOR 为深信服科技股份有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

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技术服务部。

# 前言

## 手册内容

第1部分 SANGFOR AF 产品安装指南。该部分主要介绍 AF 设备的外观特点及功能特性和性能参数，以及连接前的准备和注意事项。

第2部分 SANGFOR AF 控制台的使用，如何登陆控制台等。

第3部分 SANGFOR AF 的功能说明及使用。

第4部分 SANGFOR AF 数据中心的功能说明及使用。

第5部分 案例集。讲解各功能模块在常见环境下的配置案例。



本手册以 SANGFOR AF-1000-D600 为例进行配置。由于各型号产品硬件和软件规格存在一定差异，所有涉及产品规格的问题需要和深信服科技股份有限公司联系确认。

## 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 <b>确定</b>
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】
下拉列表、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](mailto: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：<http://bbs.sangfor.com.cn>

深信服科技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](http://www.sangfor.com.cn)



深信服，让IT更简单，更安全，更有价值

## 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、论坛或电子邮件回馈给我们，我们将不胜感谢。

# 第1章 安装指南

本部分主要介绍了 SANGFOR AF 系列产品的构成与硬件安装。硬件安装正确之后，您可以进行配置和调试。

## 1.1. 环境要求

SANGFOR AF 设备可在如下的环境下使用。

- 输入电压： 110V~230V
- 温度： 0~45°C
- 湿度： 5~90%

为保证系统能长期稳定的运行，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 AF 系列产品使用交流 110V 到 230V 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. 产品外观

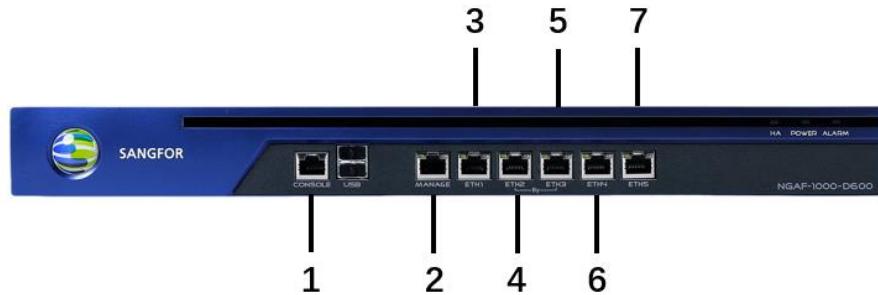


图 1：SANGFOR AF 前面板（以 AF-1000-D600 为例）

1.CONSOLE(控制)口      2. MANAGE 口(ETH0)      3.ETH1

4.ETH2      5.ETH3      6.ETH4      7.ETH5



告警灯在设备启动期间是红灯长亮的。一般一两分钟后红灯熄灭，说明正常启动。如红灯长时间不熄灭，请关闭设备等待 5 分钟后重新启动。如果还是长亮，请联系技服部门确认是否设备损坏。正常启动后，有时红灯会闪烁，这是正常现象，红灯闪烁表示设备正在写系统日志。



控制口仅供开发和测试调试使用。最终用户需通过控制台网口接入设备。

## 1.4. 配置与管理

在配置设备之前，您需要配备一台计算机，配置之前请确定该计算机的网页浏览器能正常使用（如 Internet Explorer），然后把计算机与 SANGFOR AF 连接在同一个局域网内，通过网络对设备进行配置。

AF 设备的管理口为 MANAGE(ETH0) 口，管理口默认出厂 IP 为 10.251.251.251/24。初次登陆设备，请用网线连接 MANAGE(ETH0) 口到局域网

或直接连接计算机。

## 1.5. 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 MANAGE(ETH0) 口与内部局域网连接，对 AF 设备进行配置。

登录控制面板后根据网络环境和部署要求配置『网络』和接线。（详情参见章节 3.3）



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 MODEM 和交换机应使用直联机、连接路由器和计算机网口应使用交叉线。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：

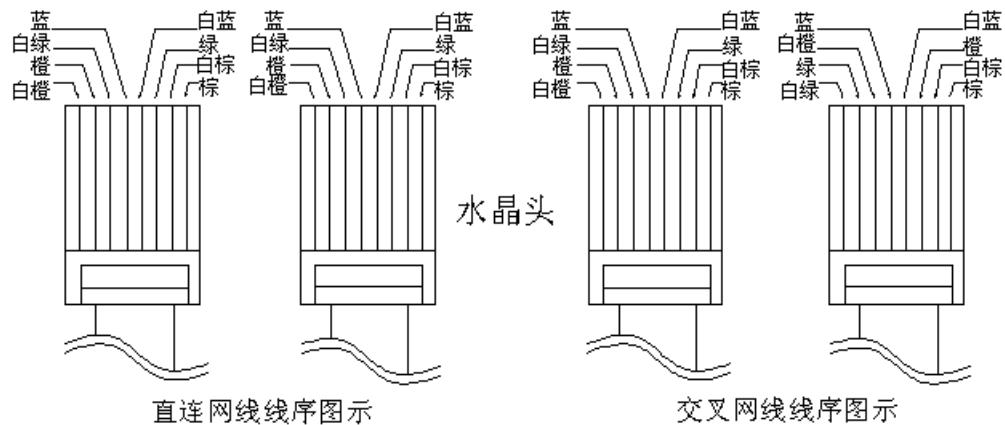


图 1 直联机、交叉线 线序

# 第2章 控制台的使用

## 2.1. 登录 WebUI 配置界面

AF 支持安全的 HTTPS 登录，使用的是 HTTPS 协议的标准端口登录。如果初始登录从管理口(MANAGE)登录，那么登录的 URL 为：<https://10.251.251.251>



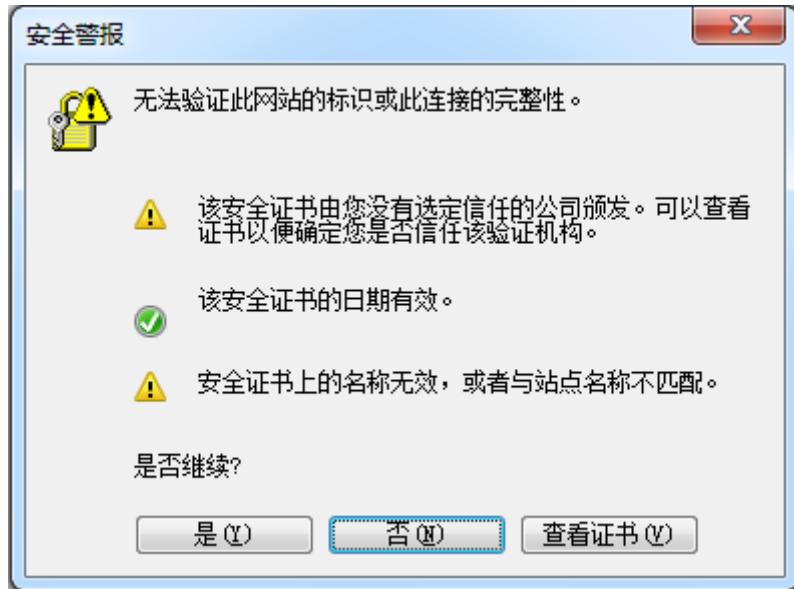
1、HTTPS 登录 WEBUI 管理 AF 可以防止配置过程在传输过程中被截获而产生的安全隐患。

2、如果开启 SSL VPN 多功能序列号，则会有提示控制台端口是否改成 4430，如果改成 4430，则控制台的登陆方式为：<https://10.251.251.251:4430>

如何登录 AF 设备控制台页面？

按照前面所示方法接好线后，通过 WEB 页面来配置 SANGFOR AF 设备。方法如下：

首先为登陆控制面板的计算机配置一个 10.251.251.X 网段的 IP（如配置 10.251.251.100），然后在 IE 浏览器中输入管理口的默认登陆 IP 及端口 <https://10.251.251.251>，出现一个如下图的安全提示：



点击**是**后出现以下的登录页面：



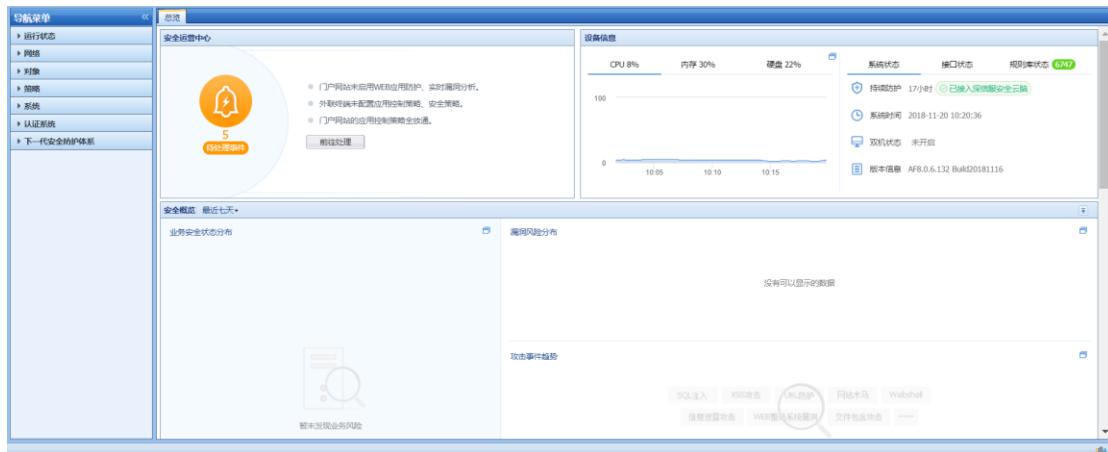
在登陆框输入『用户名』、『密码』和『验证码』，点击**登录**按钮即可登录AF设备进行配置，出厂情况下的用户名和密码为admin/admin。

登录控制面板不需要安装任何控件，支持用非IE的浏览器登录控制台。

## 2.2. 配置和使用

登录WebUI配置页面后，可以看到以下配置模块：包括『运行状态』、『网

络』、『对象』、『策略』、『系统』、『认证系统』、『下一代安全防护体系』。



控制台右下角的 用于实时通知设备的一些系统信息和告警信息。

所有配置页面中的 图标，当鼠标放到此图标上时，可以显示当前配置项的简要说明说明。后面的文档不再赘述。

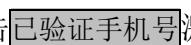
如果设备未曾激活过，登陆控制台后会出现如下在线激活页面，如下图所示：



输入手机号码和验证码，勾选“我接受深信服隐私权保护声明”激活设备，激活后在服务期内享受完整的售后服务、首次激活赠送一个月的远程服务、可查询硬件质保和在线咨询，并自动在深信服社区生成一个账号。在激活过的设备控制

台点击  [发帖求助](#)、 [在线咨询](#) 时，会自动跳转到深信服社区注册设置密码页面：



如果同一个用户有多台 Sangfor 设备，第一台设备激活后，登陆其他 Sangfor 设备的控制台，点击  已验证手机号激活快速的激活设备，如下图所示：



## 第3章 功能说明

### 3.1. 激活设备和技术社区导航

#### 3.1.1. 进入技术社区

深信服社区（bbs.sangfor.com.cn）是深信服科技向用户提供的以 SANGFOR 产品为核心，与合作伙伴和企业员工进行讨论、交流的平台。

在设备的控制台页面，有进入技术社区的入口，包括发帖求助、在线咨询和在技术社区内搜索问题和资料的功能，如下图所示：



点击 **发帖求助**、**在线咨询** 时，会在浏览器新页面自动跳转到深信服社区系统。输入注册后的手机号码和密码，就可以进入社区。

A screenshot of the Sangfor Community website homepage. The top navigation bar includes links for 'Community', 'News', 'Forum', 'Version', 'Resource Library', 'Activities', 'Self-service', and 'Search'. Below the navigation is a large banner with the text 'Green Arbor Day, Plant a Safe Tree!' and a 'Learn More' button. The main content area features a post titled 'Docker Foundation Chapter: Docker is a God?' by '规划经理', with 374 views and 10 likes. A sidebar on the right lists 'Recommended Editions' such as 'Security Dynamics' and 'Virtualization Big Lecture (Coming Soon, Please Stay Tuned)'.

通过技术社区的自助服务，可以查询到设备的服务器有效期，维修进度，渠道服务资质和渠道认证证书信息，如下图所示：

深信服社区  资讯 论坛 版块 资料库 活动 自助服务  登录 | 注册 | 找回密码

自助服务 > 信息查询

服务有效期 维修进度 渠道服务资质 渠道认证证书

最近查询记录

\* 网关序号 (8位) 或S/N码 (10位) \* 验证码

验证码 

产品名称 服务商名称 服务电话 网络远程支持有效期 同等功能软件升级有效期 硬件维保有效期

没有该设备的相关信息，请确认输入正确的网关序号 (8位) 或S/N码 (10位)

### 3.1.2. 安全助手

#### 3.1.2.1. 风险分析

风险发现的功能，一是对目标 IP 进行端口扫描，它能让管理员清楚了解服务器开放的端口和服务，以及服务器上可能存在哪些漏洞，让管理员及时关闭不必要的端口、封堵漏洞，提高服务器的安全性；二是对目标 IP 进行弱密码扫描，解决数据库弱口令访问不安全的问题。与此同时，风险分析能够做到根据扫描结果智能的生成相应的规则，为客户提供安全防护。点击 ，配置页面如下：

风险分析

不可信来访区域：  

访问的目标IP范围：  

指定端口：  启用弱密码扫描

<input type="checkbox"/> 服务器IP	开放端口	应用	协议	可访问...	可访问IP	风险等级	风险
--------------------------------	------	----	----	--------	-------	------	----

[不可信来访区域]：定义应用控制策略、漏洞攻击防护、WAF 检测的源区域，检测这个区域到目标 IP 是否有做相应的应用控制策略、漏洞攻击防护和 WEB 应用防护规则。

[访问的目标 IP 范围]：定义进行端口扫描或者是弱密码扫描的目标 IP 地址范围。

[指定端口]：定义需要对目标 IP 的哪些端口进行扫描。点击 **80,81,8001,8002...**，则弹出【选择端口】的编辑框，如下图所示：



设备内置了服务器经常开放的一些端口，若需要新增对其他端口的扫描，点击**新增**添加即可。

勾选[启用弱密码扫描]，则启用弱密码扫描功能。界面如下图所示：

风险分析

不可信来访区域: 外网区,内网区

访问的目标IP范围: 192.168.1.249

指定端口: 80,81,8001,8002/http , 443/...  启用弱密码扫描

点击【启用弱密码扫描】，弹出【启用弱密码扫描】的编辑框，如下图所示：



[扫描范围]: 勾选对哪些应用服务进行弱密码扫描。



[扫描方式]: 定义弱密码扫描的扫描方式，可以分为常规密码字典扫描和完整密码字典扫描。常规密码字典只包含系统的默认密码。

点击**高级选项**，用于设置 RDP、VNC 的完整密码扫描和自定义词典。界面如下图所示：



[执行完整扫描]: 由于 RDP、VNC 协议的密码扫描需要耗费较长的时间，若需要对这两种协议也进行完整密码字典扫描，还需要勾选上“执行完整扫描”。

[自定义用户名列表]: 用于自定义需要匹配的用户名。此时会在相应字典列表的用户名里增加自定义的用户名。比如说，此时的自定义用户名为 sangfor，AF 设备在进行弱密码扫描时，除了扫描默认的用户名以外，还会去匹配是否存在 sangfor 这个用户名。

[自定义密码字典列表]: 用于自定义需要匹配的弱密码。此时会在相应字典列表的密码里增加自定义的密码。比如说，此时的自定义密码为 sangfor，AF 设

备在进行弱密码扫描时，除了扫描默认的用户名是否匹配默认的密码以外，还会去匹配默认的用户名是否使用了 sangfor 这个密码。

设置好端口扫描和弱密码扫描后，点击  开始扫描，将会在下方显示扫描结果，界面如下图所示：



服务器IP	开放端口	应用	协议	可访问区域	可访问IP	风险等级	风险	操作
192.168.1.249	21	ftp	TCP	内网区	0.0.0.0-255.255.255.255	高	弱密码风险1个 未防护漏洞	端口开放危险
192.168.1.249	445	netbios	TCP	内网区	0.0.0.0-255.255.255.255	高	弱密码风险1个 未防护漏洞	端口开放危险
192.168.1.249	139	netbios	TCP	内网区	0.0.0.0-255.255.255.255	高	弱密码风险1个 未防护漏洞	端口开放危险
192.168.1.249	80	http	TCP	外网区,...	0.0.0.0-255.255.255.255	中	未防护漏洞 Web应用风险	端口开放危险
192.168.1.249	3389	rdp	TCP	内网区	0.0.0.0-255.255.255.255	低	端口开放危险	

点击相应扫描结果的操作  按钮，将会弹出端口屏蔽策略界面：



端口屏蔽策略

屏蔽的来源范围

来源区域： 内网区

来源IP： 0.0.0.0-255.255.255.255

屏蔽的目标服务

目标服务器： 192.168.1.249

服务： TCP/445

动作： 拒绝

日志： 记录

提交 取消

点击提交，会进行端口屏蔽，自动生成一条拒绝访问的应用控制策略。

勾选相应的扫描结果，点击**防护风险**，弹出的界面如下图所示：



勾选需要防护的风险类型，点击**提交**，将会根据风险提示自动生成漏洞攻击防护规则和 WEB 应用防护规则。

点击**导出 PDF**，将生成 PDF 格式的主动扫描分析报表。

点击**查看已添加策略**，将显示通过“防护风险”生成的防护规则。



		策略类型:		所有	
	策略名称	策略类型	目标服务器IP	添加时间	状态
<input type="checkbox"/>	scansIPS20120131...	IPS防护策略	249服务器	2012-01-31 11:29:14	✓
<input type="checkbox"/>	scansWAF20120131...	WEB应用防护策略	249服务器	2012-01-31 11:29:14	✓
<input type="checkbox"/>	scansApp20120131...	端口屏蔽策略	249服务器	2012-01-31 11:22:14	✓

此时，可以通过点击策略名称查看防护规则的配置。

### 3.1.2.2. WEB 扫描

Web 应用安全扫描仪可进行自动化的 Web 应用安全漏洞评估工作，能够快速扫描和检测所有常见的 Web 应用安全漏洞，例如 SQL 注入、跨网站脚本攻击等。

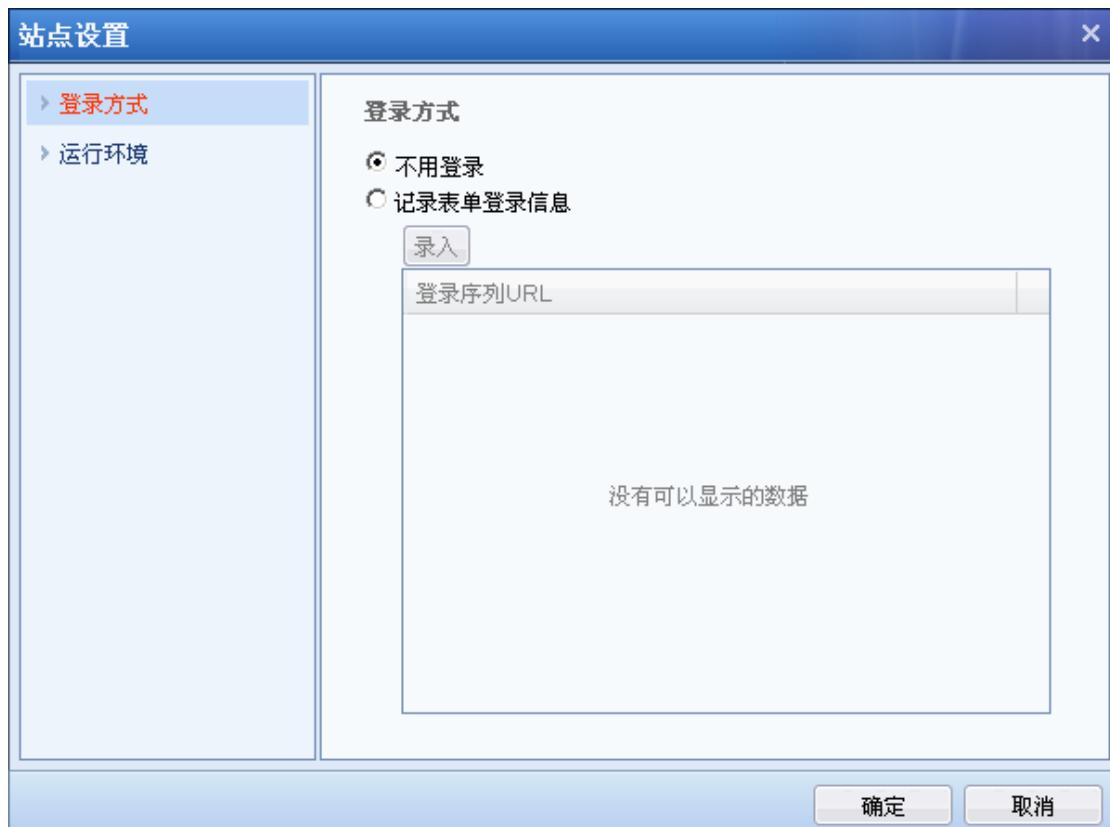
点击**WEB扫描**，配置页面如下：



The screenshot shows the 'WEB扫描' (WEB Scan) interface. At the top, there's a search bar for URLs and a dropdown for scan modes (set to '快速' - Fast). Below that is a toolbar with '开始扫描' (Start Scan), '定时扫描' (Scheduled Scan), and '查看扫描历史' (View Scan History). A '导出HTML报表' (Export to HTML Report) button is also present. The main area displays a '网站目录结构' (Website Directory Structure) on the left and a '漏洞' (Vulnerabilities) list on the right, which is currently empty.

[从以下 URL 开始扫描]: 定义需要扫描的目标网站地址，支持输入域名和 IP 地址等多种形式的 URL。

点击右边的 ，可以进行网站设置：



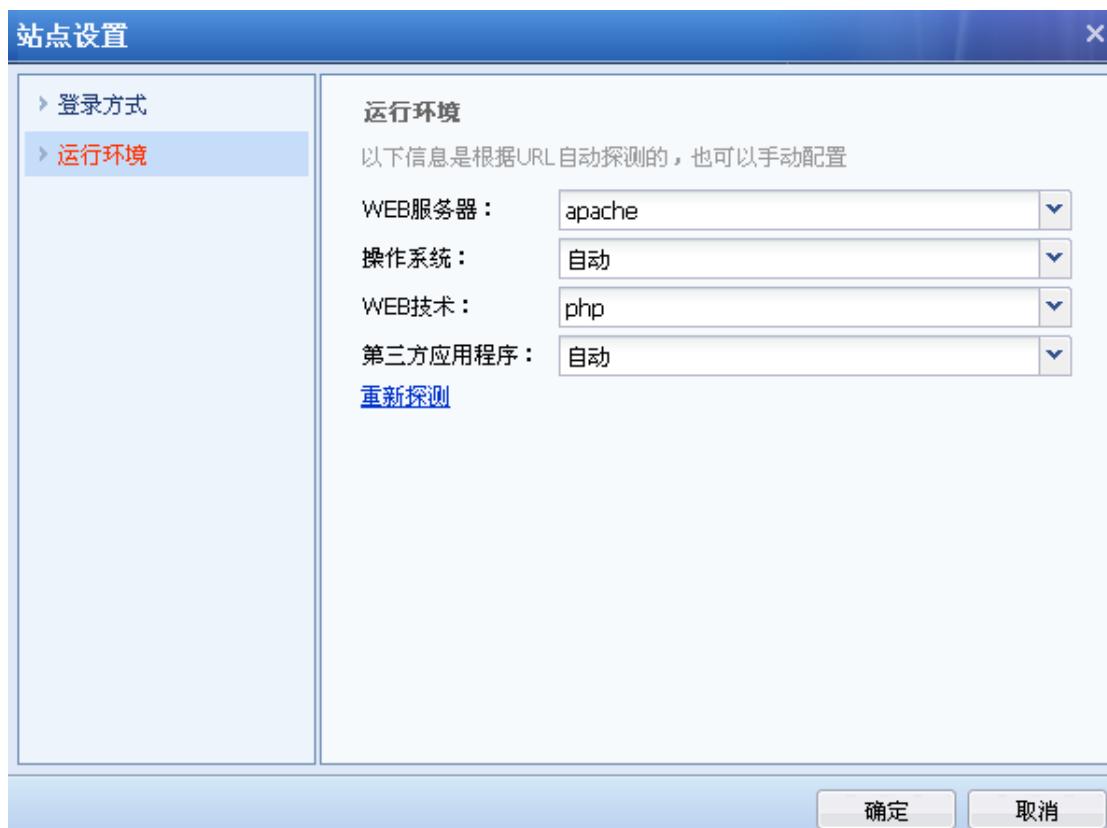
The screenshot shows the '站点设置' (Site Settings) dialog box. On the left, a sidebar lists '登录方式' (Login Method) and '运行环境' (Runtime Environment). The main panel is titled '登录方式' (Login Method) and contains two radio buttons: '不用登录' (No Login, selected) and '记录表单登录信息' (Record Form Login Information). Below these is a '录入' (Enter) button and a '登录序列URL' (Login Sequence URL) input field, which is empty. At the bottom, there are '确定' (Confirm) and '取消' (Cancel) buttons.

[不用登录]: 默认扫描过程中不需要登录网站。

[记录表单登录信息]: 扫描仪可以通过登入表单信息来记录用户的登录过程，这样扫描仪在遇到登录时，会根据用户录入的信息自行登录，进行更深入扫

描。

点击[运行环境]时，扫描仪首先根据起始 URL 自动探测目标环境，用户也可以手动进行配置：



[WEB 服务器]: 选择目标网站的服务器类型

[操作系统]: 选择目标网站上所运行的操作系统，例如 unix(linux)

[WEB 技术]: 选择目标网站所使用的 WEB 技术，例如 php, ASP 等。

[第三方应用程序]: 如果使用了第三方的应用程序，可选择相应的选项，例如 discuz 等

[扫描模板]中定义了扫描目标网站所使用的参数集合，点击  进行模板编辑：

编辑模板

X

› 基本信息	模板名称： <input type="text" value="快速"/>
› 扫描选项	描述： <input type="text" value="常规扫描，速度较快"/>
› 自定义404	
› 爬虫选项	
› 测试策略	

[模板名称]: 定义扫描模板的名称。

[描述]: 定义扫描模板的描述。

编辑模板

> 基本信息	<b>限制</b>	
> 扫描选项	请求超时时间(秒) :	3
> 自定义404	最大重试次数(次) :	1
> 爬虫选项	最大线程数(个) :	5
> 测试策略	最长扫描时间(分钟) :	120
	扫描最大文件(byte) :	400000
	<input type="checkbox"/> <b>加强扫描</b> <small>(i)</small>	
	<input checked="" type="radio"/> 一般加强	
	<input type="radio"/> 全部加强	
<b>代理</b>		
<input checked="" type="radio"/> 不使用代理		
<input type="radio"/> 指定代理		
连接地址 :		
端口 :		

**提交** **取消**

[超时时间(秒)]：设置扫描器扫描过程中等待服务器应答的超时时间。

[最大重试次数(次)]：当扫描器等待服务器应答超时时，最多重试的次数。

[最大线程数(个)]：扫描器同时处理的最大请求数目。该数值的大小主要依赖设备性能(此数值过高可能造成CPU占用较高)和服务器的性能(此数值过高可能造成服务器阻塞)。若不确定设备和服务器性能，请使用默认大小。

[最长扫描时间(分钟)]：该数值用于限制爬虫在爬取网页过程中的最大时长，超时则停止爬取，进入漏洞探测阶段。

[扫描最大文件(byte)]：扫描器爬取网页的过程中，大于该数值的网页将被忽略。

[加强扫描]：扫描程序对某些漏洞的发现采取一些绕过手段，主要为了绕过waf的防护。选择的绕过手段越强，将尝试更多的绕过，扫描时间也会相应增加。

没有任何防护措施时不建议打开。

[一般加强]：选用部分绕过手段。

[全部加强]：打开全部绕过手段。

[代理]：设置访问应用程序的代理服务器地址和端口。

[不使用代理]：不使用代理时，选中此项。

勾选[指定代理]，表明使用代理

[连接地址]：代理服务器的IP地址或域名

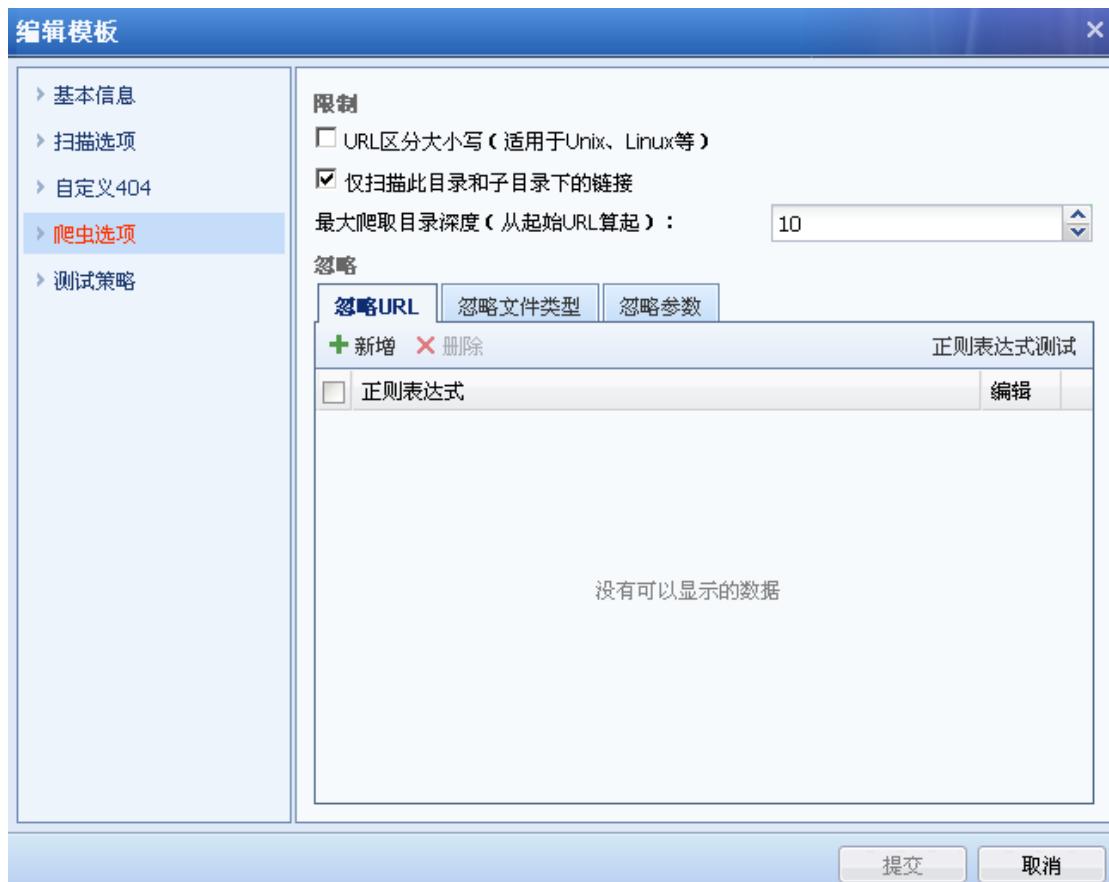
[端口]：代理服务器的端口



The screenshot shows the 'Edit Template' dialog box with the 'Custom 404' tab selected. On the left, there is a sidebar with navigation links: '基本信息', '扫描选项', '自定义404' (which is highlighted in red), '爬虫选项', and '测试策略'. The main content area has a title '自定义404' and a subtitle explaining its purpose: '符合下面正则表达式的将被识别为自定义的404页面，识别自定义的404页面可提高扫描的准确性，改善扫描结果。'. Below this is a table with columns for '正则表达式' (Regular Expression) and '编辑' (Edit). A button '正则表达式测试' (Regular Expression Test) is also present. At the bottom right of the dialog are '提交' (Submit) and '取消' (Cancel) buttons.

[自定义 404]：自定义 404 页面，扫描器爬取过程中，如果返回的页面匹配

到列表中正则表达式的将被直接认为是 404 页面。当向服务器请求不存在的页面时，如果返回的不是 404，最好在此添加。



勾选[区分大小写]，在爬取网页时，将区分 URL 的大小写。

勾选[仅扫描此目录和子目录下的链接]，在爬取网页时，将只扫描 URL 路径下的目录和子目录，不会扫描本域名外的第三方链接和同域名下的其它目录。

设置[最大爬取目录深度]，扫描器在爬取网页时将限制爬取的 URL 目录深度，从设置的 URL 算起，超过此深度值的 URL 将被忽略。

[忽略 URL]: 点击[新增]，可输入排除 URL 的正则表达式。扫描器爬取过程中，匹配上[忽略 URL]列表的 URL 将被扫描器忽略

[忽略文件类型]: 点击[新增]，可输入文件类型和扩展名(多个扩展名用分号隔开)。扫描器在爬取过程中，匹配上[忽略文件类型]列表的 URL 文件将被扫描

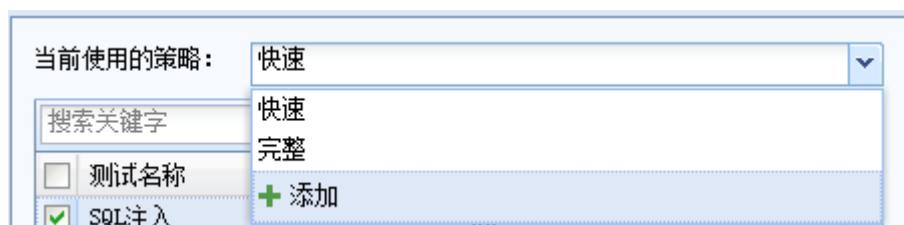
器忽略。

[忽略参数]: 扫描器在爬取过程中，匹配上[忽略参数]列表参数的 URL 将被扫描器忽略。



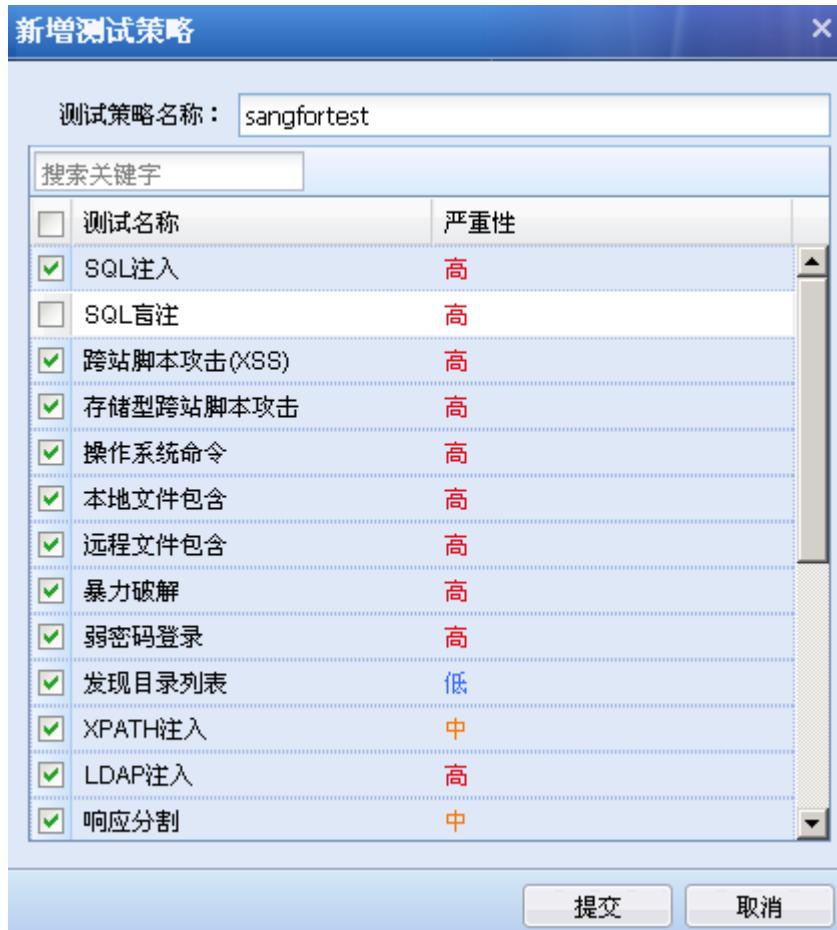
[测试策略]: 选择要测试的扫描项，扫描项分为完整和快速两种，扫描项越多耗时越长。

点击下图的[添加]，打开新增测试策略界面：

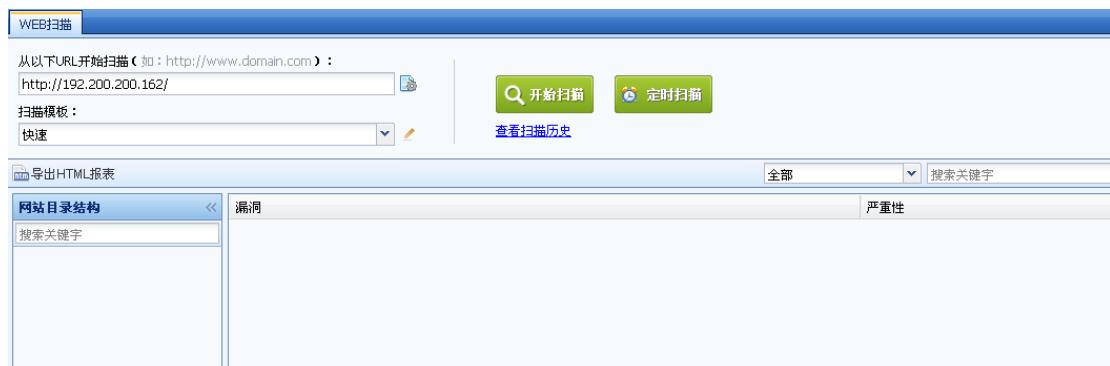


[测试策略名称]: 定义新增的测试策略名称。输入测试策略名称，并完成测

试插件勾选后，点击 **提交** 按钮，即可完成测试策略的新增。



配置好扫描模板、URL 以及网站模板后即可点击 **开始扫描** 按钮进行 web 漏洞的扫描，如下图：



扫描完毕后会显示一些统计信息，如下图：



The screenshot shows the results of a completed web scan. At the top, it says "完成100%" (Completed 100%). It indicates the scan took 59 seconds and found 154 pages and 0 test points. The start time was 2013-11-15 17:36:23 and the end time was 17:37:22. A green button labeled "返回设置" (Return to Settings) is visible.

The main area displays a table of vulnerabilities:

漏洞	严重性
phpinfo信息泄露 (1) 192.200.200.162/phpinfo.php	低
不安全的PHP配置 (1)	低

Below the table, there are tabs for "测试过程" (Test Process), "漏洞描述" (Vulnerability Description), and "建议方案" (Solution). The "测试结果" section shows the URL 192.200.200.162/phpinfo.php, the target object (empty), and the result (discovered phpinfo(): http://192.200.200.162/phpinfo.php. PHP version is: "5.2.6". System information is: "Windows NT CMS-WIKI 5.2 build 3790"). The HTML source code is displayed in a code editor-like box, with the vulnerable line highlighted.

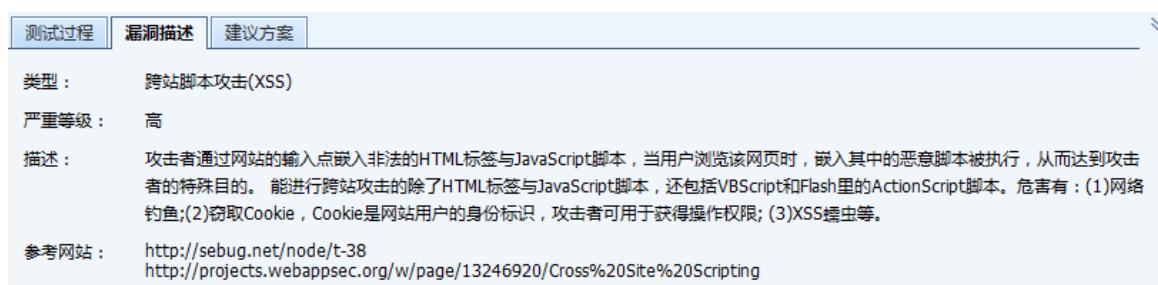
[页面 URL]: 表明扫描器从该[页面 URL]探测出漏洞。

[测试对象]: 表明扫描器从[页面 URL]中探测漏洞的位置，例如参数:  
username。



注意:若测试对象为无，则表示扫描器是基于整个页面甚至整个HTTP应答包的探测。

[测试结果]: 表明扫描器探测漏洞的过程和凭据。[测试结果]文字描述部分是扫描器漏洞探测的方法过程，文本框是漏洞探测的 html 页面源码，文本框高亮部分是触发扫描器认为存在漏洞的地方。



This screenshot shows the "漏洞描述" (Vulnerability Description) tab of a vulnerability detail page. The details are as follows:

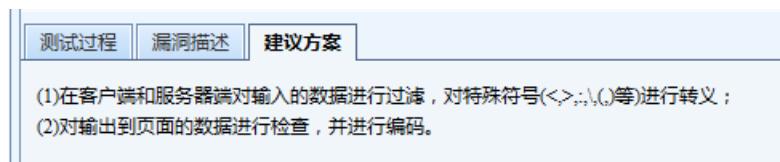
类型：	跨站脚本攻击(XSS)
严重等级：	高
描述：	攻击者通过网站的输入点嵌入非法的HTML标签与JavaScript脚本，当用户浏览该网页时，嵌入其中的恶意脚本被执行，从而达到攻击者的特殊目的。能进行跨站攻击的除了HTML标签与JavaScript脚本，还包括VBScript和Flash里的ActionScript脚本。危害有：(1)网络钓鱼；(2)窃取Cookie，Cookie是网站用户的标识，攻击者可用于获得操作权限；(3)XSS蠕虫等。
参考网站：	<a href="http://sebug.net/node/t-38">http://sebug.net/node/t-38</a> <a href="http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting">http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting</a>

[类型]: 表示漏洞的类型名称。

[严重等级]: 表示漏洞的严重等级。有“高”，“中”，“低”三种级别。

[描述]: 对该漏洞的简述

[参考网站]: 用户可以参考[参考网站]，以获得对该漏洞的进一步了解和其它帮助。



[建议方案]: 是深信服科技安全工程师针对该漏洞给出的改进建议。用户可以结合网站的实际情况进行漏洞修复，目的是要避免该漏洞对网站可能造成的影响。

点击[导出 HTML 报表](#)，用户可以通过导出的文件查看 WEB 安全报表。

### 3.1.2.3. 威胁情报与处置

『威胁情报与处置』页面用于实时推送一些热点安全事件，并可以通过此页面对这种热点安全事件进行扫描和防护。

序号	爆发日期	威胁情报描述	紧急程度	我的防护状况	操作
1	2016-05-03	ImageMagick严重漏洞	非常紧急	未防护	 立即防护
2	2016-04-21	Struts2跨站脚本漏洞	非常紧急	未防护	 立即防护
3	2016-03-25	智推Lucky病毒的勒索行为	非常紧急	未防护	 立即防护
4	2016-03-15	Apache Struts2 再曝高危漏洞	非常紧急	已防护	 查看结果
5	2015-07-29	流行DNS服务暴软件BIND曝严重DoS漏洞	非常紧急	已防护	 查看结果
6	2015-07-21	PHP CMS曝高危0day安全漏洞	非常紧急	已防护	 查看结果
7	2015-06-23	多个OA系统曝出高危漏洞	非常紧急	已防护	 查看结果
8	2015-05-14	PHP爆出远程DoS漏洞	非常紧急	已防护	 查看结果
9	2015-04-14	微软IIS曝出高危漏洞	非常紧急	已防护	 查看结果
10	2014-09-24	Bash被壳漏洞	非常紧急	未防护	 立即防护
11	2014-04-08	OpenSSL心脏滴血漏洞	非常紧急	已防护	 查看结果

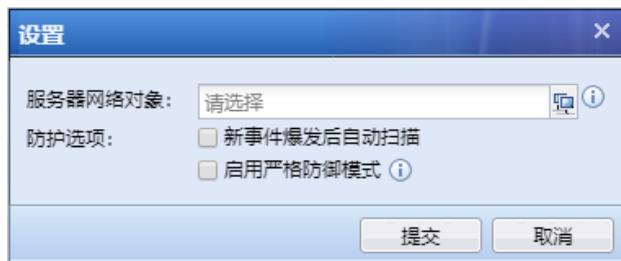
页面显示最近爆发的热点安全事件，并显示紧急程度、我的防护状况、当时操作等信息。

点击[设置](#)，弹出如下页面：

选择需要防护的网络对象，在热点安全事件发生后可以检测防护的网络对

象，是否存在相同的安全隐患。

[防护选项]勾选【新事件爆发后自动扫描】后可以在新事件发生后自动对防护的 IP 组进行扫描。



勾选【启用严格防御模式】则弱规则动作也会为拒绝。

点击获取最新情报，用于连接 SANGFOR 服务器，获取最新的热点安全事件，此功能正常使用需要保证 AF 可以连通公网。

对于未防护的安全事件，点击立即防护，出现如下页面：

这里显示了漏洞的爆发时间及渗透方式。

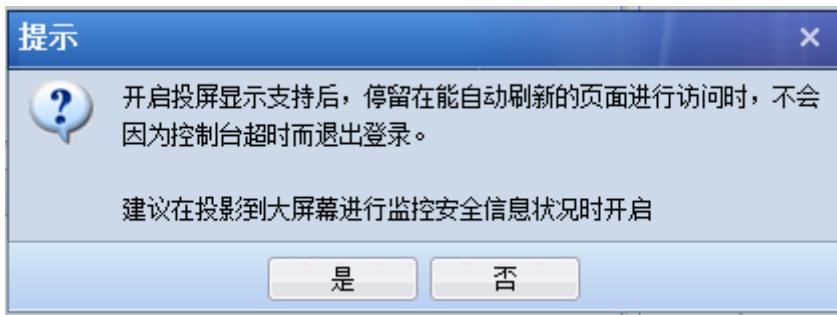
点击立即防护，弹出页面显示 AF 将自动添加的策略以及自动启用的规则，确认后点击提交，有些漏洞防护会提示需要更新到最新的规则库。



对于已经防护的安全事件，也可以点击[查看结果](#)，查看此安全事件的详细信息。

### 3.1.2.4. 开启投屏显示

点击[开启投屏显示](#)，停留在自动刷新的页面时，不会因为控制台超时而退出，建议投影到大屏幕监控安全信息状态时开启。如下图所示：



点[是](#)，保存和生效配置。

## 3.2. 运行状态

『运行状态』主要用于查看设备的基本状态信息，包括『总览』、『安全运

『运营中心』、『业务安全』、『用户安全』、『流量会话』、『DHCP运行状态』、『在线用户管理』、『封锁攻击者IP』。



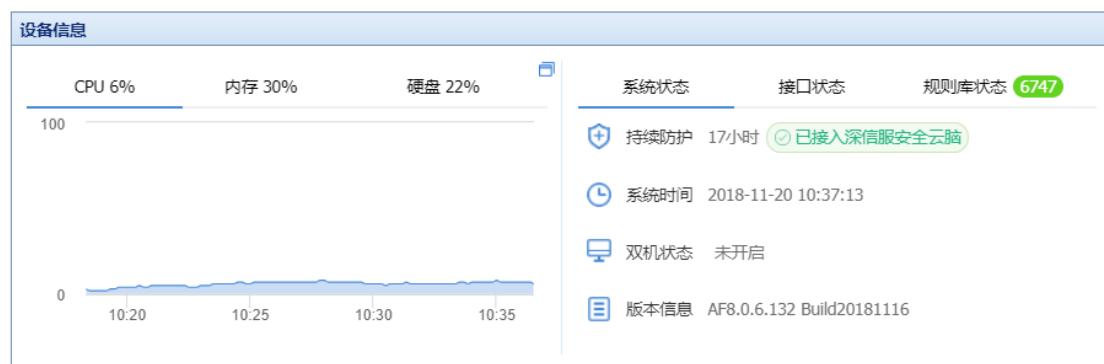
### 3.2.1. 总览

『系统状态』主要用于查看设备的安全运营中心、业务安全、用户安全、网络活动状态、设备信息等信息。

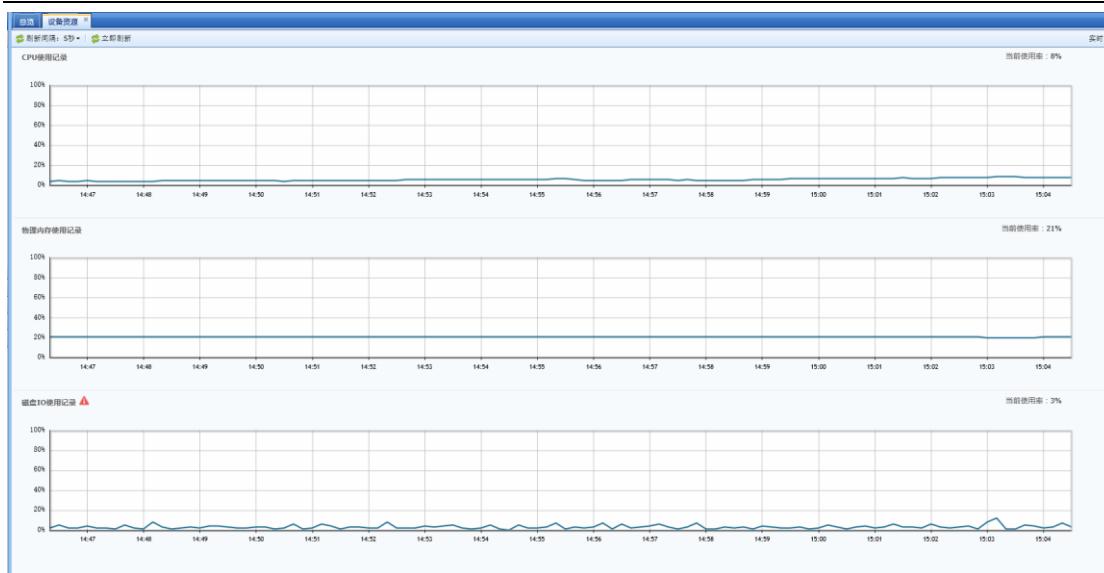
#### 3.2.1.1. 设备信息

##### 3.2.1.1.1 设备资源

【设备资源】主要用于显示设备的 CPU 使用率，内存使用率，磁盘使用率，系统状态，接口状态，规则库状态。如下图所示：



点击 查看详情，跳转到设备资源详情页面。可显示实时、最近 24 小时和最近七天的 CPU、内存和磁盘 I/O 的使用记录。如下图所示：



### 3.2.1.1.2 接口状态

【接口状态】主要用于显示设备各个网口的状态，是否接线，点击右上角的窗口最大化时，连接到接口区域中，页面如下：



接口/区域													
物理接口	子接口	VLAN接口	聚合接口	GRE隧道	区域	连接类型	IP地址	工作模式	MTU	链路状态	状态	操作	
aggr.1													
eth5		否	允许	路由	未选择区域	静态IP	---	全双工 1000Mb/s	1500	未检测			
eth6		否	允许	路由	未选择区域	静态IP	---	全双工 1000Mb/s	1500	未检测			
eth0		否	允许	路由	LAN	静态IPv4/静态IPv6	200.200.5.23/24,10.251.25.---	全双工 1000Mb/s	1500	未检测			
eth1		是	拒绝	路由	LAN	静态IPv4/静态IPv6	63.63.63.1/255.255.255.0	全双工 1000Mb/s	1500	未检测			
eth2		否	拒绝	路由	LAN	静态IPv4/静态IPv6	21.21.21.21/24-HA	全双工 1000Mb/s	1500	未检测			
eth3		否	允许	路由	WAN	静态IPv4/静态IPv6	172.16.1.2/24	全双工 1000Mb/s	1500	未检测			
eth4		否	---	透明	未选择区域	Access	---	全双工 1000Mb/s	1500	未检测			
eth7		否	允许	路由	WAN	静态IPv4/静态IPv6	192.168.1.1/24	全双工 1000Mb/s	1500	未检测			

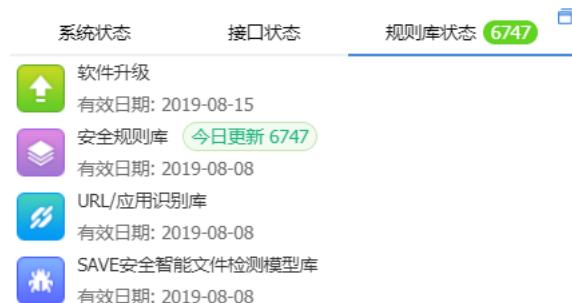
### 3.2.1.1.3 系统状态

【系统状态】主要用于显示设备的持续防护，系统时间，双机状态和版本信息。如下图所示：



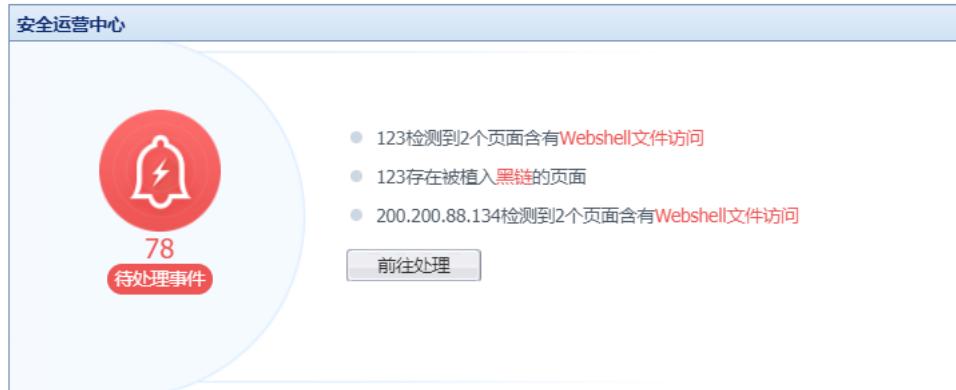
### 3.2.1.1.4 规则库状态

【规则库状态】主要用于显示设备的规则库是否开通以及是否在有效期内，同时还有当日更新的规则数量显示。如下图所示：

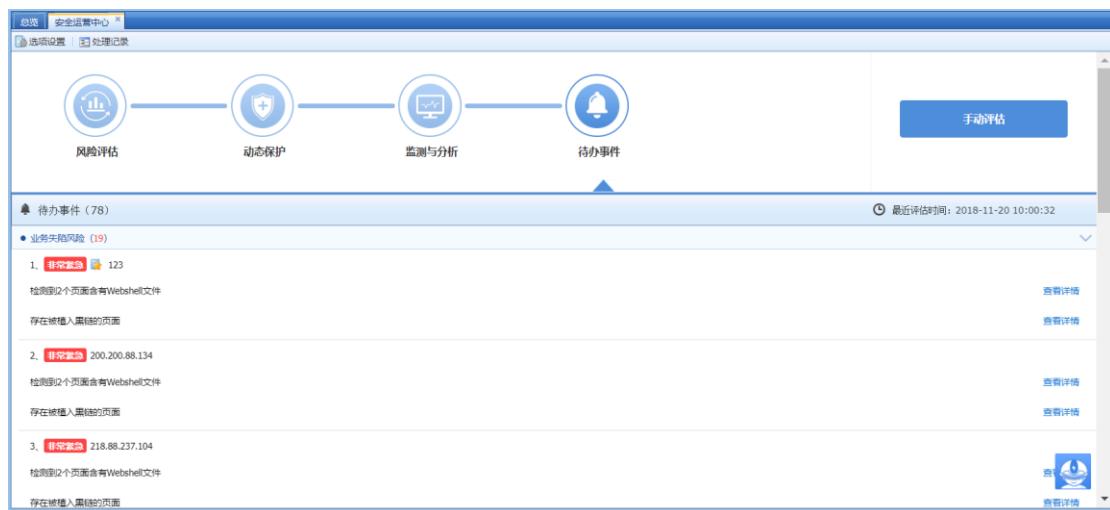


### 3.2.1.2. 安全运营中心

【安全运营中心】显示待办事件 TOP3，以及当前 AF 从风险评估、动态保护、监测与分析、待办事件这四个维度在持续评估客户的安全状况。页面如下：



点击前往处理，会跳转到待处理问题详细页面，该页面会列举网络中存在的漏洞和风险，以及建议处理方法：



### 3.2.1.3. 业务安全

【业务安全】提供迅速掌握业务整体的安全状况（业务安全状态分布、漏洞风险分布、攻击事件趋势、全网实时热点事件 TOP10）。页面如下：



### 3.2.1.4. 用户安全

【用户安全】提供迅速掌握用户整体的安全状况（包括用户安全状态分布、安全事件趋势、全网实时热点事件 TOP10）。页面如下：



### 3.2.1.5. 网络活动状态

【网络活动状态】提供用户网络的整体情况，其中【应用流量排行】中新增【标签】列，表明当前应用所属的风险类型。帮助管理员识别应用的风险类型。当前共有：安全风险、外发文件泄密风险、高带宽消耗、降低工作效率、论坛和微博发帖、发送电子邮件共 6 类风险标签。



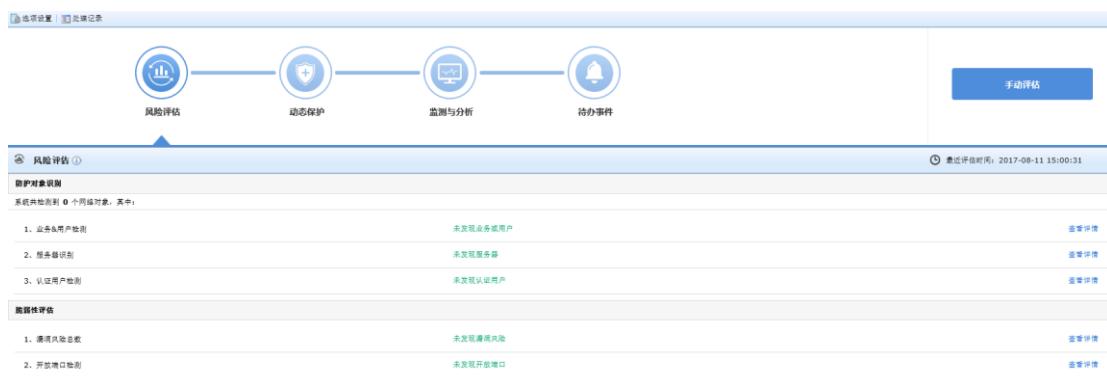
点击 ，可以将此栏置顶显示。

### 3.2.2. 安全运营中心

#### 3.2.2.1. 风险评估

『风险评估』是 AF 通过手工配置结合主动扫描感知业务和用户，使保护的服务器、终端用户等可视，方便管理；同时通过自动识别技术及时发现新增服务器，避免无法及时针对新增服务器进行防御的情况。

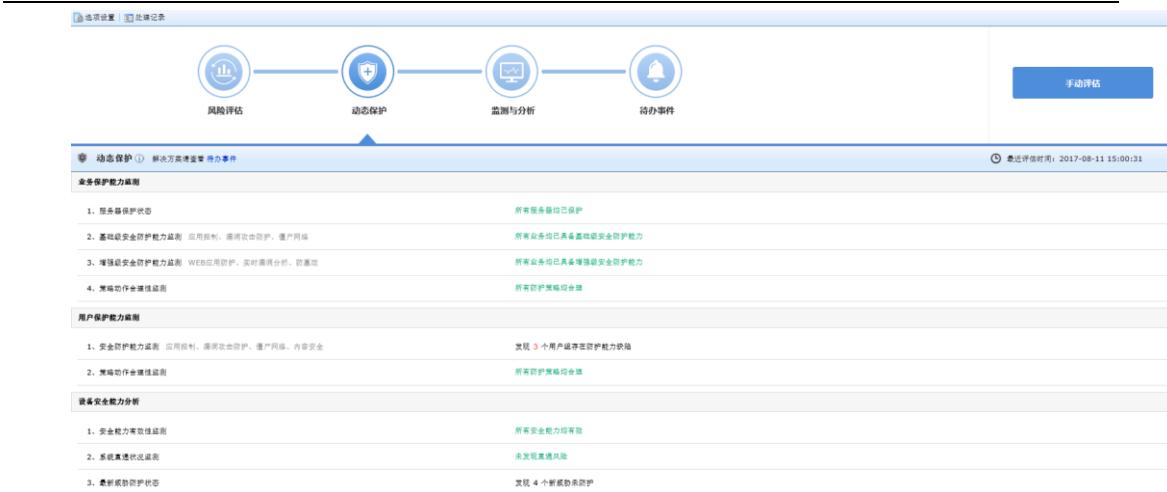
AF 提供主动与被动结合的漏洞扫描能力，发现业务系统开放的端口、存在的漏洞，并为业务系统提供安全建设的方向，从而减少业务系统漏洞被利用的概率。如下图所示：



#### 3.2.2.2. 动态保护

『动态保护』是 AF 提供基于 IP 端口的传统 ACL 管控，同时提供用户认证、应用访问控制、URL 过滤实现 L3-L7 的精细化访问管控。

AF 提供漏洞入侵防御、WEB 应用入侵防御、僵尸网络入侵防御、恶意软件入侵防御、病毒入侵防御、邮件入侵防御的能力，并结合云端安全分析，进而针对业务和用户提供全方位的攻击防御能力。如下图所示：



### 3.2.2.3. 监测与分析

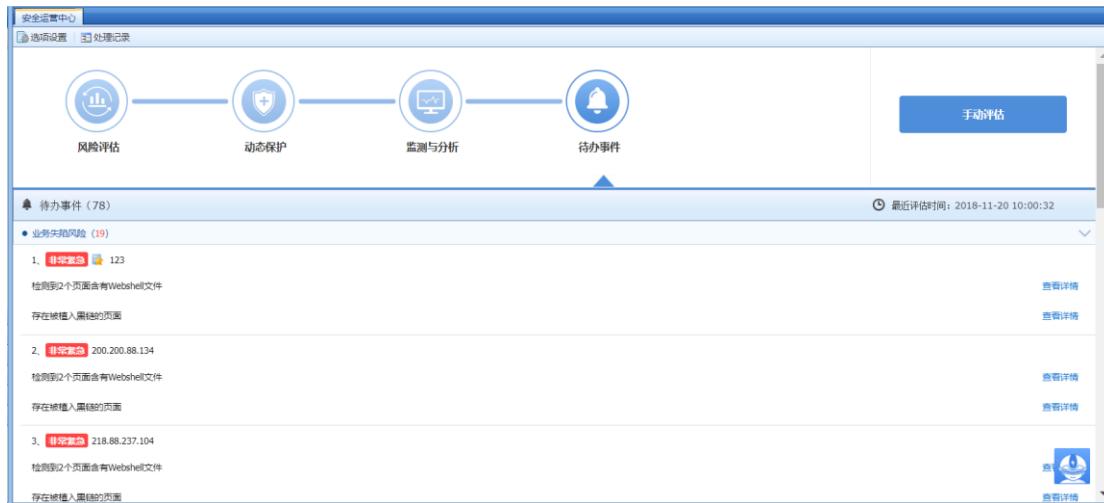
『监测与分析』是 AF 提供业务系统入侵状况、终端用户安全状况的实时监控能力，持续检视业务和用户的安全状况。

AF 提供集成的数据分析平台，综合异常访问行为、攻击事件、业务漏洞、业务和用户安全状况监控日志等进行深入分析，针对已发现的安全问题提供解决方案，持续改进业务和用户的安全。如下图所示：



### 3.2.2.4. 待办事件

『待办事件』用于查看 AF 设备检测到的网络环境中存在的风险并对风险进行处理，可设置检测的范围和检测的选项，查看处理记录，界面如下：

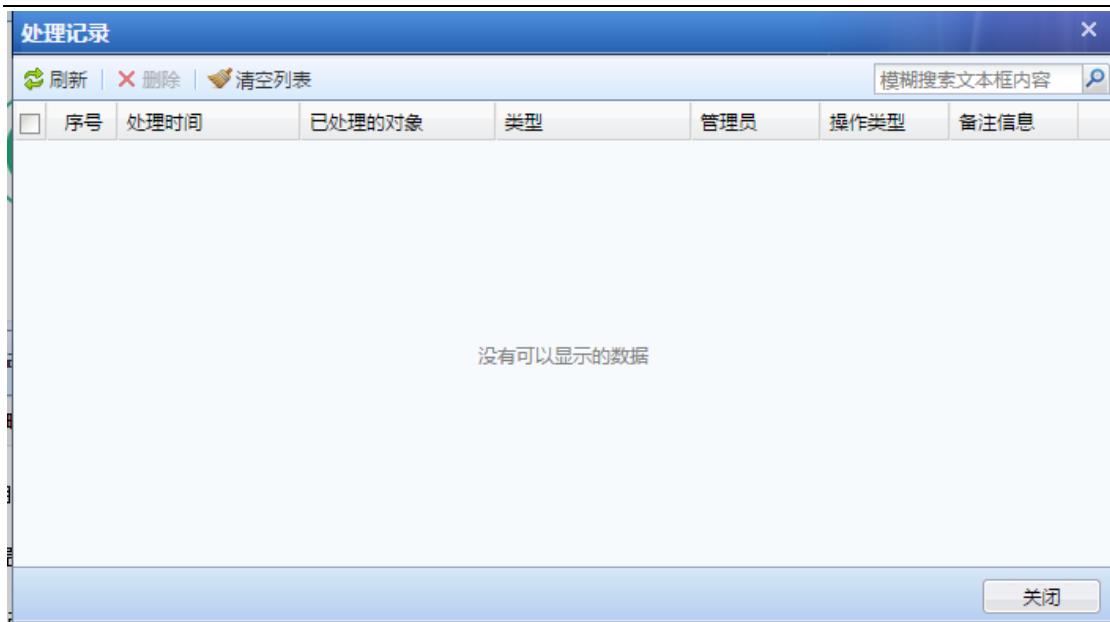


The screenshot shows the Sangfor Security Operations Center interface. At the top, there are four main functional icons: 风险评估 (Risk Assessment), 动态保护 (Dynamic Protection), 监测与分析 (Monitoring & Analysis), and 待办事件 (Pending Events). A blue button labeled '手动评估' (Manual Evaluation) is located on the right. Below these, a section titled '待办事件 (78)' lists three items under the category '业务失陷风险 (19)'. Each item includes a small icon, a number, and a brief description. To the right of each item are two '查看详情' (View Details) links.

点击**选项设置**，可设置检测范围和检测选项，如下图所示：



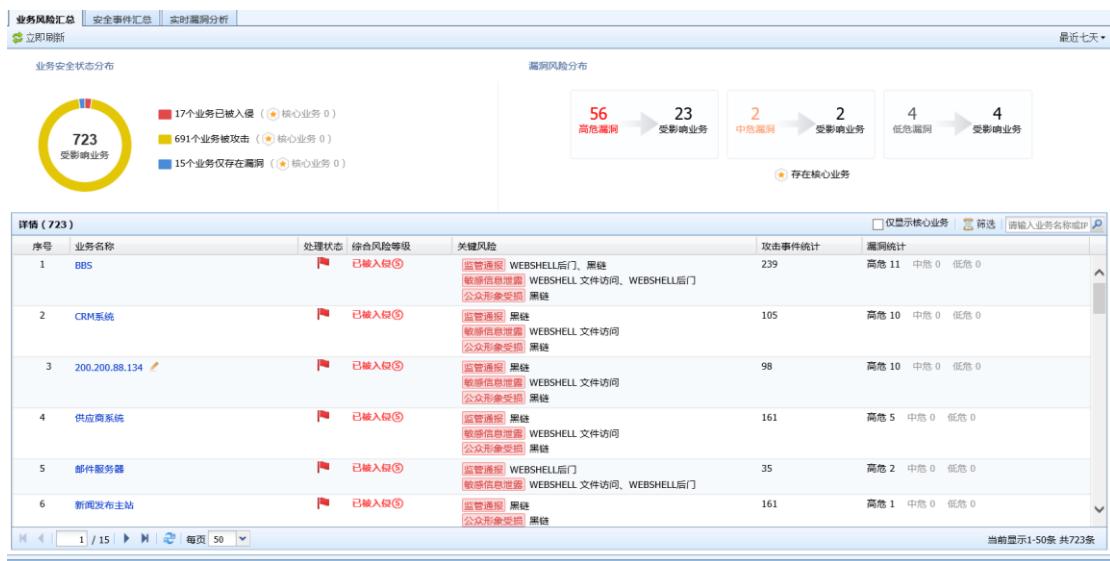
点击**处理记录**，显示管理员处理的时间，IP 等记录，可根据 IP 地址搜索处理记录，如下图所示：



### 3.2.3. 业务安全

#### 3.2.3.1. 业务风险汇总

【业务风险汇总】该页面是从业务角度进行安全展示。可以查看到业务是否存在被攻击或者看到潜在的风险。如下图所示：



关键风险类型包含：监督风险、敏感信息泄露、公众形象受损，高中低危漏洞。漏洞统计是基于实时漏洞分析的结果进行统计。

勾选仅显示核心业务，可只关注核心业务的安全状况。如下图所示：

详情 (1)		处理状态		综合风险等级		关键风险		攻击事件统计		漏洞统计	
序号	业务名称	已被入侵	已被入侵	监管通报	WEBSHELL后门	12965	高危 7	中危 2	低危 0	敏感信息泄露	WEBSHELL文件访问、WEBSHELL后门
1	核心										

勾选仅显示核心业务，可只关注核心业务的安全状况。

点击筛选，可根据综合风险等级和漏洞等级进行筛选。如下图所示：



点击业务名称即可进入安全详情，跳转后如下：

Webshell后门地址	最近检测时间	影响服务器	查看
10.0.1.78/zq_webshell/insert_mm.asp	2017-06-22 03:10:53	180.170.170.11	日志

页面上半部分是该业务的安全总览

详情项包括：

- 1、该业务当前所遭受的危害
- 2、造成该危害的具体事件类型（Webshell文件访问、Webshell后门、僵尸网络活动、内部漏洞、外部攻击…）
- 3、所处阶段：已被入侵；影响的服务器，解决建议，以及举证。

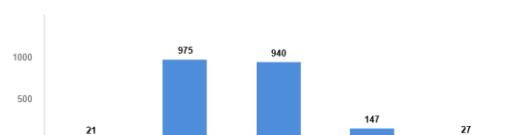
### 3.2.3.2. 安全事件汇总

【安全事件汇总】该页面是从攻击者角度进行安全展示。可看到攻击事件类型TOP5 和攻击者地图。如下图所示：

业务风险汇总 安全事件汇总 实时漏洞分析  
 立即刷新 换屏显示 最近七天

概览 攻击地图

攻击事件类型TOP5



攻击事件类型	数量
WEBSHELL...	21
SQL...	975
WEB SHELL...	940
系统命令...	147
口令暴力破解...	27

热点事件



事件名称	数量
外发攻击	1000
黑链	800
struts漏洞攻击	600
Java反序列化攻击	400
永恒之蓝	300
Locky	200

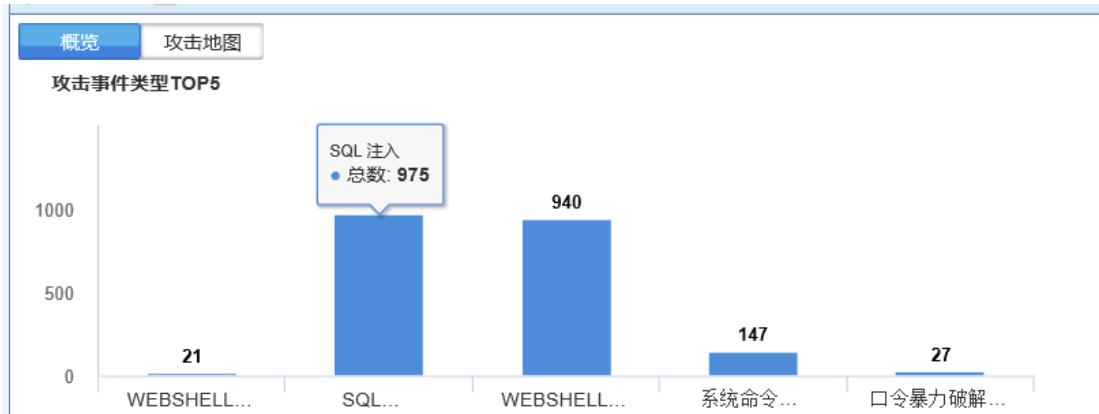
安全事件 (1318)

序号	攻击者IP	归属地	严重等级	影响业务/服务器	事件描述	攻击时间	操作
1	71.71.71.128	美国	高	192.168.254.1 192.168.254.10 192.168.254.100 ...	system漏洞攻击 (85) shellcode漏洞攻击 ( ... )	起始时间 : 2017-06-16 00:05:33 结束时间 : 2017-06-22 17:15:15	已封堵 (查看) 详情
2	202.0.187.3	澳大利亚	高	192.168.254.1 192.168.254.10 192.168.254.100 ...	system漏洞攻击 (93) shellcode漏洞攻击 ( ... )	起始时间 : 2017-06-16 00:10:12 结束时间 : 2017-06-22 17:15:17	加入封堵名单 详情
3	192.168.41.69	内部地址	高	192.168.41.67 192.168.41.68	XSS 攻击 (231) 网站扫描 (245) 系统串...	起始时间 : 2017-06-18 03:10:26 结束时间 : 2017-06-18 03:10:26	加入封堵名单 详情
4	70.70.70.78	加拿大	高	71.71.71.28 71.71.71.38	SQL 注入 (147) XSS 攻击 (14) 网站扫描...	起始时间 : 2017-06-18 03:10:26 结束时间 : 2017-06-18 03:10:26	已封堵 (查看) 详情
5	192.200.41.114	美国	高	192.168.254.1 192.168.254.10 192.168.254.100 ...	SQL 注入 (76) XSS 攻击 (69) 网页木马...	起始时间 : 2017-06-16 00:05:29 结束时间 : 2017-06-22 03:05:08	加入封堵名单 详情

当前显示1-50条 共1318条

### 3.2.3.2.1 攻击事件类型

『攻击事件类型』展示的是最近攻击事件 TOP5 的类型。如下图所示：



点击攻击事件具体类型，可在表格中过滤出该攻击事件类型相关的日志。如下图所示：



### 3.2.3.2.2 攻击者地图

『攻击者地图』用于显示 AF 设备昨天/今天/最近 7 天检测到的攻击者的 ip 来源。如下图所示：

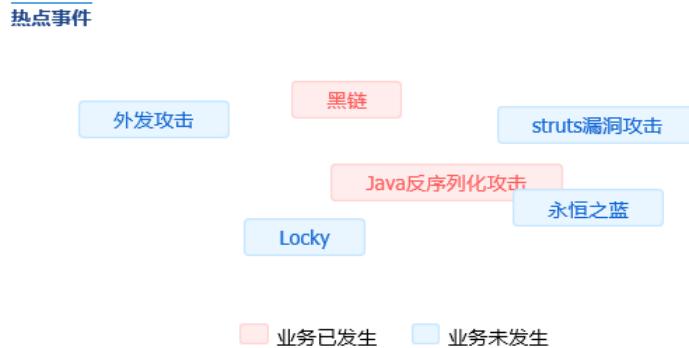


点击投屏显示，跳转到攻击者地图展示页面。如下图所示：



### 3.2.3.2.3 热点事件

『热点事件』是根据当前业务方面的热点事件进行整理，结合客户当前的攻击日志来分析，看客户业务是否有遭受热点事件的攻击。红色表示业务已发生，蓝色表示业务未发生。如下图所示：



点击击具体热点事件，可在表格中过滤出具体的日志。如下图所示：



Java反序列化攻击

序列化就是把对象转换成字节流，便于保存在内存、文件、数据库中，反序列化即是过程，由字节流还原成对象。如果Java应用对用户输入，即不可信数据做了反序列化处理，那么攻击者可以通过构造恶意输入，让反序列化产生非预期的对象，非预期的对象在产生过程中就有可能带来任意代码执行。

热点事件

外发攻击 黑链 struts漏洞攻击 Java反序列化攻击 永恒之蓝 Locky

查看详情

业务已发生 业务未发生

安全事件 (2) 热点事件: Java反序列化攻击							
序号	攻击者IP	归属地	严重等级	影响业务/服务器	事件描述	攻击时间	操作
1	202.0.187.3	澳大利亚	中	192.168.254.20 192.168.254.61 192.168.254.75	web漏洞攻击 (3)	起始时间：2017-06-17 20:40:11 结束时间：2017-06-22 09:15:13	加入封堵名单 查看详情
2	71.71.71.128	美国	中	192.168.254.69	web漏洞攻击 (1)	起始时间：2017-06-22 14:25:14 结束时间：2017-06-22 14:25:14	已封堵 (查看详情)

### 3.2.3.2.4 安全事件

『安全事件』主要用于显示最近发生的攻击事件，页面如下：



安全事件 (1311)							
序号	攻击者IP	归属地	严重等级	影响业务/服务器	事件描述	攻击时间	操作
1	71.71.71.128	美国	高	192.168.254.1 192.168.254.10 192.168.254.100 ...	system漏洞攻击 (85) shellcode漏洞攻击 ( ... )	起始时间：2017-06-16 00:05:33 结束时间：2017-06-22 15:20:15	已封堵 (查看详情)
2	202.0.187.3	澳大利亚	高	192.168.254.1 192.168.254.10 192.168.254.100 ...	system漏洞攻击 (93) shellcode漏洞攻击 ( ... )	起始时间：2017-06-16 00:10:12 结束时间：2017-06-22 15:50:19	加入封堵名单 查看详情
3	192.168.41.69	内部地址	高	192.168.41.67 192.168.41.68	XSS 攻击 (231) 网站扫描 (245) 系统命令 ...	起始时间：2017-06-18 03:10:26 结束时间：2017-06-18 03:10:26	加入封堵名单 查看详情
4	70.70.70.78	加拿大	高	71.71.71.28 71.71.71.38	SQL 注入 (147) XSS 攻击 (14) 网站扫描 ...	起始时间：2017-06-18 03:10:26 结束时间：2017-06-18 03:10:26	已封堵 (查看详情)
5	192.200.41.114	美国	高	192.168.254.1 192.168.254.10 192.168.254.100 ...	SQL 注入 (76) XSS 攻击 (69) 网页木马 ( ... )	起始时间：2017-06-16 00:05:29 结束时间：2017-06-22 03:05:08	加入封堵名单 查看详情

如图，显示的内容包括：攻击者 IP、归属地、严重等级、影响业务/服务器、攻击时间以及操作。

点击具体的攻击者 IP，可查看该攻击 IP 对客户业务的威胁情况（事件详情、攻击链展示、攻击类型 TOP10），同时提供将该 IP 加入黑名单，进行联动封锁。如下图所示：

**事件详情**

综合严重等级：高  
检测时间：2017-06-16 00:05:33至2017-06-22 16:05:11  
攻击者IP：[71.71.71.128](#)  
攻击次数：730  
影响业务数：**100**  
处理状态：该源IP已被联动封锁

**攻击链展示**

**攻击类型TOP10**

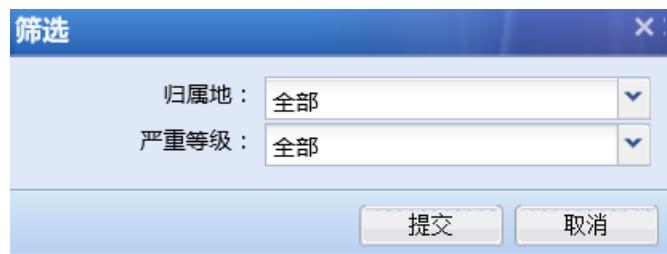
攻击类型	数量
system漏洞攻击	85
shellcode漏洞攻击	52
mail漏洞攻击	30
network_device漏洞攻击	20
口令暴力破解攻击	10
dns漏洞攻击	5
application漏洞攻击	161
tftp漏洞攻击	19
media漏洞攻击	5
web漏洞攻击	192.168.254.69

**详情 (730)**

序号	攻击时间	攻击类型	攻击描述	影响业务/服务器	所处阶段	动作	查看
1	2017-06-22 16:05:11	application漏洞攻击	PHP 4 unserialize() ZVAL引用计数器溢出(Cookie...)	192.168.254.69	尝试入侵	拒绝	日志
2	2017-06-22 15:35:14	web漏洞攻击	Sun NetDynamics会话ID劫持漏洞	192.168.254.69	尝试入侵	允许	日志
3	2017-06-22 15:20:15	tftp漏洞攻击	D-Link TFTPD传输模式远程缓冲区溢出漏洞	192.168.254.21	尝试入侵	拒绝	日志
4	2017-06-22 15:15:18	ftp漏洞攻击	FileZilla Server拒绝服务攻击漏洞	192.168.254.19	尝试入侵	允许	日志
5	2017-06-22 14:35:11	web漏洞攻击	Nginx Ngx_http_parse.c线缓冲区溢出漏洞	192.168.254.46	尝试入侵	拒绝	日志
6	2017-06-22 14:25:14	web漏洞攻击	JBoss JMXInvokerServlet 远程代码执行漏洞	192.168.254.69	尝试入侵	拒绝	日志
7	2017-06-22 14:20:17	system漏洞攻击	RPC端口映射服务BrightStor ARCServe拒绝服务U...	192.168.254.30	尝试入侵	允许	日志

勾选仅显示核心业务，可只关注核心业务的安全状况。

点击**筛选**，可根据归属地和严重等级进行筛选。如下图所示：



### 3.2.3.3. 实时漏洞分析

『实时漏洞风险』用于实时查看『策略』→『安全策略』→『安全防护策略』模块产生的信息，可以查看到网络中存在的安全漏洞风险。界面如下：

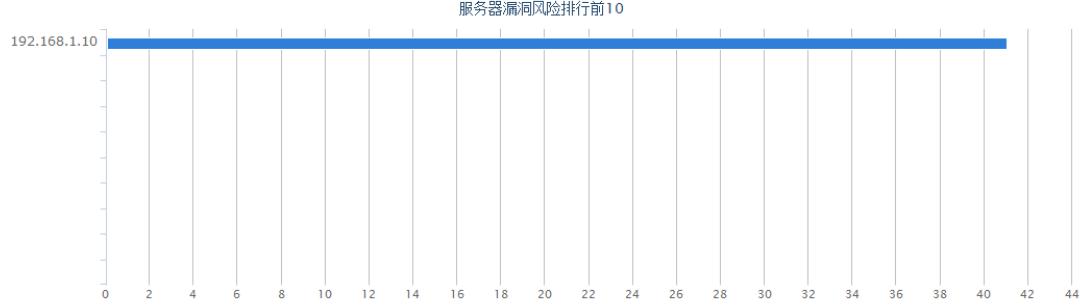
**实时漏洞风险**

### 目标服务器信息

发现存在漏洞风险的服务器总数：1  
漏洞风险总排序前10的服务器：

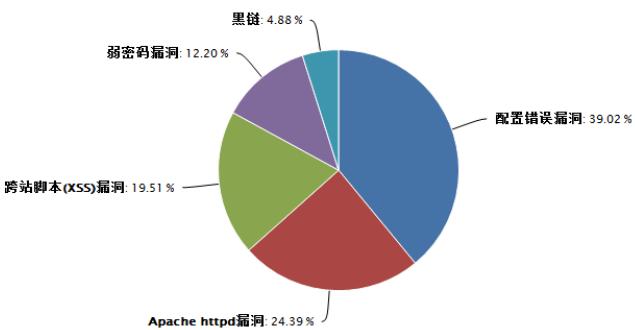
**服务器漏洞风险排行前10**



序号	服务器域名/IP	漏洞类型	风险次数	未防护风险
1	<a href="#">192.168.1.10</a>	配置错误漏洞(16) Apache httpd漏洞(10) 跨站脚本(XSS)漏洞(8) 弱密码漏洞(3) 黑链(2)	41	26

### 漏洞风险概况

发现的漏洞风险总数：41；最近7天发现的漏洞风险数：18；最近3天发现的漏洞风险数：8；今天发现的漏洞风险数：0；  
漏洞类型分布：



序号	漏洞类型	漏洞概述	存在漏洞的服务器	危险等级	防护状态
1	配置错误漏洞	配置错误漏洞是由于web服务器配置或者本身存在安全漏洞，导致一些系统文件或者配置文件直接暴露在互联网中，泄露web服务器的一些敏感信息，如用户名、密码、源代码、服务器信息、配置信息、内部ip、内部邮箱等。	192.168.1.10	高	<span style="color: red;">未防护</span>
2	Apache httpd漏洞	Apache HTTP Server是一款流行的WEB服务器。Apache支持许多特性，大部分通过编译的模块实现，像认证模块mod_access, mod_auth和mod_digest等。Apache存在多个安全漏洞，远程攻击者可以利用漏洞获得敏感信息以及其他的安全风险。	192.168.1.10	高	<span style="color: red;">未防护</span>
3	跨站脚本(XSS)漏洞	跨站脚本攻击（XSS）是由于web开发者在编写应用程序时没有对用户提交的语句和变量中进行过滤或限制，攻击者通过Web页面向数据库或HTML页面中提交恶意的html代码，当用户打开有恶意代码的连接或页面时，恶意代码会自动执行，从而达到攻击的目的。	192.168.1.10	高	<span style="color: red;">未防护</span>
4	弱密码漏洞	服务器登录密码仅包含简单数字和字母或太过简单，容易被攻击者破解。	192.168.1.10	高	<span style="color: red;">未防护</span>
5	黑链	网站被黑客植入正常访问看不到的链接，将网站内容篡改成包含如赌博、游戏、色情等非法及不良信息，存在被通报或被降权的风险。	192.168.1.10	高	<span style="color: red;">未防护</span>

### 最新公布的严重漏洞列表

序号	漏洞类型	漏洞名称	存在漏洞的服务器	公布时间	危险等级	防护状态	解决方案
没有可以显示的数据							

### 最近发现的风险详情

序号	最近一次发现时间	漏洞名称	存在漏洞的服务器	危险等级	防护状态	详细信息	最近7天	最近30天
1	2016-05-13 17:16:12	目标网站存在跨站脚本漏洞	192.168.1.10	高	<span style="color: red;">未防护</span>	<a href="#">查看</a>		
2	2016-05-13 17:16:12	目标网站存在跨站脚本漏洞	192.168.1.10	高	<span style="color: red;">未防护</span>	<a href="#">查看</a>		
3	2016-05-13 17:15:45	黑链	192.168.1.10	高	<span style="color: red;">未防护</span>	<a href="#">查看</a>		

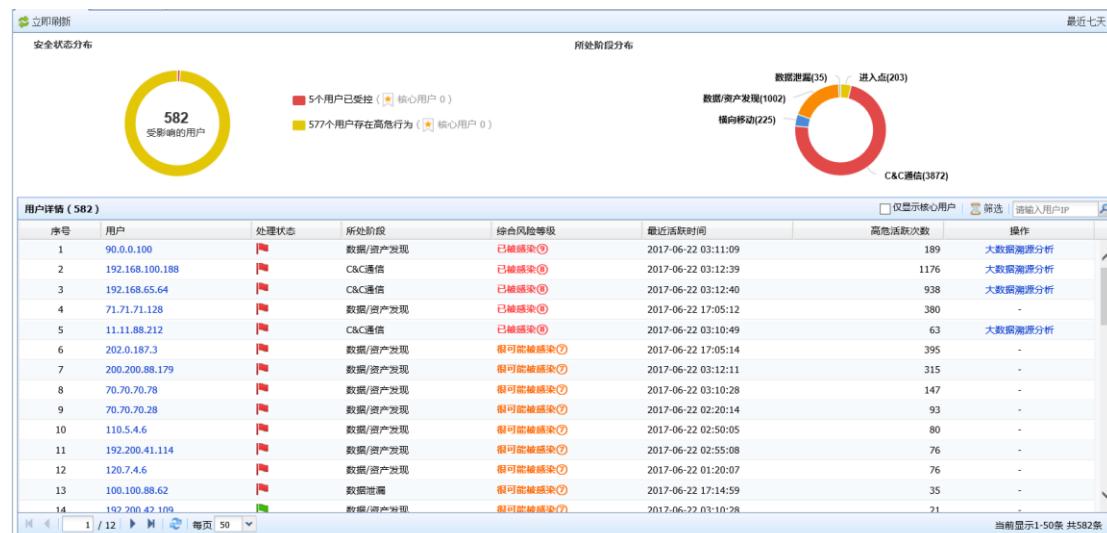
如图：显示的内容包括：目标服务器信息、漏洞风险概况、最新公布的严重漏洞列表、最近发现的风险详情。

这里只显示了漏洞风险的概要信息，如需要了解详情及解决方案，可点击[查看完整报表](#)，查看更完整的信息。

### 3.2.4. 用户安全

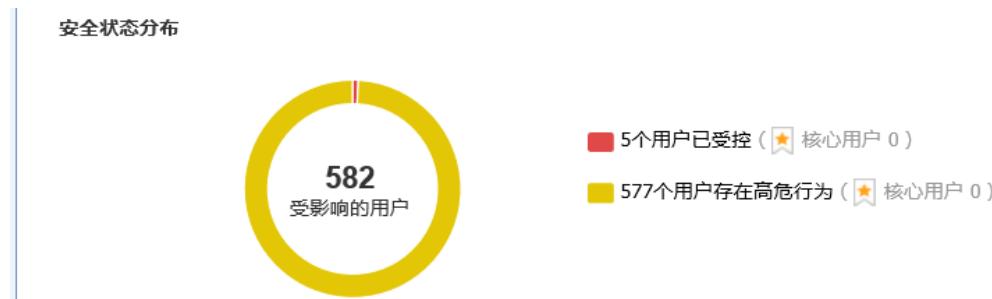
#### 3.2.4.1. 用户风险汇总

【用户风险汇总】是从用户角度进行安全展示，包括安全状态分布和所处阶段分布。如下图所示：



##### 3.2.4.1.1 安全状态分布

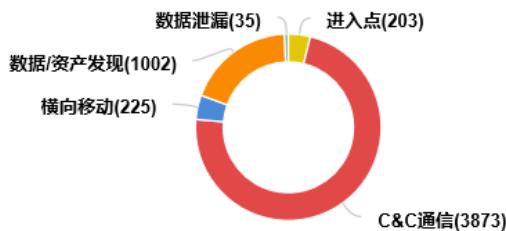
『安全状态分布』主要用于显示受影响的用户分布情况。如下图所示：



### 3.2.4.1.2 所处阶段分布

『所处阶段分布』主要用于显示所处阶段分布情况。如下图所示：

所处阶段分布



### 3.2.4.1.3 用户详情

『用户详情』主要用于显示最近用户发生的攻击事件，页面如下：

用户详情 ( 584 )							
序号	用户	处理状态	所处阶段	综合风险等级	最近活跃时间	高危活跃次数	操作
1	90.0.0.100	待处理	数据/资产发现	已感染④	2017-06-22 03:11:09	189	大数据溯源分析
2	192.168.100.188	待处理	C&C通信	已感染④	2017-06-22 03:12:39	1176	大数据溯源分析
3	192.168.65.64	待处理	C&C通信	已感染④	2017-06-22 03:12:40	938	大数据溯源分析
4	71.71.71.128	待处理	数据/资产发现	已感染④	2017-06-22 03:17:30:13	382	-
5	11.11.88.212	待处理	C&C通信	已感染④	2017-06-22 03:10:49	63	大数据溯源分析
6	202.0.187.3	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 03:17:30:15	397	-
7	200.200.88.179	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 03:12:11	315	-
8	70.70.70.78	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 03:10:28	147	-
9	70.70.70.28	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 02:20:14	93	-
10	110.5.4.6	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 02:50:05	80	-
11	120.7.4.6	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 01:20:07	76	-
12	192.200.41.114	待处理	数据/资产发现	很可能被感染⑦	2017-06-22 02:55:08	76	-
13	100.100.88.62	待处理	数据泄漏	很可能被感染⑦	2017-06-22 17:14:59	35	-
14	192.200.42.109	已解决	数据/资产发现	很可能被感染⑦	2017-06-22 03:10:28	21	-

如图，显示的内容包括：用户、处理状态、所处阶段、综合风险等级、最近活跃时间、高危活跃次数以及操作。

点击用户进行用户详情页面：可看到用户安全详情、攻击阶段图、解决方案。如下图所示：

90.0.0.100

综合风险等级：已被感染②

所处阶段：数据/资产发现

威胁情报：大数据溯源分析

解决方案

1. 请点击下载“[NGAF反僵尸网络软件](#)”，在受病毒感染的计算机上安装“反僵尸网络”软件，运行“病毒扫描”功能以彻底清除主机中的僵尸病毒。

**攻击阶段图**

```

graph LR
    1[1 进入点] --> 2[C&C通信]
    2 --> 3[3 横向移动]
    3 --> 4[4 数据/资产发现]
    4 --> 5[5 数据泄漏]
    1 --- 2
    2 --- 3
    3 --- 4
    4 --- 5
    
```

1. 进入点  
黑客通过挂马网站等方式，传播恶意软件给潜在受感染主机

2. C&C通信  
主机感染了恶意软件，并且和黑客建立了控制通道

3. 横向移动  
受感染主机扫描同网段内其它在线主机及服务，通过端口扫描等方式将恶意软件传播给它们

4. 数据/资产发现  
受感染主机扫描到内网服务器，并尝试对服务器进行暴力破解、SQL注入等攻击

5. 数据泄漏  
已有证据证明受感染主机已拿到服务器上敏感信息，并正在或即将进行数据泄密

**详情(5)**

序号	严重等级	事件类型	事件描述	所处阶段	检测时间	总检测数目	操作
1	高	僵尸网络	主机访问了concert等机构提供的C&C通信URL：droppedout.cn/upd/setup.exe 可能感染病毒：Packed.Win32.TDSS	C&C通信	最早检测时间：2017-06-16 03:10:49 最新检测时间：2017-06-22 03:10:49	49	日志
2	高	恶意软件	发现主机存在恶意软件通信特征：广告软件Bonzbuddy运行时检测	C&C通信	最早检测时间：2017-06-16 03:11:10 最新检测时间：2017-06-22 03:11:09	28	日志
3	高	异常流量	受感染主机扫描到内网服务器，并尝试对服务器进行SQL注入攻击	数据/资产发现	最早检测时间：2017-06-16 03:10:28	7	日志

勾选仅显示核心业务，可只关注核心业务的安全状况。

点击筛选，可根据所处阶段和综合风险等级进行筛选。如下图所示：

**筛选**

所处阶段：全部

综合风险等级：全部

提交 取消

### 3.2.4.2. 用户安全事件

【用户安全事件】是从攻击者角度进行用户安全展示，包括安全事件类型分布和用户热点事件。如下图所示：

用户风险汇总 | 用户安全事件

立即刷新 最近七天

安全事件类型分布

热点事件

永恒之蓝 外发攻击 网页访问  
Locky 飞奔蠕虫

用户已发生 (red) | 用户未发生 (light blue)

安全事件 (524)

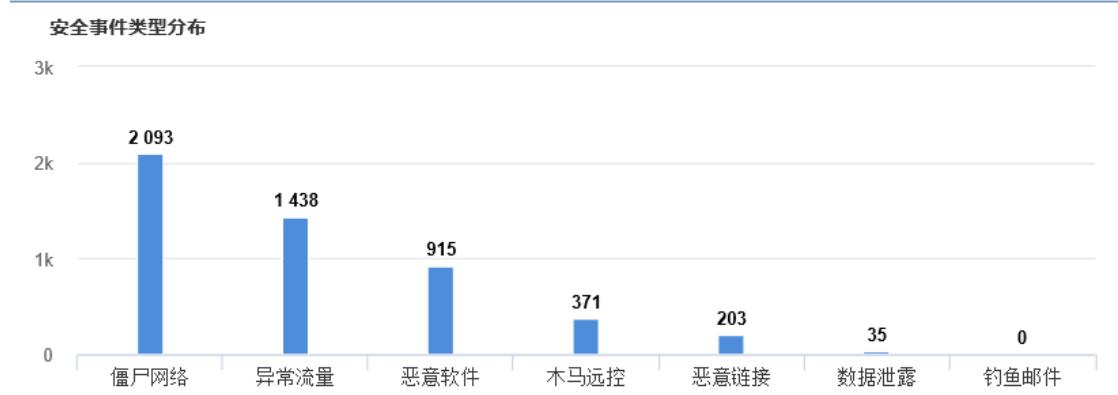
序号	访问时间	影响用户	事件类型	综合严重等级	事件描述	事件次数	操作
1	2017-06-23 17:14:59	100.100.88.62	数据泄露	致命	主机已拿到服务器上的敏感信息，并正在或即将进行数据泄密	35	日志
2	2017-06-23 03:12:39	192.168.100.188	僵尸网络	高	主机访问了oncer等机构提供的C&C通信URL	1176	日志
3	2017-06-23 03:12:40	192.168.65.64	僵尸网络	高	主机访问了oncer等机构提供的C&C通信URL： 222.186.60.89:9023/ chicostara.com/logo.gif ... 可能感染病毒： Trojan.Win32.Agentb botnet.malware	847	日志
4	2017-06-23 03:12:12	200.200.88.179	异常流量	高	受感染主机扫描到内网服务器，并尝试对服务器进行SQL注入攻击	315	日志
5	2017-06-23 08:55:10	202.0.187.3	恶意软件	高	发现主机存在恶意软件通信特征： 后门JDODT运行时检测 后门JMillennium V1.0运行时检测 后门Optix Pro V1.32运行时检测 - 上传文件 ...	294	日志

显示核心用户 | 筛选 | 请输入用户的IP地址

1 / 11 | 每页 50 | 当前显示1-50条 共524条

### 3.2.4.2.1. 安全事件类型分布

『安全事件类型分布』主要用于显示安全事件类型的分布情况。如下图所示：



点击安全事件具体攻击类型，可在表格中过滤出该攻击类型相关的日志。如下图所示：



### 3.2.4.2.2. 热点事件

『热点事件』是根据当前的热点事件进行整理，结合客户当前的攻击日志来分析，看客户内网用户是否有遭受热点事件的攻击。红色表示业务已发生，蓝色表示业务未发生。如下图所示：

#### 热点事件



点击击具体热点事件，可在表格中过滤出具体的日志。如下图所示：



### 3.2.4.2.3. 安全事件

『安全事件』主要用于显示最近发生的被攻击事件，页面如下：

安全事件 ( 525 )							<input type="checkbox"/> 仅显示核心用户	<input type="checkbox"/> 筛选	请输入用户的IP地址
序号	访问时间	影响用户	事件类型	综合严重等级	事件描述	事件次数	操作		
1	2017-06-23 17:14:59	100.100.88.62	数据泄露	致命	主机已拿到服务器上的敏感信息，并正在或即将进行数据泄密	35	日志		
2	2017-06-23 03:12:39	192.168.100.188	僵尸网络	高	主机访问了cnCERT等机构提供的C&C通信URL	1176	日志		
3	2017-06-23 03:12:40	192.168.65.64	僵尸网络	高	主机访问了cnCERT等机构提供的C&C通信URL： 222.186.60.89:9023/ chicostara.com/logo.gif ... 可能感染病毒： Trojan.Win32.Agentb botnet.malware	847	日志		
4	2017-06-23 03:12:12	200.200.88.179	异常流量	高	受感染主机扫描到内网服务器，并尝试对服务器进行SQL注入攻击	315	日志		
5	2017-06-23 09:25:12	202.0.187.3	恶意软件	高	发现主机存在恶意软件传播特征： Dirt Jumper Toolkit变形HTTP洪水攻击尝试 后门Millenium V1.0运行时检测 后门Optibx Pro V1.32运行时检测 - 上传文件 ...	295	日志		

如图，显示的内容包括：访问事件、影响用户、事件类型、综合严重等级、事件描述、事件次数以及操作。

点击具体的影响用户，可查看该用户被攻击的情况（攻击时间、攻击类型、攻击描述等），同时提供将攻击者IP加入黑名单，进行联动封锁。如下图所示：

返回安全事件汇总 立即刷新
最近七天

● 事件详情

综合严重等级： 高

检测时间： 2017-06-17 03:10:28至2017-06-23 03:10:29

攻击者IP： 100.100.1.5

攻击次数： 266

影响业务数： 1

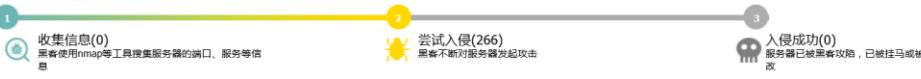
处理状态： 该源IP未被联动封禁，是否要封禁？ [加入封堵名单](#)

攻击类型TOP10



攻击类型	次数
WEB SHELL上传	266
尝试入侵	266
成功	0

● 攻击链展示



详细 ( 266 )

序号	攻击时间	攻击类型	攻击描述	影响业务/服务器	所处阶段	动作	查看
1	2017-06-23 03:10:29	WEB SHELL上传	检测到网站攻击   攻击类型 : WEB SHELL URL: 100.100.1.8/dwww/test.htm?nid=&t;?php fp;	100.100.1.8	尝试入侵	允许	<a href="#">日志</a>
2	2017-06-23 03:10:29	WEB SHELL上传	检测到网站攻击   攻击类型 : WEB SHELL URL: 100.100.1.8/dwww/test.htm?nid=&t;?php ocl	100.100.1.8	尝试入侵	允许	<a href="#">日志</a>
3	2017-06-23 03:10:29	WEB SHELL上传	检测到网站攻击   攻击类型 : WEB SHELL URL: 100.100.1.8/dwww/test.htm?nid=&t;?php ocl	100.100.1.8	尝试入侵	允许	<a href="#">日志</a>
4	2017-06-23 03:10:29	WEB SHELL上传	检测到网站攻击   攻击类型 : WEB SHELL URL: 100.100.1.8/dwww/test.htm?nid=&t;?php ms	100.100.1.8	尝试入侵	允许	<a href="#">日志</a>
5	2017-06-23 03:10:29	WEB SHELL上传	检测到网站攻击   攻击类型 : WEB SHELL URL: 100.100.1.8/dwww/test.htm?nid=&t;?php ms	100.100.1.8	尝试入侵	允许	<a href="#">日志</a>

勾选仅显示核心业务，可只关注核心业务的安全状况。

点击筛选，可根据事件类型和综合严重级别进行筛选。如下图所示：



### 3.2.5. 流量会话

#### 3.2.5.1. 用户流量排名

##### 3.2.5.1.1 查看用户流量排名

『用户流量排名』主要用于显示在线用户的使用带宽的情况，界面如下：

如图，根据用户的总流速进行排名。显示内容分别包含：用户名（显示名）、所属组、上下行流速、总流速、是否冻结上网、获取机器名和流量构成。在[冻结上网]一栏点击，用于将对应的用户冻结上网；在[获取机器名]一栏点击，用来获取对应用户计算机名；在[流量构成]一栏，点击具体应用会出现如下页面，来显示该用户具体的应用流量：

应用	线路	百分比	上传速率	下载速率	总速率
Microsoft update	线路1	95%	8.34 (KB/s)	74.97 (KB/s)	83.3 (KB/s)
其他	线路1	4%	2.17 (KB/s)	1.2 (KB/s)	3.37 (KB/s)
HTTP_POST	线路1	1%	860 (B/s)	0 (B/s)	860 (B/s)

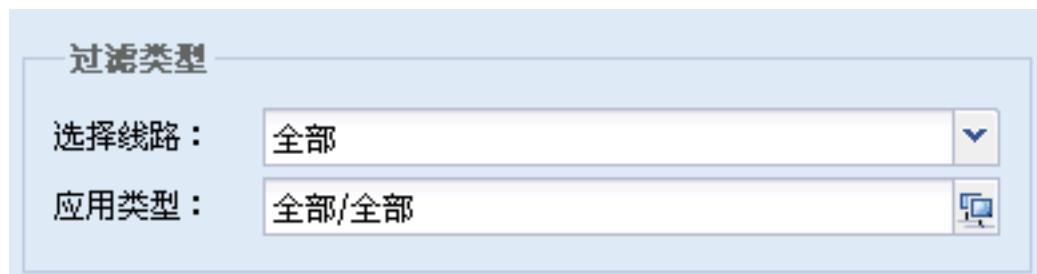
点击**刷新间隔：5秒**用于设置页面上的排行刷新时间间隔；

点击**立即刷新**可以立即进行刷新。

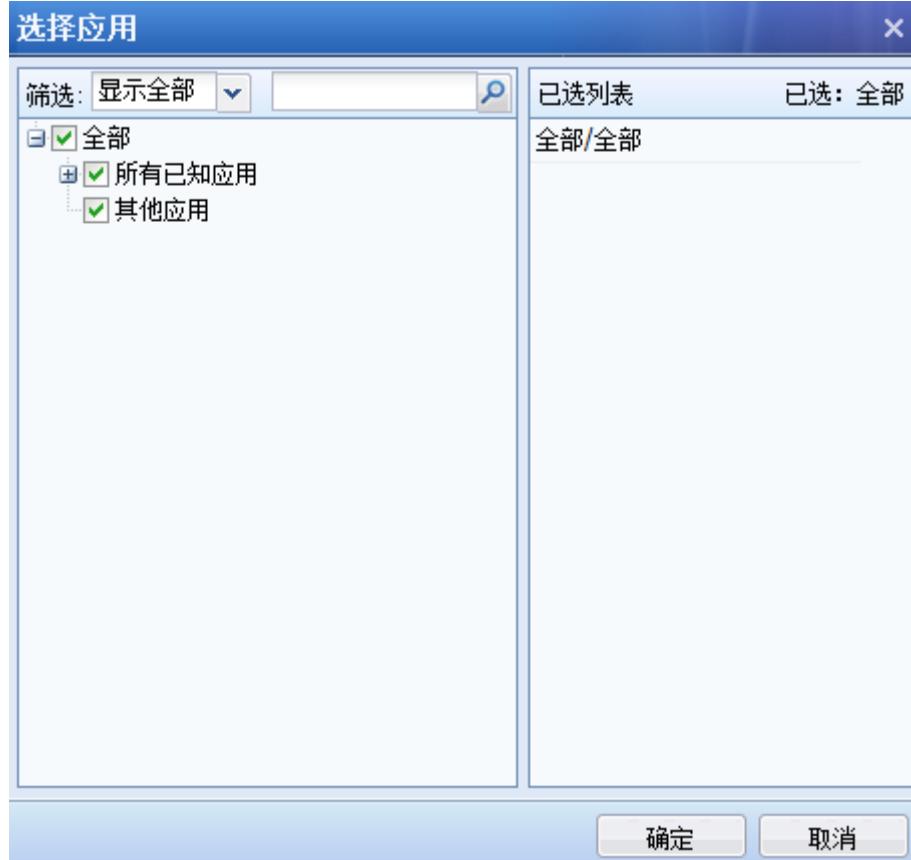
### 3.2.5.1.2 过滤用户流量排名

点击**过滤条件**，可以指定用户流量排名的过滤条件。

『过滤类型』用于设置查看的线路和应用，界面如下：



[选择线路]选择具体需要查看的线路，[应用类型]用于指定需要查看的应用服务，点击后出现如下页面：

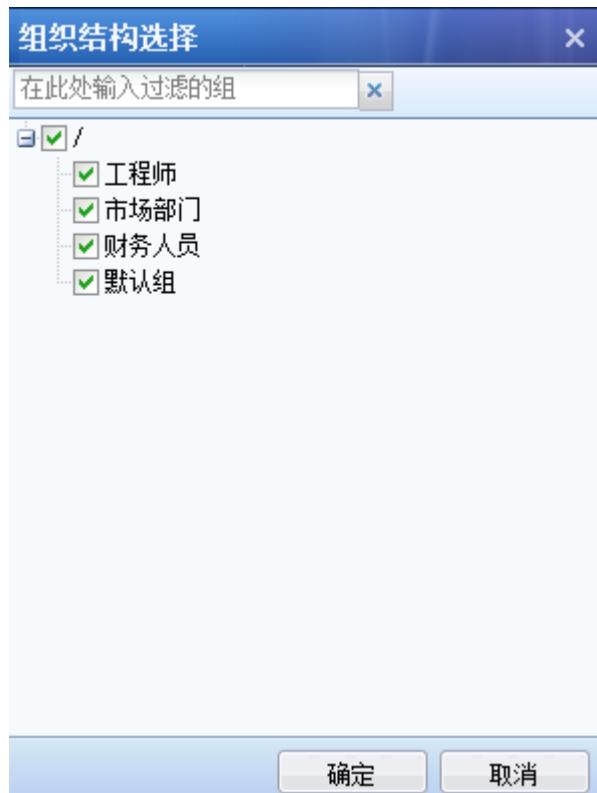


[筛选]里面有显示全部、显示选中和显示未选三种选择，下面可以勾选具体的应用，右边[已选列表]显示已经选中的应用，点**确定**即可保存。

『过滤对象』是用来设置具体的用户或者 IP，页面如下：



[组过滤]、[用户过滤]、[IP 过滤]三个条件只能选择一个，其中组过滤中“/”是表示所有组，点击**选择**会出现如下页面：



勾选需要查看的组，或者是在空行里输入相应组名，然后点击**确定**即可。

『显示选项』用于设置显示流量前多少名的用户，页面如下：



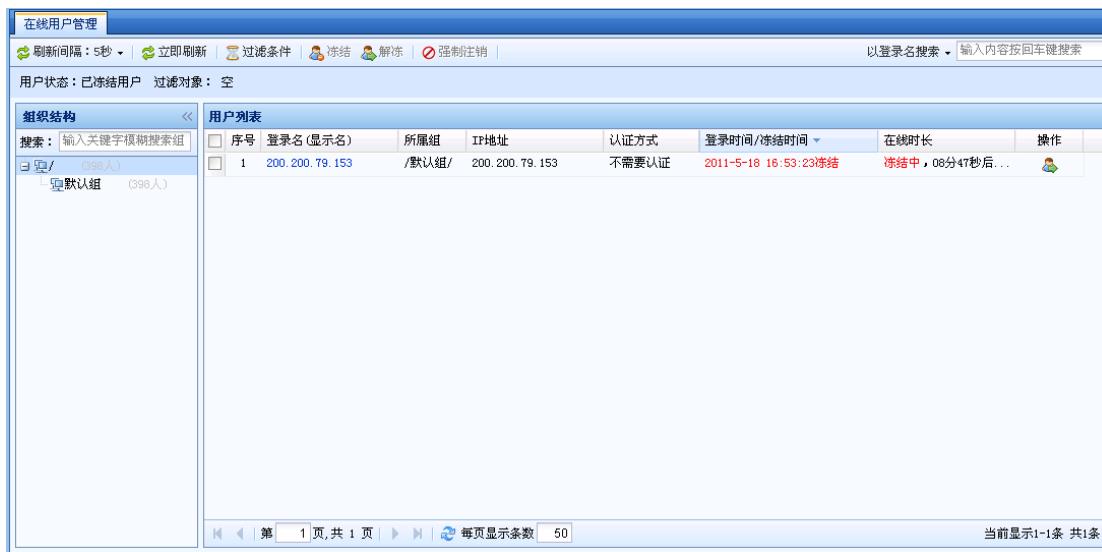
### 3.2.5.1.3 冻结用户上网

『冻结上网』用于设置立即断掉某个用户连接，使其无法上网一段时间，具体操作是选中一个『用户流量排名』里面的用户，点击**冻结**，来设置冻结上网的时间，以分钟为单位，页面如下：



### 3.2.5.1.4 解冻用户上网

如果被冻结上网的用户需要立即放开限制，解冻上网，可以点击**去用户列表解冻用户**，此时会跳转到【在线用户管理】的页面，页面如下：

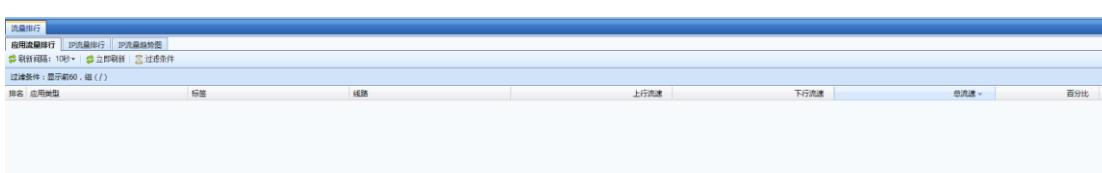


The screenshot shows the 'Online User Management' interface. On the left, there's a 'Organization Structure' tree with a single node labeled '默认组 (398人)'. The main area is titled 'User List' and displays a table with one row of data. The table columns are: 序号 (Index), 登录名 (显示名) (Login Name (Display Name)), 所属组 (Group), IP地址 (IP Address), 认证方式 (Authentication Method), 登录时间/冻结时间 (Login Time/Freeze Time), 在线时长 (Online Duration), and 操作 (Operation). The data row shows: 1, 200.200.79.153, /默认组/, 200.200.79.153, 不需要认证 (No Authentication Required), 2011-5-18 16:53:23 (Frozen), 冻结中 (Frozen), 08分47秒后... (Frozen for 8 minutes and 47 seconds). At the bottom, there are navigation buttons for page 1 of 1, a search bar, and a note indicating 1 record displayed.

在这里找到被冻结的用户，选择该用户点击解冻即可。

### 3.2.5.2. 应用流量排名

『应用流量排名』主要用于显示设备实时的应用服务的流量排名情况，界面如下：



The screenshot shows the 'Application Traffic Ranking' interface. The top navigation bar includes tabs for '应用流量排行' (Application Traffic Ranking), 'IP流量排行' (IP Traffic Ranking), and 'IP流量趋势图' (IP Traffic Trend Chart). Below the tabs, there are filter options: '刷新间隔: 10秒' (Refresh Interval: 10 seconds), '立即刷新' (Refresh Now), '过滤条件' (Filter Conditions), and '过滤条件: 显示前50, 隐 (/)'. The main table has columns: 排名 (Rank), 应用类型 (Application Type), 标签 (Label), 线路 (Line), 上行流速 (Upstream Speed), 下行流速 (Downstream Speed), 总流速 (Total Speed), and 百分比 (Percentage). The table is currently empty.

如图，根据应用占用的带宽进行排名，显示的内容包括：应用类型、标签、线路、上下行流速、总流速。

点击刷新间隔：5秒用于设置页面上的排行刷新时间间隔；

点击立即刷新可以立即进行刷新。



当前的标签有 6 种：外发文件泄密风险、高带宽消耗、降低工作效率、发送电子邮件、论坛和微博发帖。

### 3.2.5.2.2 过滤应用流量排名

点击过滤条件，可以指定应用流量排名的过滤条件，界面如下：



『过滤对象』用于设置查看的线路。

[选择线路]选择具体需要查看的线路

[显示选项]用于设置显示流量前多少名的应用。

### 3.2.5.3. IP 流量排行

#### 3.2.5.3.1 查看 IP 流量排名

『IP 流量排名』主要用于显示在线 IP 的使用带宽情况，页面如下：



The screenshot shows a network monitoring interface titled "IP流量排行" (IP Traffic Ranking). It includes tabs for "用户流量排行" (User Traffic Ranking), "应用流量排行" (Application Traffic Ranking), "IP流量排行" (IP Traffic Ranking) (which is selected), and "IP流量趋势图" (IP Traffic Trend Chart). There are also buttons for "刷新间隔: 5秒" (Refresh Interval: 5 seconds), "立即刷新" (Refresh Now), and "过滤条件" (Filter Conditions). A dropdown menu for "过滤条件" is open, showing the option "显示前60, 组 ()". Below the tabs are columns for "排名" (Ranking), "IP地址" (IP Address), "上行流速" (Upstream Speed), "下行流速" (Downstream Speed), "总流速" (Total Speed), "获取机器名" (Get Machine Name), and "流量构成" (Traffic Composition). A message at the bottom center says "没有可以显示的数据" (No data available to display).

如图，根据 IP 的总流速进行排名，显示的内容包括 IP 地址，上行流速，下行流速，总流速，获取机器名，流量构成。在[获取机器名]一栏点击**获取**，用来获取对应 IP 的计算机名；在[流量构成]一栏，点击对应的应用会出现如下页面，来显示该 IP 具体的应用流量：

应用	线路	百分比	上传速率	下载速率	总速率
网站浏览	线路1	88%	1.93 (KB/s)	2.82 (KB/s)	4.75 (KB/s)
其他	线路1	12%	426 (B/s)	246 (B/s)	672 (B/s)

点击**刷新间隔：5秒**用于设置页面上的排行刷新时间间隔；

点击**立即刷新**可以立即进行刷新。

### 3.2.5.3.2 过滤 IP 流量排名

点击**过滤条件**，可以指定 IP 流量排名的过滤条件，页面如下：

过滤条件设置 ×

过滤类型

选择线路： 全部 ▼

应用类型： 全部/全部 □

过滤对象

IP过滤(一行一个ip地址)  
可以直接在此处输入、编辑、删除

显示选项

显示前(名)： 60 ^ ▼

提交 取消

『过滤类型』用于设置查看的线路和应用类型。[选择线路]选择具体需要查看的线路，[应用类型]用于指定需要查看的应用服务，点击后出现如下页面：



[筛选]里面有显示全部、显示选中和显示未选三种选择，下面可以勾选具体的应用，右边[已选列表]显示已经选中的应用，点**确定**即可保存。

『过滤对象』用来设置具体的 IP，此处可设置 IPv4 地址。

『显示选项』用于设置显示流量前多少名的 IP。

### 3.2.5.4. IP 流量趋势图

#### 3.2.5.4.1 查看 IP 流量趋势

『IP 流量趋势图』主要用于统计 IP 的流量趋势情况，页面如下：



如图，根据 ip 的最近流速的趋势显示 Top5 或者 Top10 的 ip。

### 3.2.5.5. 异常流量

『异常流量』用于查看僵尸网络检测出的异常连接数据，前提是『僵尸网络』中启用了检测异常连接的功能，页面如下：



如图，此页面会显示异常连接的发生时间、源 IP、目的 IP、目的端口、风险等级、描述及详情。

### 3.2.5.6. 会话排行

#### 3.2.5.6.1 会话排行

『会话排行』主要用于查看通过 AF 设备的会话排名情况，可根据总会话数排行或者每秒钟新建会话数排行，显示 TOP10、TOP10、TOP30 或者 TOP60 位。

会话排行

序号	IP地址	总会话数	TCP会话数	UDP会话数	ICMP会话数	其它协议会话数	每秒新建会话数	查看会话详情
1	220.231.140.1	84	40	7	37	0	1	<a href="#">查看</a>
2	220.231.140.4	41	14	26	1	0	1	<a href="#">查看</a>
3	220.231.140.5	20	1	14	5	0	1	<a href="#">查看</a>
4	211.162.71.113	18	18	0	0	0	0	<a href="#">查看</a>
5	211.162.71.116	6	4	0	2	0	0	<a href="#">查看</a>
6	220.231.140.2	3	0	3	0	0	0	<a href="#">查看</a>
7	124.172.177.121	3	3	0	0	0	1	<a href="#">查看</a>
8	172.168.22.201	1	0	1	0	0	1	<a href="#">查看</a>

### 3.2.5.6.2 会话查询

『会话查询』主要用于查询指定的内网 IP 地址，根据会话对端的 IP 地址进行会话数的统计，如下图所示：

会话排行

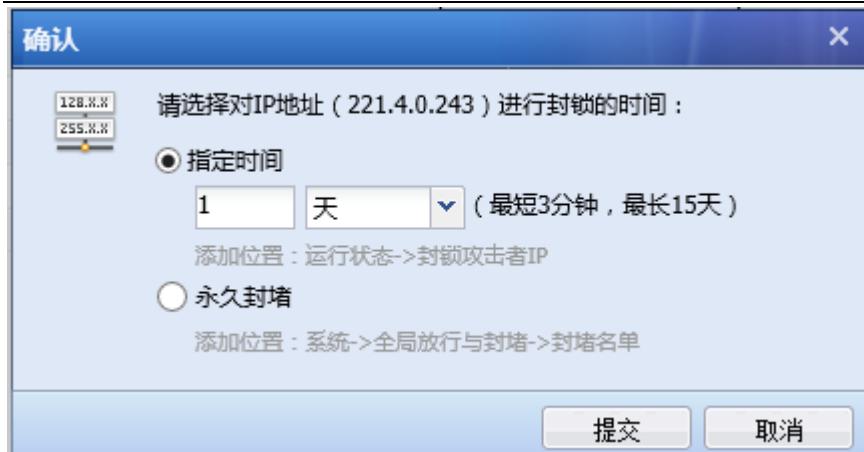
序号	会话对端的IP	归属地	总会话数	TCP会话数	UDP会话数	ICMP会话数	其它协议会话数	查看会话详情	封锁
1	221.4.0.243	中国广东	3	0	3	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
2	110.179.234.251	中国山西	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
3	113.108.77.21	中国广东	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
4	113.116.28.225	中国广东	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
5	182.254.10.120	中国上海	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
6	58.20.82.149	中国海南	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
7	111.121.124.192	中国贵州	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
8	115.159.102.12	中国上海	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
9	115.238.110.226	中国浙江	2	2	0	0	0	<a href="#">查看</a>	<a href="#">封锁</a>
10	123.207.128.11	中国广东	1	0	0	1	0	<a href="#">查看</a>	<a href="#">封锁</a>
11	所有	-	65	42	4	19	0	<a href="#">查看</a>	-

点击 [查看](#)，可以查看回话详情，如下图所示：

IP (220.231.140.1) 与对端IP (221.4.0.243) 的会话详情

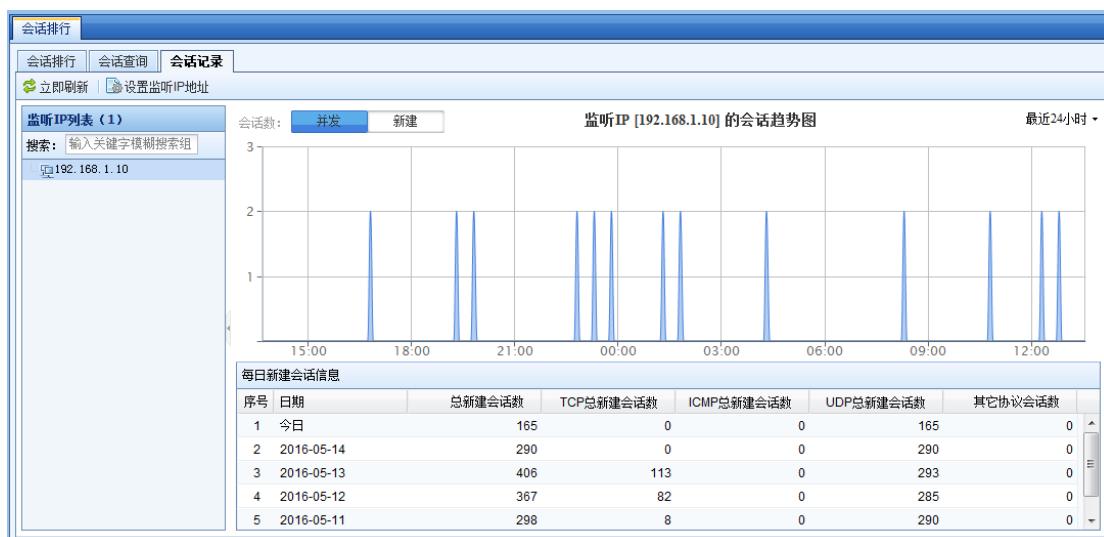
序号	源IP	NAT 源IP	源端口	目的IP	NAT 目的IP	目的端口	协议	状态	应用名称	源区域	目的区域
1	221.4.0.243	221.4.0.243	5060	220.231.140.1	220.231.140.1	10323	UDP	半连接	-	outside	-
2	221.4.0.243	221.4.0.243	5060	220.231.140.1	220.231.140.1	10282	UDP	半连接	-	outside	-
3	221.4.0.243	221.4.0.243	5060	220.231.140.1	220.231.140.1	10247	UDP	半连接	-	outside	-

点击 [封锁](#)，可以封锁回话 IP，如下图所示：

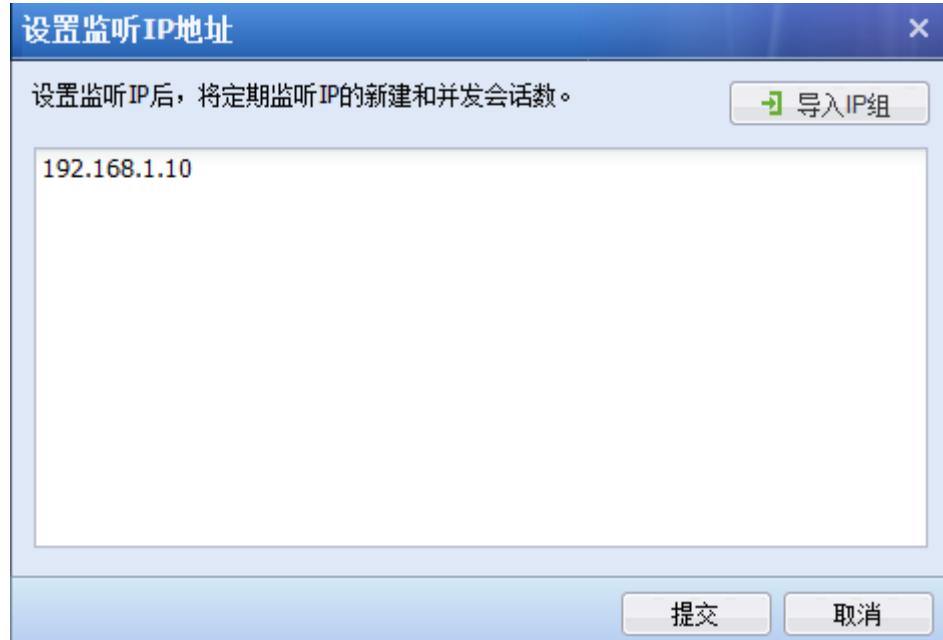


### 3.2.5.6.3 会话记录

『会话记录』主要用于定期监听 IP 的新建和并发会话数，使用时需要先设置监听 IP 组，如下图所示：



点击设置监听 IP 地址，可手动输入指定 IP，或者导入 IP 组，如下图所示：



### 3.2.5.7. 流量管理状态

『流量管理状态』主要用于查看流量管理设置通道的实时流量信息，前提是『流量管理』已经启用了流量管理的通道，页面如下：



点击**刷新间隔：5秒**用于设置页面上的排行刷新时间间隔；

点击**立即刷新**可以立即进行刷新。

**流控系统运行状态：运行中** 用于显示流量管理系统是否是启用状态，只有状态是

“运行中”此处才可以查看到流量通道的实时信息。

点击[进入流量管理系统](#)，进入流量管理页面。

### 3.2.5.7.1 查看外网速率

带宽分配						立即刷新	流控系统运行状态： <span style="color: green;">运行中</span>	<a href="#">进入流量管理系统</a>	
带宽分配		外网速率	删除策略	历史速率			线路设定速率	占用比例	历史流量
说明：每列前后两个值分别代表上行↑ / 下行↓									
名称	瞬时速率			历史速率			线路设定速率	占用比例	历史流量
总速率	10(b/s)	0(b/s)		0(b/s) 0(b/s)			116(Kb/s) 8(Kb/s)	10% 0%	0(B) 0(B)

从【外网速率】中可以看到总的流量情况，包括各条线路和总线路的瞬时速率、历史速率、线路设定速率、占用比例和历史流量等。

### 3.2.5.7.2 通道流量查看

【带宽分配】可以查看通道流量，页面如下：

带宽分配		排除策略		历史信息: [不显示] 显示选项: 全部通道					
说明：每列前后两个值分别代表上行↑ / 下行↓									
名称	线路	瞬时速率	占用比例	用户数	保证带宽	最大带宽	状态		
流控通道	线路1	37.86 (KB/s)   237.16 (KB/s)	0%   2%	-	10 (MB/s)   10 (MB/s)	10 (MB/s)   10 (MB/s)	运行中		
默认通道	全部	无	0%   0%	-	无	10 (MB/s)   10 (MB/s)	运行中		

【带宽分配】页面可以看到流量通道的名称、所属线路、瞬时速率、占用比例、用户数、保证带宽、最大带宽、状态等信息。在[历史信息]中可以选择不显示或者显示相应时间内的历史流量信息；在[显示选项]中可以选择查看“全部通道”或者是“仅运行中的通道”。

### 3.2.5.7.3 排除策略流量查看

【排除策略】主要用于查看流量管理里面排除策略的流量信息，页面如下：

带宽分配		排除策略		历史速率			
序号	名称	瞬时速率		历史速率		历史流量	
1	总速率	0		0		0	

### 3.2.6. DHCP 运行状态

『DHCP 运行状态』主要用于查看当前开启 DHCP 服务后，地址分配的相关信息。包括所分配的地址对应的计算机名称、MAC 地址、租用日期、租用时间，界面如下：



The screenshot shows a table with the following data:

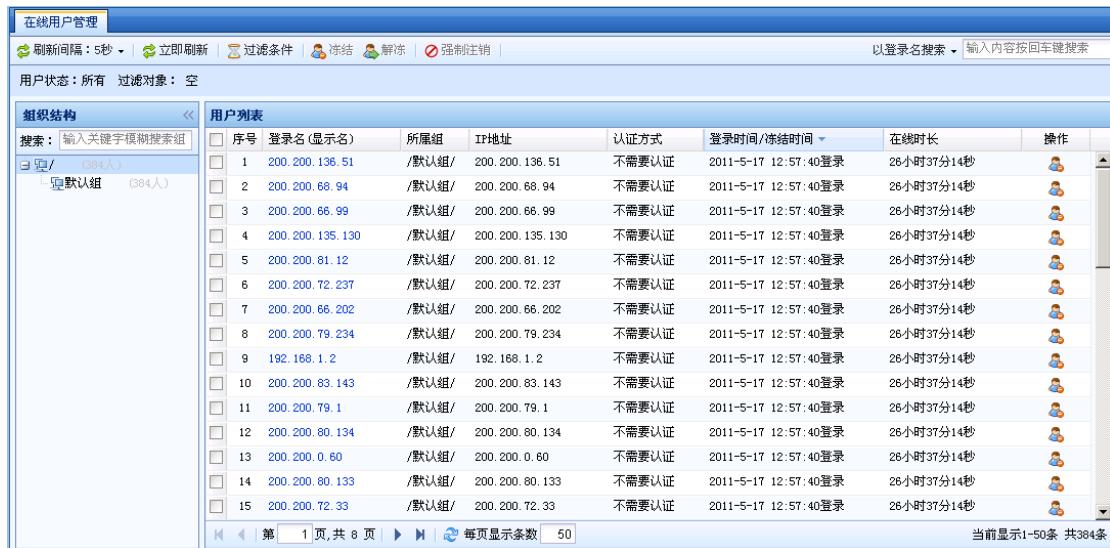
立即刷新 当前分配总数: 1 当前运行状态: 运行中				
序号	IP地址	计算机名称	MAC地址	租用日期
0	192.168.1.100	WIN-6A1RS3M72QV	0050569E5FC0	2018-11-20 15:11:02

点击 立即刷新 可以立即进行刷新。

### 3.2.7. 在线用户管理

#### 3.2.7.1. 查看在线用户

『在线用户管理』主要用于管理已经通过设备认证的在线用户，页面如下：



The screenshot shows the 'Online User Management' interface. On the left, there's a tree view under 'Organization Structure' showing a single node '默认组 (384人)'. The main area is titled 'User List' and displays a table of 384 users. The columns include: 序号 (Index), 登录名(显示名) (Login Name (Display Name)), 所属组 (Group), IP地址 (IP Address), 认证方式 (Authentication Method), 登录时间/冻结时间 (Login Time/Freeze Time), 在线时长 (Online Duration), and 操作 (Operations). Each user entry includes a checkbox, the user's IP address, group, authentication method, login time, freeze time, online duration, and a small icon for operations. At the bottom of the table, there are navigation buttons for pages and a dropdown for '每页显示条数' (Items per page) set to 50. A status bar at the bottom right indicates '当前显示1-50条 共384条' (Showing 1-50 of 384).

此处可以看到所有的通过设备认证的在线用户的登录名(显示名)、所属组、IP地址、认证方式、登录时间/冻结时间、在线时长以及对其进行操作。

在【组织结构】页面的[搜索]栏中输入关键词来搜索用户组，查询相应用户组的在线用户的情况。

在【在线用户管理】中可以[以登录名搜索]或者[以IP地址搜索]搜索指定用户，页面如下：



### 3.2.7.2. 过滤在线用户

点击**过滤条件**，可以设置指定条件查看相应的用户，页面如下：



[用户状态]可以选择所有、已冻结用户和活跃用户这三种。

[过滤对象]勾选后可以选择根据[用户过滤]或者是[IP 过滤]，输入指定的用户或者 IP 进行过滤，设置完成点击**提交**即可。

### 3.2.7.3. 冻结在线用户

选中一个或者多个用户点击**冻结**，便可以立即断开选中用户的上网连接，使其不能通过设备上网，具体操作如下：

选中一个用户：

User List						
	序号	登录名(显示名)	所属组	IP地址	认证方式	登录时间/冻结时间
<input checked="" type="checkbox"/>	1	200.200.66.99	/默认组/	200.200.66.99	不需要认证	2011-5-17 12:57:40 登录
<input type="checkbox"/>	2	200.200.0.60	/默认组/	200.200.0.60	不需要认证	2011-5-17 12:57:40 登录

点击**冻结**或者是在[b]操作[/]栏点击图示，出现如下页面：



设置[冻结上网时间]后，点击**提交**，该用户就被冻结上网了，此时该用户状态如下：

用户列表							
	序号	登录名(显示名)	所属组	IP地址	认证方式	登录时间/冻结时间	在线时长
<input type="checkbox"/>	1	200.200.66.99	/默认组/	200.200.66.99	不需要认证	2011-5-18 17:27:23冻结	冻结中，09分47秒后...

### 3.2.7.4. 解冻在线用户

被冻结的用户需要立即解冻去上网，也可以在此操作，具体操作如下：

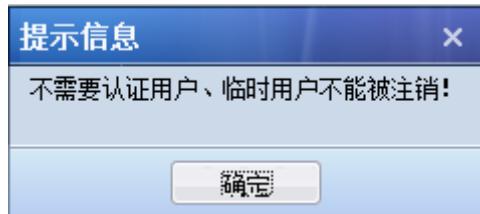
选择需要解冻的用户：

用户列表							
	序号	登录名(显示名)	所属组	IP地址	认证方式	登录时间/冻结时间	在线时长
<input checked="" type="checkbox"/>	1	200.200.66.99	/默认组/	200.200.66.99	不需要认证	2011-5-18 17:27:23冻结	冻结中，09分14秒后...

点击**解冻**或者是需要解冻的用户的[操作]一栏点击图示，即可立即解冻该用户。

### 3.2.7.5. 强制注销在线用户

管理员在该页面中可以强制注销在线用户，但不能对不需要认证和临时用户进行注销，对这类用户点击**强制注销**会出现如下提示：

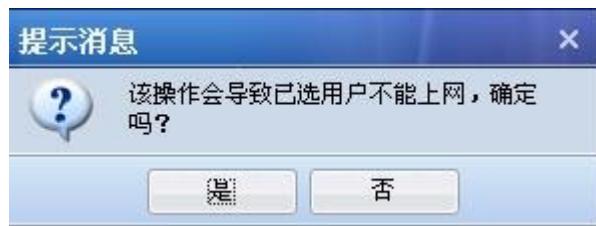


对密码认证和单点登录的用户可以进行强制注销，具体操作如下：

选中用户：

序号	登录名(显示名)	所属组	IP地址	认证方式	登录时间/冻结时间	在线时长	操作
1	sangfor	/	192.168.1.105	密码认证	2010-7-17 10:18:02登录	53秒	

点击**强制注销**，出现如下界面：



点击**是**，即可注销该在线用户。

### 3.2.8. 封锁攻击者 IP

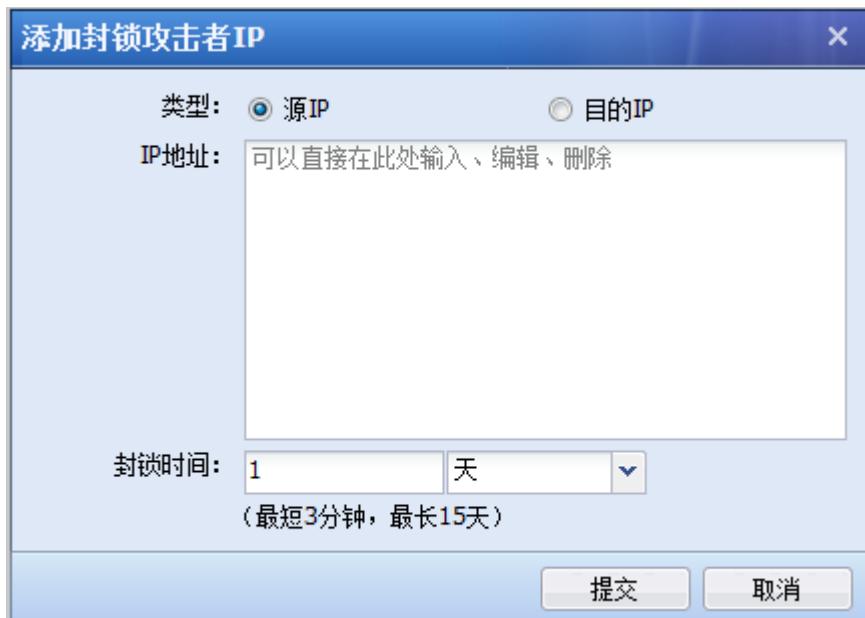
『封锁攻击者 IP』主要用于查看当漏洞攻击防护模块、WEB 应用防护模块和数据泄密防护模块、僵尸网络模块，配置启用了联动封锁后，触发封锁了哪些源 IP 以及是哪个安全策略触发的封锁。界面如下：

封锁攻击者IP						
刷新间隔：5秒		立即刷新		操作		
源IP	目的IP	目的端口	封锁时间	剩余解锁时间	触发安全模块	触发策略
60.169.75.15	211.162.71.116	3306	2016-05-15 13:...	27分7秒	IPS	IPS
222.186.34.197	220.231.140.2	3306	2016-05-15 13:...	23分48秒	IPS	IPS
222.184.120.35	211.162.71.116	3389	2016-05-15 13:...	19分49秒	IPS	IPS
202.77.40.132	220.231.140.2	3389	2016-05-15 13:...	8分42秒	IPS	IPS
116.212.114.96	220.231.140.2	3389	2016-05-15 13:...	7分59秒	IPS	IPS

点击刷新间隔：5秒用于设置页面上的刷新时间间隔；

点击立即刷新可以立即进行刷新。

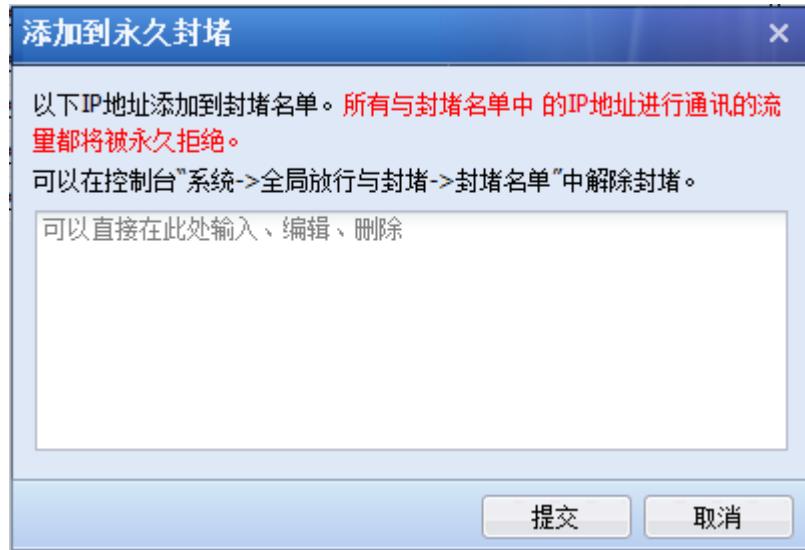
[添加攻击封锁者 IP]: 用于将攻击源 IP 或者目标 IP 加入封锁名单，并设置封锁时间，如下图所示：



[添加到放行名单]: 将设备已封锁的攻击者 IP 放行，后续该 IP 地址也不会被封锁。勾选需要放行的 IP 地址，点击添加到放行名单，如下图所示：

源IP	目的IP	目的端口	封锁时间	剩余解锁时间	触发安全模块	触发策略
106.38.210.75	220.231.140.2	3389	2016-05-15 13...	26分55秒	IPS	IPS
60.169.75.15	211.162.71.116	3306	2016-05-15 13...	22分54秒	IPS	IPS
222.186.34.197	220.231.140.2	3306	2016-05-15 13...	19分36秒	IPS	IPS
222.184.120.35	211.162.71.116	3389	2016-05-15 13...	15分36秒	IPS	IPS
202.77.40.132	220.231.140.2	3389	2016-05-15 13...	5分30秒	IPS	IPS
116.212.114.96	220.231.140.2	3389	2016-05-15 13...	3分46秒	IPS	IPS

[添加到永久封堵]: 用于将 IP 地址加入到封堵名单，所有与封堵名单中的 IP 地址的通信都会被永久拒绝，如下图所示：



勾选相应条目，点击 解除封锁 可以清除该封锁 IP 地址。

点击 清除所有封锁IP 可以清除所有源 IP，将恢复所有 IP 的访问权限。

点击 设置封锁时间 设置封锁时间，对于触发制定安全策略的源 IP，默认封锁时间为 10 分钟，10 分钟后将自动解锁，可以在此处设置更长的封锁时间。

[搜索] 可以针对某个 IP 地址进行搜索。

## 3.3. 网络

### 3.3.1. 接口/区域

『接口/区域』用于设置设备各网络接口信息，可以设置物理接口、子接口、VLAN 接口、聚合接口、GRE 隧道、区域、接口联动信息，如下图所示：

物理接口	子接口	VLAN接口	聚合接口	GRE隧道	区域	接口类型	连接类型	IP地址	工作模式	MTU	链路状态	状态	操作
agr.1													
eth3		否	允许	路由	lan	静态IP	192.168.1.1/24	—	1500	—	—	正常	
eth5		否	允许	路由	lan	静态IP	192.168.1.1/24	—	1500	—	—	正常	
eth0		否	允许	路由	未选择区域①	静态IPv4/静态IPv6	10.251.251.251/24	自动协商不成功	1500	未检测			
eth1		是	允许	路由	wan	静态IPv4/静态IPv6	10.1.129.10/24	全双工 1000Mbps 自动协商	1500	正常			
eth2		否	允许	路由	移动	静态IPv4/静态IPv6	172.31.1.1/24	自动协商不成功	1500	未检测			
eth4		否	拒绝	路由	未选择区域①	静态IPv4/静态IPv6	3.3.3.5/30-HA	自动协商不成功	1500	未检测			

### 3.3.1.1. 物理接口

『物理接口』页面可以查看各个接口名称，描述，WAN，接口类型，连接类型，区域，地址，拨号状态，MTU，工作模式，PING，网口状态，链路状态等，如下图所示：

物理接口	子接口	VLAN接口	聚合接口	GRE隧道	区域	接口联动					
接口名称	网口状态	WAN	PING	接口类型	区域	连接类型	IP地址	工作模式	MTU	链路状态	状态
eth0		否	允许	路由	未选择区域	静态IPv4	10.251.251.251/24	全双工 1000Mb/s 自动协商	1500	未检测	
eth1 内网接口		否	允许	路由	内网区域	静态IPv4	192.168.1.1/24	全双工 1000Mb/s 自动协商	1500	AVP未检测 PING正常 DNS未检测	
eth2		是	允许	路由	外网区域	静态IPv4	192.200.244.97/24,172.16.10...	全双工 1000Mb/s 自动协商	1500	未检测	
eth3		否	拒绝	路由	未选择区域	静态IPv4	12.1.1.1/24-HA	自动协商不成功	1500	未检测	
eth4		否	拒绝	路由	未选择区域	静态IPv4	...	自动协商不成功	1500	未检测	
eth5		否	拒绝	路由	未选择区域	静态IPv4	...	自动协商不成功	1500	未检测	
eth6		否	—	透明	未选择区域	Access access-3	...	自动协商不成功	1500	—	
eth7		否	拒绝	路由	未选择区域	静态IPv4	...	自动协商不成功	1500	未检测	

[接口名称]：网口的名称，物理接口不支持修改名称。

[描述]：对接口的描述。

[接口类型]：显示接口所属的类型。接口类型有路由、透明、虚拟网线和旁路镜像四种。

[连接类型]：显示接口IP地址获取的类型，包括ADSL IPv4、静态IPv4、DHCP IPv4等。

[区域]：接口所属的安全区域。

[地址]：列出为此接口配置的IP地址，没有则留空。

[拨号状态]：当接口类型为ADSL时，拨号状态显示连接、断开类型。

[工作模式]：显示接口的工作模式，如自动协商。

[PING]：显示接口是否允许PING。

[网口状态]：以图标颜色显示网口的链路状态，表示已连接，表示接口未接线或者网口DOWN掉。

[链路状态]：显示接口的链路故障状态，设备可以根据PING检测和DNS检测方式检测链路状态。

[状态]: 显示接口是否启用, 表示当前接口已启用。

如点击接口名称 **eth0**, 可以进入对应接口编辑页面进行基本设置, 如下图:



[类型]的配置即接口模式配置, 它决定了设备数据的转发功能, 有四种类型:

**路由:** 若选择为路由接口, 则需要给该接口配置IP地址, 并且该接口包含路由转发功能。

**透明:** 透明接口相当于普通的交换接口, 不需要配置IP地址, 不支持路由转发, 根据MAC地址表转发数据。

**虚拟网线:** 虚拟网线接口也是普通的交换接口, 不需要配置IP地址, 不支

持路由转发，转发数据时，直接从虚拟网线配对的接口转发。

旁路镜像：连接到有镜像功能的交换机上，用于镜像流经交换机的数据。

物理网口支持配置 IPv4 地址，其中 IPv4 支持静态 IP、DHCP、ADSL 三种配置。

有关这四种不同接口类型的详细配置说明请参考 5.1 小节的案例。

[基本属性]：设置该接口的基本属性，是否允许 PING，是否为 WAN 口，如果是 WAN 口，是否与 IPSEC VPN 出口线路匹配。

[链路故障检测]：用于检测外网线路的有效性，如果有多条外网线路的场景，某条线路故障，流量可自动切换到其他正常的线路。可通过 DNS 解析或者 PING 的方式来检测，而 ARP 探测的结果仅用于双机的切换条件使用，如下图所示：



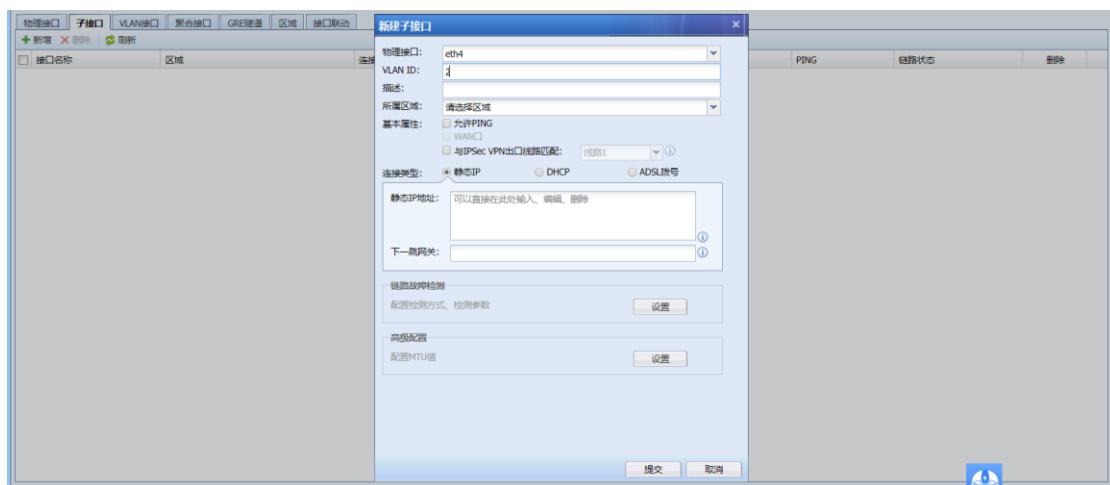
[高级配置]：可设置接口的工作模式，MTU，以及 MAC 地址：



1. **ETH0** 管理口的接口模式为路由口，不可更改接口模式。
2. **ETH0** 口可以增加管理 IP 地址，但是默认的管理 IP 地址 **10.251.251.251/24** 不能删除和更改。
- 3.任何接口的 IPv4 地址不允许设置在 **1.1.1.0/24** 网段范围。
4. 链路检测与双机热备中的抢占功能不能同时开启。

### 3.3.1.2. 子接口

子接口用于配置物理接口是路由接口，并且该路由接口需要启用 VLAN trunk 的场景，配置如下：



[接口名称]显示子接口的名称。 接口名称自动生成，且不可修改。例如 eth4

口下 VLAN2 的子接口，则自动生成为 eth4.2。

[描述]填写子接口的描述信息。

[区域]显示子接口所属区域。

[地址]显示子接口的 IP 地址。

[MTU]显示子接口的 MTU 值。

[PING]显示是否允许 PING 子接口。

[链路状态]显示子接口是否开启链路检测。

有关子接口的详细配置过程请参考 5.1.4 小节的案例。



任何接口的 IP 地址不允许设置在 1.1.1.0/24 网段范围。

### 3.3.1.3. VLAN 接口

『VLAN 接口』用于设置设备的 VLAN 列表，配置接口如下：

物理接口	子接口	VLAN接口	聚合接口	GRE隧道	区域	接口联动		
		+ 新增	- 删除	刷新				
<input type="checkbox"/>	接口名称	区域	连接类型	IP地址	MTU	PING	链路状态	删除
<input type="checkbox"/>	veth.1	lan	静态IP	172.31.100.1/24	1500	拒绝	未检测	

点击新增，添加 VLAN 接口，如下图所示：



[接口名称]设置 VLAN ID。设备需要加入哪个 VLAN，就填写对应的 VLAN ID 即可。

[基本属性]设置 VLAN 接口是否允许 PING。

[连接类型]可以选择静态 IP 或 DHCP。静态 IP 地址填写对应 VLAN 网段的 IP 地址。

[链路故障检测]与[高级配置]与路由接口设置方法相同，此处不再赘述。



任何接口的 IP 地址不允许设置在 1.1.1.0/24 网段范围。

### 3.3.1.4. 聚合接口

『聚合接口』用于设置设备的聚合接口列表，配置接口如下：

物理接口   子接口   VLAN接口   聚合接口   GRE隧道   区域   接口联动										
接口名称	WAN	PING	接口类型	区域	工作模式	IP地址	MTU	已选择接口	删除	
aggr.1	否	允许	路由接口	lan	主备模式	192.168.1.1/24	1500	eth3 eth5		

点击新增，添加聚合接口，如下图所示：

**新建聚合接口**

接口名称: aggr. 描述:   
类型: 路由 所属区域: 请选择区域 工作模式: 主备模式  
基本属性:  允许PING  WAN口  与IPSec VPN出口线路匹配: 线路1  
静态IP地址: 可以直接在此处输入、编辑、删除  
下一跳网关:   
选择汇聚接口  
可选物理接口: eth1, eth2, eth4, eth5, eth6, eth7  
已选接口:    
线路带宽  
上行:  Mbps 下行:  Mbps  
链路故障检测  
配置检测方式、检测参数   
高级配置  
配置MTU, MAC

[接口名称]: 设置聚合接口名称，

[描述]填写聚合接口的描述信息。

[类型]: 支持路由，透明和虚拟网线类型。

[所属区域]: 聚合接口所属的区域。

[工作模式]: 聚合接口所支持的工作模式，支持负载均衡-hash、负载均衡-RR、主备模式三种聚合模式。

[基本属性]: 与路由接口设置方法相同，此处不再赘述。

[选择汇聚接口]: 选择哪些接口需要进行端口聚合。

[链路故障检测]与[高级配置]与路由接口设置方法相同，此处不再赘述。



任何接口的 IP 地址不允许设置在 1.1.1.0/24 网段范围。

### 3.3.1.5. GRE 隧道

『GRE 隧道』用于配置 GRE 隧道，可以支持 GRE OVER IP、GRE OVER OSPF 和 GRE OVER IPSECVPN，设置界面如下：

物理接口	子接口	VLAN接口	聚合接口	GRE隧道	区域	接口联动
+ 新增 <span style="color:red;">X</span> 删除 <span style="color:green;">刷新</span>						
<input checked="" type="checkbox"/>	隧道	添加时间	备注	所属区域	IP地址	源端地址
<input checked="" type="checkbox"/>	Tunnel12	2016-12-11 14:18:43	-	Ian	-	192.168.1.1

点击新增，GRE 隧道新增页面如下：

新增隧道

编号 :  (i)

区域 :

基础配置

IP地址 : 格式 : 0.0.0.0/0 (i)

源端地址 : 格式 : 0.0.0.0 (i)

目的端地址 : 格式 : 0.0.0.0 (i)

GRE密钥 :  (i)

备注 :

可以为空，最长256个字符

高级配置 提交 取消

[编号]新增 tunnel 口的编号。

[区域]出接口所在的区域。

[IP 地址] 作为新增隧道的 IP 地址，该 IP 地址所在网段作为 OSPF 运行网段。

[源端地址]本端出接口实际公网路由源地址

[目的端地址]对端入接口实际公网路由目的地址

[GRE 密钥]共享密钥，两端要一致

[高级配置]用于设置 mtu 值、报文检验和和发送 Keepalive 报文的设置，页面如下：

高级配置

MTU :	1436	(i)
报文检验和 :	禁用	(i)
<input type="checkbox"/> 发送keepalive报文 (i)		
间隔时间 (秒) :	10	( 1-32767 , 默认10 )
最大发送次数 :	3	( 1-255 , 默认3 )

点击**提交**，完成 GRE 隧道设置。

### 3.3.1.6. 区域

『区域』用于设置接口所属的区域，以供业务防护策略、用户防护策略等策略模块调用。可以选择二层区域、三层区域，虚拟网线区域三种类型，二层区域可以选择所有透明接口和旁路接口，三层区域可以选择所有路由接口和 vpntun 接口，虚网线区域可以选择所有虚拟网线接口，设置页面如下：

物理接口	子接口	VLAN接口	聚合接口	GRE隧道	区域	接口联动
<span style="color: green;">+ 新增</span> <span style="color: red;">× 删除</span> <span style="color: blue;">刷新</span>						
区域名称	区域类型	接口列表		管理选项	管理地址	删除
- wan	三层区域	eth1	<span style="border: 1px solid #ccc; padding: 2px;">接口列表</span>	WebUI,ssh,snmp	全部	已被引用
移动	三层区域	eth2		WebUI	全部	×
电信	三层区域			WebUI	全部	×
server	二层区域					×
pc	二层区域					×
- lan	三层区域	veth_1,aggr_1		WebUI	全部	已被引用
wan1	虚拟网络区域					×

点击**新增**，区域新增页面如下：



[名称]设置区域的名称。

[转发类型]设置区域的类型。如果选择二层区域，接口列表会显示未被划到其他任何区域的剩余的透明接口；如果选择三层区域，接口列表会显示未被划到其他任何区域的剩余的路由接口，包括子接口和 VLAN 接口；如果选择虚拟网线区域，接口列表会显示未被划到其他任何区域的剩余的虚拟网线接口。

[接口]选择接口到区域。可通过**增加**，**移除**按钮来添加和删除接口。

[管理选项]设置是否允许从该区域登陆管理设备。可选择通过 WEBUI, SSH, SNMP 三种方式登陆，并可以设置允许管理此设备的 IP。界面如下：

允许管理设备

WEBUI  
 SSH  
 SNMP

允许管理此设备的IP：

全部 

请将允许管理此设备的IP组设为最小范围，以避免安全风险。

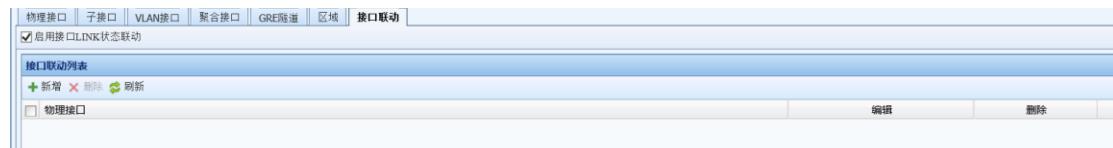
点击提交，完成区域设置。



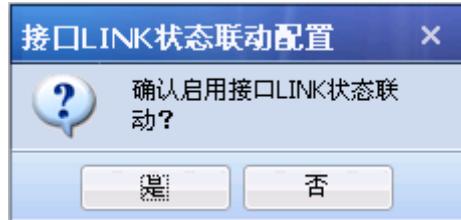
1. 一个接口只能属于一个区域，一个区域可以选择多个接口。
2. 一个区域可以同时选择 LAN 属性和 WAN 属性的接口。

### 3.3.1.7. 接口联动

『接口联动』接口联动主要用于AF设备工作在流量负载均衡模式，把负责转发数据设备的出接口和入接口添加到同一个联动组，实现同一个联动组中所有接口的状态始终保持一致。例如当一个联动组的一个接口网线掉了，则自动宕掉同一个联动组的其余接口；如果后续这个接口的网线重新插好，恢复了电信号，则恢复同一个联动组的其余接口，保证流量负载均衡的正常切换。设置页面如下：



『启用接口 LINK 状态联动』为开启接口联动功能的总开关，勾选后，出现如下页面：



点击**是**，启动接口 LINK 状态联动。

点击**新增**，添加接口联动，页面如下：



[名称]设置接口联动组的名称。

[物理接口]选择加入同一组接口联动组的接口，只能选择物理接口，可以选择多个接口属于同一个联动组。通过**增加**和**移除**按钮选择和删除接口。

点击**提交**，保存配置。



如果某接口的 IP 地址设置成“IP/掩码-HA”的形式，则此接口不能设置成接口联动。

### 3.3.2. 路由

路由配置页面包括静态路由，策略路由，多播路由，OSPF，RIP，BGP，查看路由和路由测试，当设备本身需要和不同网段的 IP 通信时，需要通过路由实现数据转发。

#### 3.3.2.1. 静态路由

在【导航菜单】页面中的『网络』→『路由』，右边进入【静态路由】编辑页面：

静态路由								
IPv4								
+ 新增   X 删除   导入   导出   刷新								
序号	目的地址	子网掩码	下一跳地址	度量值	接口	关联接口链路	状态	启用
1	0.0.0.0	0.0.0.0	192.200.244.254	10	eth2	禁用	有效	
2	192.168.20.0	255.255.255.0	192.168.1.2	0	eth1	禁用	有效	

点击新增会弹出【静态路由】的配置接口，选择新增单个静态路由或新增多个静态路由：



新增单个静态路由的页面如下：

新增单个静态路由

目的地址：	<input type="text" value="请输入目的地址"/>	(i)
子网掩码：	<input type="text" value="请输入子网掩码"/>	
下一跳IP地址：	<input type="text" value="请输入下一跳IP地址"/>	
接口：	<input type="text" value="自动选择接口"/>	(v)
度量值：	<input type="text" value="0"/>	
关联接口链路：	<input type="text" value="禁用"/>	(v) (i)

保存 取消

[目的 IP 地址]：需要到达的目标网络号。

[目的掩码]：目标网络对应的子网掩码。

[下一跳 IP 地址]：达到目标网络的下一跳地址。

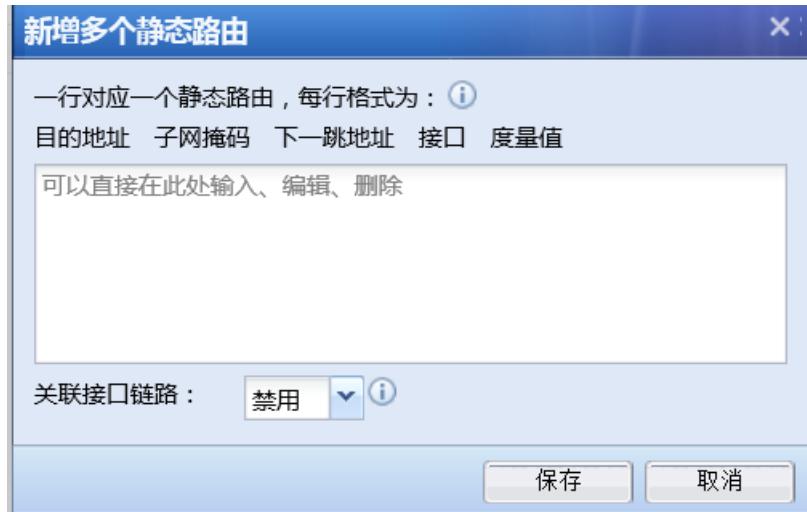
[接口]：从设备哪个接口转发。

[度量值]：静态路由的度量值。

[关联接口链路]：关联接口状态。

点击保存，保存配置。

新增多个静态路由的页面如下：



按照目的 IP，目的掩码，下一跳地址，接口，度量值的格式填写，一行对应一条静态路由。

[关联接口链路]: 关联接口状态。

点击**保存**，保存配置。



- 1、静态路由选择的接口，一般情况下建议设置“自动选择”，当设备存在多个接口 IP 在同网段的情况下，需要手动指定静态路由的接口；
- 2、导入、导出功能支持 IPv4 的路由导入导出；
- 3、关联接口链路所选的接口必须启用链路检测功能；
- 4、静态路由故障时支持邮件告警。

### 3.3.2.2. 策略路由

『策略路由』主要用于设备有多个外网口接多条外网线路时，根据源/目的 IP、源/目的端口、协议等条件进行出接口和线路选择，以实现不同的数据走不同的外网线路的自动选路功能。需要接口/区域中启用链路故障检测功能。

在【导航菜单】页面中的『网络』→『路由』，右边进入【策略路由】编辑

页面：



『策略路由』常用的两种需求是：

1、根据源 IP 地址和协议选择接口或下一跳。实现内网用户访问公网数据的分流，不同网段的内网用户，分别通过不同的线路接口访问公网；当设备上有多条外网线路时，内网用户访问网上银行、网上支付等应用会从不同链路出去，该应用安全性要求较高，因此有些服务器需要验证访问的源 IP 地址，如果多次访问的源 IP 是不同的，则会断开访问连接，此时可以通过『策略路由』功能新增源地址策略路由，实现访问这些安全应用固定从某一个接口或下一跳出去，保证每次访问安全应用的源 IP 地址是固定的。

2、设备上有多条外网线路，通过新增多线路负载策略路由，轮询，带宽比例，加权最小流量，优先使用前面的线路的接口策略，动态的选择线路，实现线路带宽的有效利用和负载均衡。

具体详细配置请参见章节 5.2



1、VLAN 和子接口不支持策略路由。

2、策略路由出接口支持不同下一跳。

3、策略路由的出接口支持选 VLAN。

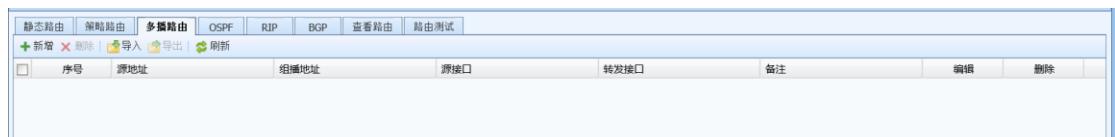
4、多线路负载策略路由支持 bond 口。

5、策略路由异常时，可以设置邮件告警

### 3.3.2.3. 多播路由

『多播路由』用于转发组播路由

如下图所示：



点击新增，如下图所示：

**新增多播路由**

源地址 :	<input type="text" value="请输入源地址"/>	<a href="#">i</a>
组播地址 :	<input type="text" value="请输入组播地址"/>	<a href="#">i</a>
源接口 :	<input type="text" value="请选择源地址"/>	<a href="#">▼</a>
<b>转发接口</b>		
可选		已选
<ul style="list-style-type: none"><li>eth0</li><li>eth1</li><li>eth2</li><li>eth4</li><li>veth.1</li><li>aggr.1</li><li>Tunnel12</li></ul>		<ul style="list-style-type: none"><li><a href="#">增加 ▶</a></li><li><a href="#">◀ 移除</a></li></ul>
备注 :		
<input type="text" value="可以为空，最长256个字符"/>		
<a href="#">提交</a> <a href="#">取消</a>		

[源地址]：发组播数据主机的地址。

[组播地址]: 组播数据包目的地址

[源接口]: 发组播数据主机的接口

[转发接口]: 组播流量向下转发的接口（可以选择多个接口）

点击提交，保存配置

### 3.3.2.4. OSPF

『OSPF』用于对 AF 设备开启和设置 OSPF 动态路由协议，包括网络配置，接口配置，参数配置，信息显示，调试选项等内容。

如下图所示：



勾选[启用 OSPF]，启用 OSPF 功能，出现如下提示信息：



点击是，保存配置。

【配置虚连接】：当 AF 设备所在的区域与 OSPF 的骨干区域不相邻的时候，需要启用和配置虚连接。点击配置虚连接，弹出如下页面：



勾选[启用]，开启虚连接。

[区域 ID]: 填写骨干区域 ID。

[Router ID]: 填写建立虚连接的对端路由器 ID，指明与哪一台路由器建立虚连接。

『定时器』：设置 hello 包间隔，重传间隔，传输时延，失效间隔，单位是秒。

[hello 间隔]: Hello 报文的重发间隔时间，默认值是 10s。

[重传间隔]: 与接口相邻的连接状态报文重发时间，默认值是 10s。

[传输时延]: 传输一个链路状态更新数据包的估计时间，默认值是 5s。

[失效间隔]: 如果超过失效间隔时间还未收到 Hello 报文，则认为该 OSPF 邻居不可达，一般设置为 hello 间隔的 4 倍，默认值是 40s。

『加密方式』：设置报文发送的加密方式，可以选择明文，MD5 或者不认证的方式。

『认证口令』：报文加密使用的口令。

点击**提交**，保存配置。

点击**高级配置**，可进行路由重发布设置和 NBMA 邻居配置，如下图所示：



### 3.3.2.4.1 网络配置

『网络』：设置设备需要发布的网段。点击**新增**，出现如下页面：

新增网络配置

运行网段：	输入IPv4或IPv6网段	/	输入掩码或前缀
区域ID：	输入IPv4地址或整数		
提交 取消			

[运行网段]：设置需要发布的网段地址，填写格式为：IP/掩码。

[区域 ID]：设置将该网段引入到哪个区域，一般填写骨干区域的 ID。

### 3.3.2.4.2 接口配置

『接口配置』显示设备在『OSPF』→『网络』中发布的网段对应的接口信息。如果在『OSPF』→『网络』下新增了如下网段：

网络配置		
+ 新增		删除
序号	运行网段	区域ID
1	202.96.137.75/29	0.0.0.0

自动生成的接口配置如下所示：

接口配置						
接口名称	IP地址	被动	认证方式	邻居老化时间	选举优先级	重传时间间隔
eth3	202.96.137.75/29	否	不认证	40	1	5

点击[接口名称]，出现如下页面：



[接口名称]: 『OSPF』 → 『网络』中发布的网段对应的接口名称。

[接口 IP]: 接口 IP 地址。

[被动接口]: 被动接口不发送 OSPF 链路状态，配置为被动接口后，直连路由可以发布，但接口的 OSPF 报文将会被阻塞，邻居无法建立。被动接口默认选“否”。

[认证方式]: 可以选择明文，MD5，不认证，默认是明文认证。

[认证口令]: 设置明文或 MD5 认证方式的口令。

[接口开销]: 指定从某条链路发送报文的开销。接口开销会影响到 LSA 的 Metric，直接影响 OSPF 的选路结果，范围为 1-65535，默认值为 1。

[邻居老化时间 (s)]: 默认失效时间为 40s。

[发送报文间隔时间 (s)]: Hello 报文的间隔时间，默认为 10s。

[选举优先级]: 优先级为 0 的路由器不会被选举成 DR 或者 BDR。DR 由本网段路由器通过 Hello 报文共同选举，设备将自己选出的 DR 写入 Hello 报文中，

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

发给网段上其他路由器。当同一网段的两台路由器都宣布自己是 DR 时，优先级高的胜出；如果优先级也相同，RouterID 大的设备胜出。选举优先级默认值是 1。

[重传时间间隔 (s)]: 缺省情况下，相邻路由重传 LSA 的时间间隔值为 5s。

[启用 DD 报文 MTU 不匹配检测]: 运行 OSPF 的设备在进行数据库同步时，使用 DD 报文描述自己的 LSDB。默认情况下，接口发送 DD 报文时不填充 MTU 值，即 DD 报文中 MTU 值为 0。

### 3.3.2.4.3 参数配置

点击『OSPF』→『参数配置』，出现如下页面：

**参数配置**

OSPFv2 Router ID :	192.168.3.1
OSPFv3 Router ID :	103.198.105.115
域内优先级: (只支持OSPFv2)	10
域间优先级: (只支持OSPFv2)	110
外部优先级: (只支持OSPFv2)	150
SPF计算间隔: (只支持OSPFv2)	5

**路由重发布配置**

重发布直连路由:	<input type="radio"/> 是	度量值:	_____
	<input checked="" type="radio"/> 否		
重发布RIP路由: (只支持OSPFv2)	<input type="radio"/> 是	度量值:	_____
	<input checked="" type="radio"/> 否		
重发布静态路由:	<input type="radio"/> 是	度量值:	_____
	<input checked="" type="radio"/> 否		
重发布默认路由:	<input type="radio"/> 是	<input checked="" type="radio"/> 否	
默认度量值:	10		

注：OSPFv3默认路由随静态路由一起发布；  
路由重发布配置中的所有度量值都只对OSPFv2有效。

[Router ID]: 设置 AF 设备的 Router ID。

[域内优先级]: 域内的 LSA 在计算后输出到路由表时，所携带的优先级(cisco 设备中称为管理距离 AD)，默认值为 10。只支持 OSPFv2。

[域间优先级]: 域间 LSA 计算后输出到路由表中的优先级，默认值为 110。只支持 OSPFv2。

[外部优先级]: 外部路由经过 SPF 计算后，输出到路由表时所赋予的优先级，默认值为 150。只支持 OSPFv2。

[SPF 计算间隔]: 当链路状态数据库 LSDB 发生变化时，需要重新计算最短路径，默认值是 5s。只支持 OSPFv2。

『路由重发布配置』：选择是否需要将直连路由，RIP 路由，静态路由、默认路由引入 OSPF 路由中作为外部路由信息，并可设置路由引入后的 metric 值。

[重发布直连路由]: 选择是否需要将直连路由引入 OSPF 路由中作为外部路由信息，并可设置路由引入后的 metric 值，默认度量值是 10。

[重发布 RIP 路由]: 选择是否需要将 RIP 路由引入 OSPF 路由中作为外部路由信息，并可设置路由引入后的 metric 值，默认度量值是 20。只支持 OSPFv2。

[重发布静态路由]: 选择是否需要将静态路由引入 OSPF 路由中作为外部路由信息，并可设置路由引入后的 metric 值，默认度量值是 20。

[重发布默认路由]: 选择是否需要将默认路由引入 OSPF 路由中作为外部路由信息。

[默认度量值]: 默认引入路由的跳数，在引入路由时，如果不分别指定各类型路由的 metric 参数，则使用该度量值作为路由引入后的跳数。度量值默认值是 10。

设置完成后，点击 **保存**，保存和生效配置。



**1、路由重发布配置中的所有度量值都只对 OSPFv2 有效。**

### 3.3.2.4.4 信息显示

通过『信息显示』可以查看 OSPF 链路信息，OSPF 路由信息，OSPF 邻接关系，OSPF 接口信息。

#### 3.3.2.4.4.1 OSPF 链路信息

『OSPF 链路信息』显示页面如下：

信息显示									
OSPF链路信息		OSPF路由信息		OSPF邻接关系		OSPF接口信息			
序号	Type	ID	Adv Router	Seq	Age	Opt	Cksum	Len	
1	Router LSA	181.8.4.76	181.8.4.76	0x80000003	546	0x02	0x0530	36	
◀◀   第 1 页, 共 1 页   ▶▶   每页显示条数 50					当前显示1-1条 共1条				

[Type]: LSA 的 type。

[ID]: LSA 所在的 Router ID。\*代表设备自己产生的 LSA。

[Adv Router]: 表示由哪个设备通告的这条 LSA 给本设备。

[Seq]: 这条 LSA 的序号。

[Age]: 表示收到该 LSA 已有多长时间。超时时间到了之后，该 LSA 将被老化。

[Opt]: 表示 Hello 报文中携带的选项信息。如果邻居与设备本身的 option 字段一致，可以拒绝接收该邻居的消息。

[Cksum]: LSA 的校验和。

[Len]: LSA 的长度。

### 3.3.2.4.4.2 OSPF 路由信息

『OSPF 路由信息』用来查看 OSPF 的路由，显示页面如下：



The screenshot shows a web-based interface titled "信息显示" (Information Display). At the top, there is a navigation bar with four tabs: "OSPF链路信息" (OSPF Link Information), "OSPF路由信息" (OSPF Routing Information) which is currently selected, "OSPF邻接关系" (OSPF Neighboring Relationship), and "OSPF接口信息" (OSPF Interface Information). Below the tabs, a section titled "路由信息" (Routing Information) displays a single row of data: "N 202.96.137.72/29 [10] area: 0.0.0.0 directly attached to eth3". At the bottom of the page, there is a pagination control with buttons for previous/next pages, a current page indicator "1 页, 共 1 页", a refresh icon, and a "每页显示条数" (Number of items per page) dropdown set to "50". To the right of the pagination, it says "当前显示1-1条 共1条" (Showing 1-1 of 1 total).

### 3.3.2.4.4.3 OSPF 邻接关系

『OSPF 邻接关系』显示页面如下：



The screenshot shows a web-based interface titled "信息显示" (Information Display). At the top, there is a navigation bar with four tabs: "OSPF链路信息" (OSPF Link Information), "OSPF路由信息" (OSPF Routing Information), "OSPF邻接关系" (OSPF Neighboring Relationship) which is currently selected, and "OSPF接口信息" (OSPF Interface Information). Below the tabs, there is a table with columns: 序号 (Sequence Number), Neighbor ID, Pri (Priority), State, Dead Time, Address, and Interface. A message "没有可以显示的数据" (No data to display) is centered in the table area. At the bottom of the page, there is a pagination control with buttons for previous/next pages, a current page indicator "1 页, 共 1 页", a refresh icon, and a "每页显示条数" (Number of items per page) dropdown set to "50". To the right of the pagination, it says "没有数据" (No data).

[Neighbor ID]: 邻接路由器的路由器 ID。

[Pri]: 邻接路由器的优先级。

[State]: 邻接路由器的功能状态。

[Dead Time]: 显示如果邻居不发 Hello 报文，还有多长时间该路由器状态变为 DEAD。

[Address]: 邻居与本设备相连接口的 IP 地址。当 OSPF 信息包被传输到邻居，此地址将是下一跳 IP 地址。OSPF\_VL1 是虚连接标识。

[Interface]: 邻居与本设备相连的接口。

#### 3.3.2.4.4 OSPF 接口信息

『OSPF 接口信息』显示页面如下：

信息显示					
OSPF链路信息		OSPF路由信息		OSPF邻接关系	
Interface	IP	Area	State	DR	BDR
eth3	202.96.137.75/29	0.0.0.0	DR	202.96.137.75	-

[Interface]: 接口名称。

[IP]: 接口的 IP 地址。

[Area]: 该接口所属区域。

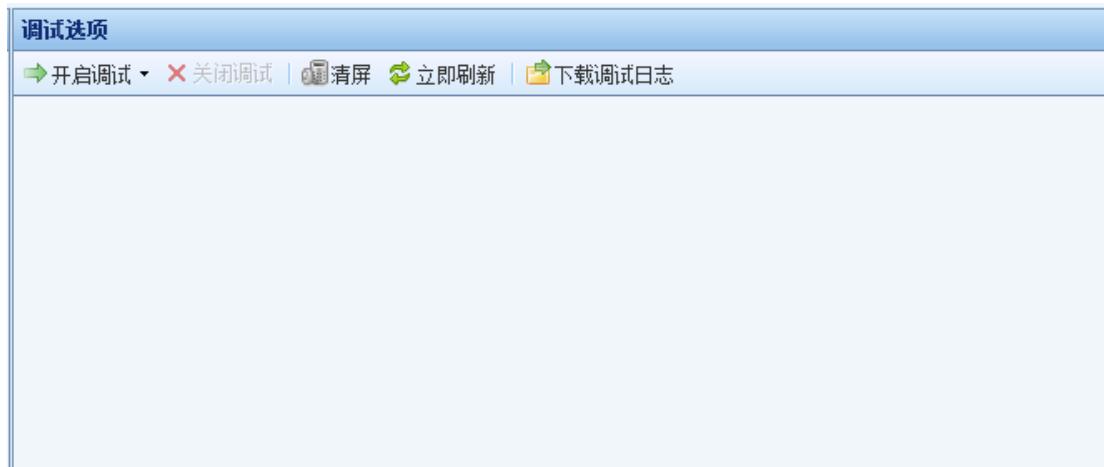
[State]: 该接口的角色。

[DR]: 该区域的 DR 地址。

[BDR]: 该区域的候选 BDR 地址。

#### 3.3.2.4.5 调试选项

通过『调试选项』可以开启和下载调试日志。



### 3.3.2.5. RIP

『RIP』用于对 AF 设备开启和设置 RIP 动态路由协议，包括网络配置，接口配置，邻居配置，参数配置内容，如下图所示：



勾选[启用 RIP]，启用 RIP 功能，出现如下提示信息：



点击**是**，保存配置。

#### 3.3.2.5.1 网络配置

『网络』：在指定接口上，将其相应的网段设置 RIP 网段。点击**新增**，出

现如下页面：



[运行网段]：设置需要发布的网段地址，填写格式为：IP/掩码。

点击[提交]，保存和生效配置。

### 3.3.2.5.2 接口配置

『接口配置』显示设备在『RIP』→『网络』中发布的网段对应的接口信息，这些接口能收发 RIP 报文。如果在『RIP』→『网络』下新增了如下网段：

网络配置	
+ 新增 X 删除	
序号	运行网段
1	202.96.137.75/29

自动生成的接口配置如下所示：

接口配置			
接口名称	IP地址	被动	认证方式
eth3	202.96.137.75/29	否	不认证

点击[接口名称]，出现如下页面：

编辑接口配置

接口名称:	eth3	
接口IP:	202.96.137.75/29	
被动接口:	<input checked="" type="radio"/> 是	<input type="radio"/> 否
版本设置（接收）:	<input checked="" type="radio"/> RIPv1	<input type="radio"/> RIPv2
版本设置（发送）:	<input checked="" type="radio"/> RIPv1	<input type="radio"/> RIPv2
执行水平分割:	<input checked="" type="radio"/> 是	<input type="radio"/> 否
毒性逆转:	<input checked="" type="radio"/> 是	<input type="radio"/> 否
认证方式:	<input checked="" type="radio"/> 明文	<input type="radio"/> MD5
认证口令:	<input type="text"/>	
<input type="button" value="提交"/> <input type="button" value="取消"/>		

[接口名称]: 『RIP』 → 『网络』中发布的网段对应的接口名称。

[接口 IP]: 接口 IP 地址。

[被动接口]: 指定 RIP 在接口上的工作状态，默认选择“否”。

[版本设置（接收）]: 指定在接口上接收的 RIP 报文的版本。当接收的版本选择为 RIPv2 时，可同时接收 RIPv1 和 RIPv2 的报文。

[版本设置（发送）]: 指定在接口上发送的 RIP 报文的版本。RIPv1 的报文传送方式为广播；RIPv2 有两种报文传送方式：广播和组播，缺省采用组播方式发送报文。当发送的版本选择为 RIPv2 时，可同时发送 RIPv1 和 RIPv2 的报文。

[执行水平分割]: 水平分割是指从哪个接口学到的路由，不能再从该接口发送出去，在一定程度上能避免产生路由环路。缺省情况下允许执行水平分割。

[毒性逆转]: 启用毒性逆转之后，从一个接口收到的路由，会从这个接口泛洪出去，但这条路由的 METRIC 是无穷大。缺省情况下不启用毒性逆转。

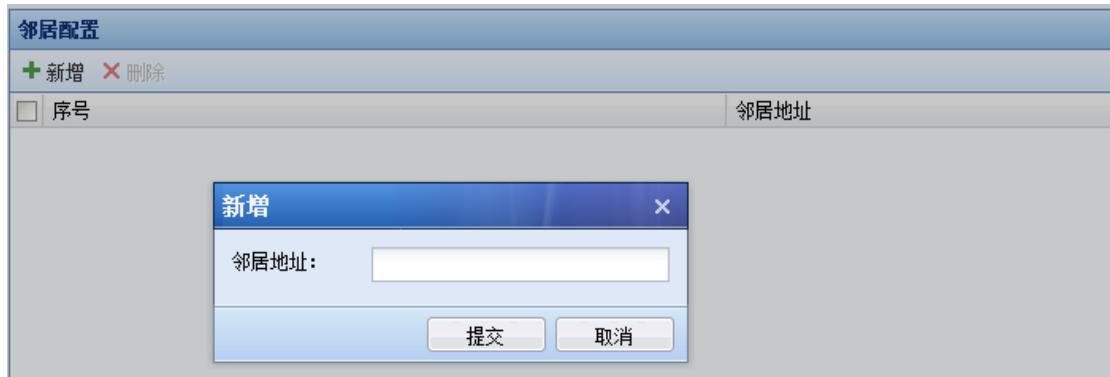
[认证方式]: 可以选择明文，MD5，不认证。RIPv1 不支持报文认证，RIPv2

支持明文和 MD5 认证。

[认证口令]: 设置明文或 MD5 认证方式的口令。

### 3.3.2.5.3 邻居配置

『邻居配置』设置相邻运行 RIP 协议的设备 IP 地址信息，如下图所示：



点击**提交**，保存配置。

### 3.3.2.5.4 参数配置

点击『RIP』→『参数配置』，出现如下页面：

**参数配置****RIP基本参数**路由优先级： (i)**设置定时器**定时更新： (i)超时定时器： (i)垃圾收集： (i)**路由重发布配置**重发布直连路由： 是  否度量值： (i) 否重发布OSPF路由： 是  否度量值： (i) 否重发布静态路由： 是  否度量值： (i) 否默认度量值： (i)**保 存****恢复默认配置并保存****『RIP 基本参数』可进行路由优先级和定时器的设置。**

**[路由优先级]**: 优先级将影响路由策略采用哪种路由协议获取的路由作为最优路由。优先级的数值越大，其实际的优先级越低。可以手工配置 RIP 的优先级，默认值是 120。

**[定时更新]**: 设置路由定期更新的时间间隔，默认为 30s。

**[超时定时器]**: 如果在此时间内没有收到某一条路由的信息，则将该路由跳数设置为 16，即不可达，默认为 180s。

[垃圾收集]: 垃圾收集定时器未超时之前，RIP 继续向外界通告不可达的路由信息，如果垃圾收集定时器也超时了，这一路由将从路由表中删除。

『路由重发布配置』配置将其他路由，如直连路由，OSPF 路由，静态路由引入 RIP 中，并设置引用路由的度量值。

[重发布直连路由]: 选择是否需要将直连路由引入 RIP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。默认度量值是 10。

[重发布 OSPF 路由]: 选择是否需要将直连路由引入 RIP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。默认度量值是 20。

[重发布静态路由]: 选择是否需要将静态路由引入 RIP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。默认度量值是 20。

[默认度量值]: 表示默认引入路由的跳数。在引入路由时，如果不分别指定各类型路由的 metric 参数，则使用该度量值作为路由引入后的跳数。默认度量值是 10。

点击**保存**，保存和生效配置。

点击**恢复默认配置并保存**，将把各个参数恢复到默认值保存。

### 3.3.2.6. BGP

『BGP』用于对 AF 设备开启和设置 BGP 动态路由协议，包括网络配置，邻居配置，参数配置等内容。

如下图所示：



勾选[启用 BGP]，启用 BGP 功能，出现如下提示信息：



点击**是**，保存配置。

【设置本机的 AS 号】：设置 AF 设备的 AS 号，如下图所示：



点击**提交**，保存配置。

### 3.3.2.6.1 网络配置

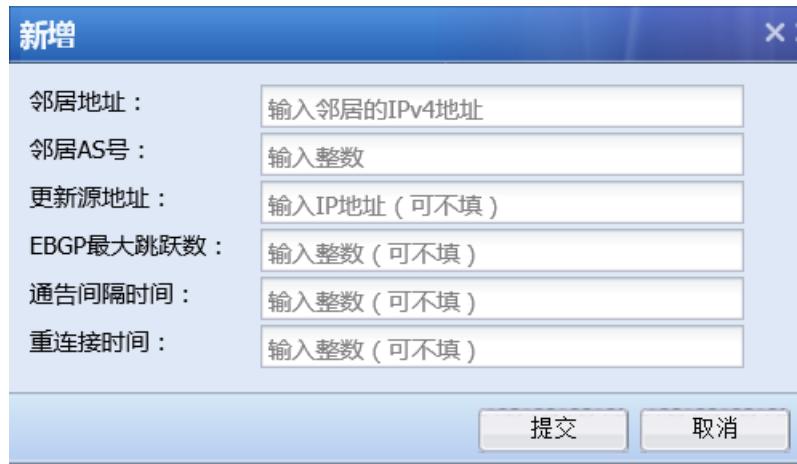
『网络』：设置设备需要发布的网段。点击**新增**，出现如下页面：



[运行网段]: 设置需要发布的网段地址，填写格式为：IP/掩码。

### 3.3.2.6.2 邻居配置

『邻居配置』：设置 BGP 的邻居信息，点击新增，出现如下页面：



邻居地址 :	输入邻居的IPv4地址
邻居AS号 :	输入整数
更新源地址 :	输入IP地址 (可不填)
EBGP最大跳跃数 :	输入整数 (可不填)
通告间隔时间 :	输入整数 (可不填)
重连接时间 :	输入整数 (可不填)

[邻居地址]: BGP 对端的地址。

[邻居 AS 号]: 与之建立 BGP 设备的 AS 号。

[更新源地址]: AF 设备 BGP 更新源地址。

[EBGP 最大跳跃数]: AF 设备 BGP 的 EBGP 最大跳跃数。

[通告时间]: AF 设备 BGP 的通告时间。

[重连接时间]: AF 设备 BGP 的重连接时间。

点击提交，保存配置。

### 3.3.2.6.3 参数配置

点击『BGP』→『参数配置』，出现如下页面：

静态路由 | 策略路由 | 多播路由 | OSPF | RIP | **BGP** | 查看路由 | 路由测试 |  
 启用BGP |  设置本机AS号

**组织结构** <> **参数配置**

**BGP基本参数**

路由ID：  
路由优先级：

设置定时器  
心跳包间隔时间：   
保持时间： 

**路由重发布配置**

重发布直连路由： 是  否  
度量值：  
重发布静态路由： 是  否  
度量值：  
重发布OSPF路由： 是  否  
度量值：  
重发布RIP路由： 是  否  
度量值：

[路由 ID]: 设置 AF 设备的 Router ID。

[路由优先级]: 设置 AF 设备的路由优先级。

[设置定时器]: 设置 AF 设备的心跳包间隔时间和保持时间

『路由重发布配置』：选择是否需要将直连路由，静态路由，OSPF 路由、RIP 路由引入 BGP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。

[重发布直连路由]：选择是否需要将直连路由引入 BGP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。

[重发布静态路由]：选择是否需要将静态路由引入 BGP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。

[重发布 OSPF 路由]：选择是否需要将静态路由引入 BGP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。

[重发布 RIP 路由]：选择是否需要将 RIP 路由引入 BGP 路由中作为外部路由信息，并可设置路由引入后的 metric 值。

设置完成后，点击**保存**，保存和生效配置。



AF 的 BGP 路由支持 **Route-map**、**AS-Path**、**next hop**、**origin**、**local preference** 和 **atomic aggregate** 公共属性。

### 3.3.2.7. 查看路由

『查看路由』页面可查看设备上所有的路由信息，包括直连路由，静态路由，通过动态路由协议学到的路由，IPSEC VPN 学到的路由和 SSL VPN 学到的路由。页面如下：

查看路由						
类型	目的地址	子网掩码/前缀	下一跳地址	度量值	接口	操作
静态路由	0.0.0.0	0.0.0.0	10.1.129.1	0	eth1	
静态路由	3.3.0.0	255.255.0.0	10.1.129.2	0	eth1	
静态路由	3.3.3.0	255.255.255.0	10.1.129.2	0	eth1	
直接路由	172.16.10.81	255.255.255.255	0.0.0.0	0	veth.1	
直接路由	3.3.3.4	255.255.255.255	0.0.0.0	0	eth4	
直接路由	192.168.1.0	255.255.255.0	0.0.0.0	0	aggr.1	
直接路由	10.1.129.0	255.255.255.0	0.0.0.0	0	eth1	
直接路由	172.31.100.0	255.255.255.0	0.0.0.0	0	veth.1	
直接路由	1.1.1.0	255.255.255.0	0.0.0.0	0	Tun0	
直接路由	1.1.1.0	255.255.255.0	0.0.0.0	0	Tun1	
直接路由	172.31.1.0	255.255.255.0	0.0.0.0	0	eth2	
直接路由	10.251.251.0	255.255.255.0	0.0.0.0	0	eth0	
VPN路由	10.20.0.0	255.255.0.0	41.210.4.50	16777215	vpntun	

点击『类型』旁边的▼，可根据路由的类型进行过滤显示。如下图所示：



点击刷新，可刷新显示的路由条目。

### 3.3.2.8. 路由测试

『路由测试』页面客户可在前端通过输入 IP 或协议或端口进行模拟路由匹配，匹配上的路由将会按优先级显示出来。页面如下：



协议 :

协议号 :

源IP地址:  源端口:

目的IP地址:  目的端口:

模拟测试结果

匹配优先级	类型	目的地址	子网掩码/前缀	下一跳地址	接口

点击『协议』旁边的▼，可以看到各种协议，可以根据协议类型来模拟路由匹配。页面如下：



输入测试条件后，点击, 可以看到路由的匹配情况。页面如下：



协议 :

协议号 :

源IP地址:

目的IP地址:

模拟测试结果

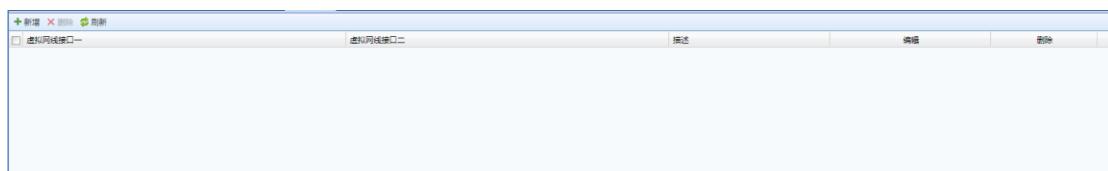
匹配优先级	类型	目的地址	子网掩码/前缀	下一跳地址	接口
1	直接路由	10.251.251.0	255.255.255.0	0.0.0.0	eth0

### 3.3.3. 虚拟网线

虚拟网线功能是指在 AF 设备上设置一个物理接口组，如 A 接口与 B 接口组成一组虚拟网线，数据包从 A 接口进入设备后，除了目标 IP 地址是 AF 设备本身的数据外，其他所有的数据均从 B 接口转发，即不经过二层 MAC 地址表查找以及三层的路由检查就将数据直接发送出去，但数据仍然受各种安全策略的控

制。通过虚拟网线功能，能提高 AF 设备数据转发的效率，也能防止由于 MAC 表的混乱导致数据转发错误。

『虚拟网线』的配置页面如下：



点击**新增**，新增虚拟网线，配置页面如下：



[描述]：填写虚拟网线的描述信息。

[虚拟网线接口一]：选择虚拟接口属性的物理接口。

[虚拟网线接口二]：选择虚拟接口属性的物理接口。

点击**提交**，保存和生效配置。



只有虚拟网线类型的物理接口或聚合接口才能配成虚拟网线，虚拟接口和虚拟网线必须同时配置才能生效。

### 3.3.4. 高级网络配置

高级网络配置包括 ARP, DNS, DHCP, SNMP, TCP MSS, HOSTS 设置。

### 3.3.4.1. ARP

『ARP 配置』包括静态 ARP 表和 ARP 代理两部分。

#### 3.3.4.1.1 静态 ARP 表

『静态 ARP 表』用于在设备设置静态绑定 IP/MAC 条目，页面如下：



点击新增，可以新增静态 ARP 条目，如下图所示：



[IP 地址]：设置需要绑定静态 ARP 条目的 IP 地址。

[MAC 地址]：设置需要绑定静态 ARP 条目的 MAC 地址。

[接口]：设置与绑定的 IP 地址相同网段的设备接口。

### 3.3.4.1.2 ARP 代理

ARP 代理功能即 AF 设备代理响应 ARP 请求，达到保护内网主机的目的。

界面如下：



有关 ARP 代理的的详细配置说明请参考 5.3 小节的案例。

### 3.3.4.2. DNS

『DNS』页面用于 AF 设备本身访问公网的 DNS 服务器设置以及 DNS 代理功能的设置，页面如下：



高级网络配置

ARP DNS DHCP SNMP TCP MSS HOSTS

**DNS服务器**  
系统自动更新及DNS代理功能均需要配置正确的DNS服务器  
首选DNS服务器： 192.200.200.199  
备选DNS服务器： 8.8.8.8

**DNS代理**  
启用后，内网计算机的DNS可以指向本设备，由本设备来代理解析DNS请求，请确保设备本身能正常解析DNS请求  
DNS代理：  启用  禁用

保存

[首选 DNS 服务器]和[备选 DNS 服务器]: 设置 AF 设备本身访问公网的 DNS 服务器。

[DNS 代理]: 开启此功能后，内网用户的 DNS 设置成 AF 设备的接口 IP，通过设备代理内网用户的 DNS 请求，转发到设备设置的首选 DNS 服务器和备选 DNS 服务器。

### 3.3.4.3. DHCP

『DHCP』页面用于 AF 设备作为 DHCP 服务器的设置以及 DHCP 中继功能的设置。

#### 3.3.4.3.1 DHCP 服务器

『DHCP 服务器』页面如下：



勾选[启用 DHCP 服务器]，出现如下提示页面：



点击**是**，保存和开启 DHCP 服务。

**【DHCP 服务接口列表】：**显示设备上所有路由接口，子接口和 VLAN 接口，可以分别设置通过这些接口分配 IP 地址。

有关 DHCP 服务器的详细配置说明请参考 5.4.1 小节的案例。

#### 3.3.4.3.2 DHCP 中继

DHCP 中继功能用于 DHCP 服务器与 DHCP 客户端 IP 在不同 IP 网段的应用场景，配置页面如下：

对以下接口启用中继	
可选:	已选:
eth0 eth2 eth3 eth0.10 veth.1	
<input type="button" value="增加 &gt;"/> <input type="button" value="&lt; 移除"/>	

DHCP 服务器地址: 127.0.0.1

有关 DHCP 中继的详细配置说明请参考 5.4.2 小节的案例。

### 3.3.4.4. SNMP

SNMP 用于支持其他网管设备或软件用 SNMP 方式来管理和查看 SANGFOR 设备的相关信息，如接口状态、接口流量、路由等系统相关信息，方便用户集中管理、维护、监控网络。

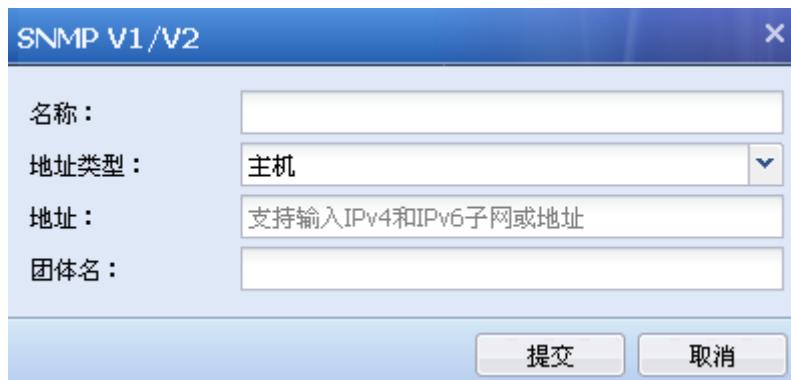
在【导航菜单】页面中的『网络』→『高级网络配置』，右边进入【SNMP】编辑页面：



勾选[开启 SNMP]，则其他设备和管理软件可以通过 SNMP 读取设备信息。

**导出 MIB:** 导出 AF 设备支持的 MIB 库，可导入 SNMP 客户端使用。

『SNMP V1/V2』用于设置允许其他设备通过 SNMP V1/V2 协议连接设备，并约定连接参数。点击**新增**，配置如下：



[名称]: 设置该管理主机的名称。

[地址类型]: 设置管理主机的类型，可选值为“主机”和“子网”。当选择“主机”则设定 SNMP 管理者为一台主机；“子网”设定 SNMP 管理者为一个子网，该子

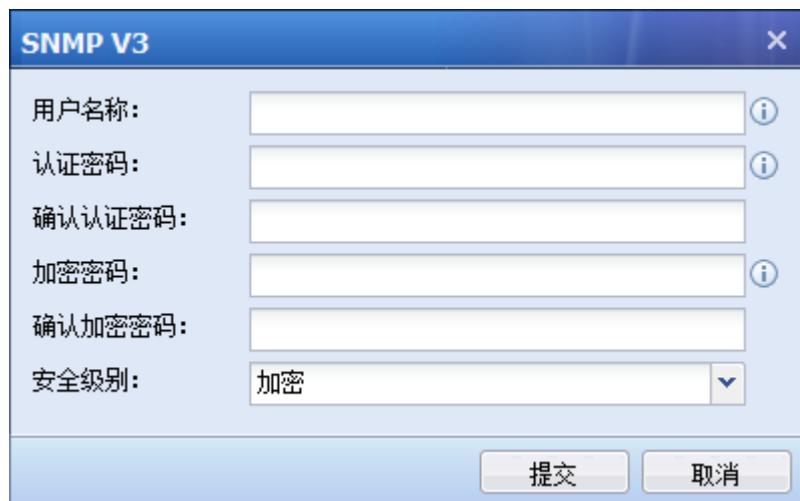
网内的主机都可以通过 SNMP 管理设备。

[地址]: 设置 SNMP 管理者的 IP 地址或地址范围, 当管理主机类型为“主机”时, 用于指定 SNMP 管理主机对象的 IP 地址; 当管理主机类型为“子网”时, 用于指定 SNMP 管理子网对象的子网地址及其掩码。

[团体名]: 指定 SNMP 管理主机访问设备时的团体名。

点击提交保存配置。

『SNMP V3』用于设置当以 SNMP V3 版本通讯时, 需要设置的一些高级扩展选项, 配置如下:



[用户名]: 添加该用户的名称。

[认证密码]和[确认认证密码]: 指定 SNMPV3 用户对象进行认证时使用的密码, 认证密码必须大于 8 位字符并且不能包含空格, 将以 MD5 算法进行加密。

[加密密码]和[确认加密密码]: 指定消息加密时使用的密码, 认证密码必须大于 8 位字符并且不能包含空格, 将以 DES 算法进行加密。

[安全级别]: 设置是否对 SNMP 认证和管理信息进行加密。可选项为: 加密、不加密。当设置加密时, 同时使用加密和认证技术, 先对数据进行加密, 然后进行认证技术的消息摘要计算。设置不加密时, 只使用认证技术。

点击提交完成配置。

『SNMP Trap』: SNMP Trap 功能用于主动发送 SNMP 信息到管理端, 以

方便管理员实时监控 AF 的运行状态。

点击**新增**，配置如下：



[Trap 消息类型]: 用于设置 AF 主动发送的消息类型，包括：热启动、网口状态、配置更新、高可用性、内置库更新、链路检测（各消息类型对应的 OID 可点击 **SNMP OID** 查看）。

[目的 IP 地址]: 设置发送 SNMP Trap 报文的目标主机地址，即 SNMP 客户端的 IP 地址。

[端口]: 用于目标主机监听的端口号。

[版本号]: 支持选择 SNMP V1、V2、V3 版本。

[团体名]: 指定发送 SNMP Trap 消息的团体名。

当[版本号]选择 SNMP V3 时，[团体名]不可填写，还需要做如下设置：



[引擎 ID]: 目标主机的引擎 ID 号 (snmpEngineID)，十六进制字符串形式，不包括前缀 0x。

[用户名]: 填写 SNMP 客户端上存在的 SNMP V3 用户。

[认证方式]: SNMP V3 用户的认证方式，支持 MD5 和 SHA (默认是 SHA)。

[认证密码]: SNMP V3 用户的认证密码

[安全级别]: 指 SNMP V3 Trap 消息的安全级别。支持的选项：加密、不加密；选择加密的时候，可以填写加密方式以及加密密码

[加密方式]: SNMP V3 Trap 消息的加密方式，支持 DES、AES (默认是 AES)

[加密密码]: SNMP V3 Trap 消息的加密密码。

### 3.3.4.5. TCP MSS

TCP MSS (Maximum Segment Size)：TCP 数据包每次能够传输的最大数据分段大小。对于匹配一定条件的数据，AF 支持更改数据包的 TCP MSS 值。使用此项的目的是为了适应更复杂的网络环境，建议在有必要时开启。

在【导航菜单】页面中的『网络』→『高级网络配置』，右边进入【TCP MSS】

编辑页面：



勾选[启用]，启用 TCP MSS 配置。

点击新增，新增一条规则：



[名称]: 设置规则名称。

[描述]: 设置规则的描述信息。

[MSS 值]: 设置需要指定的 TCP MSS 值。

[源]: 设置源 IP 组、源端口，指定匹配该规则的源条件。

[目的]: 设置目的 IP 组、目的端口，指定匹配该规则的目的条件。

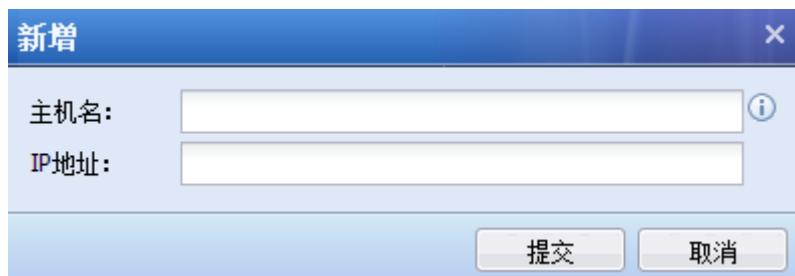
### 3.3.4.6. HOSTS

HOSTS 功能用于在 AF 的 HOST 表中添加记录，需要在 AF 上指定某个主机名对应的 IP 地址时，可以在这里添加。

在【导航菜单】页面中的『网络』→『高级网络配置』，右边进入【HOSTS】编辑页面：



点击新增，新增一条记录：



主机名：设置需要指定的主机名

IP 地址：设置主机名对应的 IP 地址

设置完成后点击提交，完成设置。

### 3.3.5. 光口 bypass 设置

支持光口 bypass 功能，配置页面如下图



[类型]: 仅支持国产 optical bypass，注意不支持光口 bypass 与双机热备同时启用。

[新增旁路光模块]: 选择相应的光模块接口进行配置。



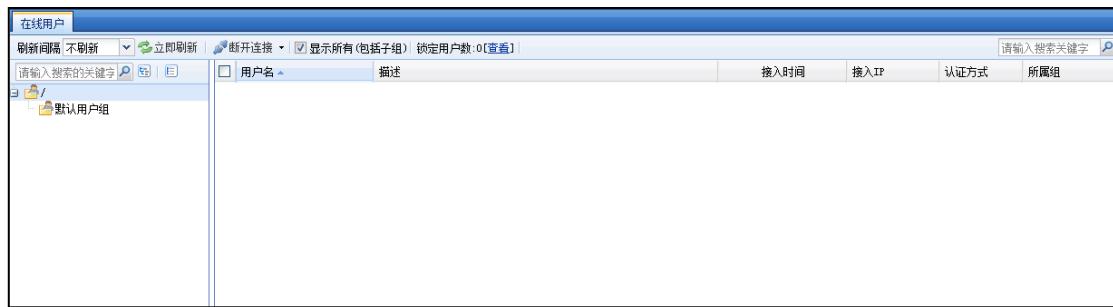
### 3.3.6. SSL VPN

SSL VPN 功能需要通过序列号开启。

#### 3.3.6.1. 在线用户

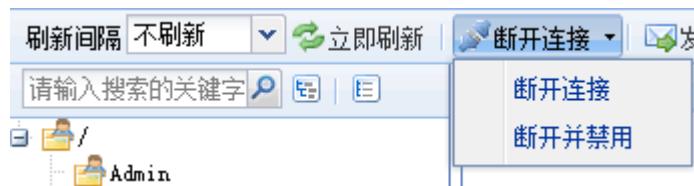
在『在线用户』里面可以查看当前登录 SSL VPN 的在线用户，可以查看到相应用户的接收发送流速/流量和接入 VPN 的时间，可以手动将接入的 VPN 用户断开或禁用。

界面如下图所示：



『刷新间隔』可以设置页面自动刷新时间，点击立即刷新则立即刷新页面信息。

点击断开连接可选择[断开连接]或者[断开并禁用]。页面显示如下：



勾选相应的用户，然后点击『断开连接』，该用户则断开 SSLVPN 的连接。如果选择『断开并禁用』，并点击立即生效，则该用户被断开后将被禁止登录。

### 3.3.6.2. 部署模式

部署模式中有两种工作模式可供选择：单臂模式和网关模式。

界面如下图所示：

选择单臂模式时，需要选择内网接口，页面如下：

部署模式

部署模式： 网关模式  单臂模式

当前部署为单臂模式，无须配置外网IP，通过前端设备连接上网。

接口设置

内网接口：eth0

保存

选择网关模式时，不仅需要配置内网接口，同时也必须指定外网接口。页面如下：

部署模式

部署模式： 网关模式  单臂模式

当前部署为网关模式，需要配置设备外网IP和内网IP，作为连接企业内网和外网的接口。

接口设置

内网接口：eth0

外网接口：--请选择外网接口--

保存

### 3.3.6.3. 用户管理

『用户管理』用于建立 SSL VPN 用户和用户组，为了管理具有某些共性的用户以及更符合企业内部管理结构，采用分层的用户组管理用户。

界面如下图所示：



The screenshot shows the 'User Management' interface. On the left is a tree view of user groups, with '默认用户组' (Default User Group) expanded. On the right, detailed information about the selected group is displayed, including its name, path, and a summary of its sub-groups and users. Below this is a table listing users under the group, showing columns for name, type, description, other information, and status.

名称	类型	描述	其他信息	状态
默认用户组	用户组	系统保留的用户组,不能被删除	公有用户组	✓
test	用户		私有用户	✓
yangtao	用户	yangtao	私有用户	✓

在『用户管理』页面，左边为用户组结构树，右边为当前光标停留的用户组中的用户以及下级用户组。勾选[显示所有（包含子组）]，则显示当前用户组下的所有子组以及包含的所有用户。

用户组结构树上方的搜索框中可输入目标用户组的关键字，点击放大镜图标进行搜索，搜索到的用户组在用户结构树中会被高亮显示。

### 3.3.6.3.1 新建用户组

点击**新建**按钮，在下拉框中选择**用户组**，弹出【新增用户组】编辑框。

界面如下图所示：

用户管理

基本信息

名称:  \*

描述:

所属组: /

最大并发用户数:  (0表示不限制)

账户状态:  启用  禁用

继承上级用户组关联角色和认证方式

继承上级用户组认证方式

继承上级用户组关联角色

认证选项

账户类型:  公有用户组  私有用户组

主要认证   
用户名/密码

辅助认证  硬件特征码

关联角色

关联角色:

『名称』即标识该 SSL VPN 用户组的名字，必须填写。

『描述』可任意填写用户组的相关说明信息。

『所属组』在其下拉框中可选择当前新建用户组所隶属的用户组。/表示根组。

『最大并发用户数』控制该用户组及其下级组可以同时登录的在线用户数。

『账户状态』中勾选[启用]激活该用户组；勾选[禁用]禁用该用户组。

勾选[继承上级用户组关联角色、认证方式]，当前用户组自动关联上级用户组的角色、认证方法。

勾选[继承上级用户组认证方式]，当前用户组『认证选项』标签内的功能项与上级用户组一致。

勾选[继承上级用户组关联角色]，当前用户组自动关联上级用户组的角色。

『认证选项』标签内是用户组的登录认证方式的相关设置。

『账户类型』分为[公有用户组]和[私有用户组]。

[公有用户组]指该用户组中的所有用户账号可以供多人同时使用登录 SSL VPN。

[私有用户组]指该用户组中的所有用户账号仅仅允许一个人使用登录 SSL VPN，两个人使用时会导致先登录的用户断线。

『主要认证』是用户名密码认证，『辅助认证』可选可不选。

[用户名/密码]认证，要求该用户组在建立用户账号时，设置用户账号的『名称』和『密码』。

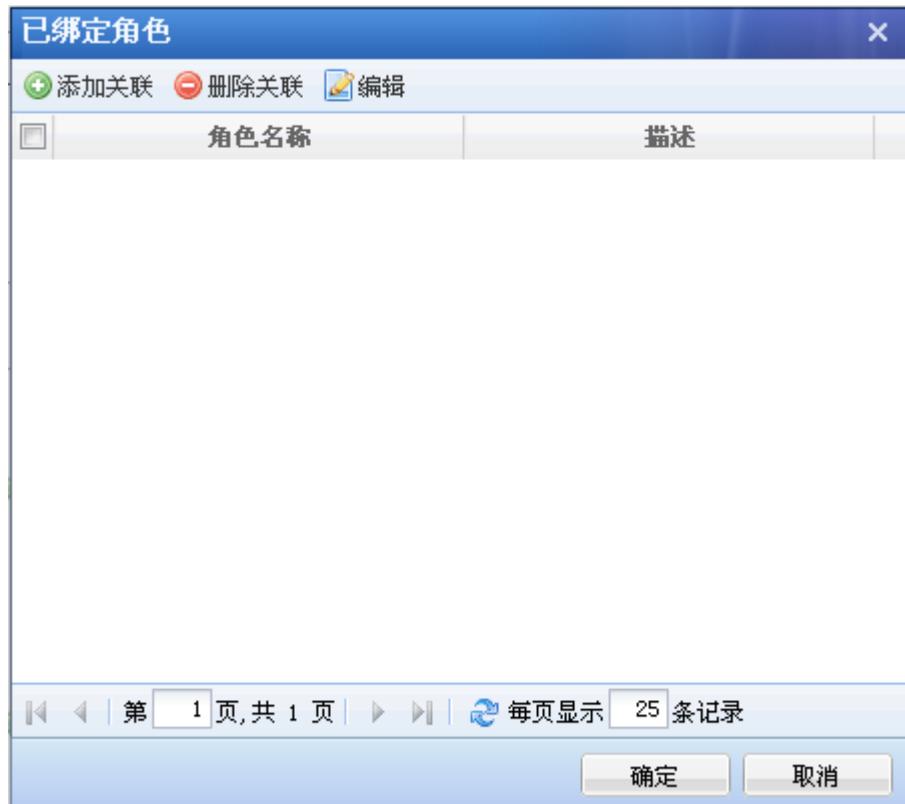
[硬件特征码]把 SSL VPN 用户账号和计算机的部分硬件特性（如网卡、硬盘等）生成的硬件特征码一一绑定。由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的。一个用户可以拥有多个特征码，即在同一个账号下，多台符合条件的电脑可以登录。也可以配置成只能拥有 1 个特征码。通过对该硬件特征码的验证，就保障了只有指定的硬件设备才能接入授权的网络，避免了安全隐患。

『关联角色』用来选择该用户组所使用的角色，角色的具体设置可以参考 3.3.7.5 『角色授权』章节。



点击新建角色并关联按钮，打开【新建角色】对话框并编辑新角色，编辑完成点击保存按钮，保存该角色并关联给当前用户组。具体设置可以参考 3.3.7.5 『角色授权』章节。

点击<sup>»</sup>为该用户组选择相应的角色，如下图所示：



点击**添加关联**按钮，用来选择需要关联的角色，弹出【添加关联角色】的对话框，如下图所示：

### 添加关联角色

请输入搜索关键字

<input type="checkbox"/>	角色名称	描述
<input type="checkbox"/>	debug	
<input type="checkbox"/>	testdsz	
<input checked="" type="checkbox"/>	sangfor	
<input checked="" type="checkbox"/>	test	

第 1 页, 共 1 页 | 每页显示 25 条记录

勾选相应的角色，点击**确定**，如下图所示：

### 已绑定角色

<input type="checkbox"/>	角色名称	描述
<input type="checkbox"/>	test	
<input type="checkbox"/>	sangfor	

第 1 页, 共 1 页 | 每页显示 25 条记录

再点击**确定**，如下图所示：



关联角色成功，该用户组关联了两个角色。

点击保存并继续添加，可继续添加角色。

点击保存按钮，保存配置。

### 3.3.6.3.2 新建用户

点击新建，在下拉框中选择用户，弹出『新建用户』的操作界面。

界面如下图所示：

『名称』即 SSL VPN 用户登录 VPN 时所使用的帐号。

『描述』可任意填写用户的相关说明信息。

『密码』和『确认密码』用于设定 SSL VPN 登录帐号的密码。

『手机号码』用于填写用户的手机号码。

『所属组』可设定该用户属于哪个用户组。勾选[继承所属组认证选项]，即当前用户继承上级用户组的认证策略。

『过期时间』，包括[永不过期]和[手动设置]两种。

若勾选[永不过期]则该用户一直都可以使用；

若勾选[手动设置]，则在后面的方框中选择日期，如果到了这个时间，那么该用户将被禁用。

『账号状态』，可选择[启用]或[禁用]。

若勾选[启用]则该账号可以正常使用；

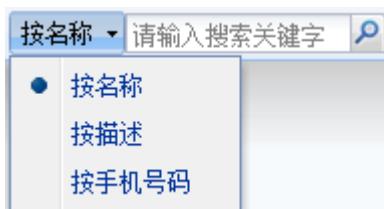
若勾选[禁用]，则该账号被禁用，无法使用。

『认证选项』和『关联角色』标签内的设置项和【新建用户组】页面的一样，此处不再赘述。

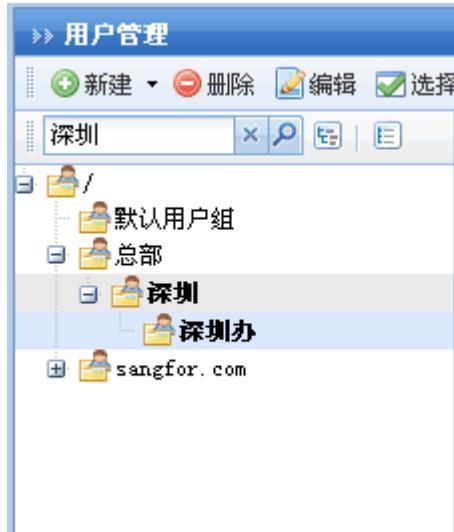
完成配置后，点击**保存**。

### 3.3.6.3.3 高级搜索

位于界面右上方的搜索框，可[按名称]、[按描述]或[按手机号码]来搜索用户，在后面的方框可填入需要搜索的具体内容，点击放大镜图标，会直接显示相关用户的相关信息。



位于用户组织结构上方的搜索框，可以查找有相应关键字的用户组，如下图所示：



点击用户列表中『名称』标签，即可对用户、用户组进行升降序排列。

点击『列』标签，可根据下拉表的选项进行显示列的筛选，如下图：

The screenshot shows a 'User Management' window with a 'Columns' dropdown menu open. The menu lists several options: '名称' (Name) is checked, while '类型' (Type), '描述' (Description), '过期时间' (Expiration Time), '最近登录时间' (Last Login Time), '手机号码' (Mobile Number), '其他信息' (Other Information), and '状态' (Status) are unchecked. To the right of the columns, there is a table listing three users: '默认用户组' (Default User Group), 'test', and 'yangtao'. The 'test' and 'yangtao' rows have a '描述' (Description) column containing the text '系统保留的用户组,不能被删除' (System reserved user group, cannot be deleted). The 'test' row also has a '状态' (Status) column with a green checkmark. The 'yangtao' row has a '状态' (Status) column with a green checkmark.

名称	类型	描述	其他信息	状态
默认用户组	正序	系统保留的用户组,不能被删除	公有用户组	✓
test	倒序		私有用户	✓
yangtao	正序		私有用户	✓

点击『类型』标签，可以选择列出不同类型的用户，方便管理，如下图所示：

The screenshot shows a user management interface with the following details:

- Group Name: /
- Group Path: /
- Group Information: 直属子组数:1, 总子组数:1, 直属用户数:2, 总用户数(包含子组):2
- Buttons: 查看或编辑组属性
- Table Headers: 名称 (Name), 类型 (Type), 描述 (Description), 其他信息 (Other Information), 状态 (Status)
- Table Data:

名称	类型	描述	其他信息	状态
默认用户组	全部	系统的用户组, 不能被删除	公有用户组	✓
test	用户组		私有用户	✓
yangtao	用户		私有用户	✓
- Type Filter: A dropdown menu showing options: 全部 (Selected), 用户组, 用户, 外部用户, 本地用户, 证书用户, 禁用用户.

点击『类型』、『描述』、『其他信息』、『状态』等标签后的▼，即可对用户/用户组进行升降序排列。

在【用户管理】界面勾选用户（组），然后点击删除按钮即可批量删除用户（组）。

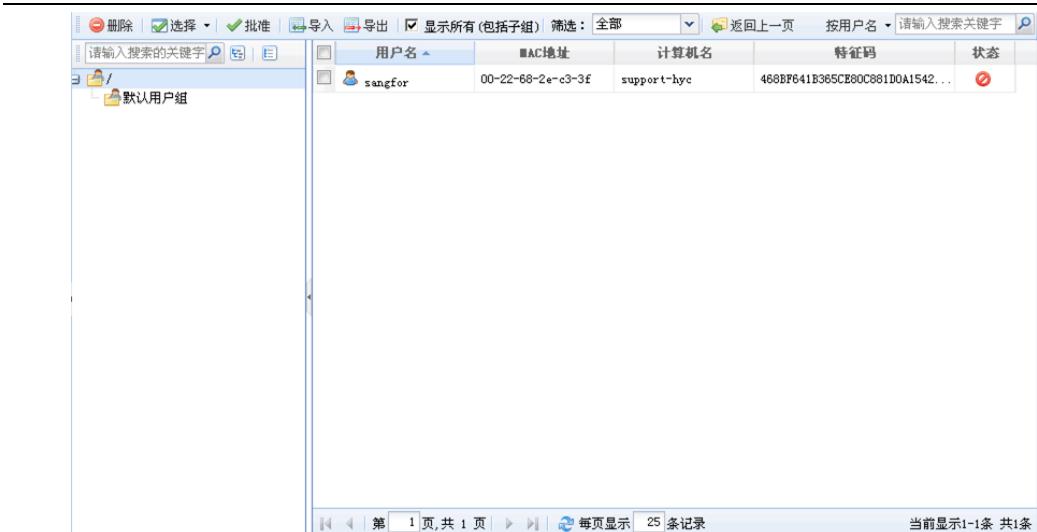
勾选好某个目标用户（组），点击编辑按钮，可进入用户（组）信息编辑页面，对目标用户（组）进行修改。

点击选择按钮，可以按照用户、用户组选择显示当前页或者所有页上的用户。也可以取消选择，如下图：



### 3.3.6.3.4 特征码管理

点击特征码管理按钮，进入【特征码管理】配置页面，如下图所示：



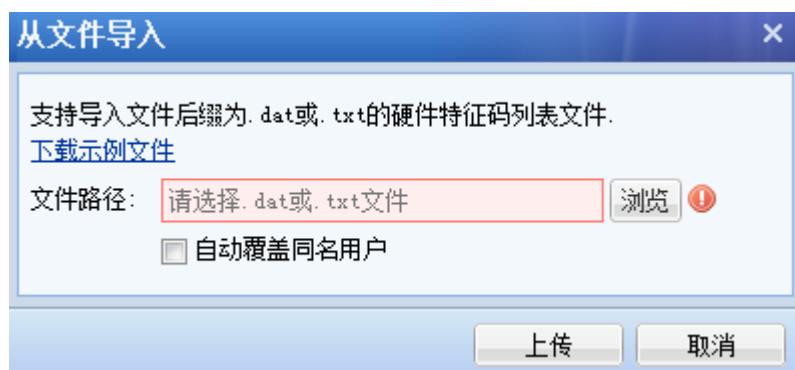
The screenshot shows a user management interface. At the top, there are buttons for Delete, Select, Approve, Import, Export, and Search. The search bar contains the placeholder "请输入搜索的关键字". Below the toolbar is a table with columns: 用户名 (Username), MAC地址 (MAC Address), 计算机名 (Computer Name), 特征码 (Feature Code), and 状态 (Status). A single row is selected, showing the username "sangfor", MAC address "00-22-68-2e-c3-3f", computer name "support-hyc", feature code "488BF641B365CE80C881D0A1542...", and status "正常" (Normal). On the left, there's a sidebar with a tree view showing a root node and a "默认用户组" (Default User Group) node.

勾选用户，点击删除按钮即可批量删除用户特征码。

点击选择按钮，可以选择所有用户的特征码或者取消选择。

勾选用户，点击批准按钮即可批量审批用户特征码。

点击导入按钮，则手动导入用户的硬件特征码，如下图所示：

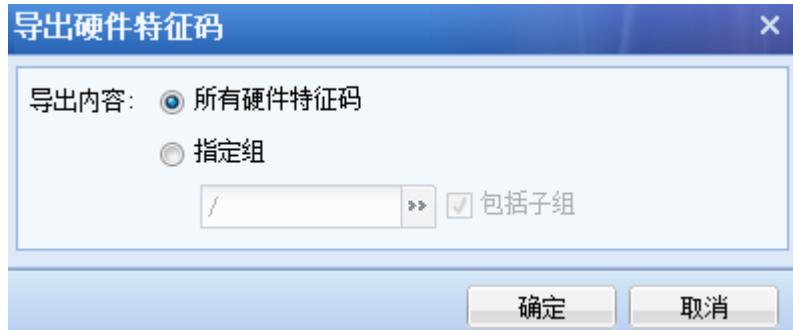


点击下载示例文件按钮，可以根据里面的示例格式来编写特征码文件。

勾选[自动覆盖同名用户]，则从文件导入特征码会自动覆盖列表中已有的同名用户的特征码。

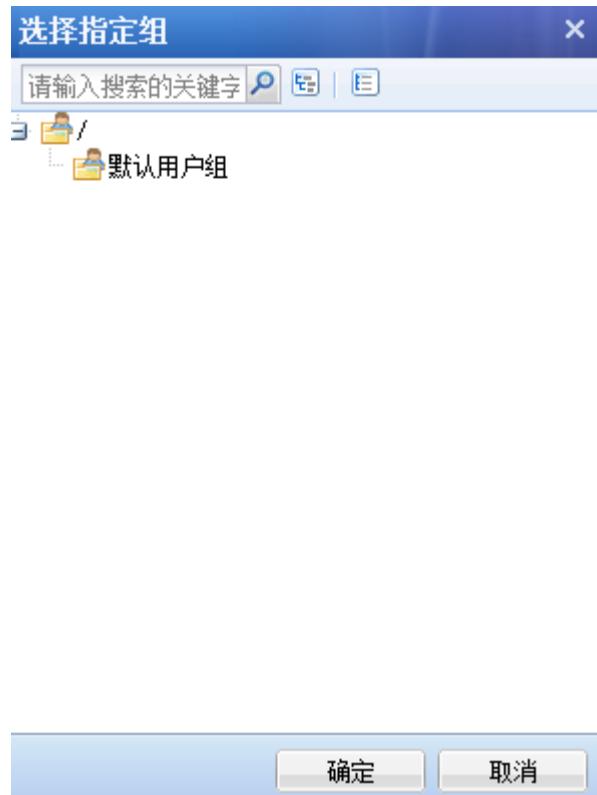
点击浏览按钮，选择编辑好的特征码文件，点击上传按钮即可。

点击**导出**按钮，则手动将列表中的硬件特征码导出到文件中，如下图所示：

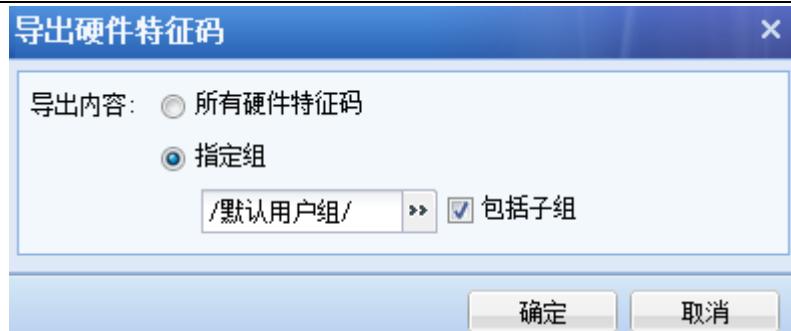


选择[所有硬件特征码]，则点击**确定**按钮，将列表中所有用户特征码全部导出到文件中。

选择[指定组]，点击下拉框，如下图所示：

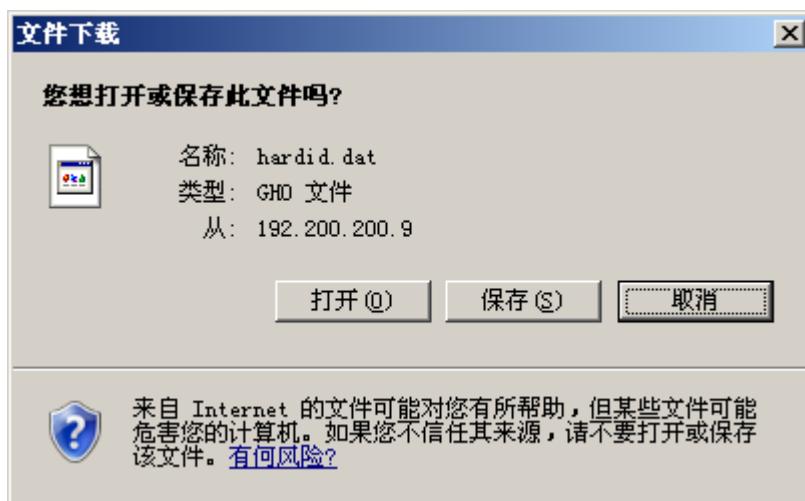


点击导出硬件特征码的用户组，点击**确定**按钮，如下图所示：



点击**确定**按钮，则将选定用户组中的用户的特征码导出到文件中。

如下图所示：



若勾选了[包括子组]，则选定用户组的子组所属用户的特征码也同样被导出。

勾选[显示所有（包括子组）]，则在列表中显示所有用户的硬件特征码，否则只显示当前用户组所属用户的硬件特征码。

在『筛选』中，可以分别选择显示[全部]、[已审批]、[未审批]的硬件特征码。

页面右上角的搜索，可以选择[按用户名]或[按计算机名]来搜索相应的硬件特征码。

### 3.3.6.3.5 导入用户

『用户管理』中的『导入』支持从文件导入用户：



The screenshot shows the 'User Management' interface. At the top, there are buttons for '新建' (New), '删除' (Delete), '编辑' (Edit), '选择' (Select), and '特征码管理' (Feature Code Management). Below these are search fields for '请输入搜索的关键字' (Enter search keyword) and '高级搜索' (Advanced search). A toolbar includes '导出' (Export), '移动' (Move), '其他操作' (Other operations), and '查看资源' (View resources). A link '显示所有(包含子组)' (Show all (including subgroups)) is also present. The main area shows a tree view under '默认用户组' (Default User Group) with three items: '默认用户组', 'test', and 'yangtao'. To the right is a table with columns '名称' (Name), '类型' (Type), '描述' (Description), '其他信息' (Other information), and '状态' (Status). The table contains three rows corresponding to the users in the tree view.

名称	类型	描述	其他信息	状态
默认用户组	用户组	系统保留的用户组,不能被删除	公用用户组	✓
test	用户	系统保留的用户组,不能被删除	私有用户	✓
yangtao	用户	yangtao	私有用户	✓

选择[从文件导入]，如下图所示：



可以通过 csv 文件批量导入用户的账号，支持“用户名”、“所属组路径”、“密码”、“手机号码”、“用户描述”等信息的导入，其中“用户名”为必填项，其他均为选填项，点击[下载示例文件](#)，查看编写导入文件的格式。

勾选[未指定用户组的用户导入到]，在下拉框中选择用户组，那么没有在文件中指定用户组的用户就会被导入到该用户组中。

勾选[用户所属组不存在时，自动创建]，如果在本地没有该用户组就会自动创建新用户组。

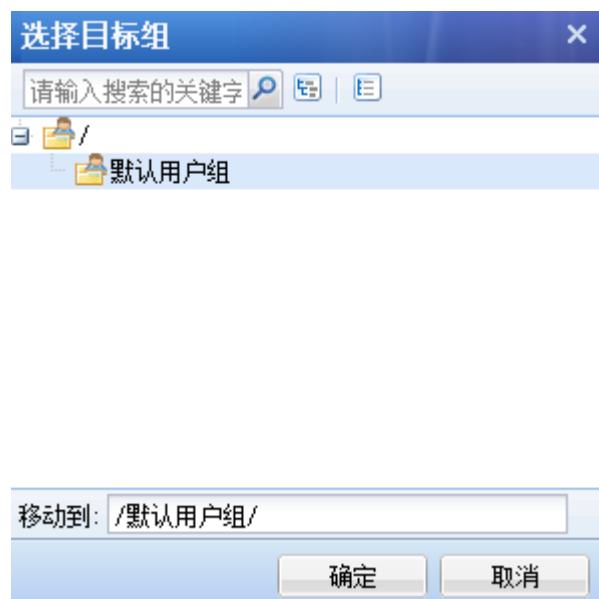
对于本地已存在的用户，若选择[继续导入，覆盖已存在的用户]，当所导入

用户列表中的用户账号和设备用户列表中的原有用户名字冲突（相同），新导入的用户信息会覆盖原有的用户信息；若选择[跳过，不导入该用户]，则不导入。

选择编辑好的文件，点击下一步，完成。

『用户管理』中的『移动』功能，可以将列表中选定的用户或用户组移动到其他用户组，

如下图所示：



选择想要移动到的目标用户组，点击确定按钮，那么在用户管理列表中选定的用户或用户组就会移动到该用户组。

### 3.3.6.3.6 其他操作

『用户管理』中的『其他操作』功能，包括[导出]、[绑定角色]和[高级搜索]。

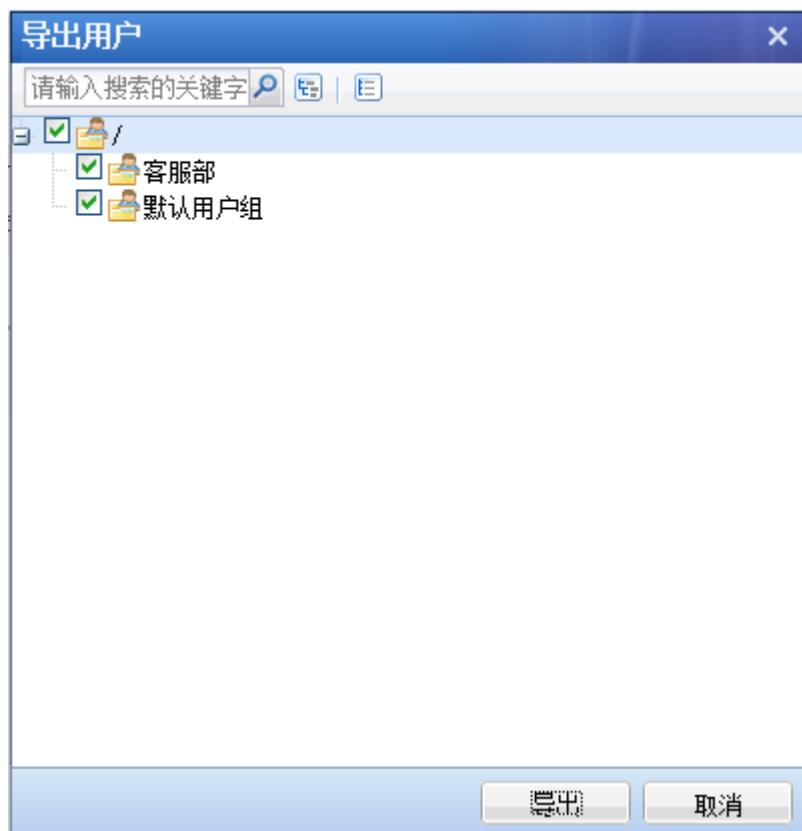


### 3.3.6.3.6.1 导出

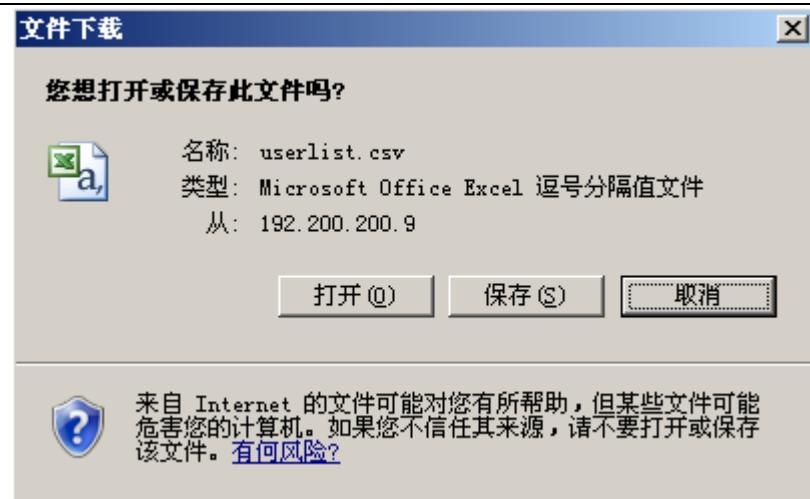
点击**导出**按钮，如下图所示：



点击选择**导出内容**按钮会显示出所有的用户组，如下图所示：



勾选需要导出的用户组，点击**导出**按钮，即可导出后缀为 csv 的文件，如下图所示：



导出信息包含所勾选的用户组中用户的用户名，所属用户组，密码（经过深信服科技研发的私有算法加密），手机号码，描述，最近一次登录信息，如下图所示：

	A	B	C	D	E	F
1	#用户名	所属组路径	密码	手机号码	描述	最近一次登陆
2	test	/	{ cd58463272fe23534 }			2014/7/30 17:44
3	yangtao	/	{ e8ac0cb11b9b2cea7 }	18688888888	yangtao	2014/7/27 20:39
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						

### 3.3.6.3.6.2 绑定角色

在『用户管理』列表中选择用户或用户组，点击**绑定角色**按钮，在此处可以给用户或用户组关联角色，如下图所示：

### 已绑定的角色

+ 添加关联 - 删除关联

角色名称	描述
没有记录	

第 1 页, 共 1 页 | 每页显示 25 条记录 | 提交 取消

点击**添加关联**按钮，会显示出所有在『角色授权』中定义的角色，如下图所示：

### 新增关联角色

请输入搜索关键字

角色名称	描述
测试	

第 1 页, 共 1 页 | 每页显示 25 条记录 | 确定 取消

勾选角色，点击确定按钮，给用户绑定角色成功，如下图所示：



已绑定的角色

+ 添加关联 - 删除关联

角色名称	描述
测试	

第 1 页, 共 1 页 | 每页显示 25 条记录 | 当前显示 1-1 条, 共 1 条

提交 取消

点击提交按钮，保存配置。

### 3.3.6.3.6.3 高级搜索

点击高级搜索按钮，如下图所示：



高级搜索

关键字: 全部

搜索对象: 全部

认证类型: 所有类型

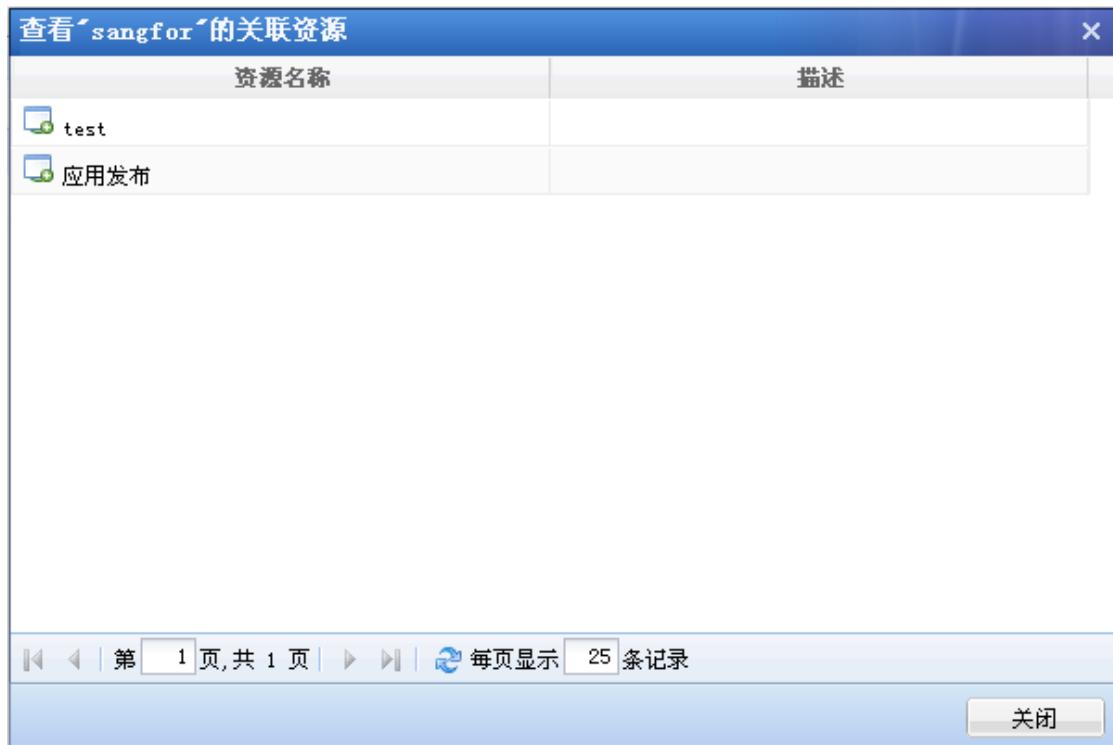
帐户过期: 3 天内过期

确定 取消

可以根据包含关键字、搜索对象、认证类型来查询相应的用户。

### 3.3.6.3.7 查看资源

在『用户管理』选择某一个用户或用户组，点击查看资源按钮，则会显示所关联的资源，如下图所示：



上图中显示用户“sangfor”关联了两个资源“test”和“应用发布”。

勾选[显示所有（包括子组）]，则会把所有用户都显示到当前页面列表中。

### 3.3.6.4. 资源管理

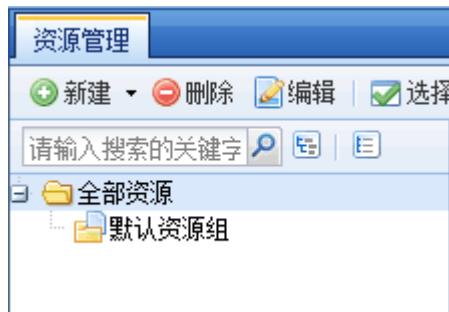
『资源管理』的主要作用是用户定义 SSL VPN 内网的可用资源。

#### 3.3.6.4.1 资源组

为了更好地对资源进行管理、更符合用户使用习惯，以及 SSL VPN 客户端

可以更有条理地显示，可以把多个“资源”添加到“资源组”。在资源列表，点击不同的“资源组”显示出该资源组对应“资源”。

系统默认存在一个『默认资源组』，界面如下图所示：

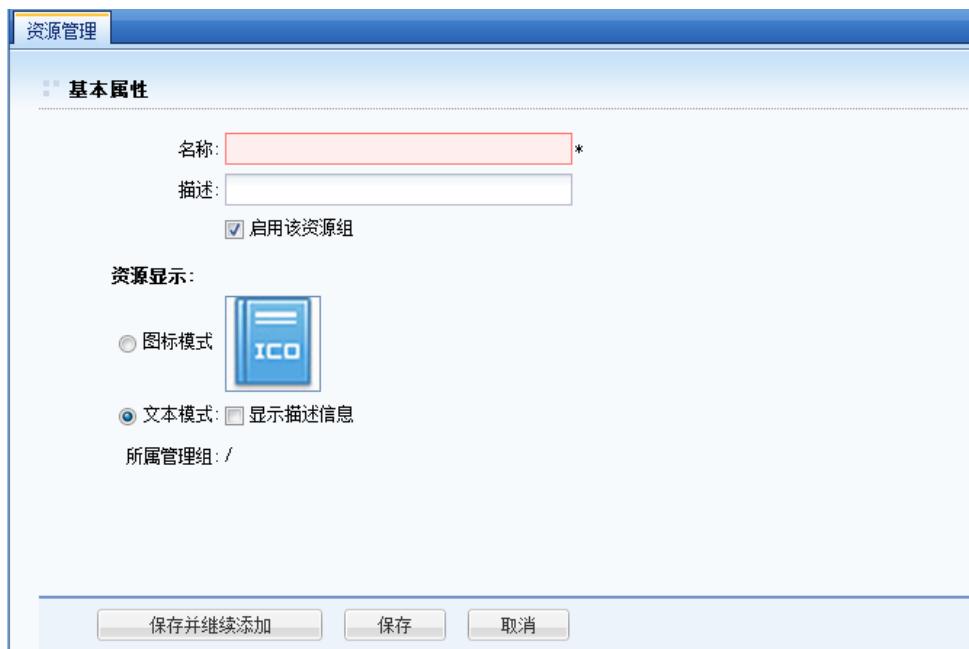


『默认资源组』系统默认保留的资源组，只能够修改，不允许删除。

点击**新建**按钮，选择[资源组]，如下图：



弹出的编辑界面如下图所示：



『名称』和『描述』可随意填写便于理解记忆的文字，在『名称』中填写的文字会显示在 SSL VPN 用户成功登录后，出现的“资源组列表”中。

同一个资源组内的资源在“资源组列表”能够以“图标”或“文本”两种方式显示。

选择[文本显示]，可勾选右边的[显示描述信息]，在“资源组列表”中显示出该“资源组”内“资源”的描述信息。最后点击**保存**。

『所属管理组』即该“资源组”能被哪些管理员编辑和使用。

### 3.3.6.4.2 TCP 应用

『TCP 应用』主要用于定义各种类型的 SSL VPN 内网资源，以适应各种各样基于 TCP 协议的应用程序访问 SSL VPN 内网资源的需求。

在『资源管理』页面，点击**新建**按钮，如下图：



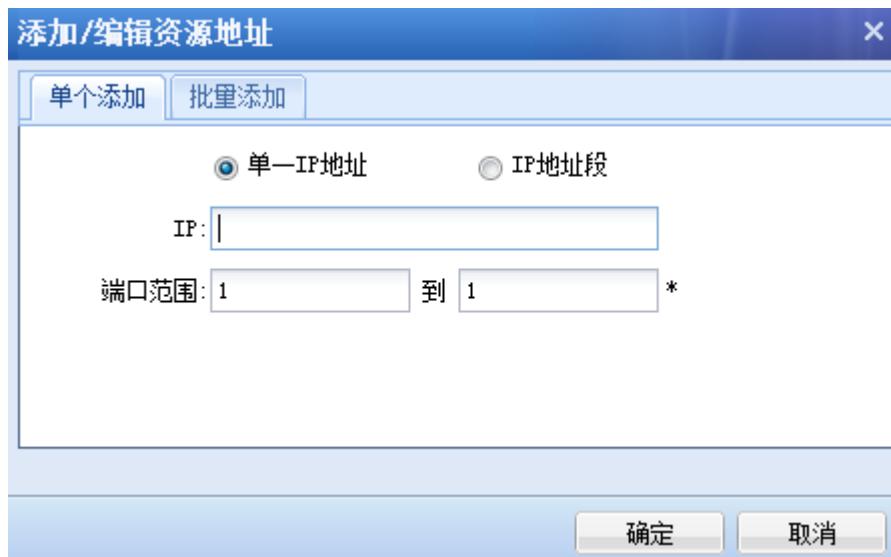
选择[TCP 应用]，弹出对话框，设置界面如下：



『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 SSL 用户成功登录 SSL VPN 后出现的“资源列表”中。

『类型』选择所建立『TCP 应用』的服务类型，设备内置了常用应用服务的定义，直接选择则会在编辑地址的页面中自动填写端口范围，如无所需的类型，可选择底部的[other]，然后自定义该服务所使用的『端口范围』。

『地址』填写提供 TCP 应用的服务器地址，支持『单一 IP 地址』和『IP 地址段』的形式，如下图所示：



『应用程序路径』此处填写某些 C/S 结构服务可能用到的客户端软件的路径。

『所属组』后面下拉框可以将该资源划入相应的“资源组”，默认属于“默认资源组”（资源组的具体设置可参考 3.3.7.4.1“资源组”章节）。

如果不勾选[允许用户可见]选项，则登录 SSL VPN 后，在“TCP 应用列表”

中不显示该资源的信息，但实际上该资源是可用的。隐藏资源有利于保护内网资源服务器的信息。



1、首次使用『TCP 应用』时计算机会自动安装控件，需要以 administrator 登录系统才可以安装上。若 PC 上有防火墙或杀毒软件，可能会阻挡 PC 安装插件，可先关闭防火墙或杀毒软件。

2、TCP 应用不支持文件共享类的资源。

### 3.3.6.4.3 L3VPN

『L3VPN』主要用于定义、配置和管理各种基于 IP 协议的 SSL VPN 内网资源，以适应各种各样不同协议（TCP/UDP/ICMP）的应用程序访问 SSL VPN 内网资源和内网服务器。

在『资源管理』页面，点击新建按钮，如下图：



选择[L3VPN]，弹出【编辑 L3VPN 资源】对话框，设置界面如下：

» 编辑L3VPN资源

基本属性

标记\*的为必须填写项目

名称:  \*

描述:

类型:  协议:

地址:   


应用程序路径:  浏览  
程序路径可以使用绝对路径也可以使用环境变量, 例如%windir%

所属组: 默认资源组

图标: 

启用该资源  
 允许用户可见

『名称』和『描述』可随意填写便于理解记忆的文字，『名称』填写的文字会显示在 SSL 用户成功登录 SSL VPN 后，出现的“资源列表”中。

『类型』选择该 L3VPN 资源的协议类型，SSL VPN 内置了常用应用服务的定义，直接选择设备会自动识别端口范围和协议，如无所需的类型，可选择『Other』，设置协议，然后自行设定下面的『端口范围』。

若类型选择为[OTHER]，则需要选择『协议』，可选择为 TCP、UDP 或 ICMP，根据定义『L3VPN』所使用的协议进行选择。

『地址』填写提供 L3VPN 服务的服务器地址，支持“单 IP 或域名”和“IP 段”的形式。点击 ，弹出【添加/编辑资源地址】对话框，可单个添加，也可批量添加，如下图：



『端口范围』定义该『L3VPN』所使用的端口，已预定义好的资源类型一般不需修改，如果前面『类型』选择了『Other』，则填写该服务所使用的端口。

『启用资源地址伪装』：勾选后将隐藏资源的真实地址，防止内部服务器地址泄露。

#### 3.3.6.4.4 其它操作

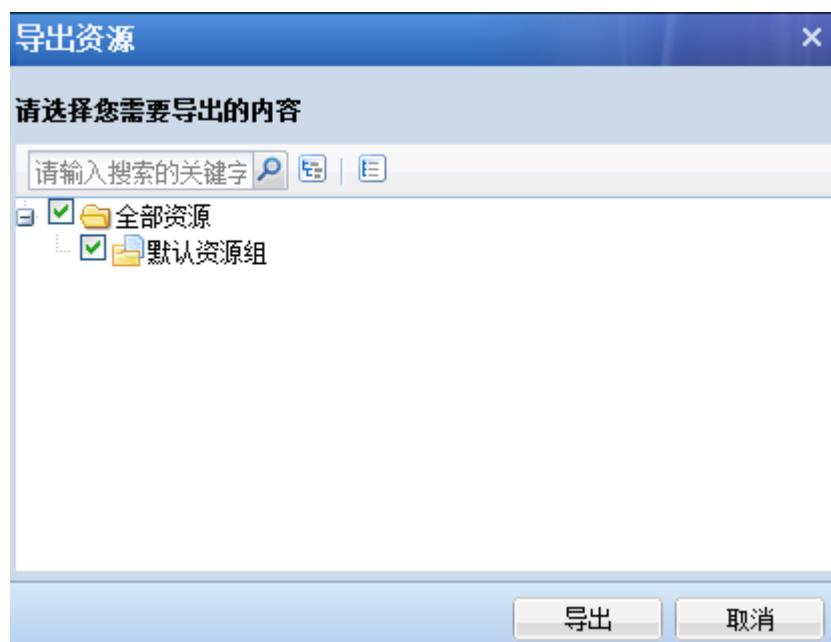
其它操作包括『导出资源』、『导入资源』和『资源排序』



#### 3.3.6.4.4.1 导出操作

『导出资源』即将『资源管理』中的资源导出到一个文件中。

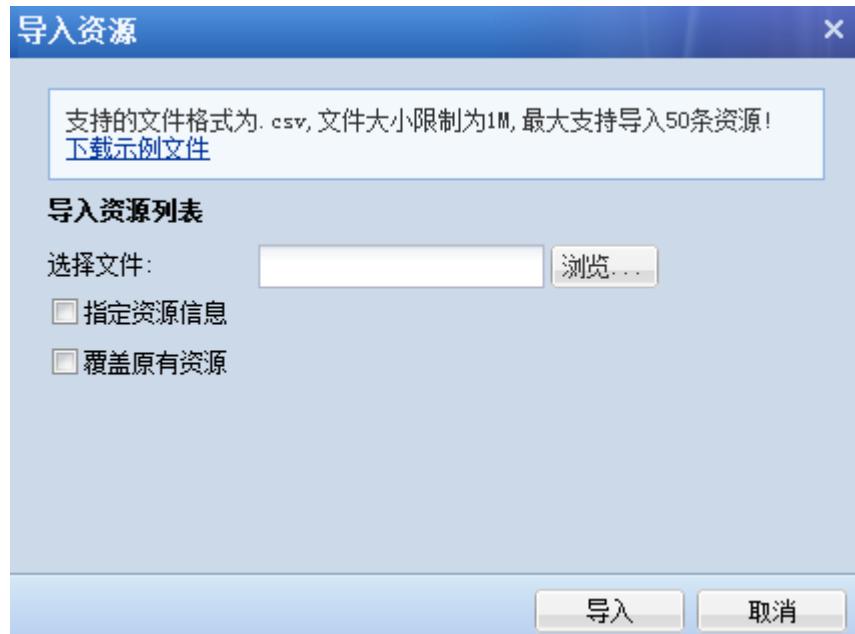
如下图所示：



点击导出按钮，将资源保存在默认生成的 rclist.csv 文件中。

#### 3.3.6.4.4.2 导入操作

『导入资源』将编辑好的资源通过文件导入到『资源管理』中。



可以通过[下载示例文件](#)来编辑资源，将编辑完成的.csv 格式的文件导入设备。

通过[指定资源信息]可以将文件中的资源导入到已存的资源组中，还可以指定添加描述信息。

勾选[覆盖原有资源]，若导入的资源名称和原有的资源名称冲突，则覆盖原有资源。

#### 3.3.6.4.4.3 资源排序

『资源排序』可以对资源组中的各个资源进行排序。可通过[上移](#)、[下移](#)、[移到底部](#)或[移到顶部](#)来调整资源顺序。如下图：

» 资源排序

-调整服务页面资源组内资源显示的顺序！

移到顶部 上移 下移 移到底部

	资源名称	描述
1	写字板	写字板
2	Microsoft Office Word	Microsoft Office Word
3	Microsoft Office Excel	Microsoft Office Excel
4	Microsoft Office PowerPoint	Microsoft Office PowerPoint
5	Adobe Reader	Adobe Reader
6	易飞ERP系统	易飞ERP系统

除了上述操作外，在资源管理页面，还可对资源进行**删除**、**编辑**、**移动**、

**筛选**等操作：

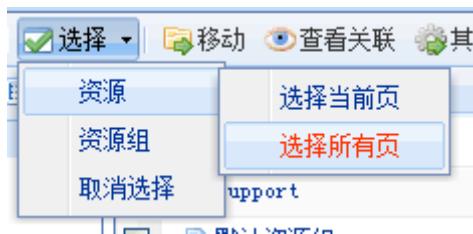
» 资源管理

新建 删除 编辑 选择 移动 查看关联 其它操作 筛选 全部

勾选相应的资源，点击**删除**，即可删除该资源。

勾选相应的资源，点击**编辑**，可以对该资源进行编辑。

点击**选择**，可选择当前页或选择所有页的资源，若之前已经选择了资源，也可以取消选择。如下图：



勾选相应的资源，点击**移动**，可将选中的资源移动到其它资源组中。



注：移动的时候，只能移动资源，不能移动资源组。

勾选相应的资源，点击**查看关联**，可以查看该资源被哪些用户关联，如下图：

查看：“SSO”	
授权访问的组或用户	路径
1 zj	/默认用户组
2 客服部	/客服部

第 1 页, 共 1 页 | 每页显示 25 条记录 | 当前显示1-2条 共2条 | 取消

『筛选』可以根据资源组或资源类型选择显示的资源。可选择显示[全部]、[资源组]、[TCP 应用]和[L3VPN 应用]。



### 3.3.6.5. 角色授权

#### 3.3.6.5.1 新建角色

『角色授权』是“用户/用户组”和“资源”的中介，SSL VPN 正是通过『角色授权』把 SSL VPN 登录用户/用户组和 SSL VPN 内网资源“关联”起来的。通过角色可以把多个“用户/用户组”、多个资源进行关联，更加有效管理资源和用户组的权限。

操作界面如下图所示：



The screenshot shows a software interface titled "角色授权" (Role Authorization). At the top, there is a toolbar with icons for "新建" (New), "删除" (Delete), "编辑" (Edit), "选择" (Select), and "生成权限报告" (Generate Permission Report). To the right of the toolbar is a search bar labeled "按名称" (Search by Name) with a placeholder "请输入搜索关键字" (Please enter search key) and a magnifying glass icon. Below the toolbar is a table with two columns: "角色名称" (Role Name) and "描述" (Description). A single row is visible, showing "测试" (Test) in the first column and "yangtao" in the second column. The status of this row is indicated by a green checkmark icon.

在右上角的输入框内填上需要搜索的目标角色的部分名字，点击即可筛选出符合条件角色，可以按名称、按描述、按关联的用户（组）来查找角色。

『角色名称』显示角色的名称。

『描述』用来显示角色的描述信息。

『授权给』显示关联了该角色的用户。

点击，用来编辑勾选的角色。

点击，用来删除勾选的角色。

点击，可以选择当前页或选择所有页。

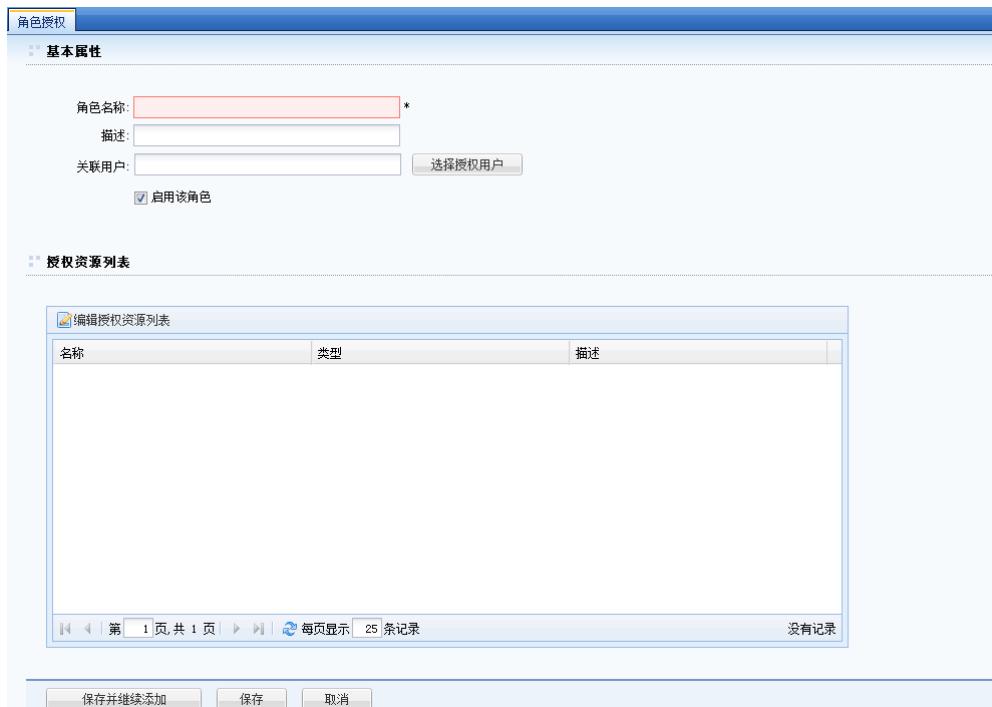


在角色管理页面，点击，可新建角色，如下图：



The screenshot shows the same "角色授权" (Role Authorization) interface. The "新建" (New) button in the toolbar is highlighted with a yellow box. A tooltip "新建角色" (New Role) appears above the "新建" button. Below the toolbar, a message box is displayed with the text "以所选角色为模板新建" (Create new role based on selected role template).

选择【新建角色】，弹出【新建角色】编辑页面，如下图：



角色授权

基本属性

角色名称:  \*

描述:

关联用户:

启用该角色

授权资源列表

名称	类型	描述
没有记录		

保存并继续添加

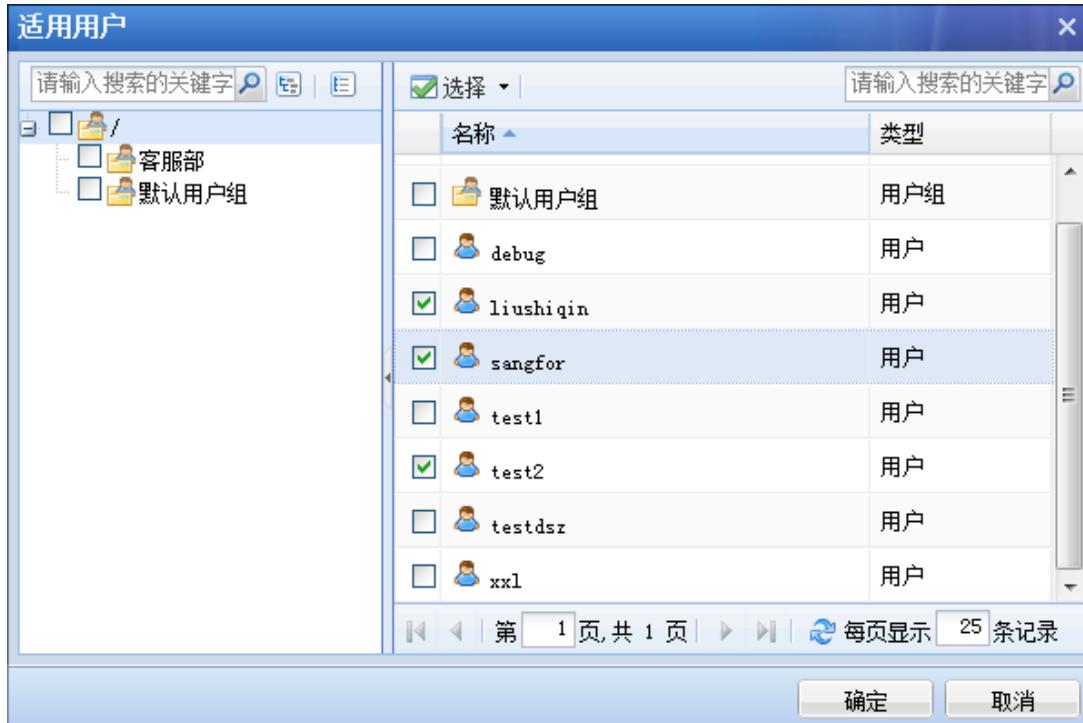
『角色名称』该条角色的名称，自定义即可。

『描述』可随意填写便于理解和记忆的描述语言。

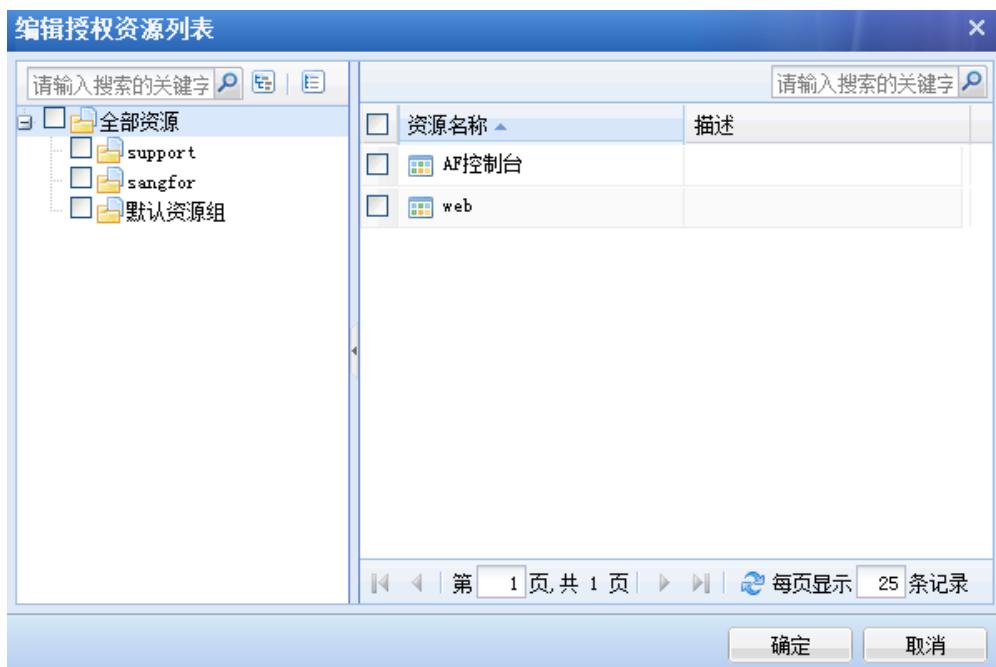
『关联用户』选择关联该条角色的用户或者用户组。

点击  按钮，下面的列表会列出『用户管理』中所定义好的用户/组（定义用户/组，请参考 3.3.7.3 章节），在列表中勾选相应的用户/组，即可完成“用户/组的关联”，属于该角色的用户，会具有访问该角色关联资源的权限。

界面如下图所示：



在『授权资源列表』设置中，可以设置该角色需要关联的资源。点击**编辑授权资源列表**按钮，弹出【编辑授权资源列表】页面，选择相应的资源。（资源添加请参考 3.3.7.4 章节）界面如下图所示：



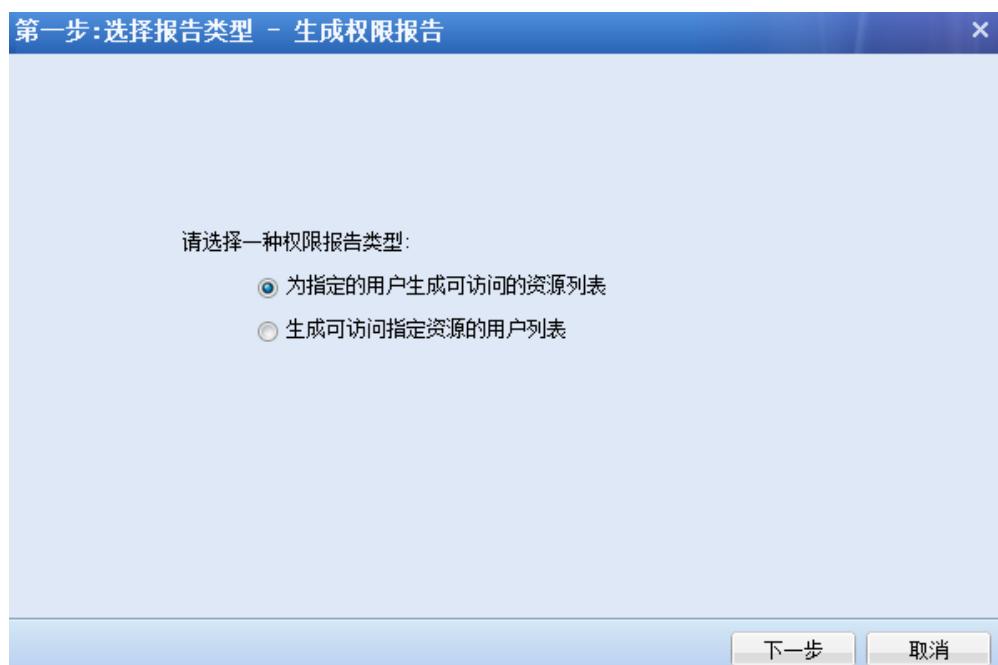
选择资源，然后点击**确定**按钮。确定保存。

最后点击**保存**，即完成一条角色配置。

### 3.3.6.5.2 生成权限报告

『生成权限报告』用来生成显示用户可访问资源的报表。

如下图所示：



勾选[为指定的用户生成可访问的资源列表]，点击**下一步**按钮，如下图所示：

第二步:选择用户 - 生成权限报告

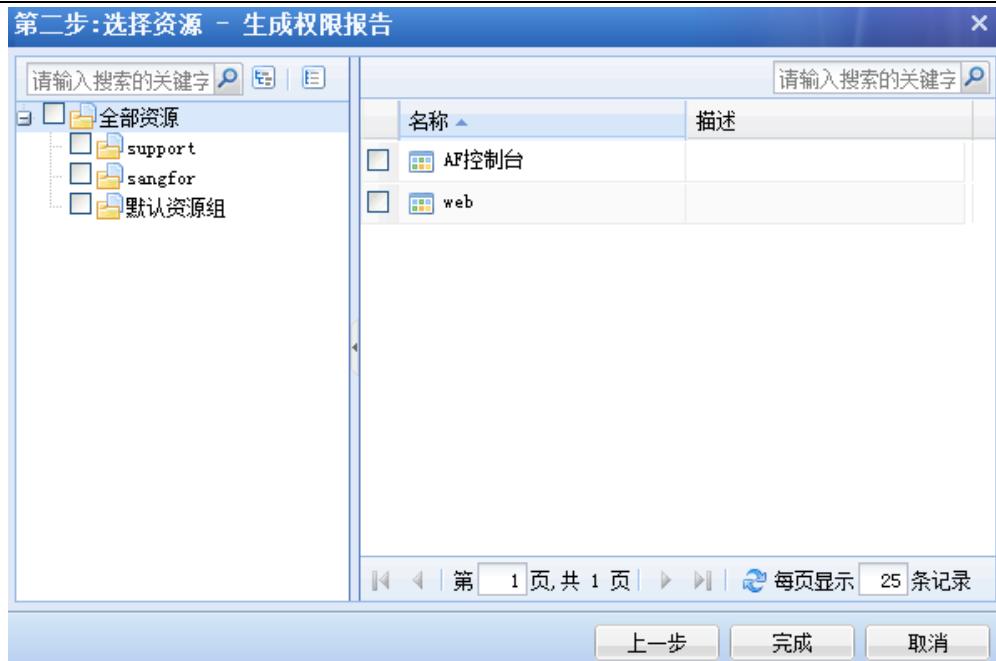
名称	类型
默认用户组	用户组
test	用户
yangtao	用户

第 1 页, 共 1 页 | 上一步 完成 取消

选择用户，点击完成，生成“.csv”格式的文件，如下图所示：



勾选[生成可访问指定资源的用户列表]，点击下一步按钮，如下图所示：



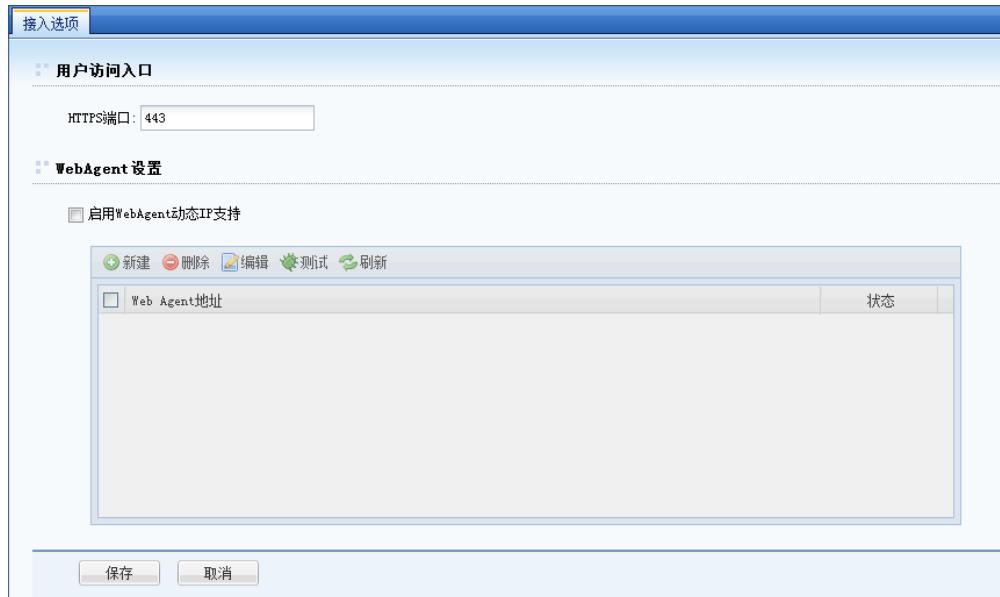
选择资源，点击完成，生成“.csv”格式的文件，如下图所示：



### 3.3.6.6. 接入选项

『接入选项』用于设置登陆 SSL VPN 的端口， webagent 设置等。

界面如下图所示：



『用户访问入口』设置 SSL VPN 服务监听端口。

『HTTPS 端口』设置 HTTPS 的监听端口，默认值为 TCP 443 端口。



1.如果更改了这些标准的协议端口，则访问 SSL 登录页面时，需要在主机地址后面添加端口来登录，所以，如无必要，请勿修改。

『Webagent 设置』当设备在没有固定公网 IP 的情况下，需要建立 SSL VPN，必须使用 WebAgent 动态寻址。

勾选『启用 WebAgent 动态 IP 支持』，即启用 WebAgent 动态寻址功能。可以在这里新增/删或修改 WebAgent。

『Webgent 地址』用于显示 Webagent 地址。

『状态』显示当前 Webagent 的状态。

点击**新建**即可新增一条 Webagnet。点击后如下图：



在弹出的输入框中输入申请到的 Webagent 地址，点击**确定**。

勾选相应的 webagent 地址，点击**Test**，如果弹出如下框的提示，证明填写正确。



勾选相应的 Webagent 地址，点击**Delete**或**Edit**可以进行删除或编辑 webagent 地址。

点击**Refresh**，可以刷新 Webagent 的当前状态。

最后点击**Save**。

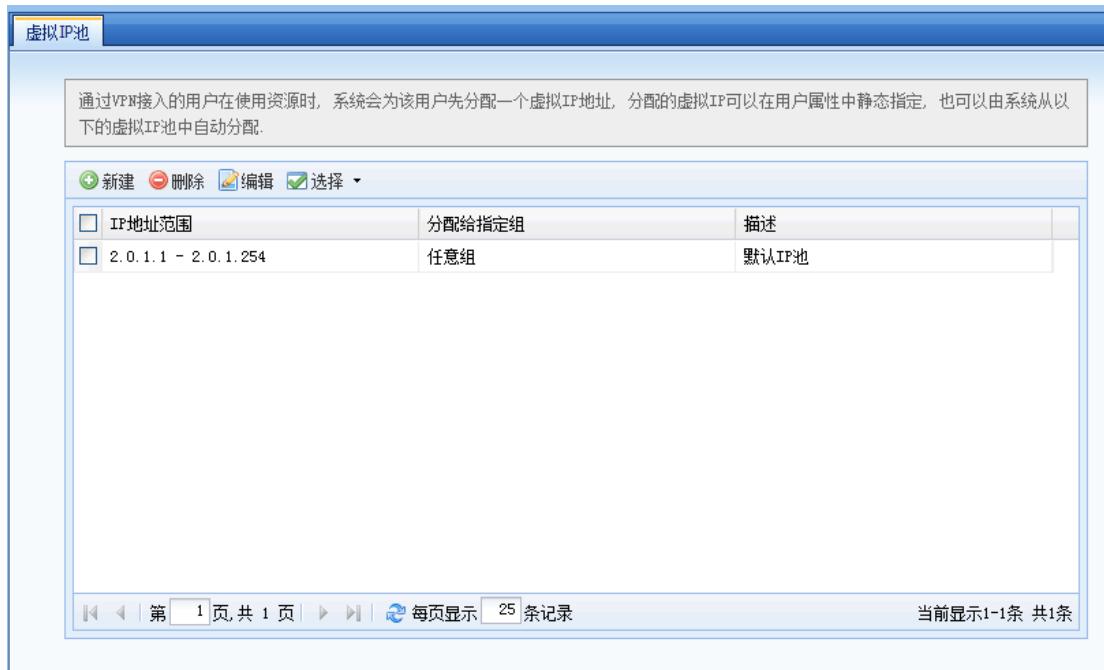


1、如果是 AF 部署在内网，公网 ADSL 拨号，通过端口映射访问 SSL VPN 的环境，不支持 Webagent 寻址。

### 3.3.6.7. 虚拟 IP 池

此页面设置 SSL VPN 用户登录访问总部 L3VPN 资源时使用的虚拟 IP。该 IP 不能够和内网其它地址冲突，建议设置成比较生僻的 IP 段，或保留默认的 2.0.1.1—2.0.1.254 等。

界面如下所示：



IP地址范围	分配给指定组	描述
2.0.1.1 - 2.0.1.254	任意组	默认IP池

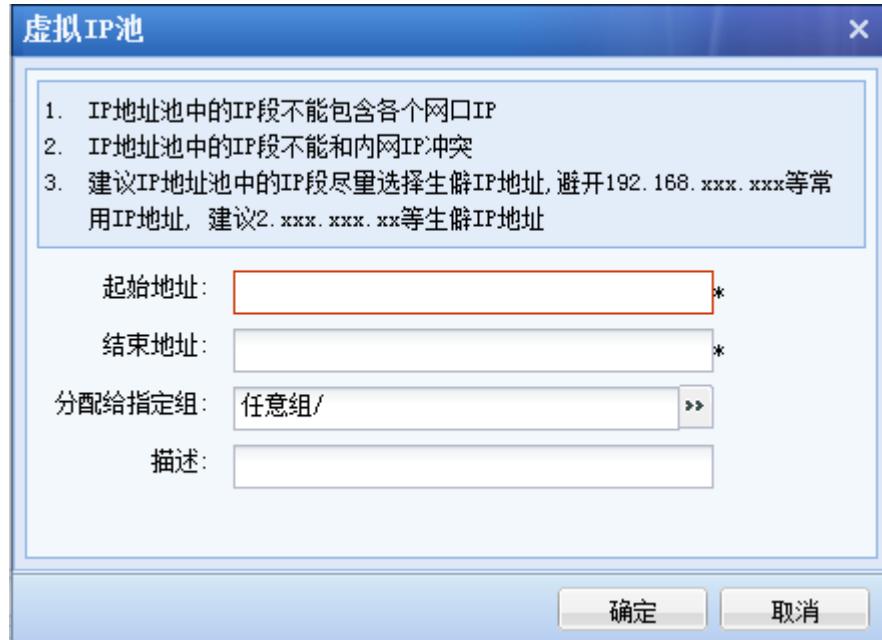
『IP 地址范围』指该虚拟地址池的起始 IP 和结束 IP。

『分配给指定组』是标识该虚拟地址池分配给指定的用户组。

『描述』该 IP 池的相关说明信息，可任意填写。

**删除**和**编辑**能够对被勾选上的地址池进行删除和编辑操作。点击**选择**选中所有规则或者取消所有选择。

点击**新建**按钮，出现【虚拟 IP 池】对话框，如下：



1. IP 地址池中的 IP 段不能包含各个网口的 IP。

2. IP 地址池中的 IP 段不能和内网 IP 段冲突。

点击**确定**，保存配置。

### 3.3.6.8. 登录管理

『登陆管理』用来设置登录页面的模板，供用户选择使用。

『页面标题』用来设置登陆 SSL VPN 后页面显示的标题信息。

『背景色』用来设置登陆 SSL VPN 后页面的背景颜色。

『公告信息』可以编写一些公告或者提示信息，支持 HTML，不能超过 1024 个字符。

### 3.3.6.9. 认证设置

『认证设置』包含『主要认证』、『辅助认证』和『认证选项设置』。

界面如下图所示：



#### 3.3.6.9.1 主要认证

主要认证方式包括本地密码认证。点击本地密码认证后面的【设置】，弹出界面如下图所示：

认证设置

**密码安全策略**

启用密码安全策略 (注意: 密码策略只对本地密码认证的私有用户有效!)

密码不能包含用户名

新密码不能与旧密码相同

限定密码最小长度为  位

每隔  天用户必须修改密码, 密码过期前  天开始提醒用户修改密码

用户必须修改初始密码 (新建用户第一次登录必须修改密码)

密码必须包括  数字  字母  特殊字符 (shift+数字)

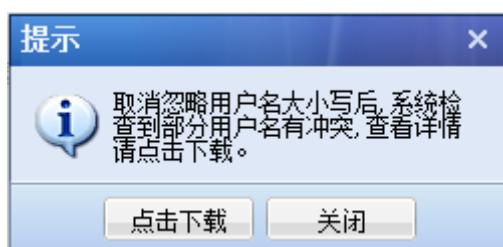
**用户名策略**

用户名不区分大小写

保存 取消

『密码安全策略』用于设置用户的一些密码策略，详细可参见上图。启用密码安全策略后，用户下次登录会进行密码安全检查，不符合安全策略的会要求修改密码。

『用户名策略』用户登录时，设置是否区分输入用户名的大小写。如果在启用该选项之前，组织结构中已经存大小写不同的相同用户名，则会修改失败并导出同名用户，需要先修改冲突的用户名，再启用该选项。



注意：上述策略只对本地密码认证的用户有效。

### 3.3.6.9.2 辅助认证

『辅助认证』包含『硬件特征码』的认证方式。

『硬件特征码』根据计算机的硬件特性按一定的算法生成的一个序号，由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的，所以对于不同的计算机，此序号必然不同。

『硬件特征码』用于对用户的硬件特征码权限进行设置。



点击[设置](#)，弹出页面如下图所示：



[启用硬件特征码收集]选择此项，则设备只收集用户登录的硬件特征码，但不会启用硬件特征码认证。

[启用硬件特征码认证]选择此项，则开启硬件特征码认证。

『自定义提示信息』提示用户提交硬件特征码时的用语。

[自动审批]勾选此项后，用户提交的硬件特征码不需要管理员手工审批，可自动通过审批。

[所有已审核的终端上，允许任意账号登录]勾选此项后，如果某一用户使用的计算机提交了硬件特征码并通过了审批，则其他用户用此计算机登录所提交的硬件特征码可自动通过审批。

[每个用户可拥有的硬件特征码个数]用于设置一个用户可对应几个硬件特征码。

点击**保存**使配置生效。

### 3.3.6.9.3 认证选项设置

『认证选项设置』包含『密码认证选项』。

『密码认证选项』用于设置当用户通过用户名密码方式认证登录 SSL VPN 时的一些相关选项设置。



点击设置，弹出页面，包含『用户登录时校验选项』和『防止暴力破解选项』，如下图：

认证设置

用户登录时校验选项

启用软键盘 (防止木马记录键盘输入信息)  
 字母键随机变化  数字键随机变化

防止暴力破解选项

连续登录错误  次, 启用图形验证码 (输入0表示强制启用; 小于3时, 非windows客户端仍然以3次为标准)  
 同名用户登录连续出错  (1-32)次后锁定用户  (30-1800)秒后恢复正常状态  
 同IP用户登录连续出错  (64-2048)次后拒绝同IP登录, 并在  (30-1800)秒后恢复正常状态

1. 登录连续出错是指两次登录错误间隔在45秒之内;  
2. 同名用户登录连续出错次数设置范围为1至32次;  
3. 同IP用户登录连续出错次数设置范围为64至2048次;  
4. 恢复正常状态时间值设置范围为30至1800秒, 0表示永远锁定, 需管理员手动释放.

保存 取消

『用户登录时校验选项』的配置页面如下：

用户登录时校验选项

启用软键盘 (防止木马记录键盘输入信息)  
 字母键随机变化  数字键随机变化

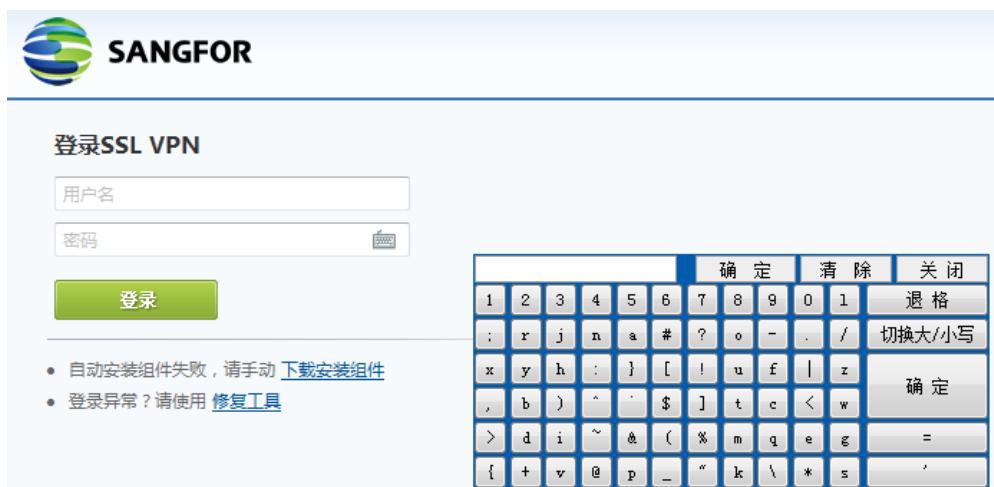
勾选[启用软键盘]，可以在 SSL VPN 登录页面启用软键盘和图形校验码，增强登录的安全性。勾选[启用软键盘]并勾选[数字顺序变化]或[字母顺序变化]则每次登录时数字顺序或字母顺序都会改变。如下图所示：

勾选『启用软键盘』，打开登录页面：



The screenshot shows the Sangfor SSL VPN login interface. It features a logo at the top left and a title "登录SSL VPN" (Log in to SSL VPN). Below the title are two input fields: "用户名" (Username) and "密码" (Password), each accompanied by a small keyboard icon. A green "登录" (Login) button is centered below the password field. At the bottom of the page, there are two bullet points: "自动安装组件失败，请手动 [下载安装组件](#)" (Automatic component installation failed, please download and install components manually) and "登录异常？请使用 [修复工具](#)" (Login abnormal? Please use the repair tool).

点击密码输入框后的小键盘图标，页面如下：



This screenshot shows the same login page as above, but with a virtual keyboard overlayed on the right side of the password input field. The keyboard has standard letters and symbols, with additional function keys like "确定" (Confirm), "清除" (Clear), and "关闭" (Close) at the top right. The text area at the bottom of the page remains the same, providing troubleshooting links.

『防止暴力破解选项』是一种安全机制，可设置用户用相同用户名连续输错多少次密码则冻结该用户，该用户在一段时间内将无法登录；或者用户用相同一个IP地址连续输错多少次密码，则启用图形验证码或者锁定该IP一段时间。配置如下图所示：

#### 防止暴力破解选项

连续登录错误  次，启用图形验证码（输入0表示强制启用；小于3时，非Windows客户端仍然以3次为标准）

同名用户登录连续出错  (1-32)次后锁定用户  (30-1800)秒后恢复正常状态

同IP用户登录连续出错  (64-2048)次后拒绝同IP登录，并在  (30-1800)秒后恢复正常状态

1. 登录连续出错是指两次登录错误间隔在45秒之内；
2. 同名用户登录连续出错次数设置范围为1至32次；
3. 同IP用户登录连续出错次数设置范围为64至2048次；
4. 恢复正常状态时间值设置范围为30至1800秒，0表示永久锁定，需管理员手动释放。

图形验证码选项设置中，输入0表示强制启用，即默认启用图形验证码；输入小于3时，非Windows客户端仍然以3次为标准。

### 3.3.6.10. 设备证书

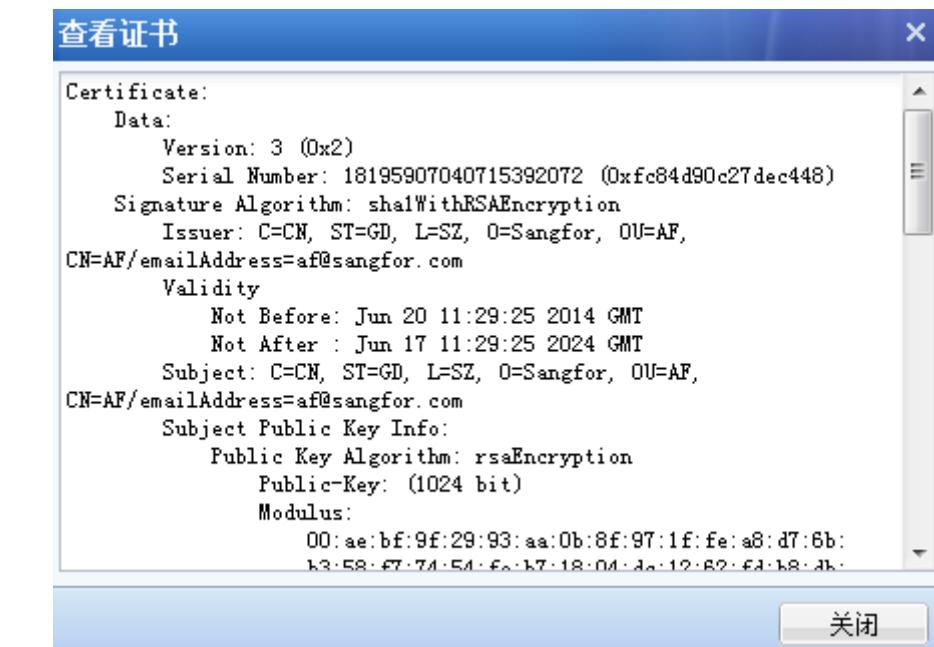
『设备证书』用于配置设备的证书，证书将用于客户端与设备建立SSL会话。

界面如下图所示：



设备支持国际商用密码标准(RSA)。

点击查看则可以查看设备当前的证书，显示如下：



点击**下载**则可以把设备证书下载下来。点击**更新**，则可以重新导入新的设备证书，将之前的设备证书替换掉。

在[为设备生成一个证书请求]下点击**下载**，即新生成一个证书请求，选择证书保存路径保存证书。显示如下：



注：这里安装的证书格式类型只支持\*.crt 或\*.cer。

### 3.3.6.11. 资源服务选项

『资源服务选项』用于配置 L3VPN 应用类型资源的参数设置。界面如下图所示：



The screenshot shows the 'L3VPN Application' configuration page. Under 'Resource Access Mode', the first option 'Use the device's IP address as the source address' is selected. Under 'Transport Protocol Selection', the first option 'Only use TCP' is selected. Below these, the 'UDP Service Port' is set to 440. A 'Advanced Settings' button is also visible.

『资源访问模式』设置 L3VPN 资源的访问模式。如果选择使用设备的 IP 地址作为源地址，那么 SSL VPN 用户访问内网服务器资源时，服务器看到的源 IP 地址为 AF 设备在 SSL 部署模式中设置的内网口地址；如果选择使用分配的虚拟 IP 地址作为源地址，那么 SSL VPN 用户访问内网服务器资源时，服务器看到的源 IP 地址为虚拟 IP 地址。（虚拟 IP 设置参考章节 3.3.7.7 错误！未找到引用源。）

『传输协议选择』选择 L3VPN 应用的传输模式。

勾选[仅使用 TCP]，则在使用 L3VPN 应用的时候，只启用 TCP 隧道进行数据传输。

勾选[自动选择 TCP 或 UDP]，则会优先启用 UDP 隧道进行数据传输。

『UDP 服务端口』使用 UDP 隧道进行数据传输的端口，如果是单臂模式，需要前端网关设备映射端口给 AF 设备，默认是 442。

点击**高级设置**，设置设备虚拟网卡的地址范围。



The screenshot shows the 'Advanced Settings' section where the 'Virtual Network Card Address Range' is set from 1.1.1.1 to 1.1.1.254.

### 3.3.6.12. 内网域名解析

SSL VPN 支持需要通过内部域名才能访问的资源应用。内网存在此类应用时，一般有一台或多台内网 DNS 服务器，给内网电脑提供内网域名解析服务。通过 SSL VPN 需要访问此类应用时，可以通过『内网域名解析』配置来实现。

界面如下所示：



在『内网域名解析』中分别把内网 DNS 服务器的 IP 地址填写在『首选 DNS』和『备份 DNS』上，如果只有一台内网 DNS 服务器，则只需填写『首选 DNS』。然后在 SSL VPN 资源设置下填写资源主机地址或 URL 时以域名方式填写（资源相关的具体设置可参考章节 3.3.7.4 资源管理）。客户端访问 SSL VPN 的域名资源时，直接由『内网域名解析』中的 DNS 服务器进行解析。

[接入计算机使用此 DNS 服务器作为首选的 DNS 服务器]：即将首选 DNS 和备选 DNS 的地址下发到登录 SSL VPN 的客户端的网卡中的主备 DNS 中。主要应用于当域控制器同时作为内网 DNS 服务器时，登录 SSL VPN 后访问的内网服务器需通过域控制器来认证的情况。

如果没有勾选[接入计算机使用此 DNS 服务器作为首选的 DNS 服务器]，且存在大量的域名应用资源，在设置好『内网域名解析』后，可以进一步采用『内网 DNS 规则设置』处理，界面如下：



点击**新建**出现【新建域名解析规则】对话框：



『域名』在规则列表中需要访问的域名。

『描述』可随意填写便于理解记忆的文字。

点击**确定**保存配置。然后在填写资源主机地址或 URL 时以 IP 方式填写（资源具体设置可参考章节3.3.7.4 资源管理）。客户端访问 SSL VPN 的域名资源时，如果访问的域名符合在此定义的域名规则，将由设备内部的 HOST 表或『内网域名解析』中的 DNS 服务器进行解析，并将解析结果发送给客户端（设备 HOST 具体设置可参考章节 3.3.4.6）。

勾选相应的域名解析规则，点击**删除或编辑**，对选中的规则进行删除和编辑操作。点击**选择**选中所有规则或者取消所有选择。



- 1.如果资源中使用的地址是内部域名，且内网有专门的 DNS 服务器进行解析，推荐在此添加规则，使得这部分域名的解析请求优先由内网 DNS 服务器解析，否则不要在此添加任何规则！
- 2.此处添加的规则最多支持 100 条；不支持中文域名解析。

### 3.3.7. IPSec VPN



需要使用 VPN 功能时，设备上必须拥有至少一个三层接口即可，VPN 功能需要开启相应的多功能授权。

#### 3.3.7.1. DLAN 运行状态

此页面可以查看当前的 VPN 连接和网络流量信息。页面如下：



The screenshot shows the 'DLAN运行状态' (DLAN Running Status) interface. At the top, there are tabs for '刷新状态' (Refresh Status), '分支NAT状态' (Branch NAT Status), and '停止服务' (Stop Service). Below these are sections for '当前DLAN状态' (Current DLAN Status) showing '运行中' (Running), '当前连接总数: 0' (Current total connections: 0), and '剩余授权数: 第三方授权 [4] 移动 [4]' (Remaining authorization count: Third-party authorization [4], Mobile [4]). There are also sections for '外网流量' (External network traffic) and 'VIM流量' (VIM traffic) with their respective receive and send counts in bytes per second. The bottom part of the interface is a table with columns for '断开连接' (Disconnect), '连接名称' (Connection name), '用户名' (Username), '描述' (Description), '类型' (Type), '实时流量(接收/发送)' (Real-time traffic (receive/send)), 'Internet IP' (Internet IP), '内网IP' (Intranet IP), '接入时间' (Access time), and '传输类型' (Transmission type). A search bar and a '显示选项' (Show options) button are also present.

点击**刷新状态**可刷新 VPN 的连接状态和流量状态。

点击**分支 NAT 状态**可查看当前分支 NAT 状态，包括用户名、原子网网段、代理子网网段、网络类型和子网掩码。页面如下：

分支NAT状态

刷新状态

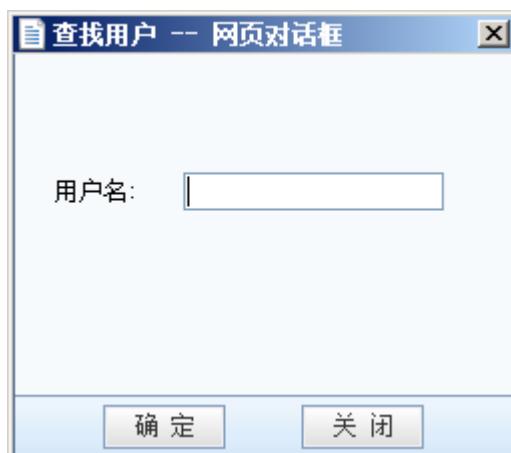
NAT用户总数: 0 NAT网段总数: 0

每页显示条数:  0/0页 共0条

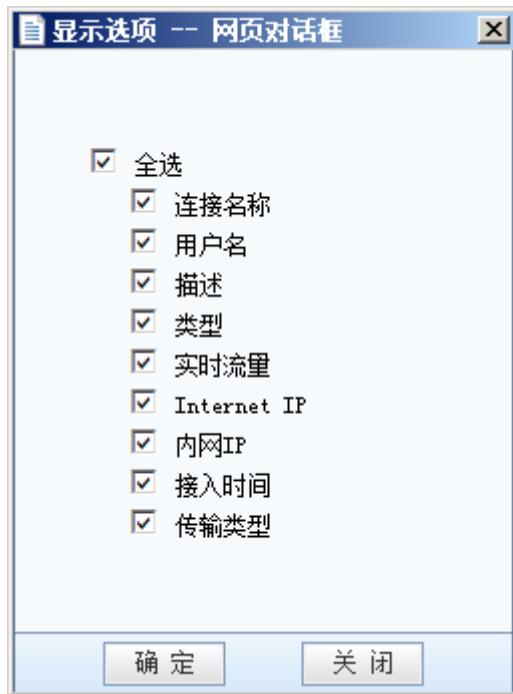
序号	用户名	原子网网段	代理子网网段	网段类型	子网掩码

点击**停止服务**可暂时停止 VPN 服务。

点击**查找用户**，输入用户名，可以快速找到当前用户的连接情况，页面如下：



点击**显示选项**，可以对显示的列进行筛选，页面如下：



### 3.3.7.2. 基本设置

『基本设置』用于设置 VPN 连接所需的 Webagent 信息、VPN 数据的 MTU 值、最小压缩值、VPN 连接鉴权监听端口、VPN 连接模式、广播包和性能设置。

[Webagent]指动态 IP 寻址文件在 WEB 服务器中的地址，包括主 Webagent 和备份 Webagent 地址。见下图：



如果是“动态寻址（总部非固定 IP）”请填写“Webagnet 网页地址”（一般为以.php 结尾的网页地址），填写完 Webagent 后可以点击测试按钮查看是否能够连通，如果总部是“固定 IP”，请按照“IP 地址：端口”的格式填写，如

202.96.134.133:4009。点击**修改密码**可以设置 Webagent 密码，以防止非法用户盗用 Webagent 更新虚假 IP 地址。点击**共享密钥**可以设置共享密钥，防止非法设备接入。



如果设置了『Webagent 密码』，一旦遗失该密码则无法恢复，只能联系深信服科技客户服务中心重新生成一个不包含 Webagent 密码的文件并替换原有文件。如果设置了『共享密钥』，则所有 VPN 网点都必须设置相同的『共享密钥』才能相互连接通信。如果是多线路且都是固定 IP 的情况下，可以采用“IP1#IP2:port”的方式来填写 Webagent。

[MTU 值]用于设置 VPN 数据的最大 MTU 值，默认为 1500。

[最小压缩值]用于设置对 VPN 数据启用压缩的最小数据包大小，默认为 100。

[VPN 监听端口]用于设置 VPN 服务的监听端口，缺省为 4009，可根据需要设置。

[修改 MSS]用于设置 UDP 传输模式下 VPN 数据的最大分片。



[MTU 值]、[最小压缩值]、[修改 MSS]一般情况下请保留默认值，如需设置，请在深信服科技技术支持工程师的指导下修改。

[直连]、[非直连]用于设置网关与 Internet 的连接方式，如果能直接获得 Internet IP 或者能通过端口映像等方式让 Internet 用户可以访问到网关设备的 VPN 端口，则可设置为“直连”，不能获得 Internet IP 的连接方式则需设置为“非直连”。

点击**高级**，可以进行 DLAN 性能设置，启用广播和组播，用来设置 VPN 的最大接入数目以及是否在 VPN 通道内传递广播和组播包。界面如下：



[线程数]: 控制设备的最大 VPN 连接个数，默认值 300，最大可支持 1280 个 VPN 接入。如需修改，请在深信服科技技术工程师的指导下进行修改。

[启用广播包]: 是否在 VPN 隧道内传递广播包，并且只传递指定端口范围的广播包，尽可能避免 VPN 两边的广播风暴产生。

[启用组播包]: 是否在 VPN 隧道内传递组播包。

### 3.3.7.3. 用户管理

『用户管理』用于管理 VPN 接入帐户信息，设置允许接入 VPN 的用户账号、密码，是否启用硬件捆绑鉴权或 DKEY 认证、是否启用虚拟 IP、设置账号使用的加密算法、账号有效时间、账号的内网权限，对用户进行分组并设置组成员的公共属性等用户策略。页面如下：



The screenshot shows a user management interface with the following details:

名称	状态	组中用户数	类型	组属性	加密算法	虚拟IP	网上邻居	描述	操作
非组用户	启用	2							
本地用户: Guest	启用	分支	否	AES	禁用			Guest	[编辑] [删除] [导出配置] [复制]
缺省用户	禁用	分支	否	AES	禁用				[编辑]

底部提示：当用户不在列表时，走此流程。

点击**检测 USB-KEY** 将检测当前登录网关控制面板的计算机是否插入了 USB Key，如没有安装 DKey 驱动则提示用户是否需要下载，用户可以点击**下载 USB KEY 驱动**直接下载安装。



生成 DKey 前必须安装好 DKey 驱动，否则计算机无法识别 DKey 硬件，为避免因程序冲突导致 DKey 驱动无法正常安装，请在安装过程中关闭第三方杀毒软件、防火墙等程序。

点击**删除**可对勾选的用户进行删除操作。

点击**导入域用户**可从域服务器中导入用户信息。



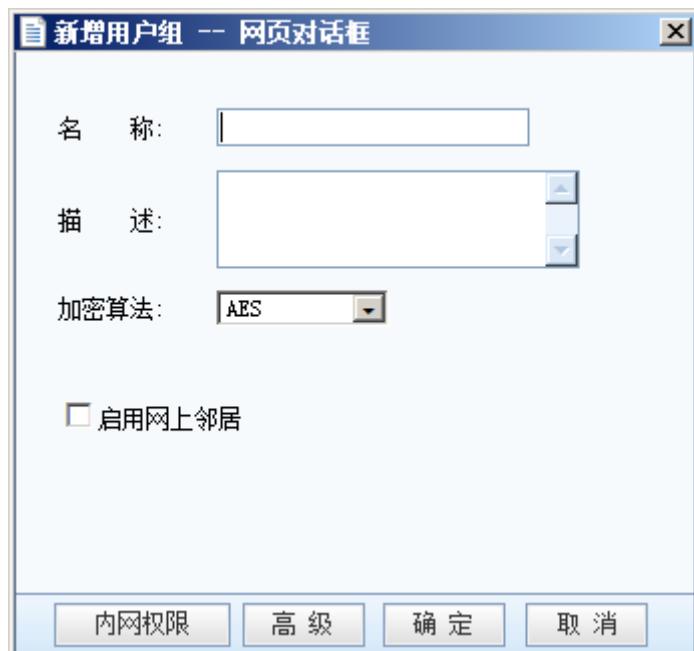
使用**[导入域用户]**功能之前，请先在**『VPN』→『高级设置』→『LDAP 服务器设置』**中设置 LDAP 服务器信息。

点击**导入文本用户**可从 TXT 或 CSV 文件中导入用户信息。

点击**导出用户**可从设备上将用户导出到本地进行保存，并可选择导出的用户密码是加密还是不加密。页面如下：



点击**新增组**可设置用户组名称、描述以及组成员公共属性（包括[加密算法]、  
[启用网上邻居]、[内网权限]三项设置），页面如下：



点击**高级**可进行 VPN 选路策略设置，组播服务设置，隧道参数设置。

点击**新增用户**可依次设置接入账号的『用户名』、『密码』、『描述』、『算  
法』等信息，如下图：

新增用户 -- 网页对话框

用户名:	<input type="text"/>	认证方式:	<input type="button" value="本地认证"/>
密码:	<input type="password"/>	算法:	<input type="button" value="AES"/>
确认密码:	<input type="password"/>	类型:	<input type="button" value="移动"/>
描述:	<input type="text"/>	用户组:	<input type="button" value="非组用户"/>
<input type="checkbox"/> 使用组属性			
<input type="checkbox"/> 启用硬件捆绑鉴权	硬件证书:	<input type="text"/>	
<input type="checkbox"/> 启用DKEY	DKEY:	<input type="text"/>	
<input checked="" type="checkbox"/> 启用虚拟IP	虚拟IP:	<input type="text" value="0.0.0.0"/>	
有效时间:	<input type="button" value="全天"/>		
<input type="checkbox"/> 启用过期时间	过期时间:	<input type="text" value="0-00-00"/>	<input type="text" value="0"/> : <input type="text" value="0"/> : <input type="text" value="0"/>
<input checked="" type="checkbox"/> 启用用户	<input checked="" type="checkbox"/> 启用网上邻居	<input checked="" type="checkbox"/> 启用压缩	
<input type="checkbox"/> 接入总部后禁止该用户上网	<input type="checkbox"/> 启用多用户登录	<input type="checkbox"/> 禁止在线修改密码	
<input type="button" value="权限设置"/>		<input type="button" value="高级"/>	<input type="button" value="确定"/>
		<input type="button" value="取消"/>	

[认证属性]用于设置用户认证类型，可选本地认证（即硬设备认证）、LDAP认证、Radius 认证。

[类型]用于设置使用此账号的 VPN 类型，可选移动和分支。

[使用组属性]选项用于对用户进行分组，如勾选[使用组属性]则可启动选择[用户组]设置，选择将该用户加入到某一个用户组并应用这个组的公共属性。



设置[使用组属性]前请先新增用户组。用户加入用户组后，该用户的[算法]、[启用网上邻居]、[权限设置]将无法再单独设置。

[启用硬件捆绑鉴权]选项用于设置基于硬件特性的证书认证，启用后请选择

对应此用户的证书文件 (\*.id)。

[启用 DKEY]选项用于设置是否对移动用户启用 DKEY 认证，启用后请先将 DKEY 插入计算机的 USB 接口再点击[生成 DKE]。

[启用虚拟 IP]选项主要用于移动客户端的接入。对于移动用户，必须勾选启用虚拟 IP。启用虚拟 IP 后，如果为该用户手动设定好一个虚拟内网 IP 地址（该 IP 必须在虚拟 IP 池范围内），则该用户接入后，会使用这个 IP 作为虚拟的内网 IP 地址。如果虚拟 IP 设置为 0.0.0.0，则系统会自动为该用户从虚拟 IP 池中分配一个内网 IP 地址。



启用虚拟 IP 功能之前，请先在『VPN』→『IPSec VPN』→『虚拟 IP 池』中设置虚拟 IP 池范围。

[有效时间]和[启用过期时间]用于设置“接入账号”的有效时间及过期时间。

如 VPN 接入用户需要使用网上邻居服务，则必须勾选[启用网上邻居]。

[启用压缩]选项用于设置对网关设备与该用户之间传输的数据使用压缩算法进行压缩。



该设置是 Sangfor VPN 的独特技术，在低带宽的环境下能有效利用有限带宽，加速数据传输，但并不适用于所有网络环境，实际应用中可根据情况进行设置。

[接入总部后禁止该用户上网]选项，该选项只对移动用户生效，勾选该选项，则可以让移动用户在连通 VPN 后，只能通过 VPN 访问总部内网，而不能访问互联网。

[启用多用户登录]选项用于设置是否允许多个用户同时共享该账号登录 VPN。

[禁止在线修改密码]选项用于设置移动用户是否能够在连上 VPN 后自行修改移动端登录密码，不勾则允许移动用户自行修改登录密码。

**权限设置**用于设置用户接入 VPN 后的访问权限，即设置用户只能访问某些服务，默认不做限制。



使用[权限设置]前，请先在『VPN』→『IPSec VPN』→『高级设置』→『内网服务设置』添加所需服务。

**高级**用于设置用户接入 VPN 后的一些高级属性，包括选路策略设置，组播服务设置、隧道参数设置、隧道间 NAT 设置等。选路策略即为不同的接入用户选择不同的线路选路策略；组播服务主要是满足总部和分支间有视频等需要组播支持的应用的需求；隧道内流控主要是避免某个接入的用户 VPN 流量过大的问题；隧道内 NAT 主要是解决两个内网网段相同的分支同时接入到总部的地址冲突问题。移动用户的高级选项设置页面如下：



分支用户的高级选项设置页面如下：



选路策略设置详见 3.5.2.8 [多线路选路策略]小节

组播服务设置详见 3.3.8.13.2 [组播服务设置]小节，页面如下：



[隧道参数设置]包括了 VPN 隧道超时时间、隧道动态速度探测、隧道内流控等内容，如下图：



[VPN 隧道超时时间]在网络时延较大、丢包率较高环境下，SANGFOR VPN 可以针对这些网络设置专门的超时时间，每个隧道的超时时间以总部配置为准， 默认超时时间为 20s，若在较差的网络环境中要适当延长超时时间。

[启用隧道动态速度探测]在本端或对端拥有多线路情况下有效，此时 SANGFOR VPN 设备将会定时探测多线路里各条线路的延时及丢包情况综合选择最优线路进行数据传输。

[启用隧道内流控] 用在多个 VPN 分支或者移动用户接入时，为了避免其中某一个分支或者移动用户将总部带宽全部占满导致其他分支或者移动用户访问速度变慢，可以针对每个接入的用户分配一个上下行带宽，从而保证所有用户都能得到较理想的访问速度。



[启用隧道内流控]设置的限制值只是一个范围值，而不是准确值，例如：流控设为 100k，则实际流量会控制在 80-120k 的范围内，是在 100k 左右上下小幅波动。

[隧道内 NAT] 用于设置将分支用户内网网段转换为虚拟 IP 池网段的地址，

地址:深圳市南山区学苑大道1001号南山智园A1栋

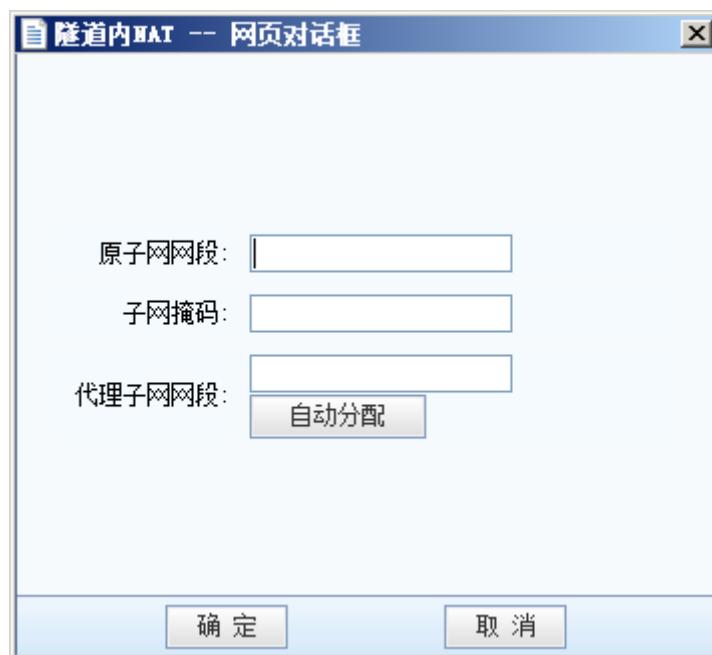
咨询热线 : 400-806-6868 | 服务热线 : 400-630-6430 | 邮箱: market@sangfor.com.cn | 网址 : www.sangfor.com.cn

如下图：



虚拟 IP 池设置详见 3.5.2.5 [虚拟 IP 池] 小节

点击 **新增**，既可在对话框中输入这条规则所需要匹配原子网网段、代理子网网段、子网掩码，也可以让设备自动从虚拟 IP 池中分配一个 IP 网段，页面如下：



[原子网网段]: 分支真实的内网子网网段。

[子网掩码]: 分支真实的内网子网掩码。

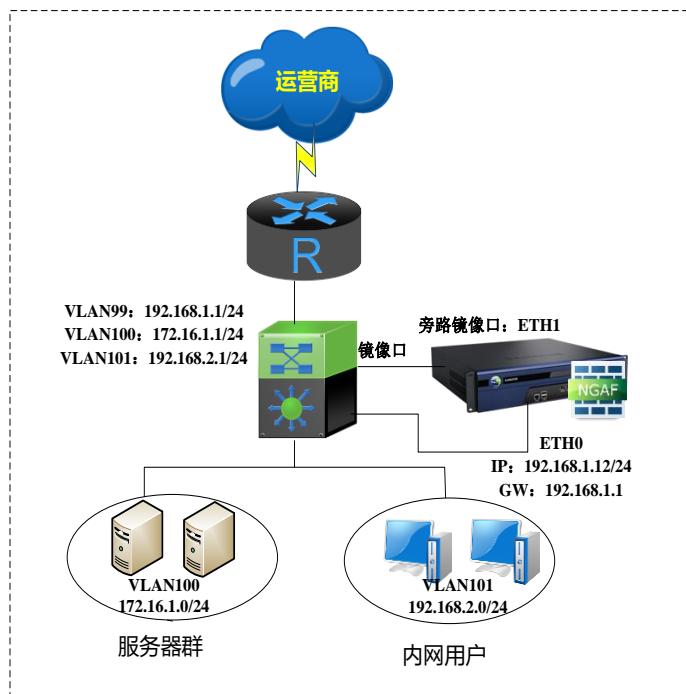
[代理子网网段]: 分支转换后的虚拟网段。

 配置时需要注意子网掩码一定要匹配，隧道内 NAT 只对掩码网段 NAT，主机号是不会改变的。

### 3.3.7.3.1 隧道间 NAT 案例学习

总部 - 北京 SANGFOR 设备采用路由模式部署，上海分公司 (192.168.2.0/24) 需要通过 VPN 接入北京总部，深圳分公司 (192.168.2.0/24) 同样需要通过 VPN 接入北京总部。则总部-北京 SANGFOR 设备需要添加隧道内 NAT 设置，解决上海分公司与深圳分公司之间内网网段冲突的问题。

步骤如下：



1、在[虚拟 IP 池]中新增一段 IP 为 192.168.20.0/24 的虚拟 IP 池范围。页

面如下：



2、在[用户管理]中新增一个分支账号，点击**高级**按钮选择[隧道内 NAT 设置]选项卡，勾选[启用隧道内 NAT]新增一条 192.168.20.0/24 网段与该分支账号进行关联。页面如下：

新增用户 -- 网页对话框

用户名:	分支-深圳	认证方式:	本地认证
密码:	*****	算法:	AES
确认密码:	*****	类型:	分支
描述:		用户组:	非组用户
<input type="checkbox"/> 使用组属性			
<input type="checkbox"/> 启用硬件捆绑鉴权	硬件证书:		
<input checked="" type="checkbox"/> 启用DKEY	DKEY:		
<input checked="" type="checkbox"/> 启用虚拟IP	虚拟IP:	0.0.0.0	
有效时间:	全天		
<input type="checkbox"/> 启用过期时间	过期时间:	0-00-00	0 : 0 : 0
<input checked="" type="checkbox"/> 启用用户	<input checked="" type="checkbox"/> 启用网上邻居	<input checked="" type="checkbox"/> 启用压缩	
<input type="checkbox"/> 接入总部后禁止该用户上网	<input type="checkbox"/> 启用多用户登录	<input checked="" type="checkbox"/> 禁止在线修改密码	

权限设置      高级      确定      取消

VPN高级属性 -- 网页对话框

选路策略设置	组播服务设置	隧道参数设置	隧道内NAT设置	帮助提示
<b>隧道内NAT</b>				
<input checked="" type="checkbox"/> 启用隧道内NAT <input type="button" value="新增"/>				
序号	原子网网段	代理子网网段	子网掩码	操作

确定      取消



点击[确定]后规则生效，则分支-深圳在不修改内网 IP 的情况下也能顺利接入总部，此时总部-北京可以通过访问 192.168.20.0/24 这个网段中对应的 IP 地址来访问分支-深圳内网提供的服务。



使用[高级]里的组播服务前，请先在『VPN』→『IPSec VPN』→『高级设置』→『组播服务』添加所需服务。

使用[高级]里的隧道内 NAT 前，请先在『VPN』→『IPSec VPN』→『虚拟 IP 池』添加所需的分支虚拟 IP 网段。



此时分支-深圳和分支-上海之间无法通过隧道间路由进行互访。如需分支-深圳和分支-上海要通过隧道间路由互访，则分支-深圳和分支-上海都需要启用隧道内 NAT 功能分别转换为 2 个不同的 IP 网段，然后再添加隧道间路由，源为真实物理 IP 网段，目地为对端虚拟 IP 网段即可。

### 3.3.7.4. 连接管理

为了实现多个网络节点的互联（组成“网状”网络），设备提供了对网络节

点互联的自主管理和设置功能。可在『连接管理』中进行相关的设置。



连接管理只有此设备当分支使用需要连接其他总部设备时才需要启用，否则本端是总部设备情况下不需要启用连接管理。

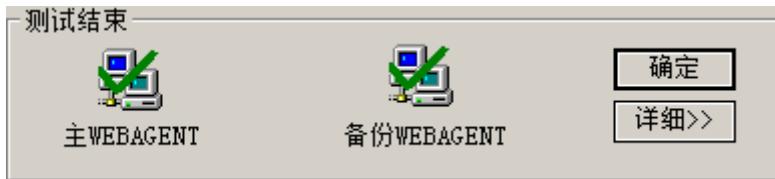


点击新增可以添加到一个总部的连接。如下图所示：



[总部名称]和[描述]用于标记连接名称，可以任意填写。

[主/备份 Webagent]用于填写需要连接的总部的对应 Webagent，点**测试**按钮可以测试 Webagent 是否工作正常，结果如下所示：



测试请求均是从本机发起的而不是设备发起的。如果 Webagent 是用域名形式，测试成功代表该网页存在，否则网页不存在。如果 Webagent 采用固定 IP 方式，则测试成功代表填写的 IP:PORT 格式正确。该测试成功并不代表 VPN 就一定能连接成功。

[传输类型]可选“TCP”或“UDP”，用于决定传输 VPN 数据包的类型，默认为 UDP 模式。

[数据加密密钥]、[用户名]和[密码]根据总部提供的接入帐户信息来填写。

[跨运营商]功能适用于总部分支采用了不同运营商线路互联经常丢包的情况下。可以选择[低丢包率]、[高丢包率]和[手动设置]。



跨运营商功能需要额外启动，否则该功能无效。如果总部启动跨运营商功能，则所有连接到该总部的移动用户可以直接使用跨运营商功能，其他所有连接到该总部的硬件分支设备，也需要启动跨运营商功能。

点击**内网权限**可以对 VPN 连接对端进行权限设置，即指定 VPN 连接对端只能访问本端的哪些服务。设置完以上信息后勾选**[启用]**选项即启动该连接。最后点击**确定**按钮保存设置信息。



### 3.3.7.5. 虚拟 IP 池

『虚拟 IP 池』是指由 SANGFOR VPN 硬件设备指定某一段空闲的 IP 地址，作为移动用户接入时的虚拟 IP 地址，或者是由 SANGFOR VPN 硬件设备指定任意的一段 IP 作为分支接入后的虚拟 IP 段，解决两个拥有相同网段的分支同时通过 VPN 接入到总部时 IP 冲突的问题。当移动用户接入后，分配一个虚拟 IP 给移动用户，移动用户对总部的任何操作都是以分配的 IP 作为源 IP，可以在高级选项里为接入的移动用户指定 DNS 等网络属性。

配置虚拟 IP 的步骤：

- 1、创建虚拟 IP 池，虚拟 IP 池中的 IP 是 SANGFOR 硬件设备所在局域网的空闲 IP。
- 2、指定移动用户使用虚拟 IP。如果设置虚拟 IP 为 0.0.0.0 表示自动分配虚拟 IP，当移动用户接入后，总部 SANGFOR 设备从虚拟 IP 池中选择一个空闲 IP 分配给移动，也可以为移动用户指定虚拟 IP。



点击**新增**按钮，出现『虚拟 IP 池』设置对话框，设置 IP 池的起止 IP 即可，  
页面如下：



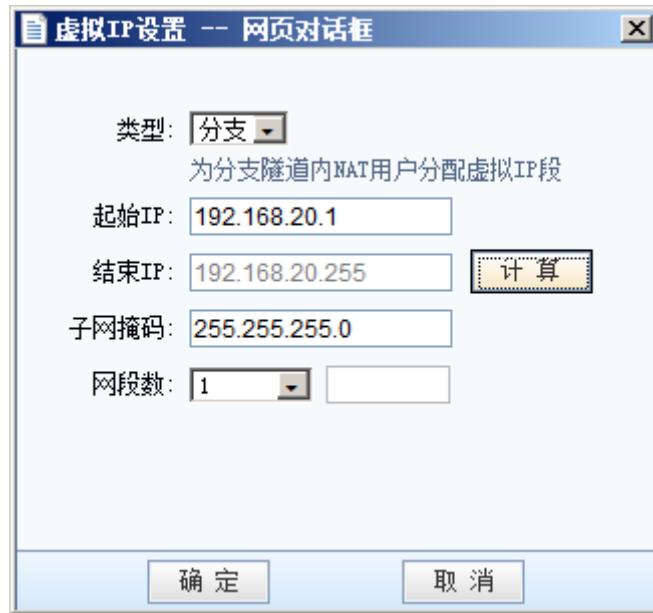
点击『虚拟 IP 池』的**高级**可以设置要分配给移动客户端虚拟网卡上的虚拟  
IP 子网掩码、DNS、WINS 服务器信息，页面如下：



当设置了“虚拟 IP 池”的[高级选项]之后，移动客户端计算机中的虚拟网卡“**SANGFOR VPN virtual network adapter**”必须设置为自动获取 IP 和 DNS，否则“高级选项”里面设置的内容不会分配到移动客户端的虚拟网卡上。

2、创建分支虚拟 IP 池。分支虚拟 IP 池中的虚拟 IP 段提供给分支接入到总部时将分支的原网段替换成虚拟 IP 池中的一个网段，以解决当两个相同网段的分支同时接入到总部时的内网 IP 冲突问题。设置时设定虚拟 IP 的开始 IP、设定虚拟 IP 的掩码和分支的网段数，点击**计算**可以自动结算出符合要求的结束 IP。

页面如下：



[起始 IP]: 分支虚拟 IP 段的第一个 IP 地址。

[结束 IP]: 分支虚拟 IP 段的最后一个 IP 地址。

[计算]: 自动计算虚拟 IP 段的最后一个 IP 地址

[网段数]: 设置多少个虚拟 IP 段。

[子网掩码]: 虚拟 IP 段的子网掩码。与分支端内网子网掩码保持一致。

设定分支虚拟 IP 段后，在[VPN/用户管理]里新建用户，用户类型选[分支]，然后在[高级/隧道内 NAT 设置]里配置需要转换的分支网段。

### 3.3.7.5.1 虚拟 IP 池案例学习

总部 SANGFOR 设备采用路由模式部署，外地移动办公用户需要通过 VPN 接入到总部远程办公。则设置步骤如下：

在『虚拟 IP 池』中新增一条规则，设置和设备 LAN 口相同网段且没有被内网用户所使用的 IP 地址段。页面如下：



在『用户管理』中[新增用户]，类型选择[移动]。虚拟IP默认为“0.0.0.0”则表示自动分配虚拟IP，如需指定用户的虚拟IP，则设置相应的虚拟IP即可。



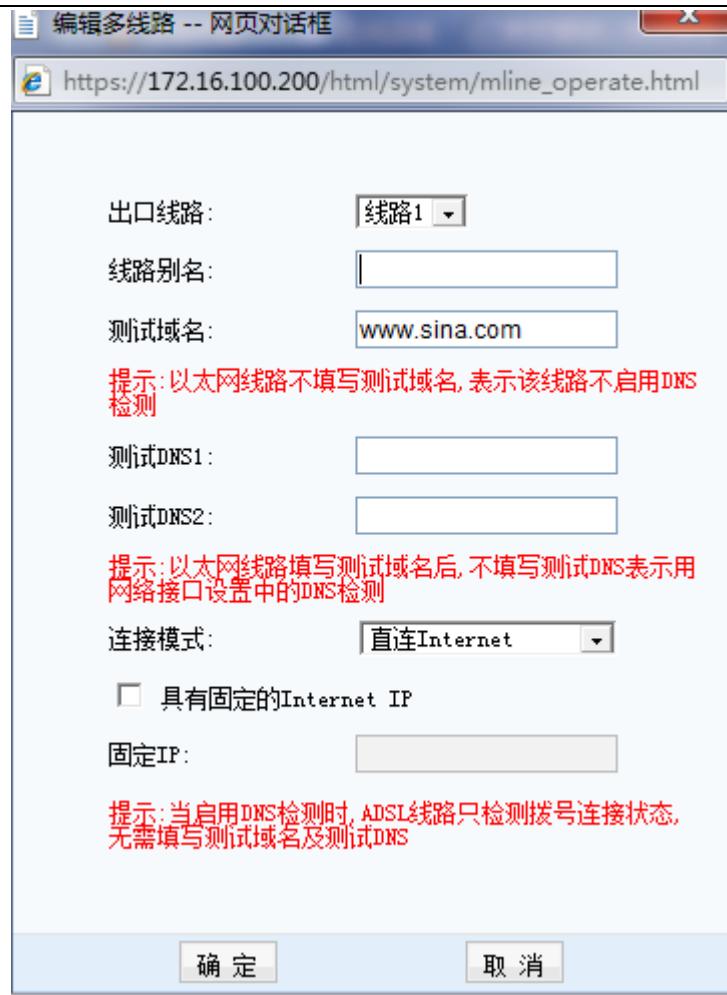
### 3.3.7.6. 多线路设置

在使用多条外网线路下，启用 VPN 的多线路功能时，都需要在此处添加“多条线路”，这里可以对线路的信息进行增删和修改。

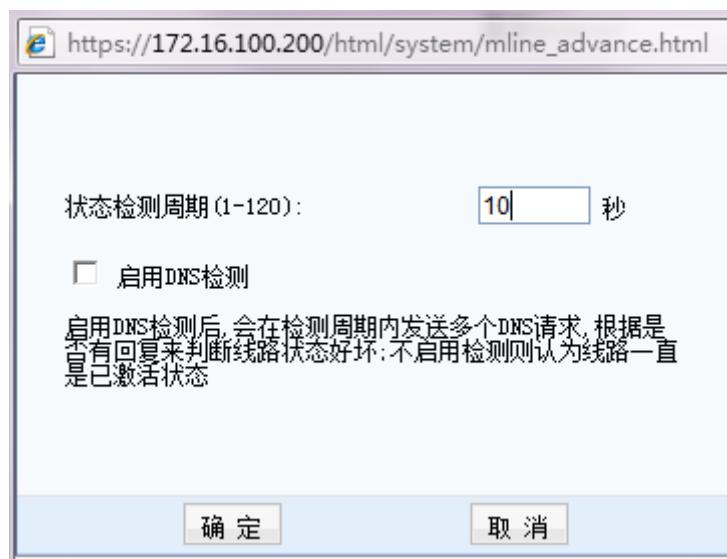


勾选[网关模式下启用多线路]，即开启 IPSEC VPN 多线路传输功能。

点击**新增**，设置出口线路、线路别名，若公网有固定的 IP 地址，则勾选[具有固定的 Internet IP]，并配置固定的公网 IP 地址。在『测试域名』和『测试 DNS』下设置相应的域名和 DNS 服务器地址，用于检测该线路的通讯状态是否正常。  
显示如下：



点击高级选项，可设置是否启用 DNS 检测，如下图所示：

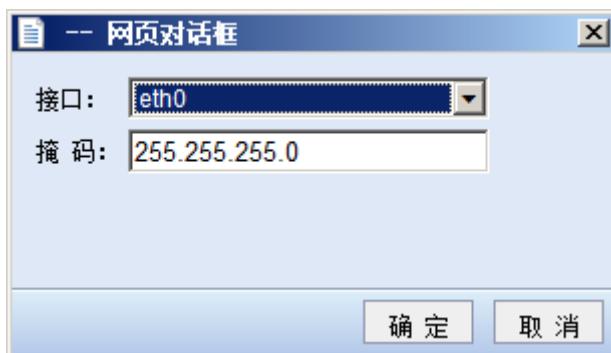


### 3.3.7.7. VPN 接口设置

『VPN 接口设置』用来定义设备需要作为 VPN 连接的内网接口，如下图：



点击添加，选定 VPN 内网接口，如下图：



只有非 WAN 口类型，固定 IP 的接口才能选择成 VPN 的内网接口。

[本机 VPN 接口设置]用于设置 VPN 服务虚拟网卡 IP。



**注意：**默认情况下请设置为[使用自动分配的 VPN 接口 IP]，如果出现 IP 冲突的提示，可改为自定义 IP 并进行设置。



**1. VPN 接口是 SANGFOR 硬件网关系统的虚拟接口，外观上并不存在对应的真实物理接口。**

**2. VPN 连接的外网接口，需要勾选“与 IPSec VPN 出口线路匹配”，如下图所示：**



### 3.3.7.8. 多线路选路策略

SANGFOR 设备提供了功能强大的 VPN 多线路选路策略，可根据本端和对端 VPN 设备的多条外网线路情况，选择不同的主，备线路组，可选择按照会话平均分配或按包平均分配的方式选择流量分配模式，如下图：



点击新增，显示【多线路选路策略编辑】对话框，如下图：

多线路选路策略编辑 -- 网页对话框

帮助提示

基本信息

策略名称:

策略描述:

线路组设置

本端线路数  条 对端线路数  条 有效负载线路选择阀值  ms

主线路组

本地线路	对端线路	操作
策略线路1	线路1	<a href="#">右移</a>
策略线路1	线路2	<a href="#">右移</a>
策略线路1	线路3	<a href="#">右移</a>
策略线路1	线路4	<a href="#">右移</a>
策略线路2	线路1	<a href="#">右移</a>
策略线路2	线路2	<a href="#">右移</a>
策略线路2	线路3	<a href="#">右移</a>
策略线路2	线路4	<a href="#">右移</a>

备线路组

本端线路	对端线路	操作

流量分配模式

按会话平均分配  按包平均分配

[确定](#) [取消](#)

[策略名称]任意设置策略的名称

[线路组设置]设置本端设备的外网线路条数，VPN 连接对端的线路条数，有效负载线路选择阀值。

[主线路组]设置首要 VPN 连接的线路组合。通过[右移](#)操作，将选中的线路组合加入到备线路组。

[备线路组]设置备份 VPN 连接的线路组合

[流量分配模式]可选择按会话平均分配或按包平均分配。



设置了多线路选路策略后，需要在『用户管理』的用户或用户组[高级]选项中选择使用。

### 3.3.7.9. 本地子网列表

『本地子网列表』用于总部硬件设备的内网有多个子网的情况下，其他 VPN 接入用户需要与总部内网的其它子网互访。例如，总部有两个子网（192.200.100.x、192.200.200.x），通过配置“本地子网列表”，可实现分支、移动与总部内网各网段相互访问。具体配置如下：

1、在『本地子网列表』里配置需要互联的子网，页面如下：



点击新增进行本地子网的添加，页面如下：



[子网网段]、[子网掩码]设置为总部内网 VPN 设备非直连网段的网络号、子网掩码。

2、在『静态路由』中为需互联的子网设置路由。（具体可参照『网络』→『路由』→『静态路由』）。



这里的『本地子网列表』仅相当于一种“声明”作用，在此定义的网段，都会被 VPN 设备和软件客户端视为 VPN 网段，所有访问这些网段的数据包经过 VPN 设备或软件后，都会被封装到 VPN 隧道中传输。所以，一般情况下，在『本地子网列表』里添加了子网网段，都需要配合『静态路由』配置来完成

对多子网的访问。

### 3.3.7.10. 隧道间路由设置

SANGFOR 设备提供了强大的 VPN 隧道间路由功能，通过设置隧道间路由，可轻松实现多个 VPN（软/硬件）之间的互联，真正实现“网状”VPN 网络，页面如下：



#### 3.3.7.10.1 隧道间路由案例学习

例如：总部（“深圳”192.168.1.x/24）同时与分支（“上海”172.16.1.x/24）、（“广州”10.1.1.x/24）建立了 VPN 连接（分支“上海”、“广州”通过设置连接管理实现与总部互联），但“上海”与“广州”之间没有 VPN 连接，通过设置适当的“隧道间路由”规则，即可实现“上海”与“广州”之间的相互访问。具体配置如下：

1、在分支“上海”的『隧道间路由设置』中勾选[启用路由]，点击新增，添加到“广州”的路由，页面如下：



[网络号（源）]设置源地址网络号，本例中应设置为 172.16.1.0

[子网掩码（源）]设置源地址子网掩码，本例中应设置为 255.255.255.0

[网络号（目的）]设置目的地址网络号，本例中应设置为 10.1.1.0。

[子网掩码（目的）]设置目的地址子网掩码，本例中应设置为 255.255.255.0。

[目的路由用户]设置路由指向的 VPN 连接用户，本例中应设置为上海与深圳建立 VPN 连接的用户。



[网络号（源）]、[网络号（目的）]用于匹配数据的源 IP 地址、目的 IP 地址，当 VPN 隧道中传输的数据匹配设置时，则此路由设置生效，数据将被转发给相应的 VPN 设备。[目的路由用户]可理解为，“要将路由的数据发往哪一个 VPN 设备”，本例中分支“上海”在『连接管理』中设置了使用用户名“深圳-上海”与总部建立了 VPN 连接，因此以用户名“深圳-上海”标示将路由的数据发往总部。

2、在分支“广州”的『隧道间路由设置』中勾选[启用路由]，点击**新增**，添加到“上海”的路由，页面如下：



[网络号（源）]设置源地址网络号，本例中应设置为 10.1.1.0。

[子网掩码（源）]设置源地址子网掩码，本例中应设置为 255.255.255.0。

[网络号（目的）]设置目的地址网络号，本例中应设置为 172.16.1.0。

[子网掩码（目的）]设置目的地址子网掩码，本例中应设置为 255.255.255.0。

[目的路由用户]设置路由指向的 VPN 连接用户，本例中应设置为广州与深圳建立 VPN 连接的用户。

隧道间路由还可用于设置将分支的上网数据全部发往总部，通过总部的公网出口上网，例如，在分支上海设置通过总部上网，页面如下：



[网络号（源）]设置源地址网络号，设置本端需要通过总部上网的网络号。

[子网掩码（源）]设置源地址子网掩码，本例中应设置为 255.255.255.0。

[目的路由用户]设置路由指向的 VPN 连接用户。

最后勾选[通过目的路由用户上网]启用设置。



1.通过总部线路上网时，则必须在总部设备『防火墙』→『地址转换』→『源地址转换』中添加对 VPN 网段的源地址转换规则，详见防火墙部分设置说明。

2.如果 AF 当总部，要实现分支通过总部上网，请在深信服科技技术工程师指导下进行操作。

### 3.3.7.11. 第三方对接

SANGFOR 设备提供了与第三方 VPN 设备互联的功能，能与第三方的 VPN

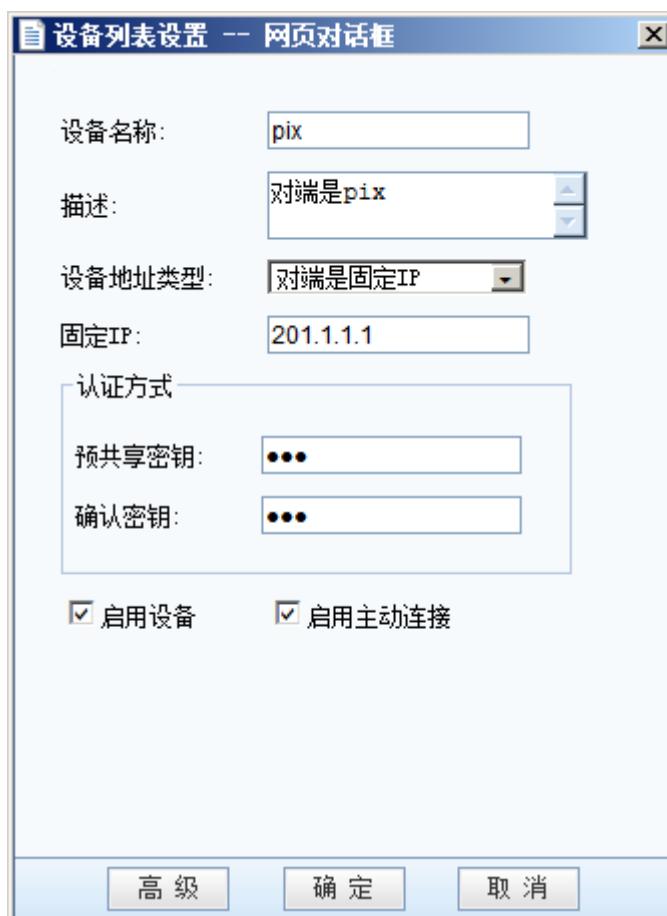
设备建立标准 IPSec VPN 连接。

### 3.3.7.11.1 第一阶段

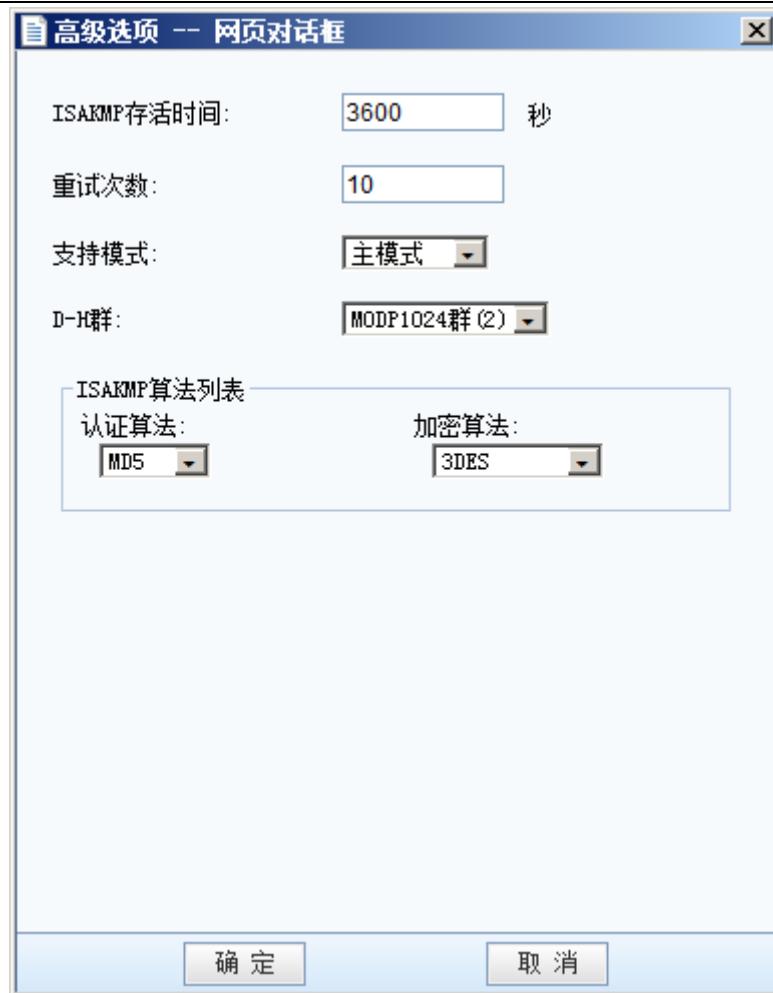
『第一阶段』用于设置需要与 SANGFOR 硬件网关建立标准 IPSec 连接的对端 VPN 设备的相关信息，也就是标准 IPSec 协议协商的第一阶段。页面如下：



选择线路出口，点击新增，显示【设备列表设置】对话框，页面如下：



点击高级，显示『高级选项』对话框，可进行其它高级设置，页面如下：



### 3.3.7.11.2 第二阶段

『第二阶段』用于设置标准 IPSec 协议协商的第二阶段的参数，页面如下：

『入站策略』用于设置由对端发到本端的数据包放行规则，点击新增，

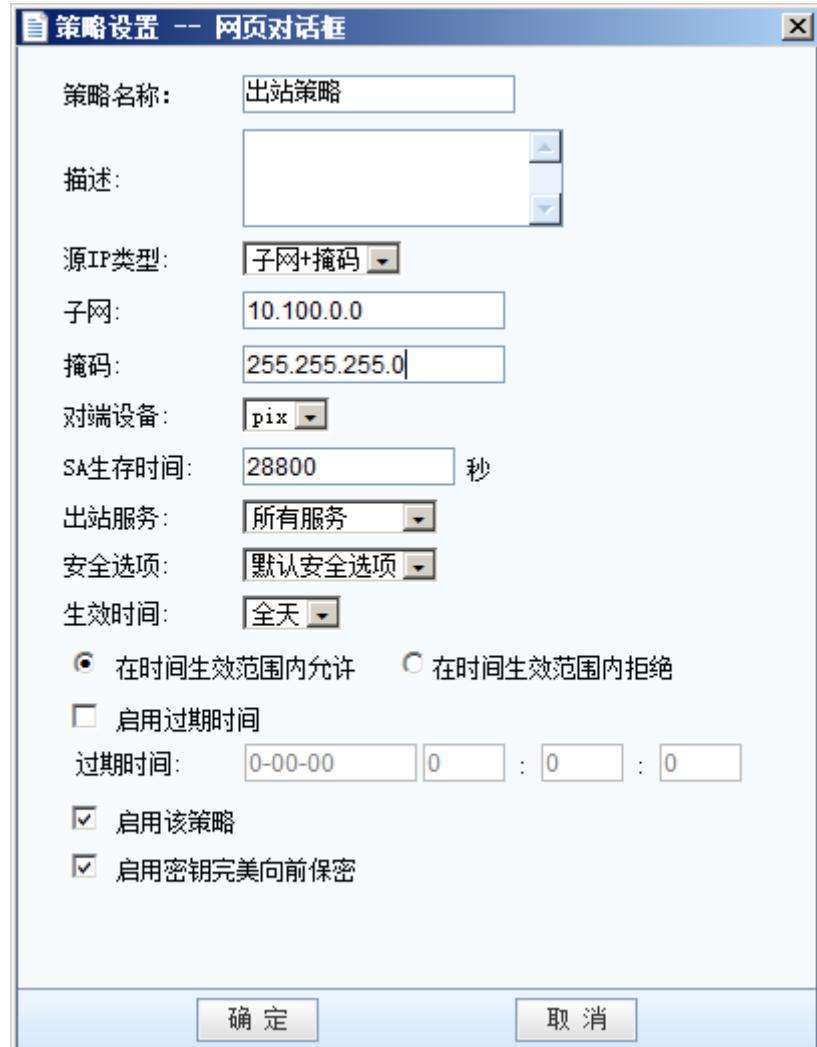
显示策略设置对话框，页面如下：

策略设置 -- 网页对话框

策略名称:	入站策略
描述:	<input type="text"/>
源IP类型:	子网+掩码
子网:	192.100.0.0
掩码:	255.255.255.0
对端设备:	pix
入站服务:	所有服务
生效时间:	全天
<input checked="" type="radio"/> 在时间生效范围内允许 <input type="radio"/> 在时间生效范围内拒绝	
<input type="checkbox"/> 启用过期时间	
过期时间: 0-00-00 0 : 0 : 0	
<input checked="" type="checkbox"/> 启用该策略	

确定 取消

『出站策略』用于设置从本端发往对端的数据包规则，点击新增，显示策略设置对话框，页面如下：



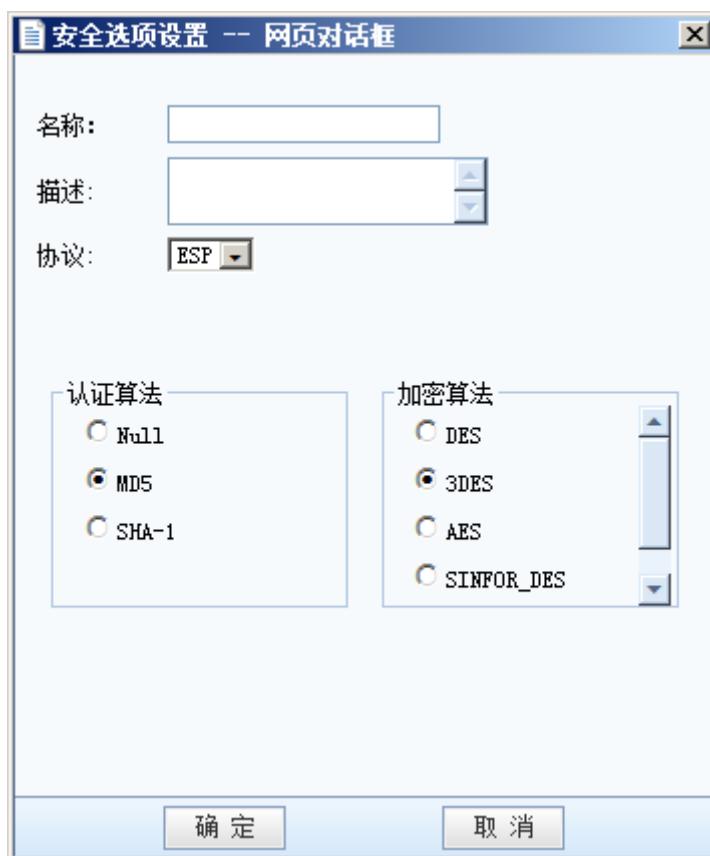
「出站策略」和「入站策略」中的[出站服务]、[入站服务]和[时间设置]均为 SANGFOR 扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立 VPN 连接的过程中不会协商此类规则。「出站策略」和「入站策略」中策略所对应的源 IP 地址是指[源 IP 类型]和[本/对端服务]中所设置的源 IP 的交集。

### 3.3.7.11.3 安全选项

『安全选项』用于与对端建立标准 IPSec 连接时所使用的参数，也就是标准 IPSec 协商的第二阶段。页面如下：



在建立与第三方设备的IPSec连接前，请先确定对端设备采用何种连接策略，包括：使用的[协议]（AH或ESP）、[认证算法]（Null、MD5或SHA-1）、[加密算法]（DES、3DES、AES或SINFOR\_DES），点击**新增**，添加新的选项，页面如下：



SANGFOR 设备会使用设置好的连接策略与对端协商建立 IPSec 连接。



『安全选项』中的[加密算法]用于设置标准 IPSec 连接的第二阶段所使用的数据加密算法，如果要与多个采用不同连接策略的设备互联，需要分别将各个设备使用的连接策略添加到『安全选项』中。

### 3.3.7.12. 通用设置

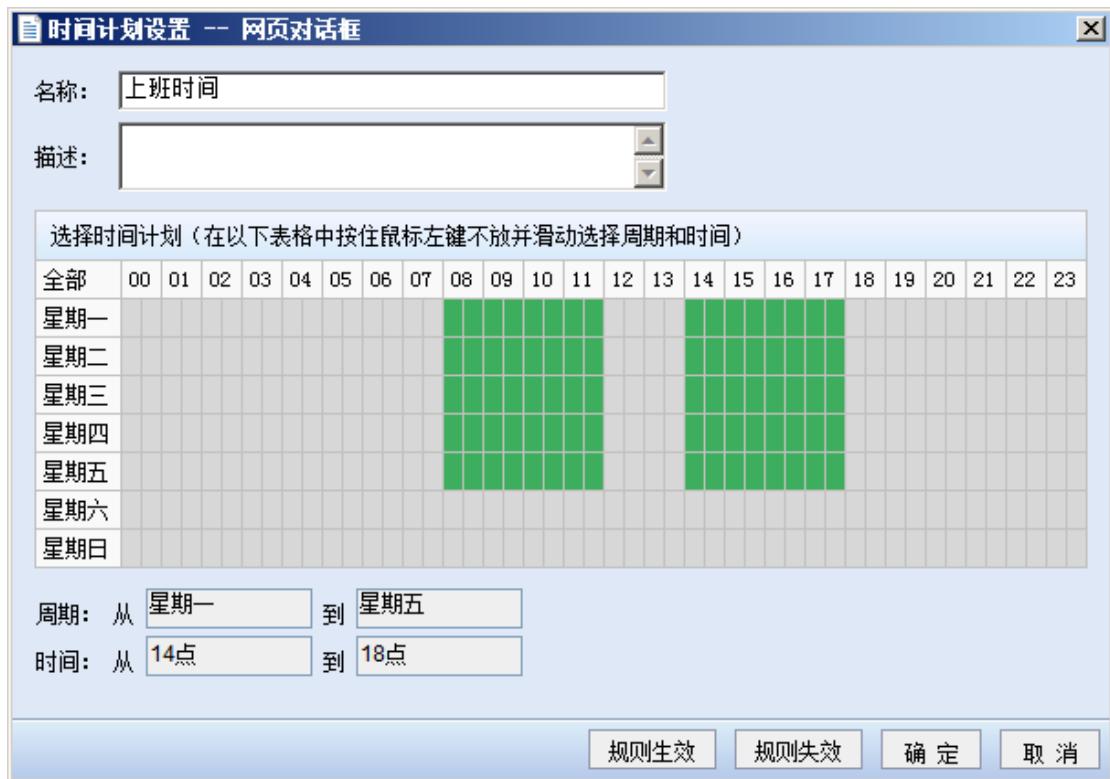
『通用设置』包含『时间计划设置』和『算法列表设置』两个子模块。

#### 3.3.7.12.1 时间计划设置

『时间计划设置』用于定义常用的时间段组合，这些时间组合可在『用户管理』、『内网权限』中使用，该时间以设备上当前时间为准。页面如下：



点击新增按钮，出现【时间计划设置】对话框，页面如下：



名称： 上班时间

描述：

选择时间计划（在以下表格中按住鼠标左键不放并滑动选择周期和时间）

全部	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
星期一																								
星期二																								
星期三																								
星期四																								
星期五																								
星期六																								
星期日																								

周期： 从 星期一 到 星期五

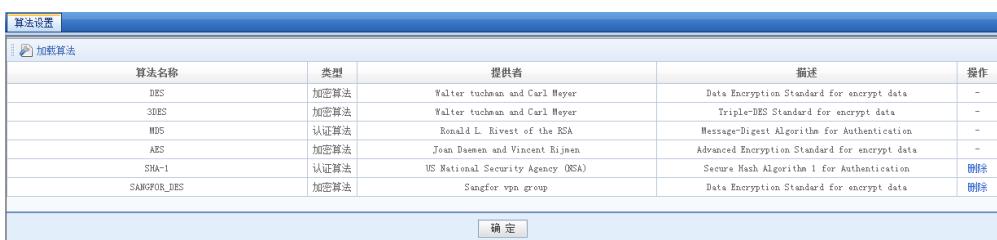
时间： 从 14点 到 18点

规则生效 规则失效 确定 取消

此例中，定义了一个名称为“上班时间”的时间段。默认情况下是所有时间周期规则生效的，选取相应的时间段组合，然后点击规则失效，则表示在选中时间段内规则失效，剩余的时间段内规则生效，最后点确定完成时间组的定义。绿色代表生效，灰色代表失效。

### 3.3.7.12.2 算法列表设置

『算法列表设置』提供了对设备支持的数据加密算法进行查看和添加的功能，加密算法会在设备所构建的 VPN 网络中对传输的所有数据进行加密，以保障数据的安全性。页面如下：



算法设置				
加载算法				
算法名称	类型	提供者	描述	操作
DES	加密算法	Walter Tuchman and Carl Meyer	Data Encryption Standard for encrypt data	-
3DES	加密算法	Walter Tuchman and Carl Meyer	Triple-DES Standard for encrypt data	-
MD5	认证算法	Ronald L. Rivest of the RSA	Message-Digest Algorithm for Authentication	-
AES	加密算法	Jean Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data	-
SHA-1	认证算法	US National Security Agency (NSA)	Secure Hash Algorithm 1 for Authentication	
SANGFOR_DES	加密算法	Sangfor vpn group	Data Encryption Standard for encrypt data	

设备内置了 DES、3DES、MD5、AES、SHA-1、SINFOR\_DES 多种加密、认证算法，并可以根据客户需要添加其它加密认证算法，如需添加其它加密认证算法请联系深信服科技。

### 3.3.7.13. 高级设置

『高级设置』用于设置『内网服务设置』、『组播服务设置』、『LDAP 服务器设置』和『Radius 服务器设置』、『动态路由设置』、『生成证书』、『与专线互备路由』。

#### 3.3.7.13.1 内网服务设置

SANGFOR 设备可以为接入的 VPN 用户指定相应的访问权限，可以限制分支用户内网的某个 IP、某个移动用户只能访问内网的特定计算机的特定服务和与第三方设备互连时设置出入站策略的服务参数。例如：仅允许用户 test 访问总

部的 WEB 服务器的 WEB 服务，对 WEB 服务器其它服务的访问请求都将被拒绝；仅允许分支用户 branch1 内网的一个 IP 访问总部的 SQL 服务器，分支内网其它 IP 的访问请求将被拒绝等。通过适当的权限设置对服务进行访问授权即可实现 VPN 隧道内的安全管理。



设置“内网服务权限”分为两个步骤：1、创建内网服务；2、为特定的用户指定权限。缺省状况下系统没有对 VPN 接入用户的访问权限做任何限制，下面以一个例子作为说明。

### 3.3.7.13.1.1 内网权限案例学习

某客户需要实现仅允许分支用户 branch 的内网 IP 172.16.1.200 访问总部的 FTP 服务器 192.168.1.20，其它 IP 发起的访问请求或对其它服务的访问请求全部拒绝，具体操作步骤如下：

在『内网服务设置』中点击【新增】出现【设置内网服务】对话框，『服务名称』可自定义一个便于识别的名称，勾选协议类型(本例中 FTP 服务使用 TCP 协议)，页面如下：



1、点击新增出现【IP 范围设置】对话框，逐项进行设置，页面如下：



[源 IP]: 本例中应设置为分支对端的内网 IP 172.16.1.200。

[源端口]: 1-65535。

[目的 IP]: 本例中应设置为总部内网的 FTP 服务器 IP 192.168.1.20。

[目的端口]: FTP 的服务端口 20-21。



这里的内网服务设置只是一种“定义”，定义好服务之后，需要在『用户管理』里面为用户账号分配内网权限来最终实现“VPN 内网权限”的设定。内网服务设置还可应用于『第三方对接』中设置『出站策略』的『本端服务』参数和『入站策略』的『对端服务』参数，具体设置可参考『第三方对接』相关章节。

2、在『用户管理』中选择编辑用户 Branch，点击权限设置，页面如下：

编辑用户: 深圳-广州 -- 网页对话框

用户名:	Branch	认证方式:	本地认证	
密码:	*****	算法:	AES	
确认密码:	*****	类型:	分支	
描述:		用户组:	非组用户	
<input type="checkbox"/> 使用组属性				
<input type="checkbox"/> 启用硬件捆绑授权	硬件证书:			
<input type="checkbox"/> 启用DKEY	DKEY:			
<input type="checkbox"/> 启用虚拟IP	虚拟IP:	0.0.0.0		
有效时间:	全天			
<input type="checkbox"/> 启用过期时间	过期时间:	0-00-00	0 : 0 : 0	
<input checked="" type="checkbox"/> 启用用户	<input type="checkbox"/> 启用网上邻居	<input checked="" type="checkbox"/> 启用压缩		
<input type="checkbox"/> 接入总部后禁止该用户上网	<input type="checkbox"/> 启用多用户登录	<input type="checkbox"/> 禁止在线修改密码		
最后登录时间:	无时间记录	最后使用时间:	无时间记录	
<a href="#">权限设置</a>		<a href="#">高级</a>	<a href="#">确定</a>	<a href="#">取消</a>

3、在『权限设置』对话框中将设置好的 Branch 服务右移到服务列表中，设置为允许，因为本例中仅允许该服务，故将『缺省动作』设置为[缺省拒绝]，页面如下：



完成以上三步设置后，即实现仅允许分支用户 Branch 的内网 IP172.16.1.200 访问总部的 FTP 服务器 192.168.1.20，分支 Branch 内网的其它 IP 发起的访问请求都会被拒绝。



这样设置完成后，总部其他计算机去访问分支 Branch 也一样会访问不到。因为总部其他计算机发起访问分支的请求，分支计算机响应该请求时，因分支计算机发回的数据包里目标 IP 不是 192.168.1.20 这台服务器，也会被内网权限给拦掉。

### 3.3.7.13.2 组播服务

为满足通过 VPN 使用 VOIP 和视频会议等需要组播支持应用的需求，SANGFOR 支持组播服务在隧道间传输。在这里可以定义组播的服务，IP 范围是 224.0.0.1-239.255.255.255，端口范围是 1-65535。页面如下：



点击**新增**出现组播服务编辑页面，在这里可以设置组播服务所用的组播地址和端口。页面如下：

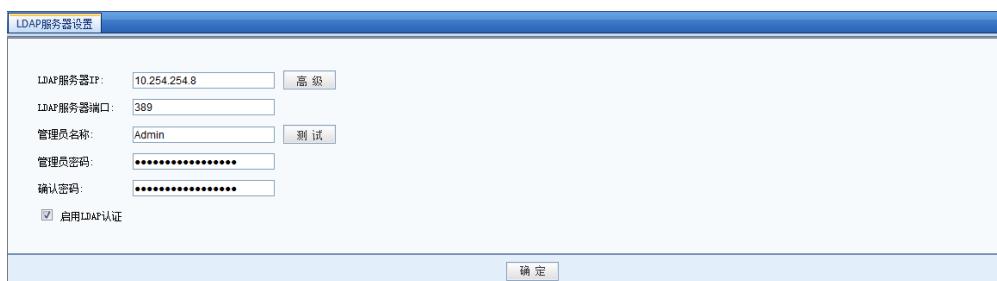


定义好组播服务后，在『用户管理』新建用户，然后在『高级』->『组播服务设置』里配置组播服务。页面如下：



### 3.3.7.13.3 LDAP 服务器设置

SANGFOR 设备的 VPN 服务支持使用第三方 LDAP 认证，如需要启用第三方认证，请在『LDAP 服务器设置』中正确设置第三方 LDAP 服务器信息（包括 LDAP 服务器 IP、LDAP 服务器端口、LDAP 管理员密码），如下图：



设置好 LDAP 服务器信息后，请点击 **高级**，显示[LDAP 高级设置]对话框，按照实际需求设置 LDAP 信息，如下图：



### 3.3.7.13.4 Radius 服务器设置

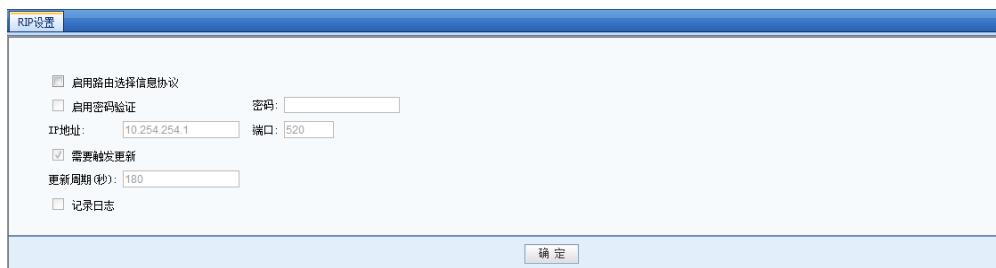
SANGFOR 设备的 VPN 服务支持使用第三方 Radius 认证，如需要启用第三方 Radius 认证，请在『Radius 服务器设置』中正确设置第三方 Radius 服务器信息（包括 Radius 服务器 IP、Radius 服务器端口、Radius 认证共享密钥、Radius 协议），如下图：



### 3.3.7.13.5 动态路由设置

『动态路由设置』主要用于设置 SANGFOR 设备通过 RIP 协议和其它网络

设备相互交换或学习路由信息，以实现路由信息的动态更新，如下图：



[启用路由选择信息协议]: 启动后，SANGFOR VPN 设备会向所设置的内网络由设备通告已与本端建立 VPN 连接的对端网络的信息（更新其他设备的路由表，添加到 VPN 对端的路由指向 SANGFOR VPN 设备，VPN 连接断开后会通告路由设备删除该路由）。

[启用密码验证]: 用于设置交换 RIP 协议信息时需要验证的密码，一般不需设置。

[IP 地址]和[端口]: 用于设置主动向哪个 IP 发布路由更新信息。

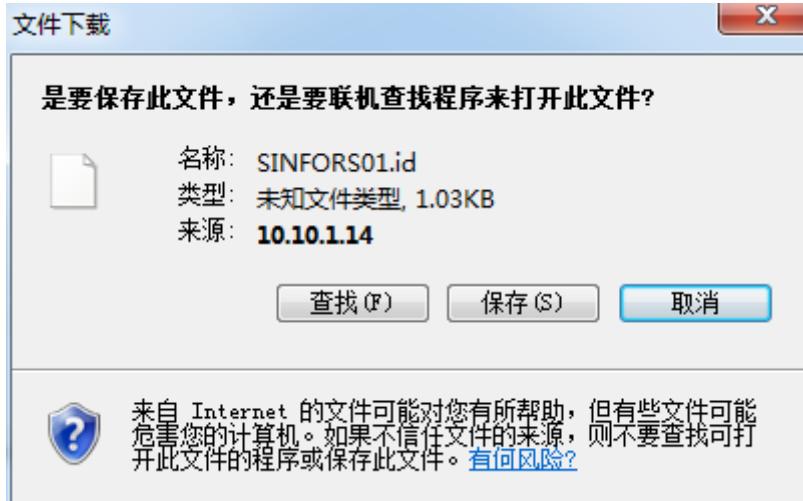
[需要触发更新]勾选后，设备则只有在系统路由有变化时才触发路由更新信息，这时下面设置的更新周期参数失效。

[记录日志]勾选，则设备会记录 RIP 路由更新的具体信息。

### 3.3.7.13.6 生成证书

基于硬件特性的证书认证系统是深信服科技的发明专利之一。硬件设备采用了该技术用于不同 VPN 节点之间的身份认证。该证书提取了设备部分硬件特性生成加密的认证证书。由于硬件特性的唯一性，使得该证书也是唯一的、不可伪造的。通过对该硬件特性的验证，就保障了只有指定的硬件设备才能被授权接入网络，避免了安全隐患。

点击生成证书选择保存路径即可生成硬件证书并保存到本地计算机上。页面如下：



将生成好的证书发给总部管理员，由总部管理员在新建 VPN 用户账号的时候选择硬件鉴权，将用户和对应的硬件证书进行绑定即可。

### 3.3.7.13.7 与专线互备路由

与专线互备路由功能源于用户网络有专线连接，VPN 需要作为专线的备份的场景。默认情况下，设备上 VPN 路由优先于静态路由，开启了 VPN 与专线互备路由功能后，路由优先级调整为：静态路由/动态路由>策略路由(专线)>VPN 路由。如下图所示：



## 3.4. 对象

『对象』中定义的各种对象是设备流量管理、防火墙和内容安全防护等模块的基础，各种策略控制和安全防护都是基于对象来做的。

### 3.4.1. 网络对象

#### 3.4.1.1. 网络对象

『网络对象』用于定义一个包含某些 IP 地址的 IP 地址组，这个 IP 组可以是内网的 IP 段，也可以是公网的某些 IP 范围，或者是全部 IP。

『网络对象』用于定义业务组、用户组和 IP 组

『IP 组设置』可以被『网络』→『地址转换』、『策略』→『访问控制策略』、『策略』→『流量管理』→『通道配置』等处引用。

在【导航菜单】页面中的『对象』→『网络对象』，右边进入【网络对象】编辑页面：

序号	名称	类型	IP范围	描述	删除
1	全部	IP组	全部	所有IP地址	已被引用
2	ma	IP组	3.3.3.3		已被引用

在【网络对象】页面点击新增，选择[新增业务]，弹出【新增业务】窗口：

**新增业务**

名称：  
例如：邮件服务器

描述：

**服务器配置**

+ 新增

服务器IP	删除
没有可以显示的数据	

**保存并继续新增** **保存** **取消**

[名称]用于设置业务的名称

[描述]用于设置业务的描述

[服务器配置]用于添加内网服务器

在【网络对象】页面点击**新增**，选择**[新增用户组]**，弹出**【新增用户组】**窗口：

新增用户组 ×

名称：

描述：

IP地址：(i)

保存并继续新增 保存 取消

[名称]用于设置用户组的名称

[描述]用于设置用户组的描述

[IP 地址] 用于设置用户组的 IP 地址



网络对象中的用户组和用户认证中的用户组并无关联

在【网络对象】页面点击新增，选择[新增 IP 组]，弹出【新增 IP 组】窗口：



[IP 组名称]用于设置 IP 组的名称

[IP 组描述]用于设置 IP 组的描述信息

在[IP 地址]中填写 IP 地址，一行一个单个 IP 地址或 IP 地址范围，IP 地址范围的格式为“起始地址-结束地址”，如“192.168.0.1-192.168.0.100”。

[解析域名]用于自动解析某些域名对应的 IP 地址，通过该功能可以自动将域名解析出来的 IP 地址追加到 IP 地址列表。

在【网络对象】页面勾选对应的业务、用户组和 IP 组，点击删除，用于业务、用户组和 IP 组。注意：已被引用的业务、用户组和 IP 组不能直接删除，需要去掉引用才可以进行删除。

在【网络对象】页面，点击导入、导出，用于导入导出 IP 组信息。



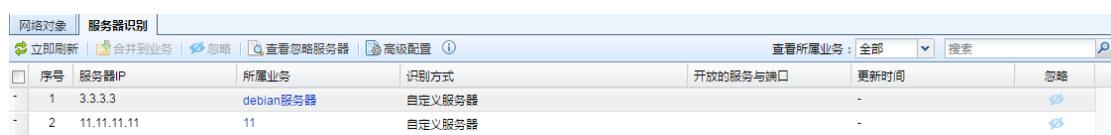
1、[解析域名]功能是通过设备进行解析，所以要求设备能正常上网，

并且配置了可用 DNS 地址，能正常解析域名。

### 3.4.1.2. 服务器识别

『服务器识别』用于设置内网的服务器地址和信息。

在【导航菜单】页面中的『对象』→『网络对象』，右边进入【服务器识别】编辑页面：

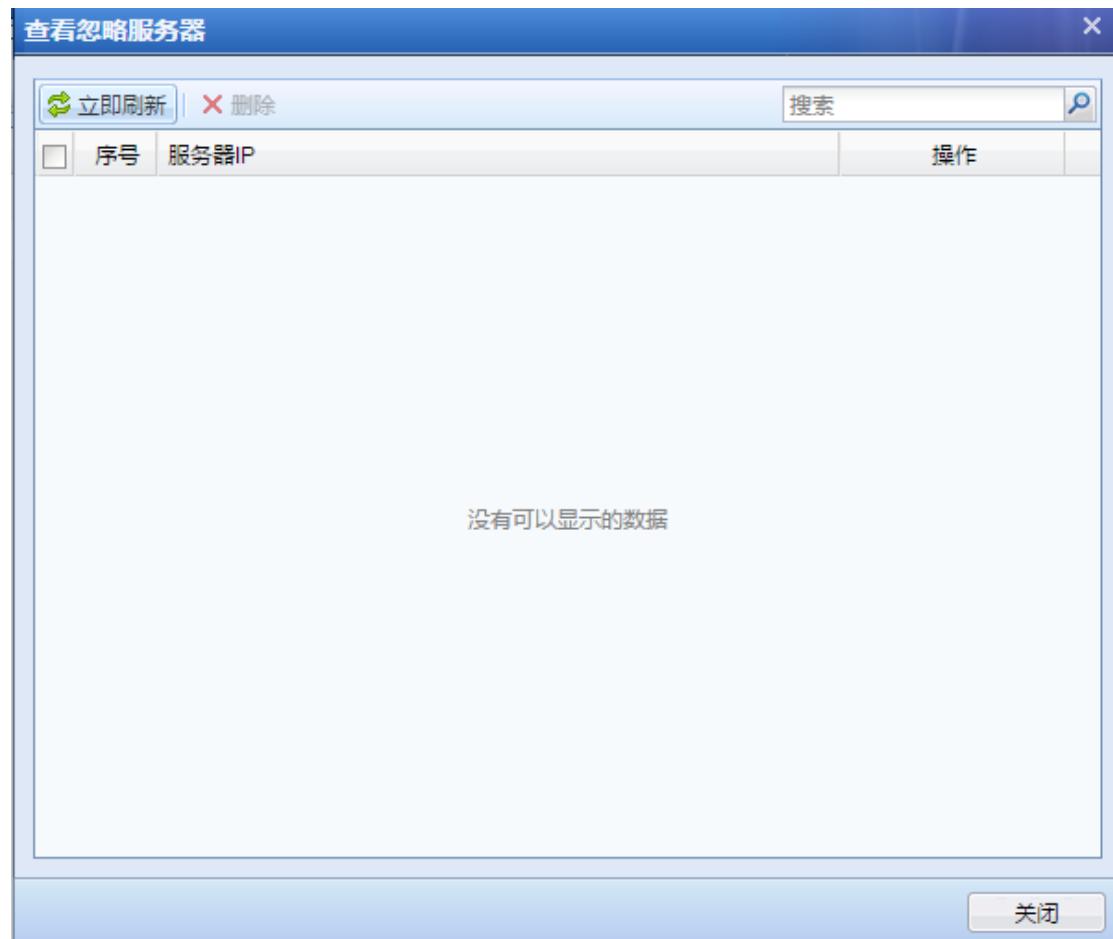


服务器识别						查看所属业务 : 全部	搜索
	序号	服务器IP	所属业务	识别方式	开放的服务与端口	更新时间	忽略
-	1	3.3.3.3	debian服务器	自定义服务器	-	-	
-	2	11.11.11.11	11	自定义服务器	-	-	

点击合并到业务，将自动识别的服务器合并到业务

点击忽略，可以将选择的服务器忽略

点击查看忽略服务器，将弹出已忽略的服务器页面：



点击【高级设置】，弹出【高级配置】窗口：



[自动识别]自动发现内网的服务器

[自定义服务器识别范围]自定义服务器识别范围来提高识别的速度和准确性



1、同时勾选自动识别和自定义服务器识别范围，就只会发现自定义服务器识别范围范围内的服务器

### 3.4.2. 服务

『服务』是一组特定的协议和端口的组合，通常代表某种网络应用，它可以被『内容安全』→『应用控制策略』调用，以实现对某些网络服务的允许、拒绝等控制。

#### 3.4.2.1. 预定义服务

『预定义服务』中内置了常见的网络服务，页面如下：

名称	协议
any	TCP:0-65535; UDP:0-65535; ICMP:type 0-255, code 0-255;ICMPv6:type 0-255, code 0-255;
bgp	TCP:179;
cluster	UDP:3343;
dns-t	TCP:53;
dns-u	UDP:53;
ftp	TCP:21;
h.225	TCP:1720;
h.225ras	UDP:1719;
http	TCP:80;
https	TCP:443;
irc	TCP:194;
l2tp	UDP:1701;
ldap	TCP:389;
ms-sql-m	TCP:1434;
ms-sql-r	UDP:1434;
ms-sql-s	TCP:1433;
mysql	TCP:3306;
netbios-ns	UDP:137;
netmeeting	TCP:1503;
nfs	UDP:2049;

预定义服务定义的是常用协议的默认端口，不允许被编辑或修改。如果预定义服务不能满足需求，可以设置『自定义服务』。

### 3.4.2.2. 自定义服务

切换到【自定义服务】页面点新增，会弹出【新增自定义服务】窗口。



[名称]设置服务的名称

[描述]设置对该服务的描述

[协议]用于设置服务的协议类型及端口号，分别点击[TCP]、[UDP]、[ICMP]、[ICMPv6]、[其他]，选择好相应的协议则在下面的窗口中添加相应的端口。

点击提交，完成网络服务对象的设置。



1. 【其他】中可填写协议号，协议号 **0** 代表所有的协议。可填写 **0-255** 的整数。

2.TCP 和 UDP 的填写格式是一行一个端口或者端口范围, ICMP 填写格式为“type:a,code:b”（不带引号）， a 和 b 是 0-255 的整数，可以输入多行。

### 3.4.2.3. 服务组

『服务组』用于将多个服务组合成一个服务组，当需要引用多个服务的时候，可以直接引用相应的服务组，页面如下：



点击新增，新增一个服务组，如下：



[名称]设置服务组的名称

[描述]设置对该服务的描述

[协议]用于设置该服务组所包含的服务，点击  选择服务，可同时选择预定

义服务和自定义服务中的多个服务。

### 3.4.3. 安全策略模板

安全策略模板用于制定个性化的防护策略，并保存为模板，供3.5章节的安全防护策略引用。

#### 3.4.3.1. 漏洞攻击防护

漏洞攻击防护依靠对数据包的检测来发现对内网系统的潜在威胁。

『漏洞攻击防护』内置上网管控和业务保护两个模板。如下图所示：



点击【新增】，则弹出【新增模板】的编辑框，配置如下：

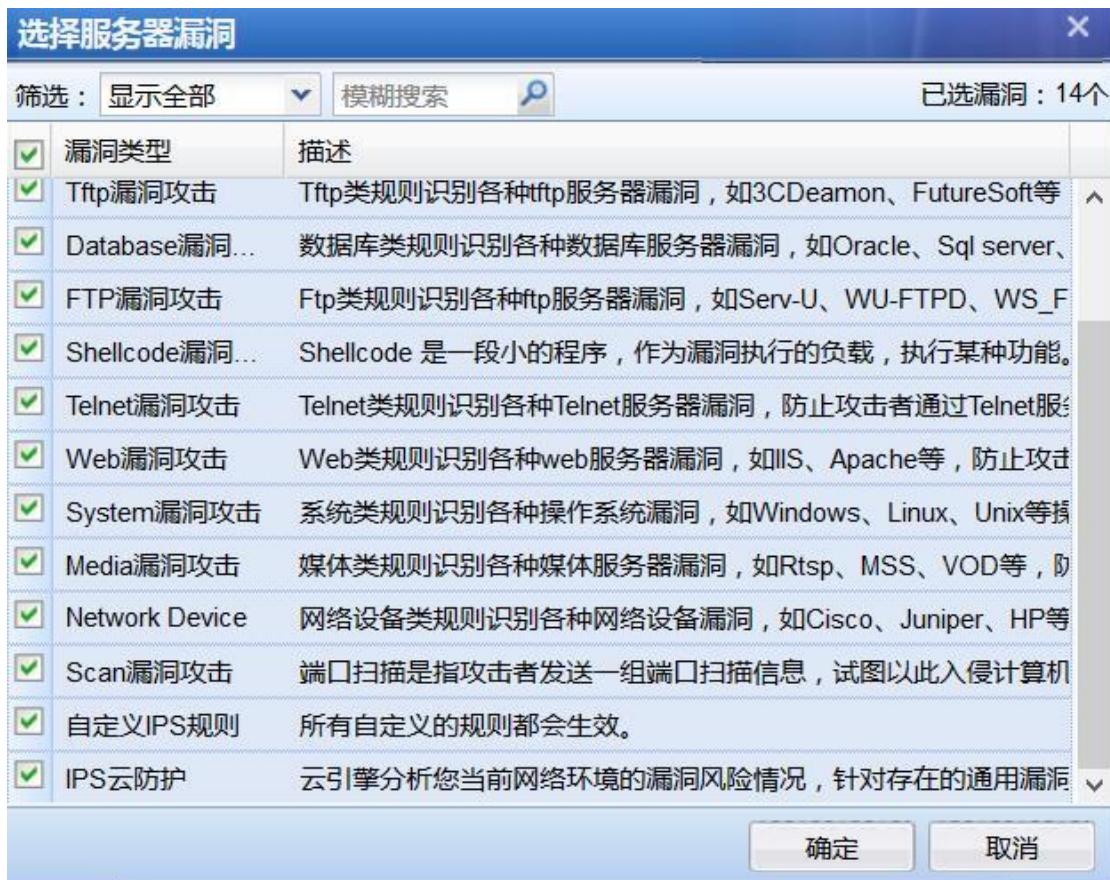


[模板名称]：定义该入侵行为防护模板的名称。

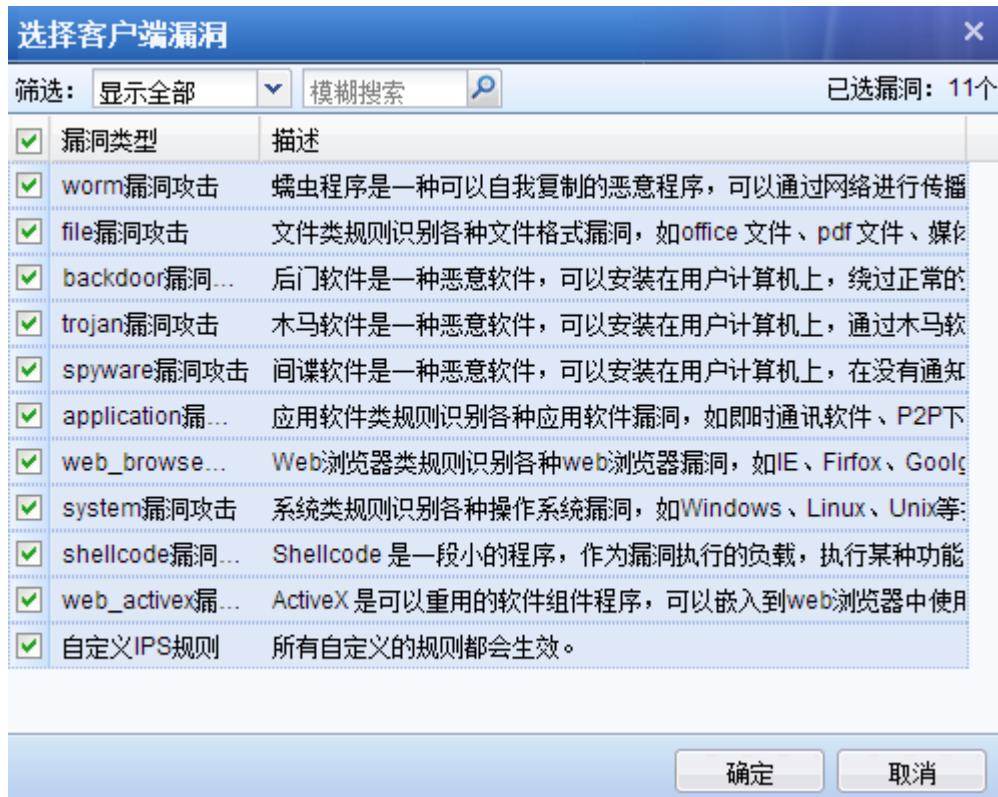
[描述]：定义对该入侵行为防护模板的描述。

[IPS选项]：设置保护的内容，勾选[保护服务器]，同时点击[已选：worm 漏洞攻击、network...] 弹出【选择服务器漏洞】编辑框，根据服务器发布的服务类型，勾选相应的[漏洞类型]，则设备会对这一种服务类型的相关漏洞进行入侵

防护：



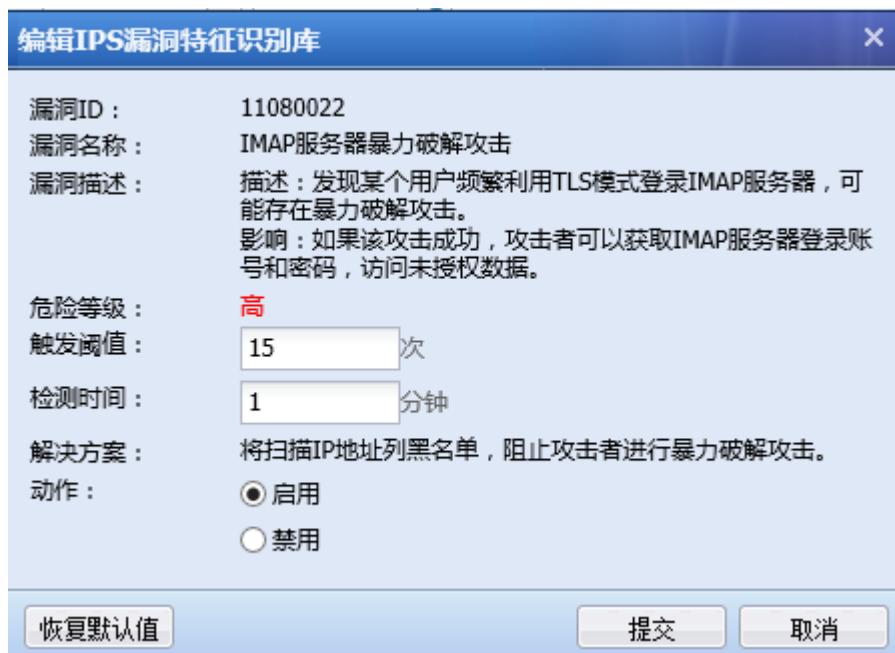
勾选[保护客户端]，同时点击[已选: worm 漏洞攻击、file 漏洞...] 弹出【选择客户端漏洞】编辑框，勾选相应的[漏洞类型]，则设备会对这种类型的客户端相关漏洞进行入侵防护：



勾选[口令暴力破解]，同时点击[已选: ftp、pop3\_standard...] 弹出【选择防暴力破解的协议】编辑框，勾选相应的[漏洞类型]，则设备对这种类型的暴力破解行为进行入侵防护：

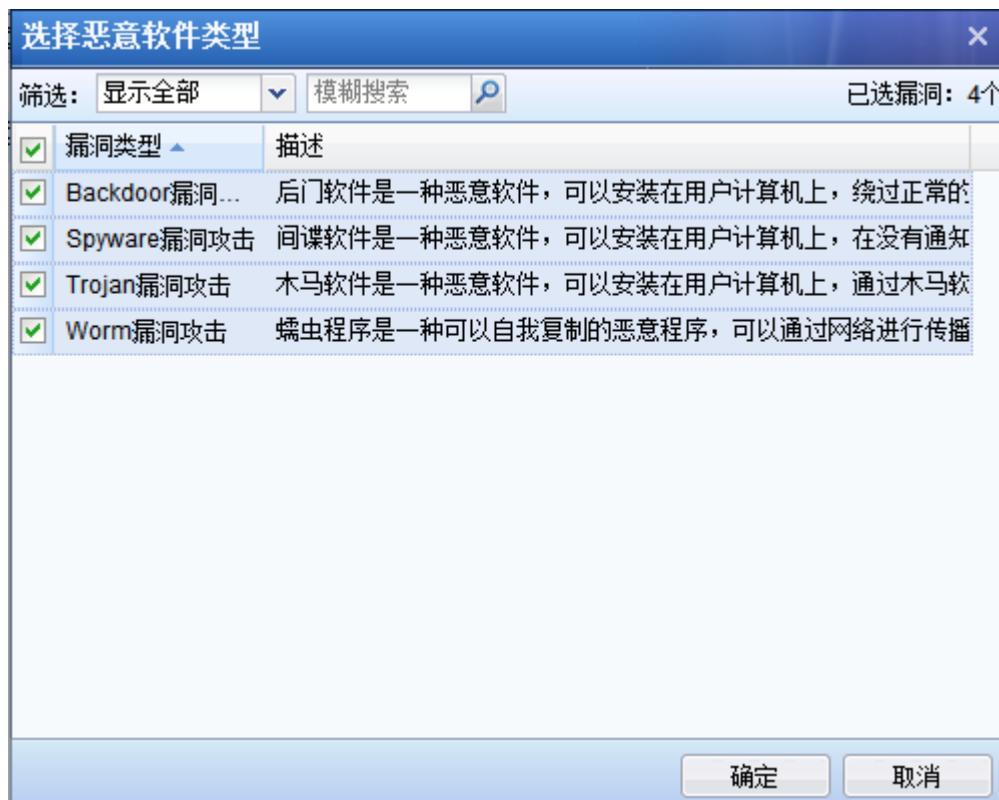


点击[漏洞类型]，跳转到编辑漏洞攻击防护漏洞特征识别库，可以设置触发阈值和检测时间，动作也可选择启用或禁用：



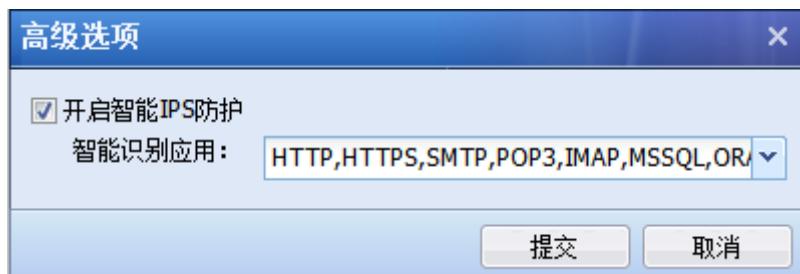
勾选[恶意软件]，同时点击[已选： Backdoor 漏洞攻击、Spy...] 弹出【选择

恶意软件类型】编辑框，勾选相应的[漏洞类型]，则设备对这种类型的恶意软件进行入侵防护：



点击**保存**，保存新增的模板

点击**高级选项**，弹出高级选项配置页面。如下图所示：



[开启智能 IPS 防护]能够使漏洞攻击防护防护基于应用识别漏洞攻击，防护漏洞，没有开启则是基于端口识别漏洞攻击防护漏洞的。



- 1、默认模板\_上网管控场景针对内网用户进行防护。
- 2、默认模板\_业务保护场景针对服务器进行防护。

### 3.4.3.2. Web 应用防护

『Web 应用防护』是专门针对客户内网的 WEB 服务器设计的防攻击策略，可以防止 OS 命令注入、SQL 注入、XSS 攻击等各种针对 WEB 应用的攻击行为，以及针对 WEB 服务器进行防泄密设置。

『WEB 应用防护』内置“默认模板”和“默认模板 II（非代理访问开启漏洞扫描）”两个模板。如下图所示：



序号	名称	防护类型	防护功能	搜索	删除
1	默认模板	SQL注入、XSS攻击、网页木马、网站扫描、WEB SHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB型...	应用隐藏、命令防护、权限控制、数据泄密防护、HTTP异常检测		X
2	默认模板 II（非代理访问开启漏洞扫描）	SQL注入、XSS攻击、网页木马、网站扫描、WEB SHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB型...	应用隐藏、命令防护、权限控制、数据泄密防护、HTTP异常检测		X

[模板名称]: 默认开启常规的 WEB 防护功能，但不开启“漏洞扫描功能”；  
[默认模板 II（非代理访问开启漏洞扫描）]: 默认开启常规的 WEB 防护功能，同时开启“漏洞扫描功能”。

点击新增，弹出新增模板页面。如下图所示：

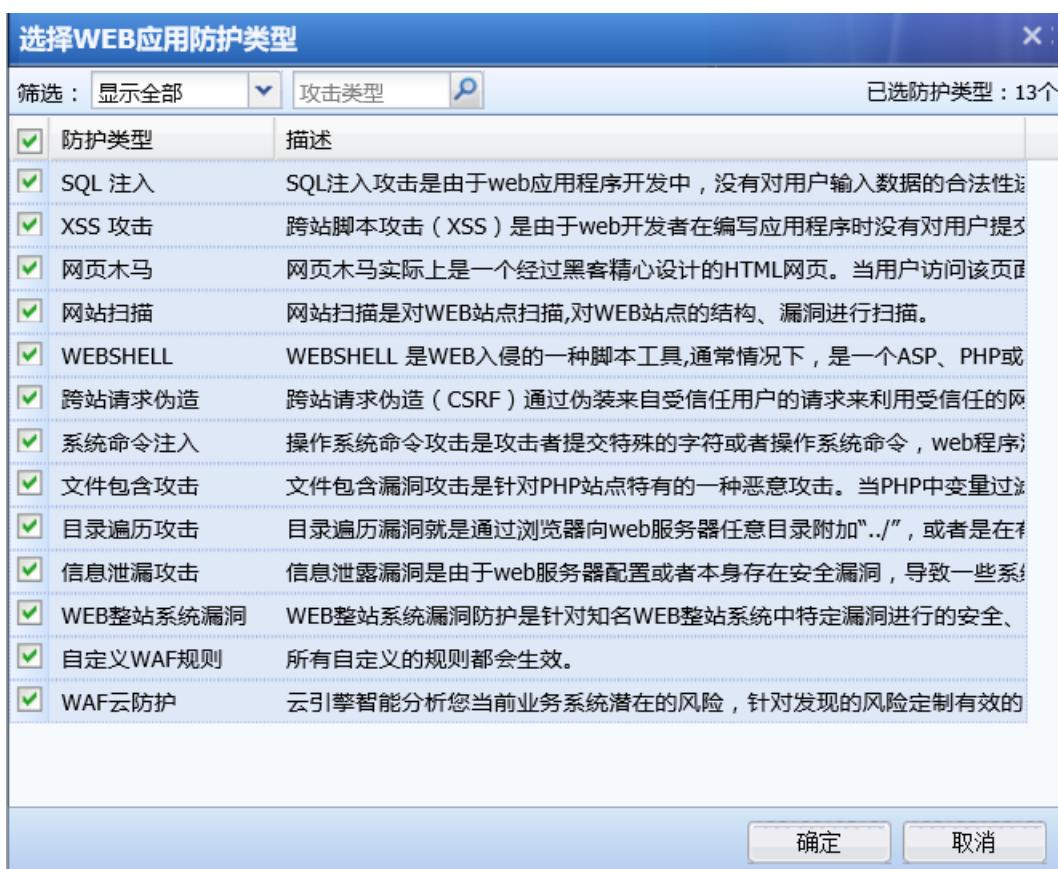


[模板名称]: 定义该模板的名称。

[描述]: 定义对该模板的描述。

[端口]: 设置保护的服务器的端口。此处一般填写服务器的端口，即用户访问服务器的该端口，则进行攻击检测等。HTTP 端口也可勾选自动识别其他HTTP 端口并防护，可以自动学习。

[防护类型]: 设置针对服务器的哪些攻击行为进行防护。点击[防护类型: SQL注入、XSS 攻击、网页木马...] 弹出【选择 WEB 应用防护类型】编辑框，勾选相应的[防护类型]，则设备会对这一种服务类型的相关攻击行为进行防护：



[SQL注入]: 攻击者通过设计上的安全漏洞，把 SQL 代码黏贴在网页形式的输入框内，获取网络资源或改变数据。AF 设备可以检测到此类攻击行为。

[XSS 攻击]: 跨站脚本攻击，XSS 是一种经常出现在 WEB 应用中的计算机安全漏洞。它允许代码植入到提供给其他用户使用的页面中。例如 HTML 代码和客户端脚本，攻击者利用 XSS 漏洞绕过访问控制，获取数据，例如盗取账号等。AF 设备可以检测到此类攻击行为。

[网页木马]: 网页木马实际上是一个经过黑客精心设计的 HTML 网页。当用户访问该页面时，嵌入该网页中的脚本利用浏览器漏洞，让浏览器自动下载黑客放置在网络上的木马并运行这个木马。AF 设备可以检测到此类攻击行为。

[网站扫描]: 网站扫描是对 WEB 网站扫描，对 WEB 网站的结构、漏洞进行扫描。AF 设备可以检测到此类攻击行为。

[WEBSHELL]: WEBSHELL 是 WEB 入侵的一种脚本工具，通常情况下，是一个 ASP、PHP 或者 JSP 程序页面，也叫做网站后门木马，在入侵一个网站后，常常将这些木马放置在服务器 WEB 目录中，也正常网页混在一起。通过 WEBSHELL，长期操纵和控制受害者网站。AF 设备可以检测此类攻击行为。

[跨站请求伪造]: 通过伪装来自受信任用户的请求来利用受信任的网站。AF 设备可以检测到此类攻击行为。

[系统命令注入]: 攻击者利用服务器操作系统的漏洞，把 OS 命令利用 WEB 访问的形式传至服务器，获取其网络资源或者改变数据。AF 设备可以检测到此类攻击行为。

[文件包含攻击]: 文件包含漏洞攻击是针对 PHP 网站特有的一种恶意攻击。当 PHP 中变量过滤不严，没有判断参数是本地的还是远程主机上的时，就可以指定远程主机上的文件作为参数来提交给变量指向，而如果提交的这个文件中存在恶意代码甚至干脆就是一个 PHP 木马的话，文件中的代码或者是 PHP 木马就会以 WEB 权限被成功执行。AF 设备可以检测到此类攻击行为。

[目录遍历攻击]: 目录遍历漏洞就是通过浏览器向 WEB 服务器任意目录附加“..”，或者是在有特殊意义的目录附加“..”，或者是附加“..”的一些变形，编码访问 WEB 服务器的根目录之外的目录。AF 设备可以检测到此类攻击行为。

[信息泄露攻击]: 信息泄露漏洞是由于 WEB 服务器配置或者本身存在安全漏洞，导致一些系统文件或者配置文件直接暴露在互联网中，泄露 WEB 服务器的一些敏感信息，如用户名、密码、源代码、服务器信息、配置信息等。AF 设

备可以检测到此类攻击行为。

[WEB 整站系统漏洞]针对知名 web 整站系统中特定漏洞进行安全可靠高质量防护。

[自定义 WAF 规则]: 用户可自定义防护规则，对服务器进行防护，自定义规则在『安全防护对象』->『自定义规则库』中进行设置。

[WAF 云防护]: 云引擎智能分析您当前业务系统潜在的风险，针对发现的风险定制有效的 WAF 防护规则，并立即推送更新。

[应用隐藏]勾选后可以在高级配置当中设置

[口令防护]勾选后可以在高级配置当中设置

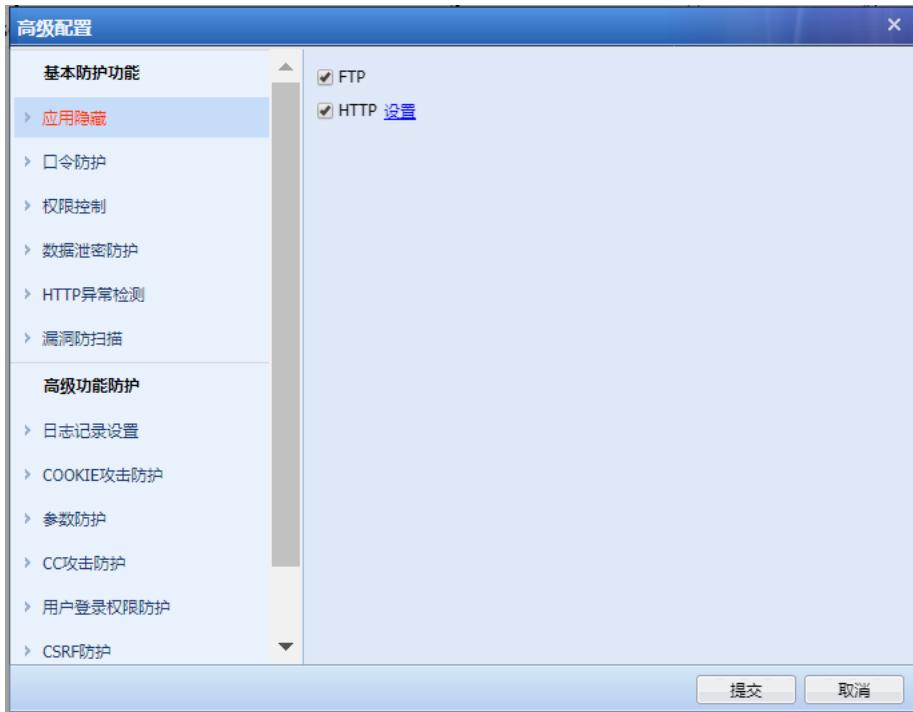
[权限控制]勾选后可以在高级配置当中设置

[数据泄密防护]勾选后可以在高级配置当中设置

[HTTP 异常检测]勾选后可以在高级配置当中设置

[漏洞防扫描]勾选后可以在高级配置当中设置

点击**高级配置**，会弹出界面如下：



1、优化 WEB 安全防护策略配置，突出重点防护功能，非重点选项全部移到高级里面，使配置更加简介，易于操作

[应用隐藏-FTP]: 客户端登录 FTP 服务器的时候，服务器会返回客户端 FTP 服务器的版本等信息。攻击者可以利用相应版本的漏洞发起攻击。该功能是隐藏 FTP 服务器返回的这些信息，避免被攻击者利用。勾选[FTP]即设置好了隐藏。

[应用隐藏-HTTP]: 当客户端访问 WEB 网站的时候，服务器会通过 HTTP 报文头部返回客户端很多字段信息，例如 Server、Via 等，Via 可能会泄露代理服务器的版本信息，攻击者可以利用服务器版本漏洞进行攻击。因此可以通过隐藏这些字段来防止攻击。勾选[HTTP]，点击**设置**，弹出的页面如下：



此处需要自定义 HTTP 报文头的内容，可以利用 HTTPWATCH 等抓包工具获取该服务器返回客户端的一些字段，并且填写到此处。勾选[替换 HTTP 出错页面]，则针对一些错误页面，例如服务器返回 500 错误的页面（该页面通常包含服务器信息），防火墙会用一个不包含服务器信息的错误页面来替换原始的错误页面。

[FTP 弱口令防护]：该防护针对 FTP 协议有效。主要是针对一些过于简单的用户名密码进行过滤，勾选[FTP 弱口令防护]，点击**设置**，弹出的页面如下：



勾选相应的弱口令规则，或者填写弱口令列表，点击**确定**保存设置即可。当防火墙检测到这种弱口令会产生日志记录提醒管理员，可以正常登录服务器。

[WEB 登录弱口令防护]针对 WEB 登录过程中的弱口令进行防护，启用即可。

[WEB 登录明文传输检测]针对 WEB 登录过程中的明文传输进行检测，启用即可。

[口令暴力破解防护]：该防护可以对 FTP 和 HTTP 生效。用于防止暴力破解密码。勾选[口令暴力破解防护]，点击**设置**，弹出的页面如下：



针对 FTP 的防暴力破解，只需要在上述页面勾选 FTP 即可。针对 HTTP 网站的登录防破解，需要填写相应的 URL。例如某网站的登录 URL 为 [http://www.\\*\\*\\*.com/login.html](http://www.***.com/login.html)。那么上述填写方式为 /login.html，如上图所示。[爆破次数]用于设置每分钟输入多少次错误密码后就被认定为暴力破解密码行为。

[文件上传过滤]: 主要是用于过滤客户端上传到服务器的文件类型，勾选[文件上传过滤]，点击**设置**，弹出的页面如下：



点击 可以下拉选择设备内置的一些文件类型，点击 ，则添加到列表。

如果要自定义的类型，可以直接在框里输入自定义的文件类型，点击 ，则添加到列表。

**[URL 防护]**: 该设置的主要功能是权限开关。例如禁止访问某个 URL，则上述的防攻击等都无效，因为客户端都无法访问，更不会存在攻击。如果此处允许某个 URL，则上述设置的防攻击等针对该 URL 都会无效，相当于一个白名单。

勾选**[URL 防护]**，点击**设置**，页面如下：

### URL防护设置

+ 添加 X 删除 | ✓ 记录日志 ⚡ 不记录日志 | 🛡 允许访问 🛡 拒绝访问

URL	描述	动作	日志	自动添加
/login.html		🛡️ ✓		否

确定 取消

此处的填写方式与防爆破类似，需要填写 URL 的后缀。例如某 URL 为 [http://www.\\*\\*\\*.com/login.html](http://www.***.com/login.html)，则此处填写 /login.html。

针对目前日益严重服务器数据泄密事件(如 CSDN、天涯被拖库)等，部署 Sangfor AF 设备后，启用数据泄密防护功能能够对这些敏感信息的泄露进行防护。

### 高级配置

**基本防护功能**

- ▶ 应用隐藏
- ▶ 口令防护
- ▶ 权限控制

敏感信息防护 [设置](#)

文件下载过滤 [设置](#)

短信告警

[防护对象排除](#)

勾选[数据泄密防护-敏感信息防护]，点击[设置](#)按钮，弹出【防护的敏感信息】编辑框，设置哪些信息是敏感信息，以及敏感信息命中次数的统计方式，页面如下图所示：



[命中次数统计方式]可以选择以 IP 统计或者以连接统计。以 IP 统计是指当有定义的敏感信息经过设备时以单个 IP5 分钟内的命中次数作为统计依据；以连接统计是指当有定义的敏感信息经过设备时以单个连接的命中次数作为统计依据。选择以连接统计后，默认会勾选上“启用联动封锁源 IP”。

点击**新增**按钮，设置敏感信息组合策略，勾选上哪些信息是敏感信息，设置这些敏感信息的组合策略，并设置界面如下：

敏感信息防护策略

选择要组合的敏感信息：(可选多条，必须同时满足勾选内容)

	序号	敏感信息名称	正则表达式
<input type="checkbox"/>	1	身份证	-
<input type="checkbox"/>	2	MD5	-
<input type="checkbox"/>	3	手机号码	-
<input type="checkbox"/>	4	银行卡号	-
<input type="checkbox"/>	5	邮箱	-

**内置敏感信息**

名称：

描述：

最低命中次数： 次

**提交** **取消**

可以在防护的敏感信息里添加多条敏感信息组合策略，每条策略称之为一个模式，每个模式里可以包含多个敏感信息，一个模式里若包含多个敏感信息，则要多个敏感信息全部匹配才算一次命中，大于等于最低命中次数后就被认为是泄密，而多个模式之间是或的关系，只要匹配其中的一个模式，就算一次命中。

由于某些敏感信息是以 word 或者是 excel 等文档形式保存的，通过从服务器上下载文档把这些敏感信息泄露出去，对于这种泄露方式，AF 可以通过过滤文件下载来进行防护。

勾选【数据泄密防护-文件下载过滤】，点击**设置**按钮，弹出【设置过滤文件类型】编辑框，选择需要过滤哪些文件后缀，页面如下图所示：



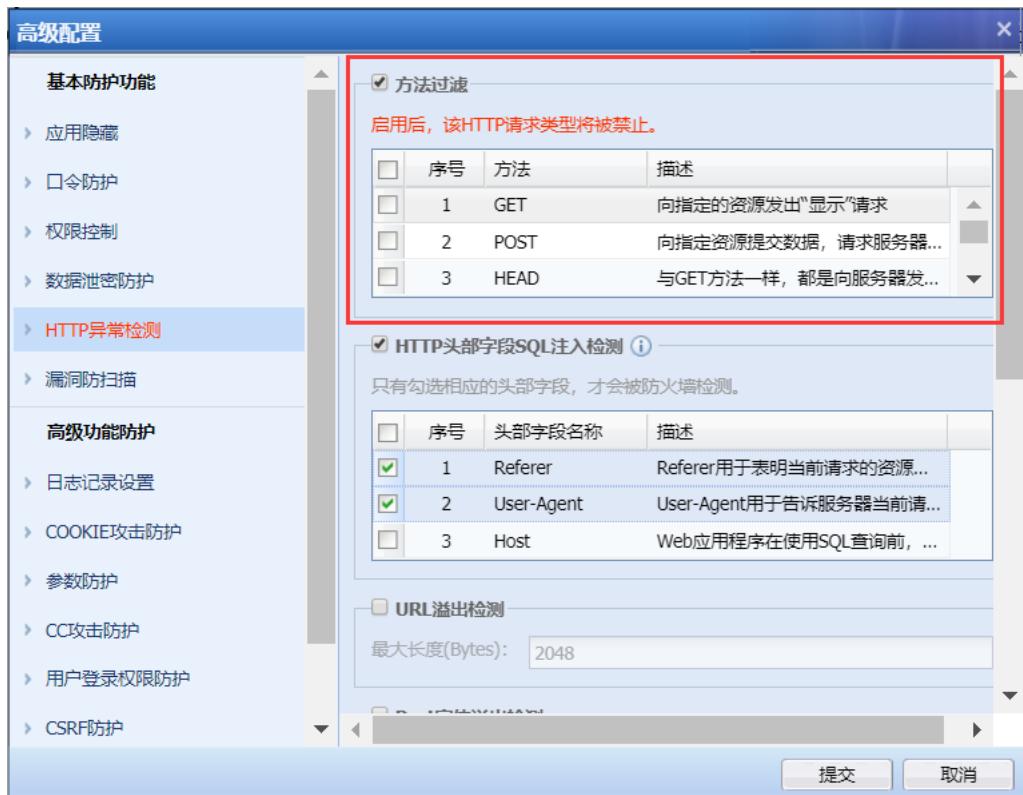
设备内置了一些常见的如网站数据备份文件后缀名、常用日志文件后缀名等，若还需要自定义文件类型，则点击**新增**按钮，添加需要过滤的文件后缀即可，界面如下：



勾选[数据泄密防护-短信告警]可对发生了数据泄密的行为进行短信告警。

点击数据泄密防护配置中的[防护对象排除](#)按钮，跳转到白名单设置，可以针对某些IP或URL进行排除设置，对于这些IP或URL不进行数据泄密防护。

[HTTP 异常检测-方法过滤]: 主要是用于设置允许的 HTTP 方法，点击[设置](#)，弹出的页面：启用后，该 HTTP 请求类型将被禁止。即勾选的 HTTP 方法会被策略判定为异常，进行拦截。



[HTTP 异常检测-HTTP 头部字段 SQL 注入检测]: 可以将 HTTP 头部中的 Referer、User-Agent、Host 字段进行 SQL 注入规则的检测。注：此功能要将 WEB 应用防护策略中的网站防护“sql注入”启用才能生效。

**HTTP头部字段SQL注入检测** (i)

只有勾选相应的头部字段，才会被防火墙检测。

序号	头部字段名称	描述
1	Referer	Referer用于表明当前请求的资源...
2	User-Agent	User-Agent用于告诉服务器当前请...
3	Host	Web应用程序在使用SQL查询前， ...

例如，勾选“Host”字段后，当检测到 SQL 注入攻击，数据中心标注的攻击类型依旧是 SQL 注入攻击，拦截部分为 HTTP 数据包的头部 Host 字段。

查询条件 | 导出日志 |

查询条件：时间(2015-09-10 00:00~2015-09-10 23:59) | 源区域(所有区域) | 源IP(所有) | 目的区域(所有区域) | 目的IP(所有) | 规则ID(所有) | 回复状态码(所有) | 域名/URL(所有) | 类型(所有类型) | 严重等级(高)

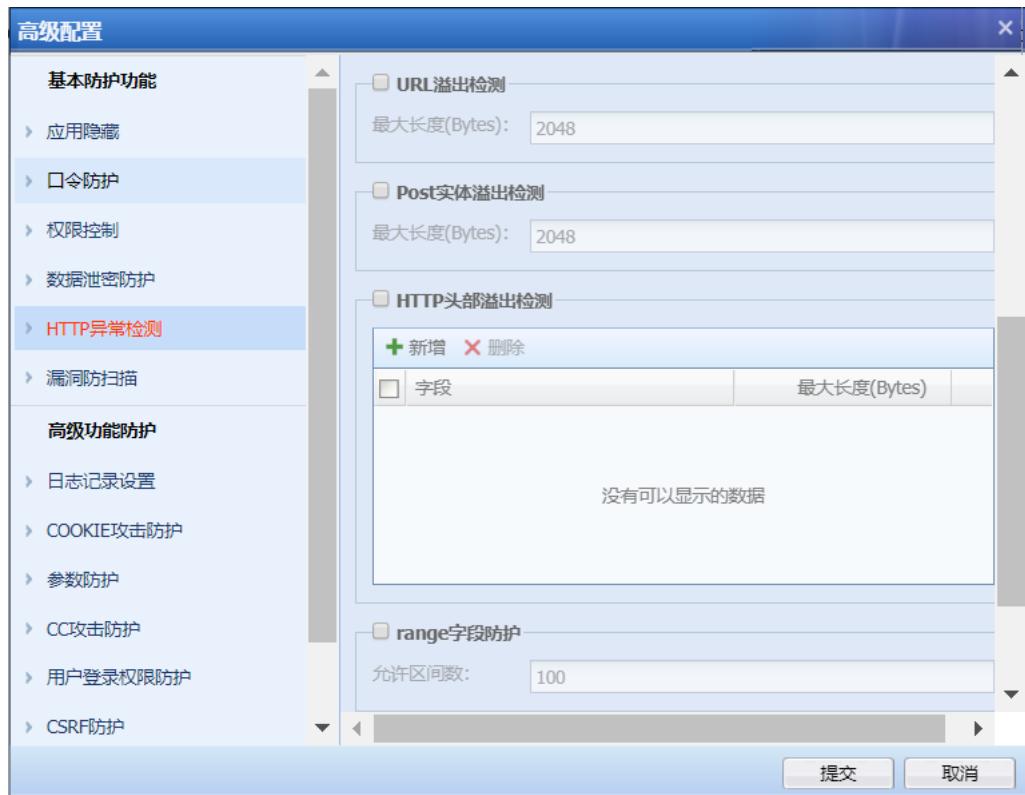
序号	时间	类型	URL/目录	源IP	源IP归属地	目的IP	规则ID号	描述	严重等级	动作	详细
1	2015-09-10 15:12:52	SQL 注入	172.16.100.220:... 192.200.200.226	-	192.168.1.20	13020001	攻击语句: and ...	高	拒绝	查看	
2	2015-09-10 15:09:47	SQL 注入	172.16.100.220:... 192.200.200.226	-	192.168.1.20	13020188	攻击语句: %0D...	高	拒绝	查看	
3	2015-09-10 15:06:39	SQL 注入	172.16.100.220:... 192.200.200.219	-	192.168.1.20	13110001	攻击语句: id=7...	低	拒绝	查看	
4	2015-09-10 14:17:23	信息泄漏攻击	172.16.100.220:... 192.200.200.226	-	192.168.1.10	13070577	攻击语句: You ...	中	拒绝	查看	

第 1 页，共 1 页 | 上一页 | 下一页 | 每页显示条数 50 | 当前显示1 - 4

**1. SQL 注入(高, 拒绝)**

时间: 2015-09-10 15:12:52      目的IP: 192.168.1.20  
源IP: 192.200.200.226      目的URL: 172.16.100.220:8080 and 1=1/jcsweb/  
数据包内容

REQUEST:  
GET /jcsweb/ HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
**Host: 172.16.100.220:8080 and 1=1**  
Referer: http://172.16.100.220:8080/  
Cookie: SF\_FIRST\_ACCESS\_SIGNPAGE=no; dbx-postmeta=grabit=0,-1,-2,-3,-4,-5,-6-&advancedstuff=0,-1,-2,-; SESSID=222CE5CED65B1C6CE906AA8B0A7CAC16BFEB275CE4D647647F9D3A742A21A5  
Connection: keep-alive

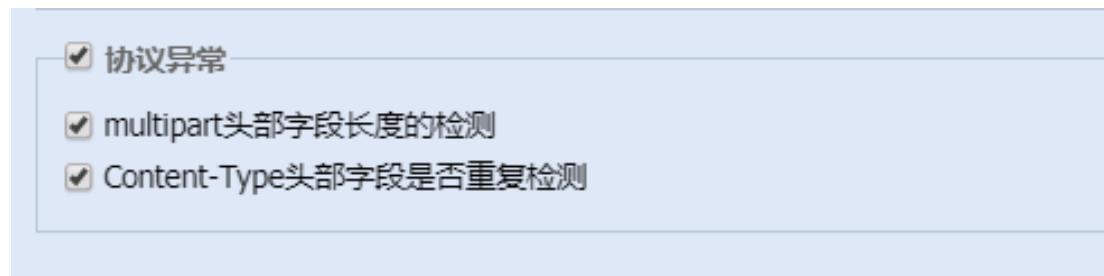


[HTTP 异常检测-URL 溢出检测]: 勾选[启用 URL 溢出检测]，设置最大长度，将会对 URL 的最大长度进行检测，防止造成缓冲区溢出。

[HTTP 异常检测-POST 实体溢出检测]: 勾选[启用 Post 实体溢出检测]，设置 Post 数据的实体部分的最大长度，防止造成服务器接收数据溢出的错误。

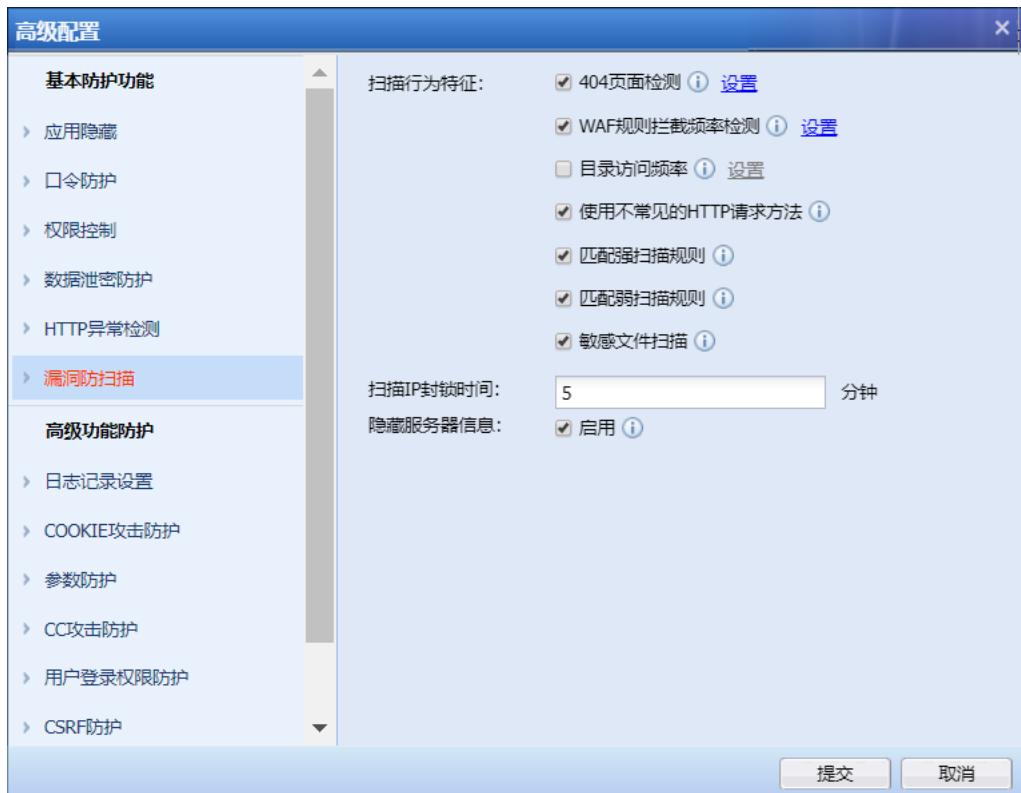
[HTTP 异常检测-HTTP 头部溢出检测]: 勾选[启用 HTTP 头部溢出检测]，点击**新增**按钮，设置需要检测 HTTP 头部中指定字段的最大长度，对该字段超出长度，进行检测。

[HTTP 异常检测-range 字段防护]: 勾选[range 字段防护]，设置允许区间数，防止 range 字段数超出允许区间。



[HTTP 异常检测-协议异常]: 主要是用于防护 ASP 和 ASPX 的页面中，请求多个参数被服务器错误处理，导致的复参攻击。同时，默认启用“multipart 头部字段长度的检测”和“Content-Type 头部字段是否重复检测”

[漏洞防扫描]用于设置 WEB 网站被扫描的行为检测，页面如下：



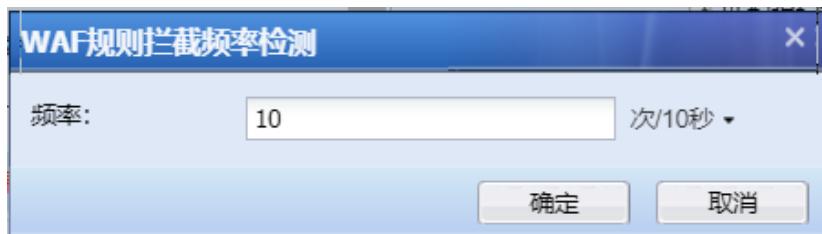
[漏洞防扫描-扫描行为特征]: 设置来访数据匹配哪些行为特征后，判定为扫描行为，并进行下一步的处置。该功能目前具备的行为特征说明如下：

[扫描行为特征-404 页面检测]: 每 N 个响应统计一次，如果 404 页面比例超过配置的百分比，认为是扫描器在扫描网站。具体的频率和比例，可以点击后面

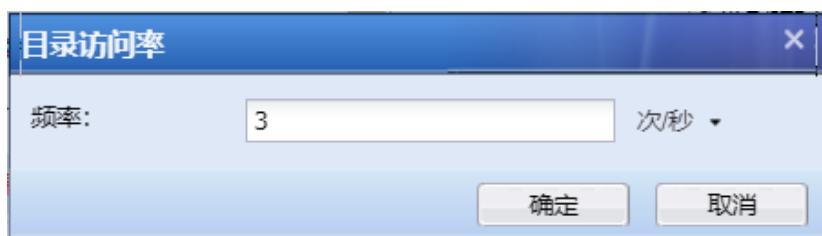
的设置进行设置，如下图：



[扫描行为特征-WAF 规则拦截频率检测]: 通过判断源 IP 在单位时间内被 WEB 应用防护规则拦截的次数来确定是否为扫描器。具体的频率设置，可以点击后面的设置进行设置，如下图：



[扫描行为特征-目录访问频率]: 通过判断源 IP 每秒访问目录的次数，来确定是否为扫描器。具体的频率设置，可以点击后面的设置进行设置，如下图：



[扫描行为特征-使用不常见的 HTTP 请求方法]: 触发 HTTP 方法过滤规则的行为将会作为扫描器的行为特征之一，需要开启方法过滤。

[扫描行为特征-匹配强扫描规则]: 通过强扫描规则进行匹配，来检测匹配上规则特征的 IP 是否为扫描器。

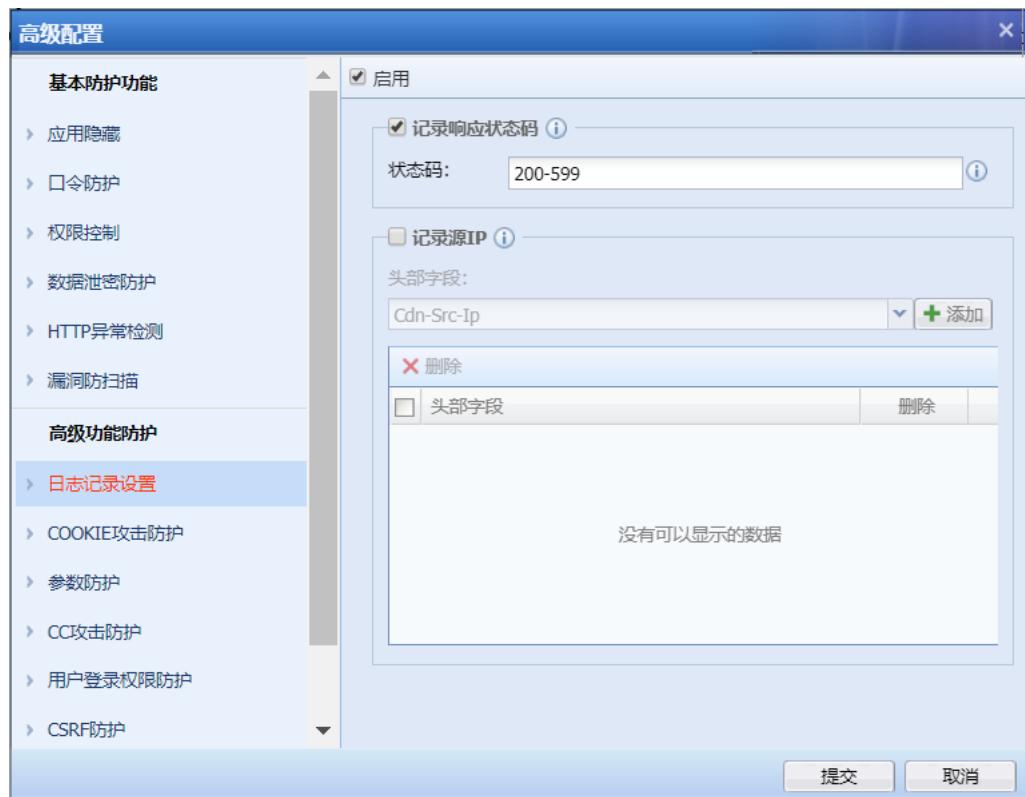
[扫描行为特征-匹配弱扫描规则]: 通过弱扫描规则进行匹配，来检测匹配上规则特征的 IP 是否为扫描器。

[扫描行为特征-敏感文件扫描]: 一般扫描器会尝试访问各种站点敏感文件，比如配置、密码、数据库文件等。通过对这些敏感文件的检测来确定 IP 是否是扫描行为。

[扫描 IP 封锁时间]: 当源 IP 被匹配为扫描行为后，会根据该选项设置的封锁时间，对源 IP 进行指定时间的封锁。封锁期，该源 IP 所有经过 AF 的数据均被拦截。

[隐藏服务器信息]: 开启此功能后，会智能识别并隐藏服务器的相关版本信息。

[日志记录设置]用于设置日志记录类型，页面如下：



[COOKIE 攻击防护] 根据 COOKIE 的属性值和客户端通信来检测 COOKIE

否被盗用或者篡改。配置如下



当 COOKIE 被篡改时可选择是否需要替换篡改,选择替换时,会将 COOKIE 替换为\*,可以指定 COOKIE 属性防护或不防护。



[参数防护-主动防御] 传统防 SQL 注入是基于特征的,但基于特征的防 SQL 注入系统无法解决 0day 和未知攻击问题。通过在设备上添加主动防御模型,提升 AF 的安全防护能力。配置如下



该项只需要启用即可，为设备自主学习，但达到主动学习阀值是，学习完成，自动绑定，相关参数。



效果图如下：

主动防御设置					所有页面	学习状态	启用否	编辑
序号	变量类型防篡改的URL	变量名			所有页面	已绑定页面	已完成学习页面	正在学习页面
1	/login.php	name, pwd			正在学习...	✓		
2	/news.php	type, id			已绑定 重学	✓		
3	/Product.php	id			完成学习 重学	✓		
4	/login.php	name, pwd			完成学习 重学	✓		

[参数防护-自定义参数防护]和主动防护功能类似，只是是自定义相关参数，支持正则表达式匹配，表示满足设置相关正则表达式的条件后，匹配动作为拒绝。

自定义参数规则设置

<input type="checkbox"/>	序号	URL	区分大小写	变量, 匹配条件, 取值正则表达式	状态	编辑
<input checked="" type="checkbox"/>	1	/bbs/login.asp	是	userid, 等于, qq号码		

[CC 攻击防护]: 用于防止针对网站发起的 CC 攻击。配置如下

启用

配置项

动作： 允许  拒绝

来源IP防CC

次数限制： 启用 [\(i\)](#)

检测时间：10 秒

触发阈值：500 次

Referer防CC

次数限制： 启用 [\(i\)](#)

检测时间：10 秒

触发阈值：500 次

特定URL防CC

次数限制： 启用 [\(i\)](#)

检测时间：10 秒

<a href="#">新增</a>	<a href="#">删除</a>	<a href="#">关键字搜索</a>
序号	目的URL	触发阈值(次)

没有可以显示的数据

[CC防护规则配置](#)

『来源 IP 防 CC』启用后，来源 IP 地址的访问次数超过设定上限的，禁止该 IP 地址的任何后续访问。

『Referer 防 CC』启用后，对于 Referer 中相同的 URL，累计访问次数超过设定上限的，禁止具有相同 Referer URL 的任何来源 IP 地址的访问。

『特定 URL 防 CC』启用后，来源 IP 地址对目的 URL 的访问次数超过设定

上限的，禁止该 IP 地址的任何后续访问。

『CC 防护规则配置』可以自定义 CC 防护规则。

[登录防护-用户登录权限防护] 客户网站中有管理页面，但不允许对管理页面的直接登陆，必须通过 AF 设备的短信认证后才能登陆管理页面，这就是用户登陆权限防护。支持 web 登录权限防护和非 web 登录权限防护。

### 用户登录权限防护设置

**WEB登录路径**

URL: WEB资源防护--即登陆URL的防护，  
200.200.155.192/phpwind/  
200.200.155.55/phpwind/login.php?  
200.200.155.55/phpwind/search.php  
200.200.155.55/p12.html

**非WEB资源防护**

非WEB登录方式  
选择需要保护的服务 (i) 预定义服务/ftp 选择需要防护的非WEB资源-TCP类型  
配置用于非WEB登录方式认证的URL (i) 主动认证的URL--访问后返回认证页面  
URL: http://200.200.155.192/phpwind/member.php

**允许短信验证号码**

一行一个，手机号和描述用空格隔开 (i)  
手机号 描述(可不填)  
12222222222 管理员手机号码  
测试短信猫是否可用  
发送测试短信

**验证通过后有效时间**

每次短信验证通过后,将在以下时间范围内不再验证  
30 分钟 白名单时间，认证后这段时间内无需再认证  
bypass，若无短信猫或短信猫失败，不做短信认证  
 允许Bypass,当检测到短信网关失败后,登录防护将自动取消短信认证



**配置用于非 WEB 登陆方式认证的 URL:** 此处配置一个不存在的 url, 用户访问此 url 时必须经过 AF 设备, AF 设备会抓取 TCP 连接并返回短信认证页面。若此处配置的 url 与客户内部网站的真实 URL 冲突, 用户将只能浏览到短信认证页面。

[CSRF 防护] 跨站伪造请求(Cross Site Request Forgery, CSRF), 也被称成为“one click attack”或者 session riding, 通常缩写为 CSRF 或者 XSRF, 是一种挟制终端用户在当前已登录的 Web 应用程序上执行非本意的操作的攻击方法。通过配置 CSRF 防护, 可以有效防止该类攻击行为。配置页面如下。

序号	需要防护的页面 (Target)	允许访问的来源页面 (Referer)	状态	编辑
1	/bbs.asp	/*	✓	

通过配置需要进行防护的域名, 已经新增需要防护的页面和允许访问的来源页面, 保证跳转只能从允许访问的来源页面 (Referer) 来访问需要防护的页面 (Target)。达到组织 CSRF 攻击的目的。

[受限 URL 防护] 保护用户的关键资源不被非法客户端强制浏览。配置如下。

受限URL防护设置

+ 新增		- 删除	✓ 启用	✗ 禁用	请输入搜索关键字	🔍
序号	网站域名	允许访问的起始页	状态	编辑		
1	www.sangfor.com.cn	/bbs/index.html	✓	✎		

仅允许从 [www.sangfor.com.cn/bbs/index.html](http://www.sangfor.com.cn/bbs/index.html) 访问 [www.sangfor.com.cn](http://www.sangfor.com.cn) 的域名主页，不允许通过其他方式的访问该域名。



1.URL 防护里的允许与拒绝操作是单独的，被策略引用后，与策略里匹配的检测攻击后操作[拒绝]没有关联，以 URL 防护里设置动作为为准。

2.短信告警只对数据泄密防护有效，对 WEB 应用防护无效。

### 3.4.3.3. 僵尸网络

『僵尸网络』主要用于发现和追踪内网感染了病毒、木马等恶意软件的 PC，当病毒、木马试图与外部网络通信时，AF 识别出该流量，并根据用户策略进行阻断和记录日志，其模板配置页面如下：

僵尸网络

+ 新增		- 删除	刷新	搜索
序号	名称	安全选项	删除	
1	默认模板	木马监控, 恶意链接, 移动安全, 异常流量	已被引用	×
2	防勒索-病毒扫描检测	木马监控, 恶意链接, 移动安全		

点击『安全策略模板』→『僵尸网络』进入模设置页面，在此页面可以对僵尸网络检测模板进行新增、删除。点击新增，弹出新增模板页面如下：



[模板名称]: 定义模板名称。

[描述]: 定义模板描述。

[安全选项]: 设置需要检测的攻击类型:

**木马远控:** 会对防护区域发出的或是请求防护区域的数据都进行木马远控安全检测。

**恶意链接:** 这里针对的是可能导致威胁的 URL, 如网页挂马、病毒下载链接。

**移动安全:** 针对智能移动终端的数据进行安全检测。

**异常流量:** 分两种, 一是对基于端口和协议不匹配的异常情况进行检测, 二是对异常的外发流量进行检测。对于检测出来的异常流量只记录日志, 不进行阻断。点击设

置, 选择需要检测的异常流量:

选择异常流量检测规则	
<input type="checkbox"/>	规则名称
<input type="checkbox"/>	3389端口异常
<input type="checkbox"/>	3389目的端口运行非RDP协议
<input type="checkbox"/>	RDP协议异常
<input type="checkbox"/>	RDP协议运行在非3389的目的端口
<input type="checkbox"/>	53端口异常
<input type="checkbox"/>	53目的端口运行非DNS协议
<input type="checkbox"/>	80/8080端口异常
<input type="checkbox"/>	80/8080目的端口运行应用识别无法识别的应用
<input type="checkbox"/>	21端口异常
<input type="checkbox"/>	21目的端口运行非FTP控制连接数据
<input type="checkbox"/>	69端口异常
<input type="checkbox"/>	69目的端口上运行非TFTP协议数据
<input type="checkbox"/>	443端口异常
<input type="checkbox"/>	443目的端口运行应用识别无法识别的应用
<input type="checkbox"/>	25端口异常
<input type="checkbox"/>	25目的端口运行非SMTP协议
<input type="checkbox"/>	110端口异常
<input type="checkbox"/>	110目的端口运行非POP3协议
<input type="checkbox"/>	143端口异常
<input type="checkbox"/>	143目的端口运行非IMAP协议
<input type="checkbox"/>	ICMP协议异常
<input type="checkbox"/>	ICMP包大于64Byte
<input type="checkbox"/>	22端口异常
<input type="checkbox"/>	22目的端口运行非SSH协议
<input type="checkbox"/>	SSH协议异常
<input checked="" type="checkbox"/>	外发流量异常 配置
	检测外发流量中的异常行为，识别被植入木马的情况

确定

取消

[外发流量异常]:一种启发式的dos攻击检测方法,能够检测源IP不变的syn flood、icmp flood、dns flood、udp flood攻击,当这些协议的外发包超过阀值时认为有异常流量,并自动开启抓包。检测阀值可以进行设置,配置界面如下:

高级配置

外发流量异常阈值配置

使用默认阈值      [查看默认阈值](#)

自定义阈值

ICMP外发流量异常      阈值:  包/秒

UDP外发流量异常      阈值:  包/秒

SYN外发流量异常      阈值:  包/秒

DNS外发流量异常      阈值:  包/秒

[确定](#) [取消](#)



1、异常流量的数据只记录日志不会进行阻断。

2、在『安全防护规则库』→『安全规则库』中可以设置每个僵尸网络规则的动作，设置为禁用的规则不会被拒绝。

#### 3.4.3.4. 内容安全策略

『内容安全策略』主要有邮件安全、URL 过滤、文件安全三种安全设置。[邮件安全]包含邮件内容检测和邮件附件过滤、邮件附件杀毒；[URL 过滤]主要是用于过滤符合设定条件的网页 URL 地址；[文件安全]包含文件过滤和文件杀毒；其配置页面如下：

序号	名称	邮件安全	URL过滤	文件安全	删除
1	默认模板	启用	禁用	禁用	X
2	防勒索-文件下载阻塞	启用	禁用	启用	X

点击『安全策略模板』→『内容安全策略』进入模板设置页面，在此页面可以对内容安全策略模板进行新增、删除。点击新增，弹出新增模板页面如下：

The dialog box contains the following fields:

- 名称:** (Name) input field.
- 描述:** (Description) input field.
- 安全配置 (Security Configuration):**
  - 邮件安全 (包含邮件内容检测和邮件附件过滤、邮件SAVE安全智能文件检测)
  - 邮件服务器端口: 25,110,143
  - 恶意邮件提示文本: 杀毒网关检测出该邮件携带恶意内容
- URL过滤 (URL Filtering):**
  - 已选站点: 成人内容,色情,赌博,非法药物,反动及其他非法内容,钓鱼及恶意网站
  - 文件安全 (包含文件过滤和SAVE安全智能文件检测)
- 生效时间 (Effective Time):** 全天 dropdown.
- Buttons:** [高级选项] (Advanced Options), [确定] (Confirm), and [取消] (Cancel).

[名称]: 定义模板名称。

[描述]: 定义模板描述。

[邮件安全]: 包含邮件内容检测和邮件附件过滤、邮件附件杀毒。

**邮件服务器端口:** 默认有 25,110,143 三个端口，如果是加密的邮件协议，需要开启上网场景解密功能。

**恶意邮件提示文本:** 用户在接收到恶意邮件时，邮件主题上会增加该风险提示。

[URL]过滤: 主要是用于过滤符合设定条件的网页 URL 地址。

[文件安全]: 包含文件过滤和文件杀毒。

[生效时间]: 过滤条件，在指定的时间内过滤规则才生效。该处是调用『对象』→『时间计划』中定义好的时间对象。

[高级选项]: 设置邮件安全、URL 过滤、文件安全里的相关过滤条件、过滤类型和阀值



## 邮件安全设置

[内容检测]: 针对异常账号检测到连续失败次数超过了阀值则被认为是威胁，如果勾选了检测出威胁后操作为[拒绝]，则检测到威胁后，会拒绝异常账号的邮件发送。

[附件过滤]: 设置需要过滤的邮件附件类型，如果检测威胁后动作为拒绝的话，附件包含此列表中文件类型的邮件将被拒绝发送。

[SAVE 安全智能文件检测]: 用于定义需要杀毒的附件类型，仅对此列表中的附件类型进行邮件杀毒。

## URL 过滤设置

[URL 过滤类型]: 用于设置针对指定的 URL 分类进行 HTTP(get)、HTTP(post)、HTTPS 过滤。例如需要过滤内网用户不能浏览某种类型网页就勾选 HTTP(get)；需要设置内网用户只能浏览网页但不能上传文件到网站上（如 BBS 发帖），则勾选 HTTP (post)；如需要对 HTTPS 类型的网站不允许访问网站或者仅允许浏览网页不允许上传，则可同时勾选 HTTPS 和 HTTP(get) 或者同时勾选 HTTPS 和 HTTP (POST)。

## 文件安全设置:

[文件过滤]: 用于过滤通过 HTTP 上传或者下载某些格式的文件

[SAVE 安全智能文件检测]: 用于定义需要杀毒的文件扩展名，仅对此列表中的文件类型进行杀毒。此文件类型杀毒仅适用于 HTTP 和 FTP 应用。

## 3.4.4. 安全防护规则库

『安全防护规则库』包含安全规则库和自定义规则库。

### 3.4.4.1. 安全规则库

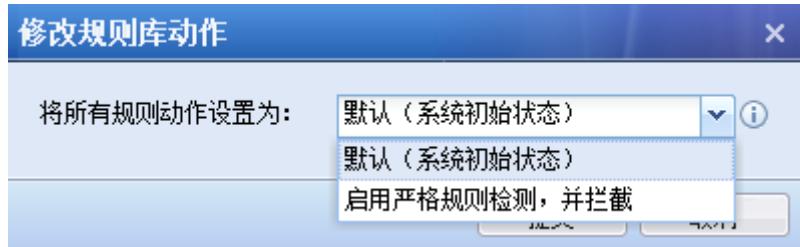
『安全规则库』包含 WEB 应用防护特征库、漏洞攻击特征识别库、数据泄密防护识别库、热门威胁库、实时漏洞分析识别库和云防护规则库。选择不同的识别库类型进行不同的设置。

#### 3.4.4.1.1 WEB 应用防护特征库

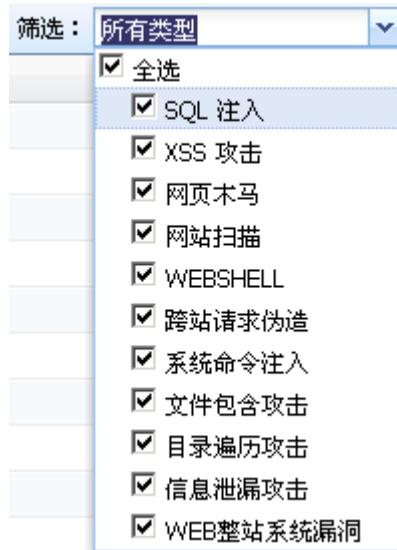
『WEB 应用防护特征库』内置了利用 SQL 注入、XSS 攻击、网站木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等的应用层攻击包特征，当这些攻击包穿越设备时，可以根据用户设置拦截该攻击包，以保护服务器。界面如下：

安全规则库					
识别类型：WEB应用防护识别库		修改规则库动作			
规则ID	防护名称	类型	危险等级	动作	筛选：所有类型
13121087	用友 param 远程代码执行漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121086	Phpcms query.php SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121085	Phpcms2008 search.php XSS注入攻击	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121084	Phpcms Authkey 任意世界漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121083	Phpcms 后台远程代码执行漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121082	Phpcms2008 data.php SQL注入攻击	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121081	Phpcms v9 poster_click SQL注入攻击	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121079	Discuz X3 奇子直播间块代码型XSS注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121078	Discuz 7.2 search.php SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121077	Discuz 6.0 viewthread.php XSS注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121076	Discuz 5.5/6.0 SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121075	WordPress Plugin Automatic SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121074	Wordpress membership-simplified-for-oap-members-only 插件目录遍历漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121073	Joomla com_flexicontent 远程代码执行漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121072	Discuz 全版本 memcp.php 远程SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121071	Discuz 7.2 admincp.php XSS注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121070	Discuz 7.x 代码执行漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121069	Dedecms sys_verifies.php 远程代码执行漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121068	Dedecms search.php SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121067	ECSHOP user.php 远程代码执行漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
13121066	用友致远A6协同管理软件信息泄露漏洞	WEB整站系统的漏洞	中	启用, 检测后放行	
13121065	Dedecms recommend.php SQL注入漏洞	WEB整站系统的漏洞	高	启用, 检测后拦截	
显示 1 - 50 条, 共 3595 条					

点击 **修改规则库动作** 用于统一的修改 WEB 应用防护规则。若选择[默认（系统初始状态）]，则将保留系统自带的规则状态；若选择[启用严格规则检测，并拦截]，则对于所有防护规则的动作都将设置为“启用，检测后拦截”。对于危险等级为中的规则来说，系统默认的状态会放行的，启用严格检测后，危险等级所有的规则也将被拦截。



『防护类型』显示当前防护类型的规则库，点击▼，可以根据防护类型查看对应的规则 ID。界面如下：

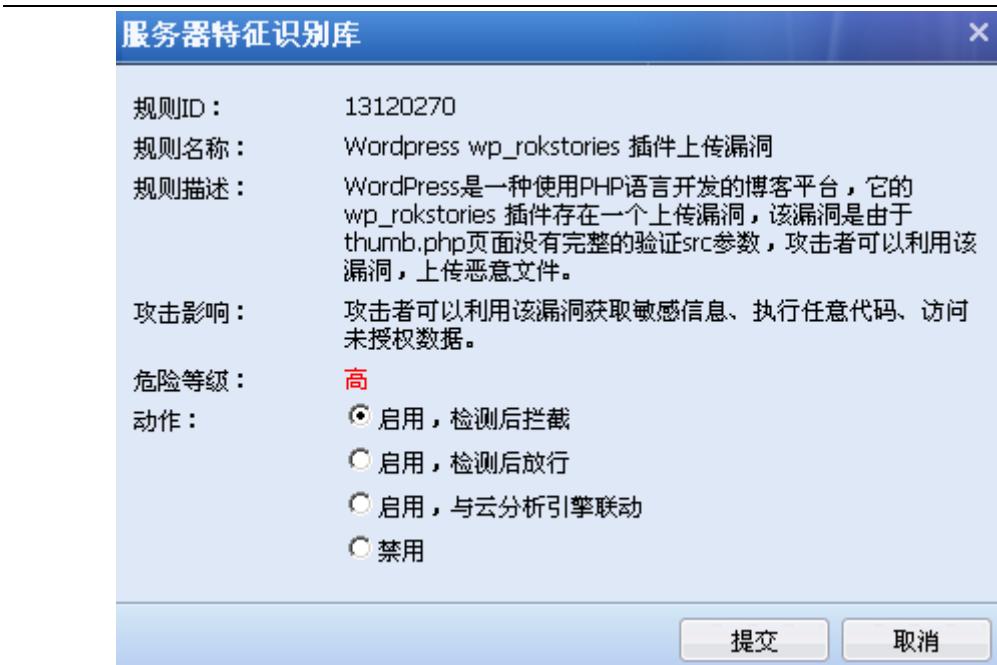


『防护名称』显示该防护规则对应的名称。

『类型』显示当前防护规则对应的防护类型，如 SQL 注入。

『危险等级』描述此漏洞的危险等级，一般有高、中、低三个等级，等级越高的则危险程度越高。

『动作』描述如果设备检测到该攻击行为时，设备所采取的动作，包括[启用，检测拦截]、[启用，检测后放行]、[启用，与云分析引擎联动]、[禁用]四种。这个动作可以自定义，点击『防护名称』即可进入编辑页面，如下图：



[启用, 检测后拦截]: 表示启用当前规则, 当检测到此攻击的行为时, 拦截相应的数据包。

[启用, 检测后放行]: 表示启用当前规则, 当检测到有攻击的行为时, 只是记录日志, 并不会拦截。

[启用, 与云分析引擎联动]: 表示启用当前规则, 当有利用此漏洞进行攻击的行为时, 拦截相应的数据包, 并利用云技术进行分析检测。

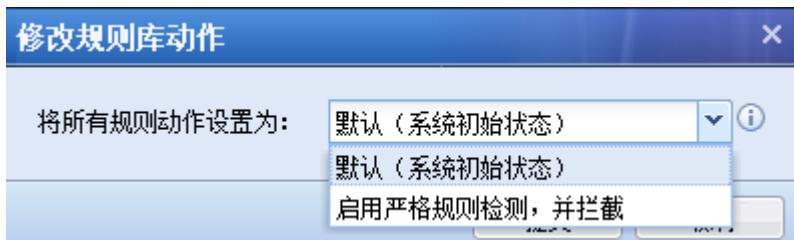
[禁用]: 表示禁用当前规则, 当规则禁用后, 设备不会对该规则进行检测。

### 3.4.4.1.2 漏洞攻击特征识别库

『漏洞攻击特征识别库』内置了利用系统、应用程序漏洞而进行攻击的攻击包特征, 当这些攻击包穿越设备时, 可以根据用户设置拦截该攻击包, 以保护服务器。界面如下:

安全规则库		漏洞类别: 所有漏洞		查询类别: 漏洞名称		输入进行搜索
<input checked="" type="checkbox"/>	修改规则库动作					
<input type="checkbox"/>	启用					
<input type="checkbox"/>	禁用					
<input type="checkbox"/>	恢复规则默认动作					
漏洞ID - 漏洞名称		类型	危险等级	动作		
<input type="checkbox"/>	12030569 Ghostscript 远程代码执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030568 UEEditor任意文件上传漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030567 Parallel Plesk Panel任意PHP代码注入漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030566 Dolibarr 多个HTML注入漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030565 ManageEngine Applications Manager 远程代码执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030564 Oracle Financial Services Analytical Applications Infrastructure 远程安全漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030563 Apache Solr Lucene 信息泄漏和远程代码执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030562 Supervisor 任意命令注入漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030561 Memcached 多个整数溢出漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030560 NUUO 和 Netgear Network Multiple Products远程代码执行身份验证	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030559 ManageEngine SelfService Plus 远程代码反射型XSS漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030558 Manage Engine应用管理模块任意命令执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030557 Polycom RealPresence资源管理模块路径泄露漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030555 Polycom RealPresence资源管理模块路径泄露漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030549 Novel ZenWorks Configuration Management 11.3.1目录穿越与命令执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030548 PHPMyAdmin 1.1.2远程代码执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030546 IBM Tivoli Endpoint Manager程序HTML注入漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030545 Persistent Systems Radia Client Automation远程代码执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030544 Lexmark MarkVision Enterprise任意文件上传漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030543 ManageOwnage系列产品非认证用户上传漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030542 Lotus Mail Encryption Server异地文件包含漏洞	Application漏洞攻击	高	启用, 检测后拦截		
<input type="checkbox"/>	12030541 Enalean Tuleap远程代码执行漏洞	Application漏洞攻击	高	启用, 检测后拦截		

『修改规则库动作』：用于统一的修改漏洞攻击特征识别规则。若选择[默认（系统初始状态）]，则将保留系统自带的规则状态；若选择[启用严格规则检测，并拦截]，则对于所有识别规则的动作都将设置为“启用，检测后拦截”。对于危险等级为中的规则来说，系统默认的状态会放行的，启用严格检测后，危险等级所有的规则也将被拦截。



『恢复规则默认动作』：用于将修改过的规则动作全部恢复到默认状态。

漏洞攻击漏洞规则支持搜索功能，可以通过设置[漏洞类别]、[查询类别]，输入漏洞名称、ID 等关键词进行搜索，如下图所示：

漏洞类别:	所有漏洞	查询类别:	漏洞ID	输入进行搜索
-------	------	-------	------	--------

『漏洞 ID』显示当前漏洞的 ID，主要作用是当服务器被某个漏洞攻击规则拦截了，可以到数据中心查看到漏洞 ID，通过此处的漏洞 ID 查询，可以设置不拦截此规则。

『漏洞名称』显示漏洞名称。

『类型』显示当前漏洞的类型，如 backdoor。

『危险等级』描述此漏洞的危险等级，一般有高、中、低三个等级，等级越高的则危险程度越高。

『动作』描述当存在利用该漏洞进行的攻击时，设备所采取的动作，包括[启用、检测后拦截]、[启用，检测后放行]、[禁用]四种。这个动作可以自定义，点击『漏洞名称』即可进入编辑页面，如下图：



[启用，检测后拦截]: 表示启用当前规则，当有利用此漏洞进行攻击的行为时，拦截相应的数据包。

[启用，检测后放行]: 表示启用当前规则，当有利用此漏洞进行攻击的行为时，只是记录日志，并不会拦截。

[禁用]: 表示禁用当前规则，当规则禁用后，设备不会对该漏洞进行检测。



1.漏洞特征库的放行和拦截属性出厂已经配置好，当需要修改某条规则的时候，编辑该条规则即可。

### 3.4.4.1.3 数据泄密防护识别库

『数据泄密防护识别库』内置了一些敏感信息的正则表达式，如身份证、手机号码、银行卡号等等，和允许自定义敏感信息，启用了数据泄密防护功能后，当这些敏感信息经过设备时，设备会进行拦截，以保护用户敏感信息不被泄露出去。这些内置的规则不允许编辑或删除，支持在线升级。界面如下：



序号	名称	描述
1	身份证	居民身份证
2	MDS	MDS值,支持32位
3	手机号码	手机号
4	银行卡号	常见银行卡号
5	邮箱	常用电子邮箱

点击 **白名单设置** 用于设置针对哪些 IP、以及哪些 URL 不进行数据泄密防护，界面如下：



编号	排除IP	描述	删除

点击**新增**按钮，弹出【排除 IP】对话框，界面如下：

**排除IP**

**排除IP:** (可输多个, 每行一个)

可以直接在此处输入、编辑、删除

**描述:**

对IP进行描述, 也可以为空

**提交** **取消**

选择“排除 URL”点击**新增**按钮，弹出【排除 URL】对话框，界面如下：

**排除URL**

**排除URL:** ⓘ

例如: /path/index.html  
/admin/index.asp  
/path/directory/

**描述:**

对URL进行描述, 也可以为空

**提交** **取消**

#### 3.4.4.1.4 热门威胁库

『热门威胁库』包含了木马、木马远控、僵尸网络、蠕虫、未知、恶意脚本、

勒索软件、病毒文件、仿冒页面、非法内容、挖矿这 11 类规则防护类型，页面如下：

序号	类型	标签	危险等级	所有类型	标签
1	病毒文件	HTML/ScrInject.B.Gen, Gen	高	木马	
2	病毒文件	JS/TrojanDownloader.Iframe.NKE, NKE	高	木马远控	
3	病毒文件	HTML/ScrInject.B.Gen, Gen	高	僵尸网络	
4	病毒文件	HTML/ScrInject.B.Gen, Gen	高	蠕虫	
5	病毒文件	HTML/ScrInject.B.Gen, Gen	高	未知	
6	病毒文件	HTML/ScrInject.B.Gen, Gen	高	恶意脚本	
7	病毒文件	HTML/ScrInject.B.Gen, Gen	高	勒索软件	
8	病毒文件	HTML/ScrInject.B.Gen, Gen	高	病毒文件	
9	病毒文件	AdWare.Win32.OutBrowse.ch, OutBrowse	低	仿冒页面	
10	病毒文件	HTML/ScrInject.B.Gen, Gen	高	非法内容	
11	病毒文件	HTML/ScrInject.B.Gen, Gen	高	挖矿	
12	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
13	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
14	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
15	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
16	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
17	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
18	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
19	病毒文件	Adware.Win32.AdwareSig.att, AdwareSig	高		
20	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
21	病毒文件	HTML/ScrInject.B.Gen, Gen	高		
22	病毒文件	HTML/ScrInject.B.Gen, Gen	高		

『规则状态』：可以查看所有启用或禁用状态下的规则。

『类型』：包括木马、木马远控、僵尸网络、蠕虫、未知、恶意脚本、勒索软件、病毒文件、仿冒页面、非法内容、挖矿这 11 种防护类型

『启用』：启用选定的规则库。

『禁用』：禁止选定的规则库。

### 3.4.4.1.5 实时漏洞分析识别库

『实时漏洞分析识别库』内置了一些漏洞规则，用于发现用户网络中存在的 一些安全漏洞问题，并以报表的形式把漏洞的危害和解决办法展现给用户。漏洞 规则包括了：WEB 服务器漏洞、database 服务器漏洞、FTP 服务器漏洞、mail 服务器漏洞、ssh 服务器漏洞等。

通过在『策略』→『安全策略』→『安全防护策略』→『业务防护策略』→『实时漏洞分析』中进行设置，对指定的数据进行实时漏洞分析。

界面如下：

规则ID	规则名称	类别	危险等级	动作
15090285	SMB 远程代码执行漏洞	SMB漏洞	高	启用
15090284	Drupal拒绝服务漏洞	cms漏洞	高	启用
15090283	WordPress拒绝服务漏洞	cms漏洞	高	启用
15090282	JCMS 2010 数据库本地文件读取漏洞	cms漏洞	高	启用
15090281	JCMS 2010 SQL注入漏洞	cms漏洞	高	启用
15090280	JCMS 2010 文件上传漏洞	cms漏洞	高	启用
15090279	JCMS 2010 文件包含漏洞	cms漏洞	高	启用
15090278	KingCMS 5.0 Fckeditor上传webshell漏洞	cms漏洞	高	启用
15090277	Joomla Zap Calendar组件跨站脚本漏洞	cms漏洞	高	启用
15090276	Joomla Flexicontent 组件远程代码执行漏洞	cms漏洞	高	启用
15090275	Joomla Explorer组件跨站脚本漏洞	cms漏洞	高	启用
15090274	Joomla Multi Calendar组件跨站脚本漏洞	cms漏洞	高	启用
15090273	Joomla 2.5 远程权限漏洞	cms漏洞	高	启用
15090272	Joomla 3.2 SQL注入漏洞	cms漏洞	高	启用
15090271	Joomla 3.2 HTML注入漏洞	cms漏洞	高	启用
15090270	Joomla Simple File Lister 组件本地文件包含漏洞	cms漏洞	高	启用
15090269	Joomla Jobloader 组件本地文件包含漏洞	cms漏洞	高	启用
15090268	Joomla JoomTouch 组件本地文件包含漏洞	cms漏洞	高	启用
15090267	Drupal v6 OpenID模块认证绕过漏洞	cms漏洞	高	启用
15090266	Drupal v6 上传模块多个权限许可和访问控制漏洞	cms漏洞	高	启用
15090265	Drupal v6 OpenID模块用户认证绕过漏洞	cms漏洞	高	启用
15090264	Drupal v6 OpenID模块用户认证绕过漏洞	cms漏洞	高	启用

页面右上角，可以输入规则名称或规则 ID 查找规则。

在[筛选]中点击 ，出现如下页面：显示设备内置的漏洞类型，可勾选相应  
的类型筛选规则：

筛选: 所有类型

全选

WEB服务器漏洞

database服务器漏洞

ftp服务器漏洞

mail服务器漏洞

ssh服务器漏洞

vnc服务器漏洞

ldap服务器漏洞

网页编辑器漏洞

cms漏洞

SQL注入漏洞

远程文件包含漏洞

系统命令注入漏洞

文件上传漏洞

跨站脚本(XSS)漏洞

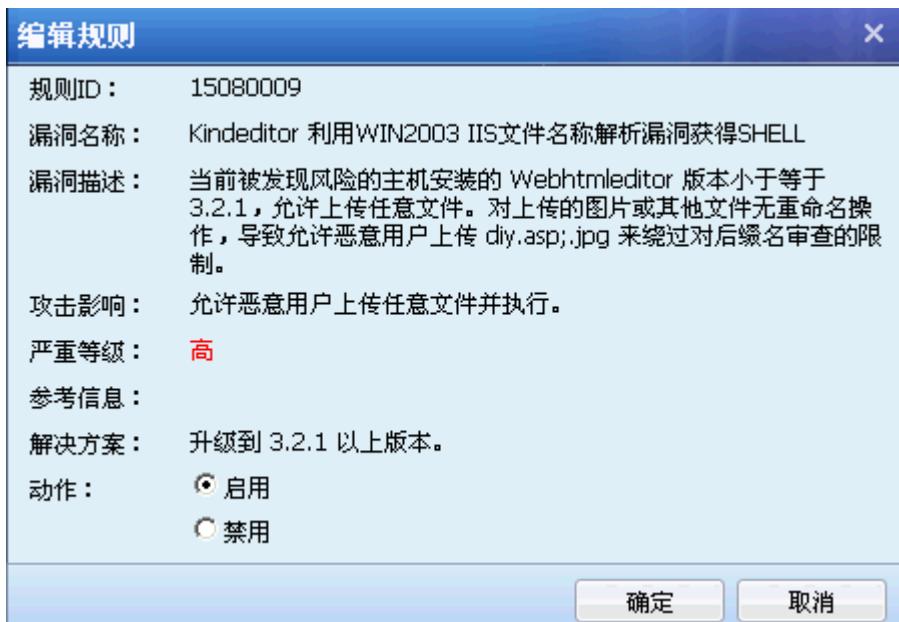
目录遍历漏洞

配置错误漏洞

WEBSHELL 文件访问

其他类型漏洞

点击某一条规则的名称，可以查看到规则详情：



『漏洞名称』：显示该漏洞对应的名称。

『漏洞描述』：显示关于该漏洞的详细解释。

『攻击影响』：显示该漏洞可能导致的后果。

『严重等级』：描述此漏洞的危险等级，一般有高、中、低三个等级，等级越高的则危险程度越高。

『解决方案』：显示避免改漏洞可采用的方法。

『动作』：包括启用和禁用两类，当漏洞禁用后，设备不会对该漏洞进行检测。

### 3.4.4.1.6 云防护规则库

『云防护规则库』是收集一些异常的流量上报云端，云引擎自动分析，发现风险或漏洞后由防火墙技术专家审核并制定规则有效的防护规则，及时下发生

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

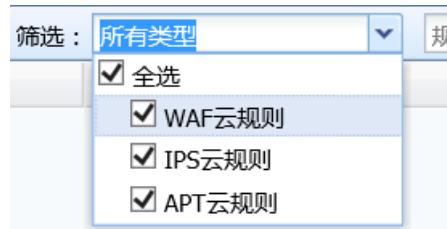
效。 界面如下：



规则ID	规则名称	规则类型	危险等级	动作
21130006	恶意IP(180.97.106.162)封禁	IPS云规则	高	启用, 检测后拦截
21130005	恶意IP(180.97.106.161)封禁	IPS云规则	高	启用, 检测后拦截
21130004	恶意IP(180.97.106.37)封禁	IPS云规则	高	启用, 检测后拦截
21130003	恶意IP(180.97.106.162)封禁	IPS云规则	高	启用, 检测后拦截
21130002	恶意IP(180.97.106.161)封禁	IPS云规则	高	启用, 检测后拦截
21130001	恶意IP(180.97.106.37)封禁	IPS云规则	高	启用, 检测后拦截

『修改规则库动作』：用于统一的修改云安全防护规则。若选择[默认（系统初始状态）]，则将保留系统自带的规则状态；若选择[启用严格规则检测，并拦截]，则对于所有识别规则的动作都将设置为“启用，检测后拦截”。对于危险等级为中的规则来说，系统默认的状态会放行的，启用严格检测后，危险等级所有的规则也将被拦截。

『筛选』：可以查看所有规则类型，包含 WAF 云规则、IPS 云规则和僵尸网络云规则。页面如下：



1、下发弱规则，只收集异常流量，上传云端。

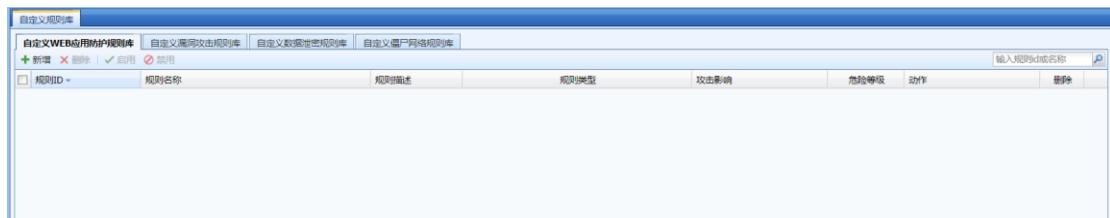
2、再有这种异常流量即可防护，现在可以针对 utm、漏洞攻击防护、waf 策下规则。

### 3.4.4.2. 自定义规则库

『自定义规则库』分为『自定义 WEB 应用防护规则库』、『自定义漏洞攻击规则库』、『自定义数据泄密规则库』和『自定义僵尸网络规则库』四类，可根据需要自定义相关规则。

### 3.4.4.2.1 自定义 WEB 应用防护规则库

『自定义 WEB 应用防护规则库』包括自定义 waf 规则和 CC 防护规则。界面如下：



在『自定义 WEB 应用防护规则库』页面，点击新增：

『规则名称』、『描述』、『攻击影响』可根据情况自己定义。

『规则名称』：可选自定义 WAF 规则和 CC 防护规则。

『危险等级』：可以选择高、中、低三个级别，用于定义规则的等级。

『动作』：可选择[启用，检测后拦截]、[启用，检测后放行]、[禁用]三类。

[启用，检测后拦截]：表示启用当前规则，当检测到此攻击的行为时，拦截相应的数据包。

[启用，检测后放行]：表示启用当前规则，当检测到有攻击的行为时，只是记录日志，并不会拦截。

[禁用]：表示禁用当前规则，当规则禁用后，设备不会对该规则进行检测。

『字符串』、『正则表达式』、『匹配方向』用于设置规则内容，其中前两项可留空，留空则代表跳过此项匹配。

### 3.4.4.2.2 自定义漏洞攻击规则库

在『自定义漏洞攻击规则库』页面，点击新增：

### 新增自定义IPS规则

规则ID: 12990000 (i)

规则名称:

描述: 可以直接在此处输入、编辑、删除

攻击影响: 可以直接在此处输入、编辑、删除

危险等级: 高

动作: 启用, 检测后拦截

字符串:  区分大小写 (i)  
可以直接在此处输入、编辑、删除

正则表达式:  区分大小写 正则表达式测试  
可以直接在此处输入、编辑、删除

匹配方向: 请求方向

协议: TCP

端口:

保护类型: 保护服务器

保存并新增 提交 取消

『规则名称』、『描述』、『攻击影响』可根据情况自己定义。

『危险等级』：可以选择高、中、低三个级别，用于定义规则的等级。

『动作』：可选择[启用, 检测后拦截]、[启用, 检测后放行]、[禁用]三类。

[启用, 检测后拦截]: 表示启用当前规则，当检测到此攻击的行为时，拦截相应的数据包。

[启用, 检测后放行]: 表示启用当前规则，当检测到有攻击的行为时，只是记录日志，并不会拦截。

【禁用】：表示禁用当前规则，当规则禁用后，设备不会对该规则进行检测。

『字符串』、『正则表达式』、『匹配方向』、『协议』、『端口』用于设置规则内容及数据匹配条件，其中前两项可留空，留空则代表跳过此项匹配。

『保护类型』：用于选择漏洞攻击防护规则保护的对象类型。

### 3.4.4.2.3 自定义数据泄密规则库

『自定义数据泄密规则库』用于用户自己定义哪些信息是敏感信息，页面如下：



点击新增按钮，弹出【新增敏感信息】对话框，用户输入敏感信息的正则表达式即可自定义敏感信息，界面如下：



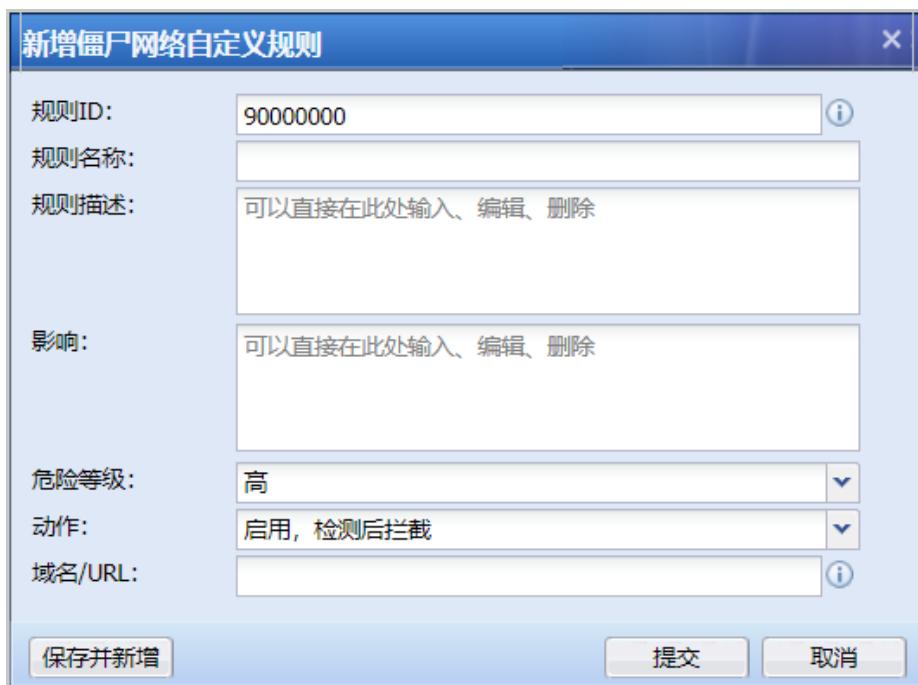
点击 白名单设置 用于设置针对哪些 IP、以及哪些 URL 不进行数据泄密防护。同『数据泄密防护规则库』页面中的功能一致。

### 3.4.4.2.4 自定义僵尸网络规则库

『自定义僵尸网络规则库』用于用户自己定义哪些 URL 属于僵尸网络需要检测和防护的，页面如下：



点击新增按钮，弹出【新增僵尸网络自定义规则】对话框，界面如下：



『规则 ID』：自定义的规则 ID 编号

『规则名称』、『规则描述』、『影响』：可根据情况自己定义。

『危险等级』：可以选择高、中、低三个级别，用于定义规则的等级。

『动作』：可选择[启用，检测后拦截]、[禁用]两类。

『域名/URL』：定义规则需要匹配的域名/URL。。

### 3.4.5. 内容识别库

#### 3.4.5.1. 应用识别库

##### 3.4.5.1.1 应用特征识别库

应用特征识别库是用来判断和检测上网数据的应用类型的，根据数据包的特征值或者协议、端口、方向、数据包长度匹配、数据包内容匹配等多个条件来检测应用类型，能够很好的检测通过端口或协议无法区分的应用类型，比如 QQ、P2P 等。

应用特征识别库分为内置规则和自定义规则，内置规则不可修改，由设备定时更新，更新内置库需要序号授权，且保证设备能够上网；自定义规则可以增加、删除、修改等（自定义规则详细介绍见章节 3.4.5）。

用户可以在『策略』→『应用控制策略』中引用应用识别规则，对相关的应用做控制。

##### 3.4.5.1.1.1 查看应用识别规则

在【导航菜单】页面中的『对象』→『内容识别库』，右边进入【应用特征识别库】页面：

应用识别库

应用总数：1209; 规则总数：3029

筛选：全部 搜索：请输入搜索关键字

应用分类	具体应用（网络流媒体）	规则数量	应用规则状态	操作
IM类文件(116)	RTSP MMS WinMediaPlayer Flash视频 MP4视频 M4V视频 Silverlight Macromedia视频 腾讯视频 优酷视频 新浪视频 搜狐视频 酷6视频 56网视频	2 2 1 5 2 1 1 3 20 17 14 23 6 6	全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用 全部启用	[规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置] [规则设置]
游戏(216)				
IM(169)				
P2P流媒体(47)				
P2P(25)				
下载工具(21)				
HTTP应用(12)				
FTP(5)				
邮件(7)				
DNS(2)				
远程登录(37)				
网络会议(34)				
网络共享(1)				
TCP(1)				
SSL(1)				
数据库(6)				
代理工具(33)				
办公OA(38)				
木马控制(67)				
网上银行(17)				
软件更新(24)				
股票行情(61)				

显示 1 - 15 条, 共 55 条

[应用总数：1209； 规则总数：3029]：显示的是设备当前内置的规则识别库中的应用总数和规则总数。

[应用特征识别库版本]：显示当前的内置规则识别库的版本。

[升级有效期至]：显示的是内置规则识别库的升级有效期。

【应用分类】中显示的是应用识别规则的分类，如 IM，游戏等。

选择对应的应用类型，【具体应用】中会显示此类应用中包含的具体应用，属于某个大的应用类别中细化的分类，如 IM 中的 QQ，MSN 等。

在[筛选]中选择需要查询的规则类型：勾选【全部】表示筛选符合条件的全部规则；勾选【启用】表示筛选已经启用了的符合搜索条件的规则；勾选【禁用】表示筛选已经禁用了的符合条件的规则。在[搜索]中需要查询的规则关键词，如筛选条件设置为“QQ”，回车后如图：

应用识别库

应用总数：1209; 规则总数：3029

筛选：全部 搜索：QQ

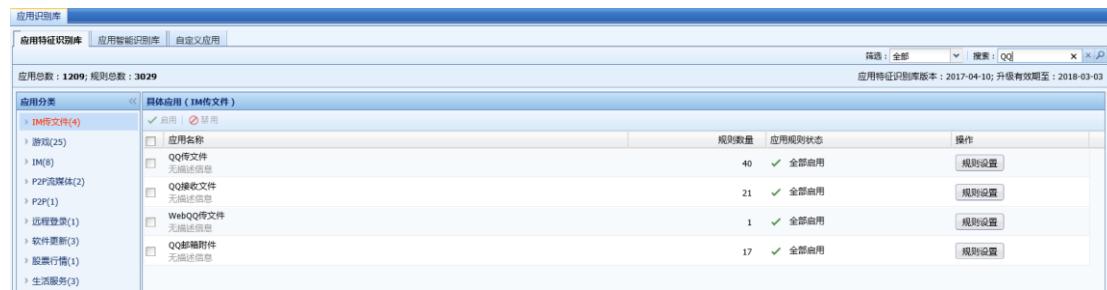
应用分类	具体应用（IM优化文件）	规则数量	应用规则状态	操作
IM类文件(4)	QQ音乐文件 QQ聊天文件 QQ接收文件 WebQQ文件 QQ邮箱附件	40 21 1 17	全部启用 全部启用 全部启用 全部启用	[规则设置] [规则设置] [规则设置] [规则设置]
游戏(25)				
IM(8)				
P2P流媒体(2)				
P2P(1)				
远程登录(1)				
软件更新(3)				
股票行情(1)				
生活服务(3)				

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

### 3.4.5.1.1.2 启用/禁用应用识别规则

在【导航菜单】页面中的『对象』→『内容识别库』，右边进入【应用特征识别库】页面，先筛选出想要设置的规则（具体筛选方法见 3.4.5.1），比如需要对 QQ 的规则进行禁用，如图筛选出 QQ 相关的应用：

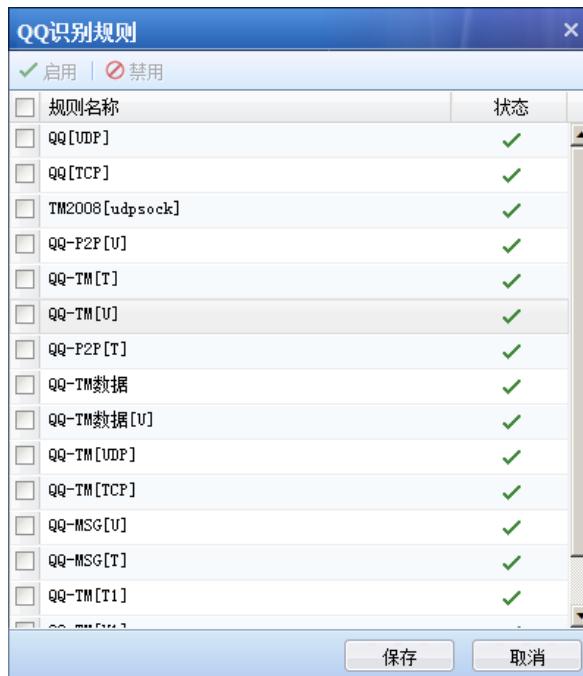


The screenshot shows the 'Application Feature Recognition Library' interface. In the left sidebar, under '应用分类' (Application Categories), 'IM类文件(4)' is selected. The main area displays a table titled '具体应用 (IM类文件)' with the following data:

应用名称	规则数量	应用规则状态	操作
QQ聊天文件	40	全部启用	规则设置
QQ接收文件	21	全部启用	规则设置
WebQQ传文件	1	全部启用	规则设置
QQ邮箱附件	17	全部启用	规则设置

勾选具体应用“QQ”，点击启用或者禁用，即可对 QQ 登录的所有规则进行禁用或启用。

如果需要禁用或启用具体应用中的某条规则，比如禁用“QQ”应用识别中的某条规则，点击规则设置，会弹出一个【QQ 识别规则】的编辑框，列出所有“QQ”的相关规则，勾选规则，点击启用或者禁用，即可对规则进行禁用或启用。



The screenshot shows the 'QQ Recognition Rule' dialog box. It has two tabs at the top: '启用' (Enable) and '禁用' (Disable). The '启用' tab is selected. Below it is a table with columns '规则名称' (Rule Name) and '状态' (Status). Most rules have a green checkmark in the '状态' column. The rules listed are:

规则名称	状态
QQ[UDP]	✓
QQ[TCP]	✓
TM2008[udpsock]	✓
QQ-P2P[U]	✓
QQ-TM[T]	✓
QQ-TM[U]	✓
QQ-P2P[T]	✓
QQ-TM数据	✓
QQ-TM数据[U]	✓
QQ-TM[UDP]	✓
QQ-TM[TCP]	✓
QQ-MSG[U]	✓
QQ-MSG[T]	✓
QQ-TM[T1]	✓

At the bottom of the dialog box are '保存' (Save) and '取消' (Cancel) buttons.



1、某些基础协议的应用识别规则是不能被禁用的，比如：HTTP，这种基础协议如果禁用的话，会影响其他基于 HTTP 协议的数据识别。所以设备限制此类规则不能被禁用掉。

2、此处禁用规则并不是封堵相应的应用，封堵规则请查看内容安全章节部分的内容。此处如果禁用 QQ，就表明设备无法识别 QQ 这种应用。一般情况下不需要禁用这些规则，排查故障的情况下可能会使用。

### 3.4.5.1.2 应用智能识别库

『应用智能识别库』也是用于识别各种上网数据的应用类型的，它和『应用特征识别库』的判断方式有所不同，可以识别一些加密的数据，比如明文或密文等形式 P2P 应用、skype、SSL、SANGFOR VPN 数据的识别、自由门，无界浏览等代理工具数据。配置页面如下：

序号	应用名称	应用类型	规则数量	应用规则状态	操作
1	P2P行为	P2P	1	全部启用	规则设置
2	skype	P2P	1	全部启用	规则设置
3	SSL	SSL	1	全部启用	规则设置
4	Sangfor VPN	Sangfor VPN	1	全部启用	规则设置
5	Freegate	Freegate	1	全部启用	规则设置
6	WuJie	WuJie	1	全部启用	规则设置

#### 3.4.5.1.2.1 启用/禁用应用智能识别规则

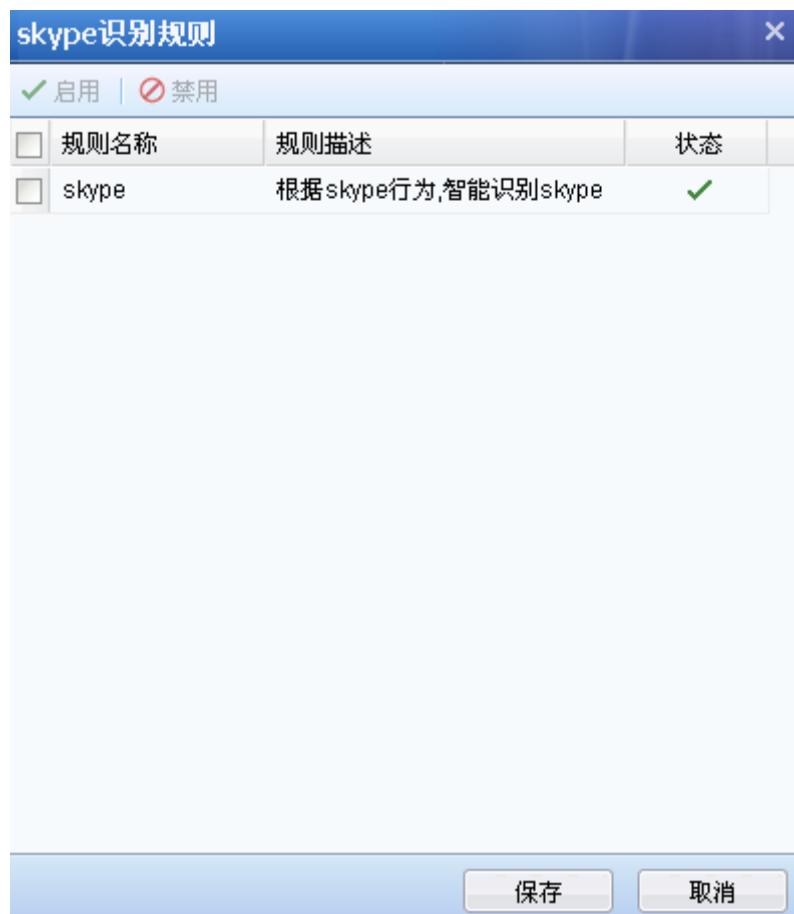
在【导航菜单】页面中的『对象』→『应用智能识别库』，右边进入【应用智能识别库】页面：

序号	应用名称	应用类型	规则数量	应用规则状态	操作
1	P2P行为	P2P	1	全部启用	规则设置
2	skype	P2P	1	全部启用	规则设置
3	SSL	SSL	1	全部启用	规则设置
4	Sangfor VPN	Sangfor VPN	1	全部启用	规则设置
5	Freegate	Freegate	1	全部启用	规则设置
6	WuJie	WuJie	1	全部启用	规则设置

勾选应用名称“skype”，点击禁用或者启用，即可对 skype 的智能识别规则

进行禁用或启用。

如果需要禁用或启用具体应用中的某条规则，比如禁用“skype”中的某条规则，点击**规则设置**，会弹出一个【skype】的编辑框，列出所有“skype”的相关规则，勾选规则，点击**启用**或者**禁用**，即可对规则进行禁用或启用。



### 3.4.5.1.2.2 编辑 P2P 行为识别规则

P2P 行为识别规则是应用特征识别的补充，对于应用特征识别库中识别不出来的 P2P 数据进行智能识别。P2P 行为规则是可以进行编辑的，点击**P2P 行为**，会弹出规则编辑框：

**应用智能识别库**

**是否启用该规则**

规则名称：

规则分类：

规则描述：

**规则配置选项**

检测灵敏度：  
 高  
 中  
 低  
 极低

排除扫描端口：  
备注：一行一个端口  
可以直接在此处输入、编辑、删除

**提交** **取消**

[是否启用该规则]可以勾选该项，启用该规则。

[规则名称]智能识别规则的名称。

[规则分类]规则所属的应用类别。

[规则描述]对该规则的简单描述。

以上三项均不能编辑。

[检测灵敏度]对规则的灵敏度设置，可设置为高、中、低、极低四项，可以根据需要调整检测灵敏度。智慧识别 P2P 可能存在误判，所以通过灵敏度来设置判断的标准，从“高”级别到“极低”级别灵敏度依次降低。客户可以根据具体数据的识别情况来调整灵敏度级别，比如如果有大量未识别的数据，且数据连接的端口都是随机的高端端口，目标地址不定，那么这些数据可能是未识别的 P2P 数据，这时可以将此处的灵敏度调高一些。比如有一些应用本不是 P2P 的数据，

却被识别成 P2P，那么可能是灵敏度级别设置高了，此时可以将灵敏度设置低一点。

[排除扫描端口]设置排除端口项，数据的目标端口是排除端口的话，设备不对此类数据进行 P2P 智能识别，可以避免部分误判的情况。

### 3.4.5.1.3 自定义应用

『自定义应用』用于自定义应用识别特征规则，用户可以定义一些内置的『应用特征识别库』中没有的应用，自定义应用可以通过数据方向、IP、协议、端口等进行定义。

在【导航菜单】页面中的『对象』→『内容识别库』→『应用识别库』，右边进入【自定义应用识别规则】编辑页面：



#### 3.4.5.1.3.1 新增自定义应用规则

在【自定义应用识别规则】编辑页面点新增，弹出【新增自定义规则】窗口，具体设置方法如下：

配置举例：需要对公司的邮件做流量保证，但是选择应用类型的时候无法单独选择公司邮件，这时候可以自定义一个公司邮件的应用。

第一步：启用规则，并设置应用基本信息，设置规则名称，描述信息，以及应用类型和应用名称（可以选择已有的类别，也可以自定义类别）：

### 新增自定义应用

启用应用

#### 应用基本信息

规则名称：	公司邮件
描述信息：	公司邮件
应用类型：	邮件
应用名称：	自定义邮件

第二步：设置匹配数据包的类型

#### 数据包特征 i

数据包方向： 只有符合该方向的数据包才会进行特征识别。  
 LAN<->WAN  
 LAN->WAN  
 WAN->LAN

3层协议： TCP

协议号：

目标端口：  
 所有端口  
 指定端口或范围 i

IP地址：  
 所有IP  
 指定IP或范围 i

匹配目标域名：i

[方向]：设置数据通过设备的方向，匹配到此方向的才会继续往下识别；

[协议]：设置数据所采用的协议类型，此例中邮件发送是 TCP 协议；

[目标端口]：设置数据所访问的目标端口，此例中邮件发送是 TCP25 端口；

[IP 地址]: 设置源 IP、目标 IP 或者是代理识别后的目标 IP。

[匹配目标域名]: 设置数据包访问的目标域名地址，此例中设置公司的域名邮箱地址，比如“*mail.sangfor.com.cn*”。

第三步：设置完成后点击**提交**，完成此条规则的设置。

应用列表					
序号	应用名称	描述	应用类型	状态	删除
1	公司邮件	公司邮件	邮件	√	×

第四步：设置用户自定义的规则优先级：因为内置应用特征识别库中也有邮件的识别规则，如果内置的规则优先的话，数据可能会优先匹配到内置的邮件规则，而不会匹配到“公司邮件”这条自定义的规则了，所以此处要设置自定义的规则优先匹配。在【自定义应用】页面勾选[用户自定义规则优先]即可。

第五步：在『流量管理』→『通道配置』中设置此应用的保证通道，保证使用公司邮箱发送邮件的带宽。（参见章节 3.5.4.1）



建议设置自定义规则时要加上目标端口、IP 和域名等识别信息，如果识别的条件过于宽泛，可能会和内置的应用识别规则有冲突导致应用识别混乱，从而导致部分控制和审计失效。

#### 3.4.5.1.3.2 启用/禁用/删除自定义应用规则

在【自定义应用】页面中，勾选自定义的规则，点击**启用**、**禁用**或者**删除**对自定义规则做相应的操作。

应用列表					
序号	应用名称	描述	应用类型	状态	删除
1	公司邮件	公司邮件	邮件	√	×

### 3.4.5.1.3.3 导入/导出自定义应用规则

点击导入，用于导入自定义的应用规则。

点击导出，用于导出自定义的应用规则。

### 3.4.5.2. URL 分类库

『URL 分类库』包括设备内置的 URL 库和用户自定义的 URL 库。内置 URL 库由设备定时更新，但更新内置库需要序号授权，且保证设备能够上网。自定义 URL 库可以进行增加、删除和修改等操作（参见章节 3.4.5.2 小节）。

在【导航菜单】页面中的『对象』→『内容识别库』→『URL 分类库』，右边进入【URL 分类库】页面：点击【URL 库列表】页面，页面上方显示了内置 URL 库版本以及内置 URL 升级的有效期。

URL分类库			
+ 新增 × 编辑 刷新 Q URL查询 内置规则库版本: 2018-11-12 升级有效期至: 2019-08-08			
URL类别名称	描述	类型	删除
求职招聘	包括各种涉及求职招聘相关信息的网站	内置	×
成人内容	包括含有成人用品、性教育、不露点裸体、人体艺术、夜总会等成人娱乐场所资料和点评、销售女士内衣和泳装的网站	内置	×
网上购物	包括支持在线购买商品与服务的网站	内置	×
新闻门户	包括提供最新新闻实时事评论的网站，包括新闻媒体、各种报刊、发行流通的杂志或其它媒体所创办的网站	内置	×
IT相关	包括IT行业资讯、IT人才培养设计、网络资料及各种针对开发者的网站	内置	×
教育	包括各种文化(如教育机构、及销售和提供教育资料、书籍、考试信息等网站	内置	×
游戏	包括国家体育管理部门及各类游戏网站，各种合法游戏相关信息网站	内置	×
非营利组织	包括慈善机构、义工组织、行业协会等不以盈利为目的的社会组织创办的网站	内置	×
科学技术	包括有关研究发现事物存在及其相关规律的学说及传播科学技术的网站	内置	×
<b>Web应用</b>			
微博	包括提供一种可以即时发布消息，类似博客系统的非正式的迷你型博客	内置	×
Web邮箱	包括提供电子邮件服务的网站	内置	×
搜索引擎	包括提供搜索、网页目录、索引等服务的网站	内置	×
社区论坛	包括提供留言板、BBS等各种论坛的网站，行业相关的社区论坛除外	内置	×
网上聊天	包括即时通信软件的WEB版本，以及聊天室可以即时发送和接收消息的网站	内置	×
网络游戏	包括将文件存储在特定的服务器上以供于备份或共享的网站	内置	×
软件下载	提供各种软件下载或者主要以软件下载为服务的网站	内置	×
个人网站及博客	包括博客、主页空间、个人网站等主要关于个人观点、信息的网站；行业相关的博客和个人网站除外	内置	×
<b>非法及不良</b>			
色情	包括含有淫秽文字、图片、音频、视频等色情讯息的网站	内置	×
赌博	包括提供在线赌博或赌博相关信息的网站	内置	×
非法药物	包括销售、贩卖或提供毒品、迷药、兴奋剂、其他受管制的麻醉和精神活性药品信息	内置	×
反动及其他非法内容	包括涉及政治敏感话题、民运、分裂主义等反政府信息的网站，或暴力描述或暗示、种族歧视和仇恨、暴力及不道德内容	内置	×
<b>生活相关</b>			

### 3.4.5.2.1 URL 查询

在【导航菜单】页面中的『对象』→『内容识别库』→『URL 分类库』，右边进入【URL 分类库】编辑页面。点击  URL查询，会弹出一个【URL 查询】窗口，输入想要查询的域名，点击查询后，查询结果中会显示 URL 对应的类别。



URL 查询不支持模糊查询。

### 3.4.5.2.2 新增 URL 组

新增 URL 组，用于用户自定义 URL。在【URL 库列表】页面，点击新增，弹出【新增 URL 类型】窗口：



『URL 组名称』 定义方便理解的名称

## 『URL 组描述』 定义方便理解的描述

『URL』添加需要设置的 URL，一个 URL 组可以包含多个 URL，URL 支持通配符匹配。

『域名关键词』根据 URL 中的关键词自动匹配 URL 组，访问域名中包含所设置的关键词则被识别成该 URL 组，域名关键词匹配优先级低于内置 URL 库和自定义 URL 库。



用\*号表示通配，比如要设置一个 URL 表示新浪的子页面，包括新浪新闻（news.sina.com.cn）、新浪体育（sports.sina.com.cn）、新浪娱乐（ent.sina.com.cn）等，那么就在[URL]中输入“\*.sina.com.cn”。注意：\*号只能表示一级域名的匹配，另外\*号只能放在 URL 的最前面，不能放在中间，否则此 URL 将不会生效。

### 3.4.5.2.3 删除 URL 组

删除 URL 组用于删除用户自定义的 URL 组，设备内置的 URL 组是不能删除的，在【URL 库列表】页面，勾选自定义的 URL 库，点击 **删除**，则可删除对应的 URL 组。

### 3.4.5.2.4 修改 URL 组

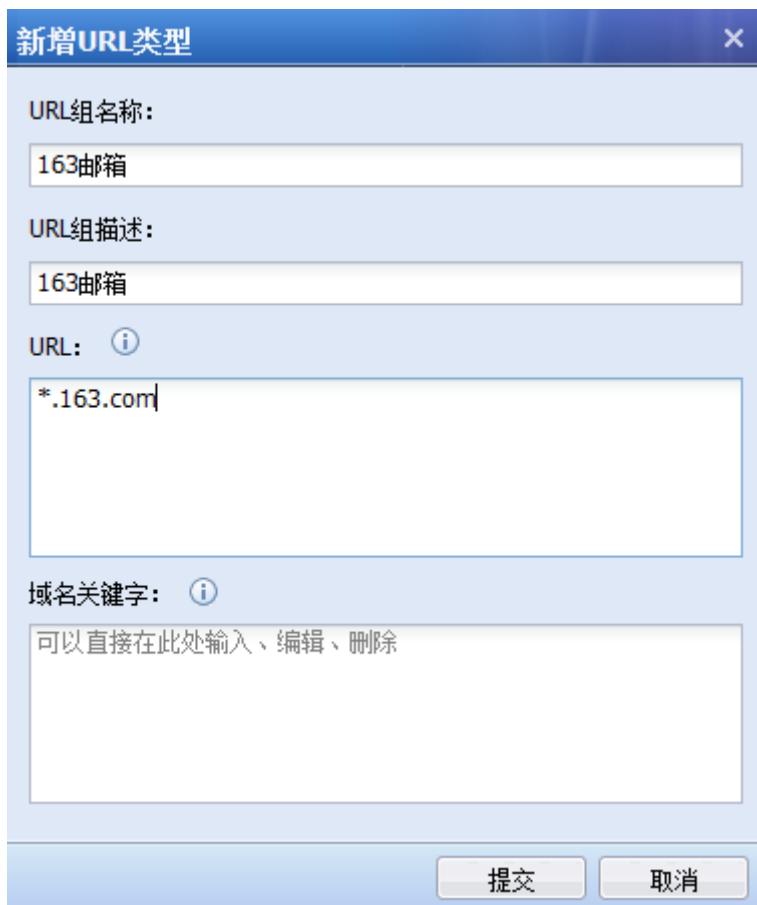
修改 URL 组既可以修改用户自定义的 URL 组也可以修改内置的 URL 组，不过两者有些区别：

对于用户自定义的 URL 组，进行编辑时，可以编辑 URL 组的描述以及 URL、域名关键词等。

对于设备内置的 URL 组，进行编辑时，不能编辑 URL 组的名称和描述，并且不能编辑内置库中已有的 URL，只能在[URL]和[域名关键词]中添加 URL 和关  
地址:深圳市南山区学苑大道1001号南山智园A1栋

键词，作为对内置 URL 库的补充。

直接点击需要修改的 URL 组的名称，然后弹出【编辑 URL 类型】窗口中设置。



### 3.4.5.3. 文件类型组

『文件类型组』用于定义需要的文件类型，并可应用到『对象』→『安全策略模板』→『内容安全』的文件过滤中，限制文件 HTTP 和 FTP 的上传和下载，也可用于『策略』→『流量管理』→『通道配置』→『带宽分配』的规则中设置文件类型上传下载的流量控制。

在【导航菜单】页面中的『对象』→『内容识别库』→『应用识别库』，右边进入【文件类型组】页面：

文件类型组		
序号	名称	描述
1	电影	电影格式文件
2	音乐	音乐格式文件
3	图片	图片格式文件
4	文本	文本文件等
5	压缩文件	压缩文件后缀
6	应用程序	可执行文件、脚本
7	杀毒文件列表	文件文件格式
8	邮件附件过滤列表	邮件附件过滤格式文件

在【文件类型组】页面点击新增，则弹出【新增文件类型组】窗口，如图：



[文件类型组名称]用于设置名称

[文件类型组描述]用于设置文件组的描述信息

在[文件类型]输入框中输入各种类型文件的后缀名，如“\*.mp3”或者“mp3”等。



设备默认自带有电影、音乐、图片文本、压缩文件、应用程序的大部分文件类型，如无法满足需求，才需要手动添加。

## 3.4.6. IP 地址库

### 3.4.6.1. ISP 地址库

『ISP 地址库』用于设置网络运营商的 IP 地址段，此 IP 地址段主要用于『策略路由』中的多线路负载路由调用。

IP地址库		
ISP地址段		
+ 新增	X 删除	刷新
<input type="checkbox"/> 名称	WHOIS标记	删除
· 全部	...	×
· 联通 (原网通)	MAINT-CNCGROUP	×
· 电信	MAINT-CHINANET	×
· 中国移动 (原铁通)	MAINT-CN-CRTC	×
· 教育网	MAINT-CERNET-AP	×

点击 **删除**，用于将已选的 ISP 信息删除，默认的 ISP 库不能删除和修改。

点击 **新增**，用于新建 ISP 信息，配置页面如下：



The window title is "ISP地址段". It contains three input fields: "名称:" (Name), "地址范围:" (Address Range), and "WHOIS标志:" (WHOIS Mark). Each field has a tooltip indicating it can be directly edited or deleted. At the bottom are "提交" (Submit) and "取消" (Cancel) buttons.

『名称』用于设置 ISP 名称。

『地址范围』用于手动设置该运营商的网络 IP 段。

『WHOIS 标志』用于设置相应的 ISP 地址段对应的 whois 标志，便于根据标志识别不同运营商的地址。



设备出厂默认有联通、电信、中国移动、教育网四个 ISP 地址库

### 3.4.6.2. IP 归属地

『IP 归属地』用于设置和查看 IP 地址的归属地，主要用于『地域访问控制』和『策略路由』中的源地址策略路由调用。



点击 **新增**，弹出 IP 归属地纠正页面，可以对 IP 进行归属地纠正。页面如下：



点击 **归属地查询**，弹出归属地查询页面，可以对 IP 地址进行归属地查询。页面如下：



点击 **更新地址库**，可以对 IP 地址库进行更新，一般是自动更新的。

### 3.4.7. 时间计划

『时间计划』用于定义常用的时间段组合，然后在『策略』→『访问控制』、『策略』→『流量管理』→『通道配置』等设置时，可以选择设置好的时间段定义，以设定这些规则生效或失效的时间。

时间计划包括【单次时间计划】和【循环时间计划】。

### 3.4.7.1. 单次时间计划

【单次时间计划】指定计划执行的起始日期和时间，设备将在指定的时间范围启动该计划，只会被执行一次，通常用于比较特殊的日期，比如可以通过该计划指定一条应用控制策略，国庆节期间禁止玩游戏，那么国庆节过去，设备会自动放行游戏，不需要手动操作。

在【导航菜单】页面中的『对象』→『时间计划』，点击进入【单次时间计划】编辑页面：



在【单次时间计划】页面点**[新增]**，则弹出【新增单次时间计划】页面。



[名称]用于设置时间计划组的名称

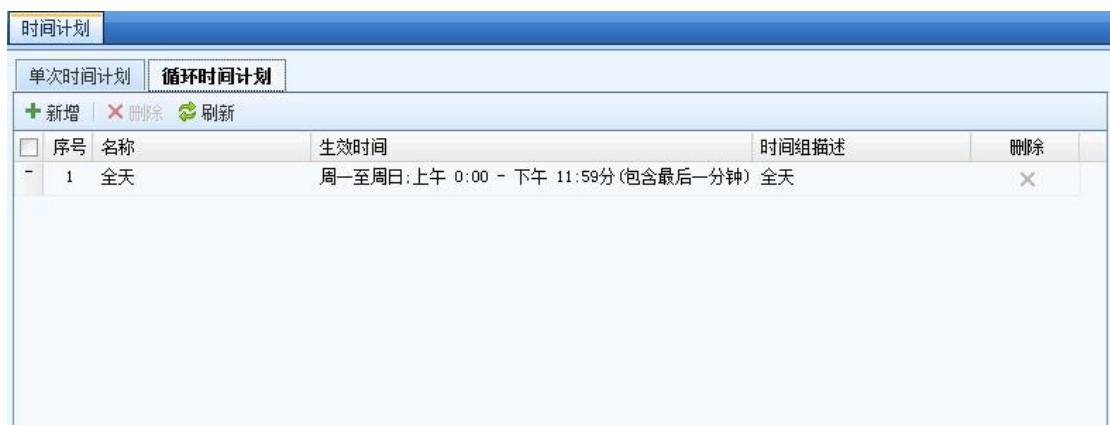
[开始时间]用于设置该时间计划的开始日期和时间。

[结束时间]用于设置该时间计划的结束日期和时间。

### 3.4.7.2. 循环时间计划

【循环时间计划】指定周一至周日的某个时间段，设备将在这个指定的时间段循环执行计划。

在【导航菜单】页面中的『对象』→『时间计划』，点击进入【循环时间计划】编辑页面：



序号	名称	生效时间	时间组描述	删除
1	全天	周一至周日: 上午 0:00 - 下午 11:59分 (包含最后一分钟)	全天	X

在【循环时间计划】页面点新增，则弹出【时间组计划设置】页面。

### 时间组计划设置

名称：

描述：

**+ 新增时间段** **删除**

<input type="checkbox"/> 周期	时间段	编辑	删除
没有可以显示的数据			

**时间组分布预览**

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
星期一																								
星期二																								
星期三																								
星期四																								
星期五																								
星期六																								
星期日																								

**提交** **取消**

[名称]用于设置时间计划组的名称

[描述]用于设置时间计划组的描述信息

点击**新增时间段**可以设置具体的时间周期以及时间范围。如图：

### 时间组计划设置

周期： 星期一 到 星期五

时间： 9点 00分 到 17点 00分

**确定** **取消**

如果需要设置几个不连续的时间段，可以新增多个时间段。

[删除时间段]勾选需要删除的时间段，点击**删除**即可删除相应的时间段。

[时间分布预览]显示时间段的情况，横轴为时间点，纵轴为日期范围。

### 3.4.8. 信任的证书颁发机构

『信任的证书颁发机构』用于设置受信任的证书颁发机构。用户可以导入或者删除这个证书库里的证书。

在【导航菜单】页面中的『对象』→『信任的证书颁发机构』，右边进入【信任的证书颁发机构】页面：



序号	证书颁发机构	起始日期	终止日期	剪除
1	FESTE, Public Notary Certs	May 13 19:21:28 1999 GMT	Jan 1 19:21:28 2020 GMT	
2	Certisign Autoridade Certificadora ACIS	Jun 27 00:00:00 1999 GMT	Jun 27 00:00:00 2018 GMT	
3	CAW HKT SecureNet CA Root	Jun 30 00:00:00 1999	Oct 15 23:59:00 2010	
4	UTH - DATACorp SGC	Aug 20 00:57:10 1999 GMT	Jun 24 07:00:00 2019 GMT	
5	SinforCA	Dec 13 07:12:13 2006 GMT	Dec 13 07:14:59 2011 GMT	
6	DSTCA E1	Dec 10 18:10:23 1998 GMT	Dec 10 18:40:23 2018 GMT	
7	FNMT Clase 2 CA	Mar 18 14:56:19 1998 GMT	Mar 18 15:26:19 2019 GMT	
8	VeriSign Trust Network	May 18 00:00:00 1998 GMT	Aug 1 23:59:59 2028 GMT	
9	Microsoft Root Authority	Jan 10 07:00:00 1997 GMT	Dec 31 07:00:00 2020 GMT	

在【信任的证书颁发机构】页面点击 **添加信任的证书颁发机构**，选择证书并导入，只支持从本地导入证书格式为 crt 或 cer。

检查证书异同是根据证书 MD5 值来判断的，如果 MD5 值不一样那么就判断为不同的证书，相同证书无法重复导入。



证书主体的名称一般是 IE 里对应这个证书主题的 CN 名，如果该证书的主题里不存在 CN 名，则采用主题最后一个字段的名字（主题字段的排列顺序和 IE 有可能不一样）。

### 3.5. 策略

『策略』中包含地址转换、访问控制、安全策略、解密、流量管理、配置向导、黑白名单和页面定制功能。

### 3.5.1. 地址转换

『地址转换』用于将符合条件的数据进行 IP 地址转换，包括源地址转换、服务器映射，如下图：

序号	名称	转换类型	源区域	目的区域/端口	原始数据包			转换后数据包			匹配	状态	复制	删除	
					源网关对象	目的网关对象	协议	源端口	目的端口	源网关对象	目的网关对象	目的端口			
1	远程桌面	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	3389	-	192.168.1.20	不转换	8409	✓	✖
2	网站映射	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	80	-	192.168.1.30	不转换	0	✓	✖
3	ftp映射	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	21	-	192.168.1.30	不转换	0	✓	✖
4	ssh映射	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	22	-	192.168.1.30	不转换	0	✓	✖
5	代理上网	源	内网区域	外网区域	全部	所有协议	所有端口	所有端口	出接口	-	-	不转换	1870	✓	✖

#### 3.5.1.1. 源地址转换

『源地址转换』用于将符合条件的数据进行源 IP 地址转换，最常用的是设备部署在公网出口时，代理内网用户上网，需要设置源地址转换规则进行源地址转换。在【源地址转换】页面可以对源地址转换规则进行管理、添加和删除。源地址转换页面如下：

新增源地址转换 (SNAT)

启用  
将来自源区域的 - 网络对象去访问目的区域的 - 网络对象的流量，  
源地址转换为出接口地址

基础信息

名称:

描述:

插入到序号: 5

原始数据包

源区域: 流量流入的区域

网络对象: 请选择源网络对象

目的区域/接口: 区域  流量流出的区域

网络对象: 请选择目的网络对象

协议: 所有协议

转换后数据包

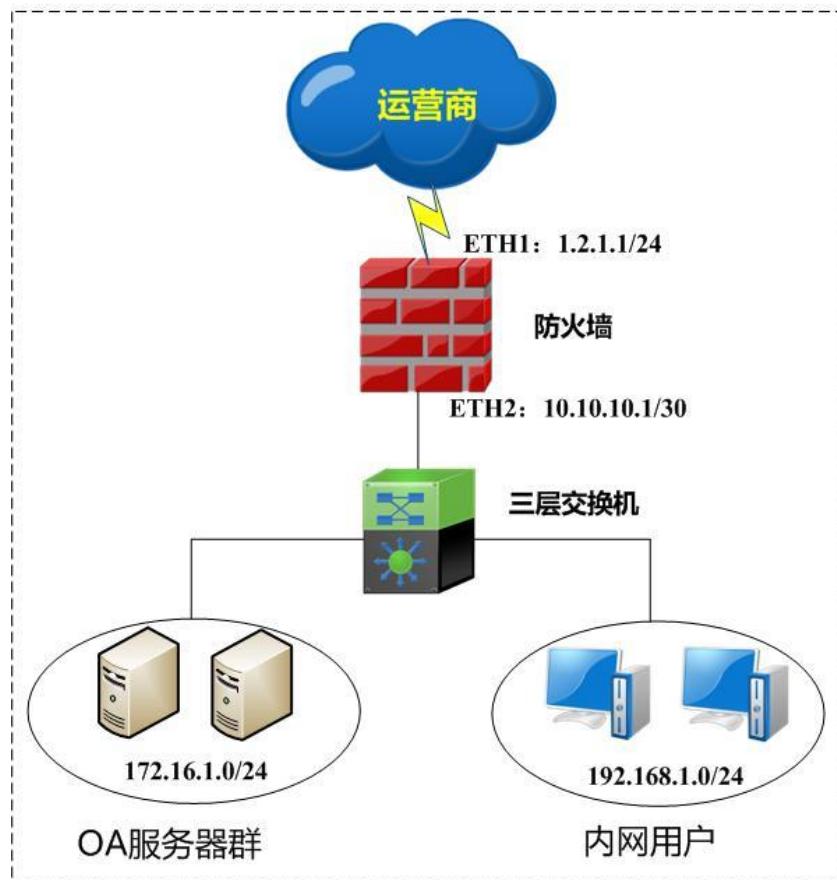
源地址转换为: 出接口地址



- 1、地址转换可以设置插入到某条之前。
- 2、源地址转换转换后的源是范围的时候，支持一对一 nat，方便溯源。

### 3.5.1.1.1 源地址转换配置案例

某客户拓扑图如下，客户需要让内网用户和服务器群都能够通过 AF 防火墙上网，此时需要在 AF 设备上添加源地址转换规则，将 192.168.1.0/24 和 172.16.1.0/24 上网的数据经过 AF 后转换成 1.2.1.1，也就是 AF 设备出接口 ETH1 的 IP 地址。



第一步：在配置源地址转换规则之前，首先要在『网络』→『接口/区域』定义好接口所属的【区域】，『对象』→『网络对象』定义好内网网段所属的【IP组】。详细配置，请参考 3.3.1.6 和 3.4.1 案例中将 ETH1 定义为[外网区]，ETH2 定义为[内网区]。172.16.1.0/24 和 192.168.1.0/24 定义成 IP 组[内网]。如图：

接口/区域					
	物理接口	子接口	VLAN接口	聚合接口	区域
	新增		删除		刷新
<input type="checkbox"/>	区域名称	转发类型	接口列表	管理选项	管理地址
<input type="checkbox"/>	内网区	三层区域	eth2	WebUI, ssh, snmp	全部
<input type="checkbox"/>	外网区	三层区域	eth1	WebUI, ssh, snmp	全部

网络对象					
服务器识别					
新增    删除    刷新    导入    导出    搜索					
序号	名称	类型	IP范围	描述	删除
30	建工系机房	IP组	172.16.27.0/255.255.255.0	建工系机房	
31	604机房	IP组	172.16.26.0/255.255.255.0	604机房	
32	610机房	IP组	172.16.22.0/255.255.255.0	610机房	
33	606机房	IP组	172.16.21.0/255.255.255.0	606机房	
34	601机房	IP组	172.16.19.0/255.255.255.0	601机房	
35	电子阅览室	IP组	172.16.18.0/255.255.255.0	电子阅览室	
36	内网	IP组	172.16.1.0/24 192.168.1.0/24		

第二步：在【地址转换】—【IPv4 地址转换】页面点击新增，选择[源地址转换]弹出新增页面。勾选[启用]，不勾选则规则不生效，在“基础信息”栏的[名称]中填写规则的名称，自定义好描述信息。如图：



第三步：设置原始数据包的匹配条件。

『源区域』和『网络对象』，用于设置需要进行源地址转换即匹配此条规则的源 IP 条件，只有来自指定的源区域和指定网络对象的数据才会匹配该规则、进行源地址转换。如路由接口代理内网上网，则一般配置源区域为内网、源网络对象为内网 IP 网段，或者全部。此案例中选择区域为[内网区域]，网络对象为[内网]。

『目的区域/接口』和『网络对象』，用于设置匹配条件的目的数据，数据到哪个目标区域、访问哪些目标 IP 组、或者从哪个接口出去的数据，才匹配该规则。如路由接口代理内网上网，则一般配置目标区域为公网、网络对象为全部。本案例中选择目标区域为[外网区域]，网络对象为[全部]，

『协议』，如果需要设置符合指定协议、源端口、目标端口的数据才进行源地址转换，则可以定义这部分。点击下拉框进行设置，本案例中不需要设置此项，使用默认“所有协议”即可。

**原始数据包**

源区域:	内网区域	
网络对象:	内网	
目的区域/接口:	区域	外网区域
网络对象:	全部	
协议:	所有协议	

第四步：设置转换后的数据包，『源地址转换』设置当源地址、目标地址、协议等条件都匹配的数据，进行IP地址转换时，将源IP转换为哪个IP地址。可以选择防火墙接口的【出接口地址】、某一段【IP范围】、单个【指定IP】、【网络对象】或者【不转换】。本案例中选择出接口地址。

**转换后数据包**

源地址转换为:	出接口地址
---------	-------

**地址转换**

保存并继续新增      保存      取消

最后点击**保存**，完成源地址转换规则的配置。如图：



The screenshot shows a list of configured source address translation rules in a software interface. The columns include: 序号 (Index), 名称 (Name), 转换类型 (Conversion Type), 源区域 (Source Area), 目的区域/端口 (Destination Area/Port), 源网络对象 (Source Network Object), 目的网络对象 (Destination Network Object), 协议 (Protocol), 源端口 (Source Port), 目的端口 (Destination Port), 源网络对象 (Source Network Object), 目的网络对象 (Destination Network Object), 转换后数据包 (Converted Data包), 转换类型 (Conversion Type), 匹配 (Match), 状态 (Status), 复制 (Copy), and 删除 (Delete). Rule 5, '代理上网', is highlighted with a red border.

1.如果需要修改已设置的源地址转换规则，则点击规则名称即可到编辑页面。

2.如果需要删除规则，则勾选上需要修改的规则，点击**删除**来删除该策

略。或者点击  根据提示进行删除操作。

3.如果需要禁用某条规则，可以点击  把规则状态改为禁用。禁用后显示  。如果需要再次启用该规则，点击  根据提示操作即可。

4.IP 组除了在对象中添加外，还可以直接在转换规则的选择框中新增。

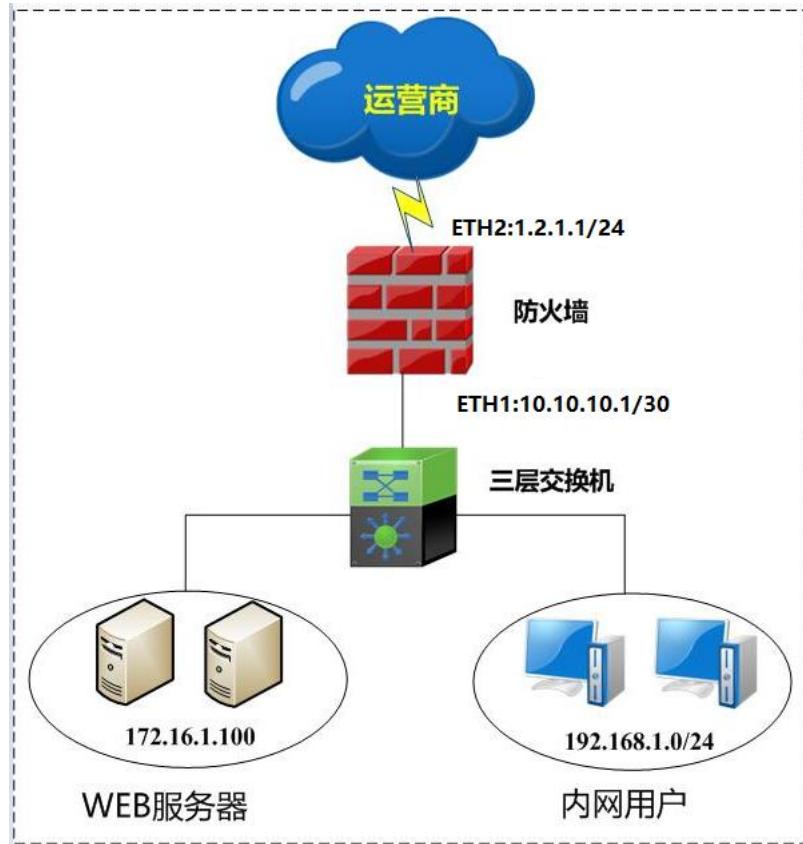
### 3.5.1.2. 服务器映射

『服务器映射』即常说的“目的地址转换”，用于对经过设备的数据做目标地址转换。常应用于发布服务器，将内网服务器的服务映像到公网，使 Internet 用户可以通过公网地址访问到网络内部服务器。下图为服务器映射页面：



### 3.5.1.2.1. 服务器映射配置案例

某客户拓扑如下，客户内网有一台 WEB 服务器 172.16.1.100 的 80 端口提供服务，并且已经申请了一个域名 www.xxx.com 指向 1.2.1.1。客户希望外网用户输入 <http://www.xxx.com> 能访问到内网 172.16.1.100 服务器。同时内网用户组也可以通过访问 <http://www.xxx.com> 也能访问到内网 172.16.1.100 服务器，此处需要使用服务器映射规则来实现。



第一步：在配置目标地址转换规则之前，首先要到『网络』→『接口/区域』定义好接口所属的【区域】。详细配置请参考 3.3.1.6 章节。此案例中将 ETH2 定义为[外网区]，ETH1 定义为[内网区]。如图：



第二步：在【地址转换】—【IPv4 地址转换】页面点击新增，选择【服务映射】弹出新增页面。勾选[启用]，不勾选则规则不生效。在“基础信息”的【名称】中填写规则的名称，自定义好描述信息。如图：



### 第三步：设置原始数据包的匹配条件

[源区域]指明从哪个区域进入的数据才进行目标地址转换，如发布内网服务器到公网时，允许来自公网的用户对该服务器的访问，同时也允许内网用户通过公网域名发起访问。所以本案例中设置区域为[外网区域]和[内网区域]。

[外网地址]指明公网用户访问哪个地址的时候，才进行目标地址转换。此处目的 IP 是数据包目的地址转换之前用户访问的地址，一般是设备自身接口的公网 IP。本案例中设置为“1.2.1.1”。

[协议&端口]设置进行目的地址转换的协议以及目的端口。本案例中协议类型需要选择 TCP，因为 HTTP 服务 80 端口属于 TCP 协议。目的端口指定为 80。

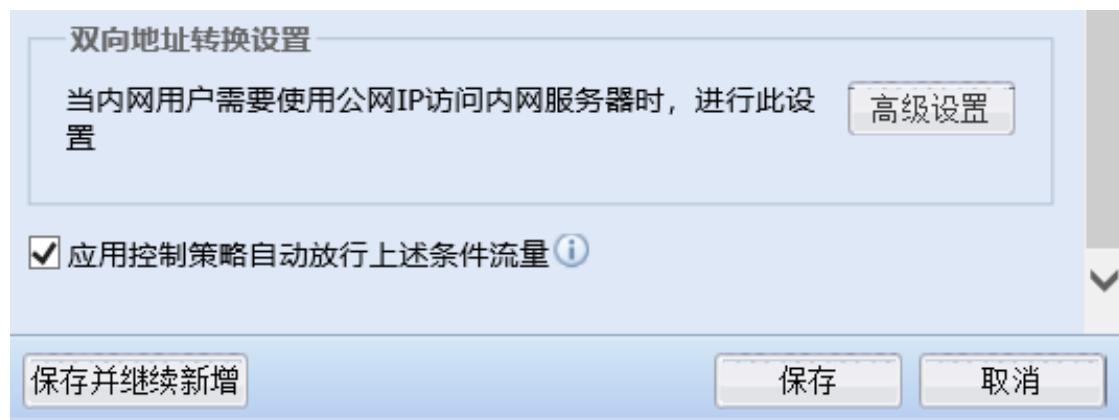


### 第四步：设置转换后数据包匹配条件

[内网地址]指明将目的地址转换为什么地址，以及是否进行目的端口的转换。本案例中真正提供 TCP 80 端口服务的内网服务器 IP 为 172.16.1.100，并且只转换目标 IP，不转换目的端口，页面设置如下：



第五步：设置双向地址转换，用来实现内网网段用户，可以通过<http://www.xxx.com> 域名来访问 172.16.1.100 服务器，如下页面：



点击[双向地址转换设置]的[高级设置]按钮，完成内网用户的条件匹配设置，如下图：



[目的区域/接口]: 内网数据最终从哪个区域发送出去，匹配到该规则。本例

中内网用户访问的服务器在内网区域，数据最终需要从设备定义的内网区域转发出去，所以目的区域选择“内网区域”。

[源地址转换为]：即转换后的源地址，本案例中直接将源地址转换为ETH1内网接口地址，也即出接口地址。

[源网络对象]：设置符合哪些条件的源IP组，才匹配该规则，本案例中涉及到外网和内网的用户，所以建议选择“全部”来进行该转换。

第六步：勾选上[应用控制策略自动放行上述条件流量]的选项，该功能会自动在应用控制层面放通匹配该规则的所有流量。最后点击**保存**，则完成配置。页面如下：

序号	名称	转换类型	源区域	目的区域/接口	源网对象	目的网对象	协议	源端口	目的端口	源网对象	目的网对象	目的端口	转换类型	状态	复制	删除	原始数据包		转换后数据包	
																	转换规则名	匹配		
1	远程桌面	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	3389	-	192.168.1.20	不转换	110	✓						
2	网站映射	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	80	-	192.168.1.10	不转换	0	✗						
3	http映射	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	21	-	192.168.1.10	不转换	0	✓						
4	ssh映射	目的	外网区域	-	全部	192.200.244.97	TCP	所有端口	22	-	192.168.1.10	不转换	0	✓						
5	代理上网	源	外网区域	内网用户组	全部	所有协议	所有端口	所有端口	出接口	-	-	不转换	8653	✓						
6	WEB服务器	定向	外网区域/外网区域	内网区域	全部	1.2.1.1	TCP	所有端口	80	出接口	172.16.1.100	不转换	0	✓						

1.如果需要将 1.2.1.1 的 80 端口映像成内部服务器 172.16.1.100 的 8080 端口。则可以设置目的端口转换为[转换]，并设置端口为 8080。页面如下：

原始数据包	
源区域:	外网区域
外网地址:	指定IP 1.2.1.1
协议&端口:	TCP 80
转换后数据包	
内网地址:	指定IP
指定IP:	172.16.1.100
端口转换为:	8080

2.如果需要修改已设置的目的地址转换规则，则点击规则名称即可到编辑界面。

辑页面。

3. 如果需要删除规则，则勾选上需要修改的规则，点击  来删除掉该策略。或者点击  根据提示进行删除操作。

4. 如果需要禁用某条规则，可以点击  把规则状态改为禁用。禁用后显示  。如果需要再次启用该规则，点击  根据提示操作即可。

### 3.5.1.3. DNS-Mapping

DNS Mapping 的应用场景用于内网用户通过公网域名访问内网的服务器，实现的效果与双向地址转换规则一样。设置 DNS Mapping 后，当内网用户发送 DNS 请求的时候，防火墙设备主动将域名解析成服务器的内网 IP 地址，返回给客户端，客户端实际是直接访问了服务器的内网 IP，没有经过规则转换。

DNS Mapping 与双向地址转换的区别是：

1. 设置 DNS Mapping 后，内网访问服务器的数据将不会经过防火墙设备，而是直接访问服务器内网 IP。双向地址转换则是所有数据都会经过防火墙去访问。所以通过 DNS Mapping 可以减轻防火墙压力。

2. DNS Mapping 的设置方法比双向转换规则简单。不涉及区域、IP 组、端口等设置。页面设置如下：



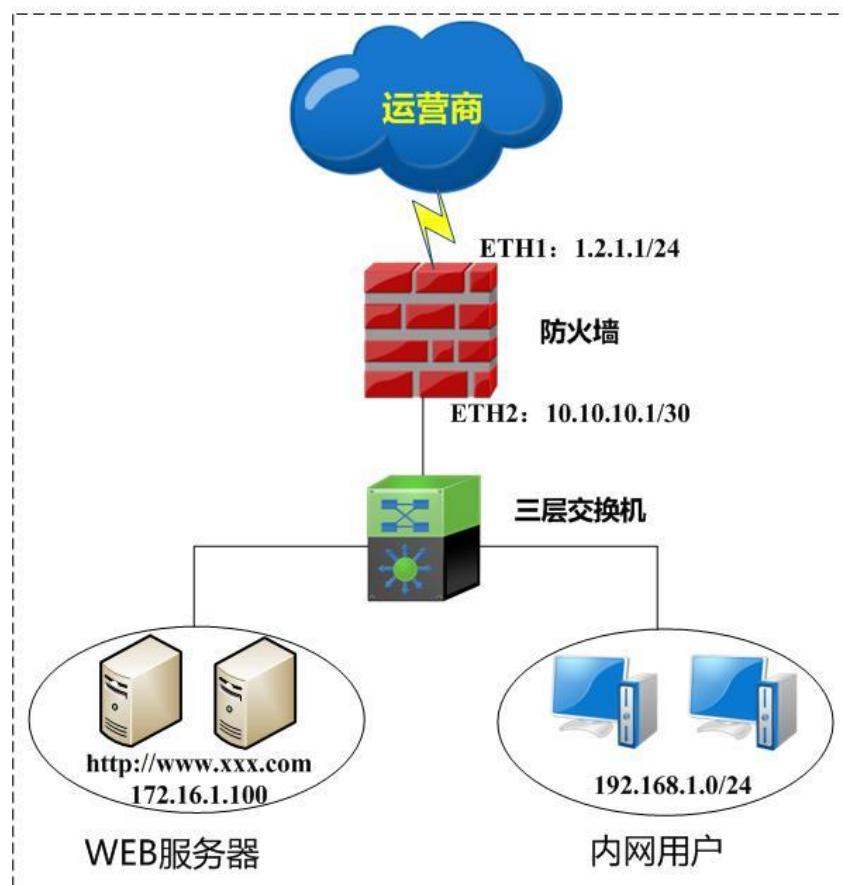
[域名]: 设置用户访问的域名。

[公网 IP 地址]: 设置内网用户访问的域名对应的公网 IP。

[内网 IP 地址]: 设置实际要访问的内网服务器地址。

### 3.5.1.3.1. DNS Mapping 配置案例

某客户拓扑如下，内网有一台 WEB 服务 172.16.1.100。已经申请了一个域名 www.xxx.com 指向 1.2.1.1。客户要求内网用户 192.168.1.0/24 输入 www.xxx.com 即可访问到 172.16.1.100 服务器。此时可以使用 DNS Mapping 来实现内网用户输入域名访问到 WEB 服务器。



第一步：进入『网络』→『地址转换』→『DNS Mapping』菜单，点击新增。



The screenshot shows a software interface for managing DNS mappings. At the top, there are tabs for 'IPv4地址转换' (IPv4 Address Translation), 'IPv6地址转换' (IPv6 Address Translation), and 'DNS-Mapping'. The 'DNS-Mapping' tab is selected. Below the tabs is a toolbar with a green plus sign labeled '新增' (Add) and a red minus sign labeled '删除' (Delete). A table below the toolbar has columns for '序号' (Index), '域名' (Domain Name), '公网IP' (Public IP), and '内网IP' (Private IP). There are '编辑' (Edit) and '删除' (Delete) buttons at the bottom right of the table.

第二步：在弹出的对话框中填写公网 IP，域名等信息。本案例中的填写方法如下：



第三步：点击**保存**，完成配置。此时，内网用户访问 www.xxx.com 即可以  
直接访问到 172.16.1.100。

### 3.5.2. 访问控制

『访问控制』中包含的应用控制策略、地域访问控制和连接数控制。

#### 3.5.2.1. 应用控制策略

根据数据包的应用层特征来过滤上网数据，也可以根据数据包的端口来进行过滤。例如可以实现上班时间禁止内网用户玩游戏。该模块的设置需要调用『对象设置』里面的服务、网络对象、时间计划、应用特征识别库等对象。

点击『策略』→『访问控制』→『应用控制策略』进入应用控制策略设置页

面，在此页面可以对应用控制策略进行新增、删除、启用、禁用以及搜索。设备默认存在一条拒绝所有服务/应用的控制策略。设置页面如下：



点击**新增**，进入【新增应用控制策略】页面，设置如下：

**新增应用控制策略**

启用

**基础信息**

名称:

描述: 可以为空，最多为256个字符

分组和优先级: 默认分组  之前

**访问者条件**

区域:

地址: 网络对象

端口: 非必填，默认为全部端口

**被访问者条件**

区域:

网络对象: 全部

服务/应用: 服务

**生效条件设置**

动作选项:  允许  拒绝

生效时间: 全天

高级选项:

勾选[启用]则启用该应用控制策略。

### 基础信息设置：

[名称]: 定义规则名称。

[描述]: 定义规则的描述信息。

[分组和优先级]: 设置策略的所属组，可以按照分组/名称等来改变显示顺序。

---

同时将新增的策略放在某条策略之前

### 访问者条件设置：

[区域]：选择需要控制数据的源区域。

[地址]：选择需要控制的源IP地址或者用户。包括[网络对象]和[用户/组]两个选项，[用户/组]是从『用户认证』→『用户管理』→『组/用户』的组织结构中调用的用户信息。

[端口]：指定需要控制数据的源端口，一般源端口都是随机，所以这里如若没有特殊情况，无需设置，保持默认即可。

### 被访问者条件设置：

[区域]：选择需要控制数据的目的区域。例如要针对内网用户上外网的数据进行控制，则此处应该选择外网区域。

[网络对象]：选择需要控制的数据的目的IP组。例如要针对内网用户上外网数据进行控制，则此处目标IP可以选择所有。

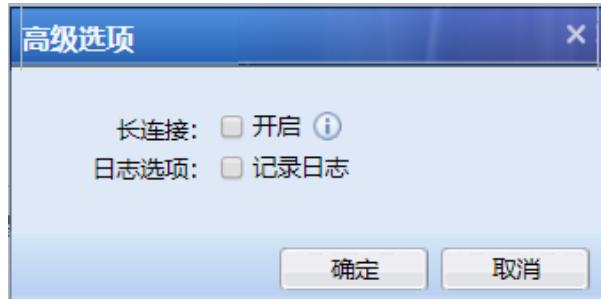
[服务/应用]：选择需要做控制的应用或者服务。[应用]是调用『对象』→『内容识别库』→『应用识别库』里的应用特征。服务是调用『对象』→『服务』中定义的服务。

### 生效条件设置：

[动作选项]：设置满足上述定义的条件的数据包是放行还是丢弃。

[生效时间]：过滤条件，在指定的时间内过滤规则才生效。该处是调用『对象』→『时间计划』中定义好的时间对象。

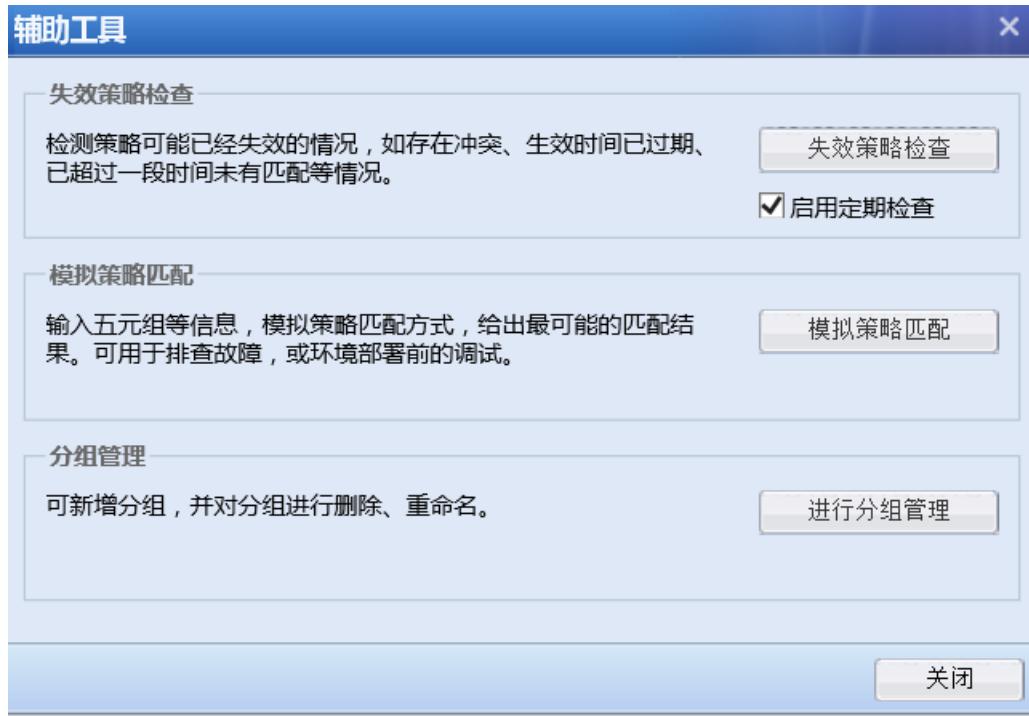
[高级选项]：点击设置按钮，弹出如下对话框：



[长连接]: 此功能仅用于支持访问有长连接请求的特殊服务器，使连接请求不受防火墙连接超时的影响，开启此功能会使连接释放变慢，时间可以选择最短1天、最长15天，请谨慎使用。

[日志]: 勾选“记录”，则把控制行为记录到内置数据中心里面。应用控制日志过大将导致系统磁盘读写缓慢，建议使用外置数据中心或syslog存储该日志。详见3.6.1.2章节。

点击『辅助工具』可以配置失效策略检查、模拟策略匹配和分组分组管理。



[失效策略检查]: 可以检查已失效的策略

[模拟策略匹配]：可以根据五元组来模拟策略的匹配情况。如下图所示：

模拟策略匹配

\*号为必填项，其他输入项为空时不做模拟。尽量输入准确。

协议

协议 : TCP 协议号 : 6

源

IP地址 : \* 端口 :

区域 : 请选择

目的

IP地址 : \* 端口 :

区域 : 请选择

时间

访问时间 :  不指定  具体时间

开始模拟 关闭

[分组管理]可以设置策略的所属组。



开启应用控制日志记录功能，流量日志审计功能均会增加设备的性能开销，建议要关闭内置数据中心，部署外置数据中心。

### 3.5.2.2. 地域访问控制

『地域访问控制』用于设置允许或拒绝指定国家或地区的IP流量访问AF设备保护的内网区域。如下图所示：



点击**[新增]**，如下图所示：



[名称]和[描述]: 设置规则的名称和描述信息。

[外网区域]: 选择 AF 设备的外网区域。

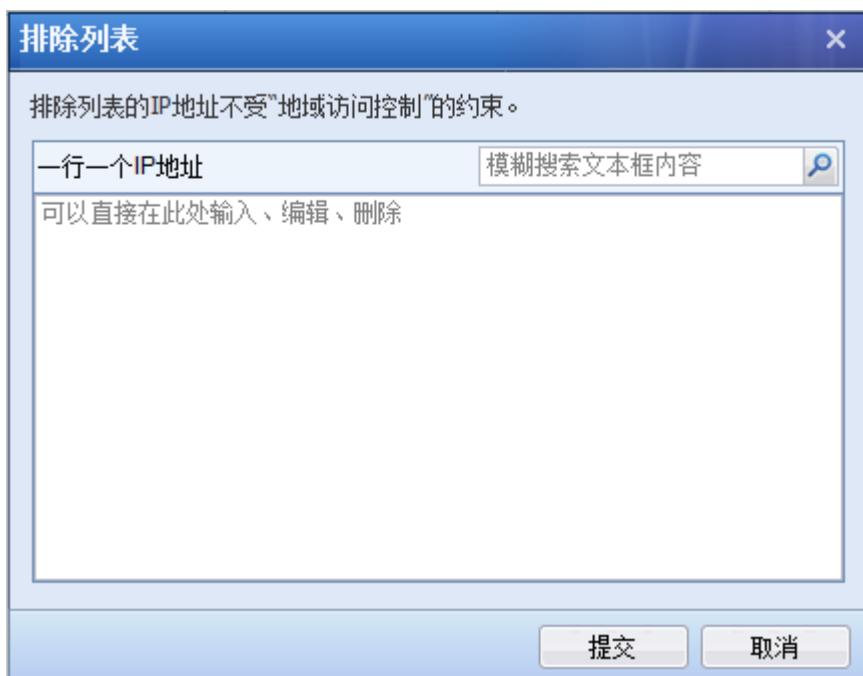
[网络对象]: 选择内网需要保护的 IP 组，或者服务器 IP 组。

[控制方式]: 选择只允许以下国家/地区访问，或拒绝以下国家/地区访问。

[国家/地区]: 选择国家/地区，如下图所示:



点击 **排除列表**，添加不受地域访问控制的 IP 地址，如下图所示：



点击  已拒绝的IP，显示被地域访问控制策略拒绝的 IP 地址记录，如下图所示：



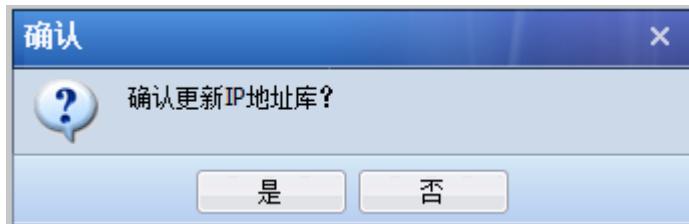
点击  纠错反馈，将错误的 IP 地址和归属地记录反馈到 SANGFOR 厂家，如下图所示：



点击  归属地查询，可以输入 IP 地址查询对应的归属地，如下图所示：



点击  [更新地址库]，将手动更新 ISP 地址库，如下图所示：



点击 ，保存和生效配置。

### 3.5.2.3. 连接数控制

『连接数控制』用于设置单个 IP 的最大会话数。分为源 IP 连接数控制、目的 IP 连接数控制和双向 IP 连接数控制。

『源 IP 连接数控制』：当内网用户下载 P2P 等应用以及内网用户计算机感染病毒时，短时间内会发送很多连接，影响网络使用，此时可以使用『源 IP 连接数控制』限制单内网 IP 的最高会话，减少网络损耗。页面如下：



新增源并发连接数限制

启用

名称：

描述：

源

区域： 请选择源区域

网络对象： 请选择源网络对象

每IP最大并发连接数：  
 指定值  
32768  
 不限制

提交 取消

[名称]：填写规则的名称。可自定义。

[描述]: 填写针对该规则的详细描述信息。可定义。

[源区域]: 选择需要做会话数限制的源区域。区域的设置方法请参考章节

### 3.3.1.5

[网络对象]: 选择需要做会话数限制的网络对象。

[每 IP 最大并发连接数]: 设置每个 IP 的最大并发连接数。

『目的 IP 连接数控制』：针对目标 IP 控制并发连接数，如下图所示：



[名称]: 填写规则的名称。可自定义。

[描述]: 填写针对该规则的详细描述信息。可定义。

[目的区域]: 选择需要做会话数限制的目的区域。区域的设置方法请参考章节 3.3.1.5。

[网络对象]: 选择需要做会话数限制的网络对象。

[每 IP 最大并发连接数]: 设置每个 IP 的最大并发连接数。

『双向 IP 连接数控制』：针对双向 IP 控制并发连接数，如下图所示：



[名称]: 填写规则的名称。可自定义。

[描述]: 填写针对该规则的详细描述信息。可定义。

[源区域]: 选择需要做会话数限制的源区域。区域的设置方法请参考章节 3.3.1.5。

[IP 组]: 选择需要做会话数限制的 IP 组。

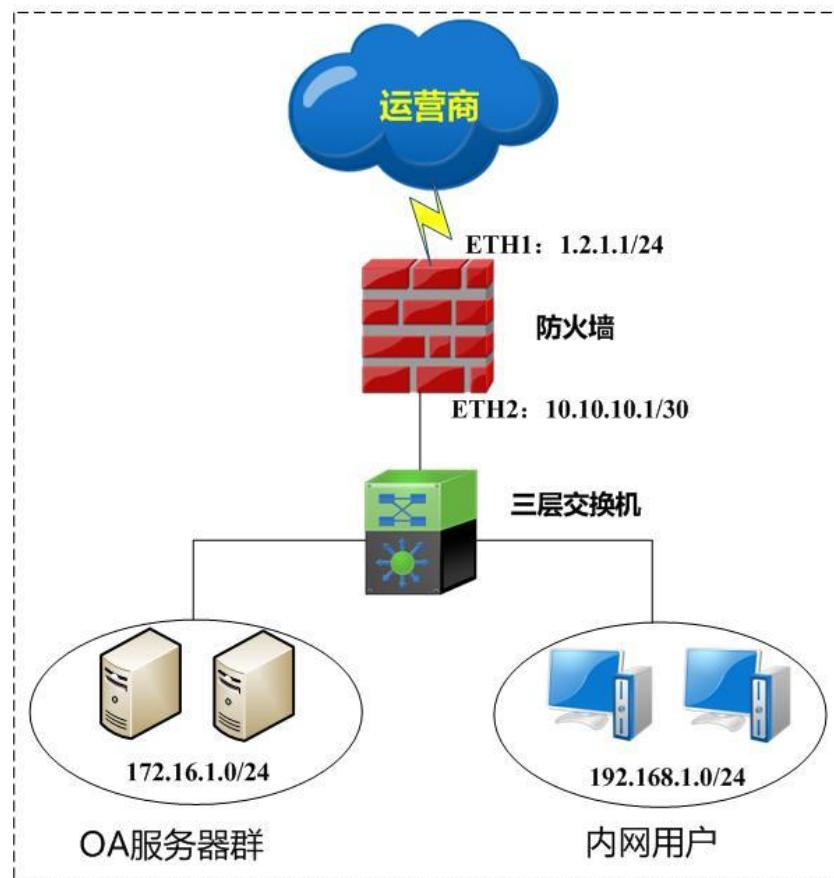
[目的区域]: 选择需要做会话数限制的目的区域。区域的设置方法请参考章节 3.3.1.5。

[IP组]：选择需要做会话数限制的IP组。

[最大并发连接数]：设置最大并发连接数。

### 3.5.2.3.1 连接数配置案例

某客户拓扑如如下，管理员希望针对内网用户 192.168.1.0/24 网段限制会话数，单用户最高并发 500 个会话。



第一步：在配置连接数控制之前，首先要在『网络』→『接口/区域』定义好接口所属的【区域】、【对象】→『网络对象』定义好外网接口 IP 所属的【IP 组】。详细配置请参考 3.3.1.5 和 3.4.1 章节。此案例中将 ETH2 定义为[内网区]，192.168.1.0/24 定义成 IP 组[内网用户]。如图：

The screenshot shows two main sections. The top section is titled '接口/区域' (Interface/Area) with tabs for Physical Interface, Sub-interface, VLAN Interface, Aggregation Interface, Area, and Interface联动 (Interface Linkage). It displays two entries: '内网区' (Intranet Zone) with interface 'eth2' and '外网区' (Extranet Zone) with interface 'eth1'. The bottom section is titled '网络对象' (Network Object) and shows a table of network users. There are two entries: '内网用户(wangshiyuan)' and '内网用户'. Both are of type 'IP组' (IP Group) with IP ranges 192.168.1.1-192.168.1.10 and 192.168.1.0/24 respectively.

第二步：进入连接数控制页面，点击**新增**，新增『源 IP 连接数限制』，本案例中由于内网用户在 ETH2 方向，需要针对内网用户做连接数限制，此处应选择[内网区]。IP 组选择[内网用户]，页面如下：

This dialog box is titled '新增源并发连接数限制' (Add Source IP Connection Limit). It contains the following fields:

- 启用 (Enabled)
- 名称 : 限制500 (Name: Limit 500)
- 描述 : 限制500会话 (Description: Limit 500 sessions)
- 源** (Source):
  - 区域 : 内网 (Area: Intranet)
  - 网络对象 : 内网用户 (Network Object: Intranet User)
- 每IP最大并发连接数 : (Maximum concurrent connections per IP):
  - 指定值 (Specified Value): 32768
  - 不限制 (Unlimited)

At the bottom are '提交' (Submit) and '取消' (Cancel) buttons.

第三步：点击**提交**即可生效。



此处的会话数限制是 TCP 与 UDP 所有会话的总和。

### 3.5.3. 安全策略

『安全策略』中包含安全防护策略、Dos/DDos 防护和 ARP 欺骗防护。

### 3.5.3.1. 安全防护策略

『安全防护策略』统一配置安全功能的入口，在这里可配置实时漏洞分析、漏洞攻击防护、内容安全、WEB 应用防护、防篡改 2.0、僵尸网络等 6 大安全功能。如下图所示：

安全防护策略							
优先级	名称	要保护的对象	需抵制的对象	评估	防御	检测响应	状态
1	testy	区域：LAN 网络对象：pc1,ser1,ser2	区域：WAN 网络对象：全部	实时漏洞分析	[入侵行为防御] [内容安全] [Web应用防护] [网站防篡改]	[僵尸网络] [高危行为联动封禁]	√
2	test	区域：LAN,WAN,aaa 网络对象：test_1	区域：LAN,WAN,aaa 网络对象：全部		[网站防篡改]		√
3	realtime_analysis	区域：LAN 网络对象：全部	区域：LAN,WAN,aaa 网络对象：全部	实时漏洞分析	[入侵行为防御] [Web应用防护] [网站防篡改]		√
4	内容安全	区域：LAN,WAN 网络对象：全部	区域：LAN,WAN 网络对象：全部		[入侵行为防御] [内容安全] [Web应用防护] [网站防篡改]		√
5	失陷主机监测	区域：LAN,WAN 网络对象：全部	区域：LAN,WAN 网络对象：全部	实时漏洞分析	[入侵行为防御] [内容安全] [Web应用防护] [网站防篡改]		√
6	恶意软件	区域：LAN 网络对象：测试PC组,测试服务器网段	区域：WAN 网络对象：全部		[入侵行为防御]		√
7	保护客户端	区域：LAN 网络对象：测试PC组	区域：WAN 网络对象：全部		[入侵行为防御]		√
8	保护服务器	区域：LAN 网络对象：测试服务器网段	区域：WAN 网络对象：全部		[入侵行为防御]		√
9	waf	区域：LAN 网络对象：测试服务器网段,测试web服务	区域：WAN 网络对象：全部		[Web应用防护]		√
10	botnet	区域：LAN 网络对象：全部	区域：LAN,WAN,aaa 网络对象：全部		[入侵行为防御] [Web应用防护] [僵尸网络] [网站防篡改]		√

可以对应用控制策略进行新增、删除、启用、禁用、上移、下移、移动、刷新、高级设置和筛选操作。

### 3.5.3.1.1 业务保护策略

『业务保护策略』主要对客户的业务进行保护。

点击新增，选择业务保护策略，弹出新增业务保护策略界面。如下图所示：

新增业务防护策略

常规 → 评估 → 防御 → 检测响应

策略名称:

描述: 可以为空，最多为95个字符

状态:  启用

源

区域:  

网络对象/用户:  网络对象  
 

目的

区域:  

网络对象:  

策略优化项 

业务访问场景:  

[策略名称] 定义策略名称。

[描述] 定义描述信息。

[状态] 定义策略是否启用。

#### 源:

[区域]: 选择攻击数据发起的方向所在的区域。一般为公网的区域

[网络对象/用户]: 选择攻击数据发起的方向所在区域的源 IP 地址。一般选择全部

#### 目的:

[区域]: 选择数据被动接受的方向所在的区域。一般为服务器所在的区域

[网络对象/用户]: 选择数据被动接受的方向所在区域的目的 IP 地址。一般选择需要防护的服务器网段

#### 策略优化项:

[业务访问场景]: 提前明确访问过程中，是否存在源地址转换或者 CDN 等代理的场景，共两个选项，“访问源未经过源地址转换或 CDN”和“访问源经过源地址转换或 CDN”。主要是为后面防扫描策略做选择参考，如果选择的是“访问源经过源地址转换或 CDN”，那么当选择带“防扫描功能的 WEB 应用防护模板”时，会有警告提示。

点击**下一步**，进入评估。如下图所示：



[实时漏分析]是通过内置了一些漏洞规则，对网络中指定的数据进行实时分析，用于发现用户网络中存在的一些安全漏洞问题，并以报表的形式把漏洞的危害和解决办法展现给用户。

点击**下一步**，进入防御。如下图所示：



### 基础防御:

[漏洞攻击防护] 选择是否启用漏洞攻击防护，这里可以调用 3.4.3 中的漏洞攻击防护模板。

[动作]: 设置满足上述定义的条件的数据包是放行还是丢弃。

[内容安全] 选择是否启用内容安全，这里可以调用 3.4.3 中的内容安全策略模板。

[动作]: 设置满足上述定义的条件的数据包是放行还是丢弃。

### 增强功能:

[Web 应用防护策略] 选择是否启用 Web 应用防护策略，这里可以调用 3.4.3 中的 Web 应用防护模板。

[动作]: 设置满足上述定义的条件的数据包是放行还是丢弃。

[网站篡改防护] 在对服务器进行文件系统防护时，需要在服务器上安装一个防护客户端，通过设置地址、网站目录、允许修改应用程序等保护服务器的文件

系统。

点击**下一步**，进入检测响应。如下图所示：



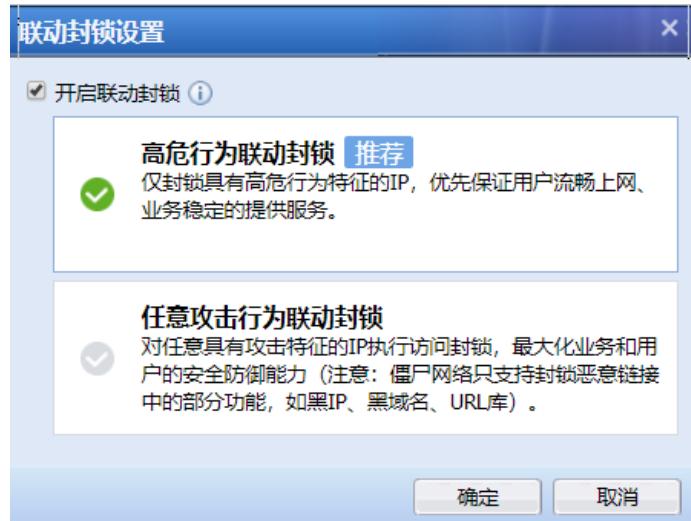
### 检测：

[僵尸网络] 选择是否启用僵尸网络，这里可以调用 3.4.3 中的僵尸网络模板。

[动作]：设置满足上述定义的条件的数据包是放行还是丢弃。

### 响应：

[联动封锁] 点击**设置**选项，开启联动封锁，则漏洞攻击防护规则、WAF 规则或者是数据防泄密模块，这三者的任何一个模块检测到攻击后，即会封锁攻击的源 IP 地址。注意：其中爆破攻击默认就会启用联动封锁，不管这里是否有勾选。



[记录日志]: 勾选记录日志，会记录相应日志到数据中心。

### 3.5.3.1.2 用户保护策略

『用户保护策略』主要对客户的终端用户进行保护。

点击新增，选择用户保护策略，弹出新增用户保护策略界面。如下图所示：



[策略名称] 定义策略名称。

[描述] 定义描述信息。

[状态] 定义策略是否启用。

源：

[区域]：选择攻击数据发起的方向所在的区域。

[网络对象/用户]：选择需要控制的源 IP 地址或者用户。[用户/组]是从『用户认证』→『用户管理』→『组/用户』的组织结构中调用的用户信息。

目的：

[区域]：选择数据被动接受的方向所在的区域。

[网络对象]：选择需要控制的目标 IP 地址。

点击**下一步**，进入防御。如下图所示：



基础防御：

[漏洞攻击防护] 选择是否启用漏洞攻击防护，这里可以调用 3.4.3 中的入漏洞

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

攻击防护模板。

[动作]: 设置满足上述定义的条件的数据包是放行还是丢弃。

[内容安全 (SAVE 安全智能文件检测) ] 选择是否启用内容安全，这里可以调用 3.4.3 中的内容安全策略模板。

[动作]: 设置满足上述定义的条件的数据包是放行还是丢弃。

点击下一步，进入检测响应。如下图所示：



### 检测：

[僵尸网络] 选择是否启用僵尸网络，这里可以调用 3.4.3 中的僵尸网络模板。

[动作]: 设置满足上述定义的条件的数据包是放行还是丢弃。

### 响应：

[联动封锁] 点击设置选项，开启联动封锁，则漏洞攻击防护规则模块检测

到攻击后，即会封锁攻击的源 IP 地址。注意：其中爆破攻击默认就会启用联动封锁，不管这里是否有勾选。



[记录日志]：勾选记录日志，会记录相应日志到数据中心。

### 3.5.3.1.3 高级设置

点击高级设置，弹出高级设置页面，如下图所示：



## 邮件安全排除设置：

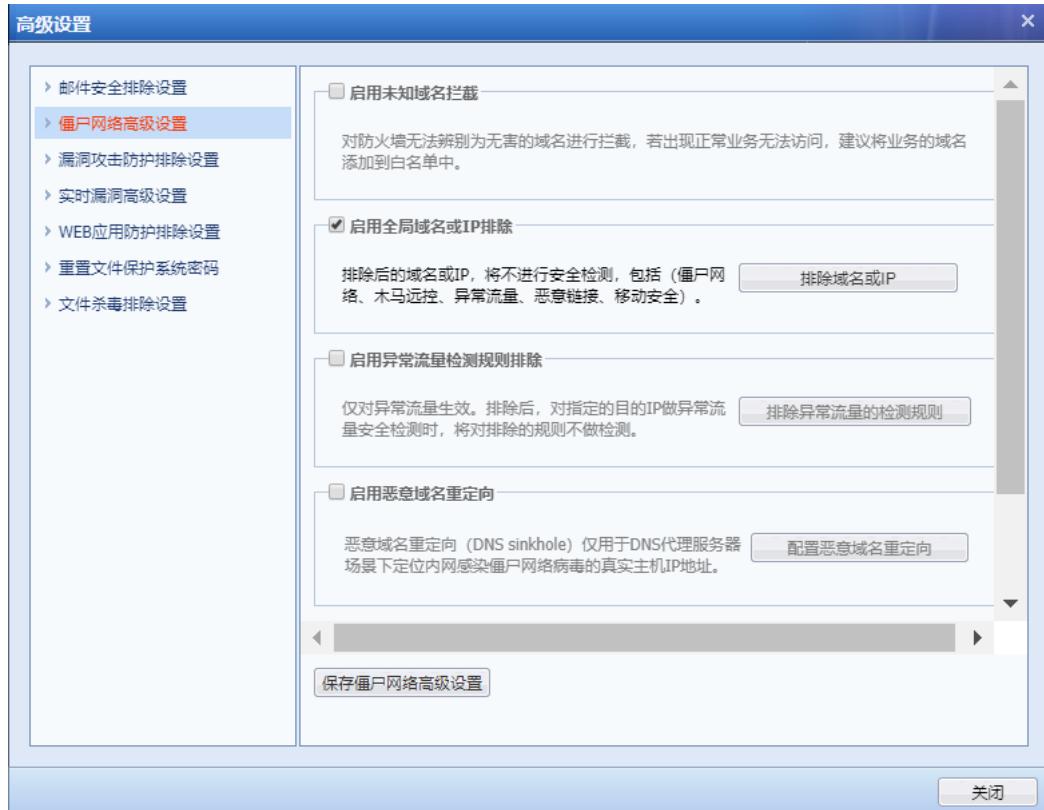
[邮件安全排除设置]：可以设置源 IP、目的 IP、收件人地址、发件人地址的排除，添加到下面的列表里的地址，所有邮件安全相关功能将不生效。如下图所示：



点击 **保存邮件安全排除设置**，对邮件安全排除设置进行保存。

## 僵尸网络高级设置：

[僵尸网络高级设置]：可以对僵尸网络的高级功能进行设置。如下图所示：



[启用未知域名拦截]: 对无法匹配 AF 设备域名库的 URL 访问进行拦截，常用于对安全要求较高的场景。

[启用全局域名或 IP 排除]: 设置排除的域名或 IP，将不进行安全检测，包括（僵尸网络、木马远控、异常连接、恶意链接、移动安全）。

[启用异常连接检测规则排除]: 此设置仅对异常连接生效。排除后，对指定的目的 IP 做异常连接安全检测时，将对排除的规则不做检测。

[启用恶意域名重定向]: 恶意域名重定向（DNS sinkhole）仅用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址。



[僵尸网络行为检测]: 通过配置的可疑行为做检测，定位出疑似僵尸网络的主机，但所有规则不阻断数据通信，只做检测并记录日志。

配置僵尸网络行为检测

序号	事件	启用/禁用	阈值	描述
1	HTTP从未知分类站...	✓		- 某主机从未知分类网站中下载可执行文件
2	HTTP浏览IP域	✓		- 某主机绕过域名，直接使用IP地址浏览网站，...
3	HTTP下载可疑文件	✓		- 某主机HTTP下载文件后缀名和真实文件格式不...
4	浏览最近30天注册...	✓		- 某主机浏览了最近30天注册的域名
5	端口扫描	✓	60	1秒内，某主机发起SYN包扫描某目的IP所有端...
6	IP扫描	✓	120	15分钟内，某主机向同一目的端口发送数据包...
7	HTTP浏览恶意动态...	✓		- 某主机浏览恶意动态域名
8	访问随机算法生成域...	✓		- 5分钟内，检测到访问疑似DGA算法生成的域名...
9	内网主机存在进行暴...	✓		- 主机感染恶意软件后，对内网目标进行暴力破...

点击 保存僵尸网络高级设置，对僵尸网络高级设置进行保存。

### 漏洞攻击防护排除设置：

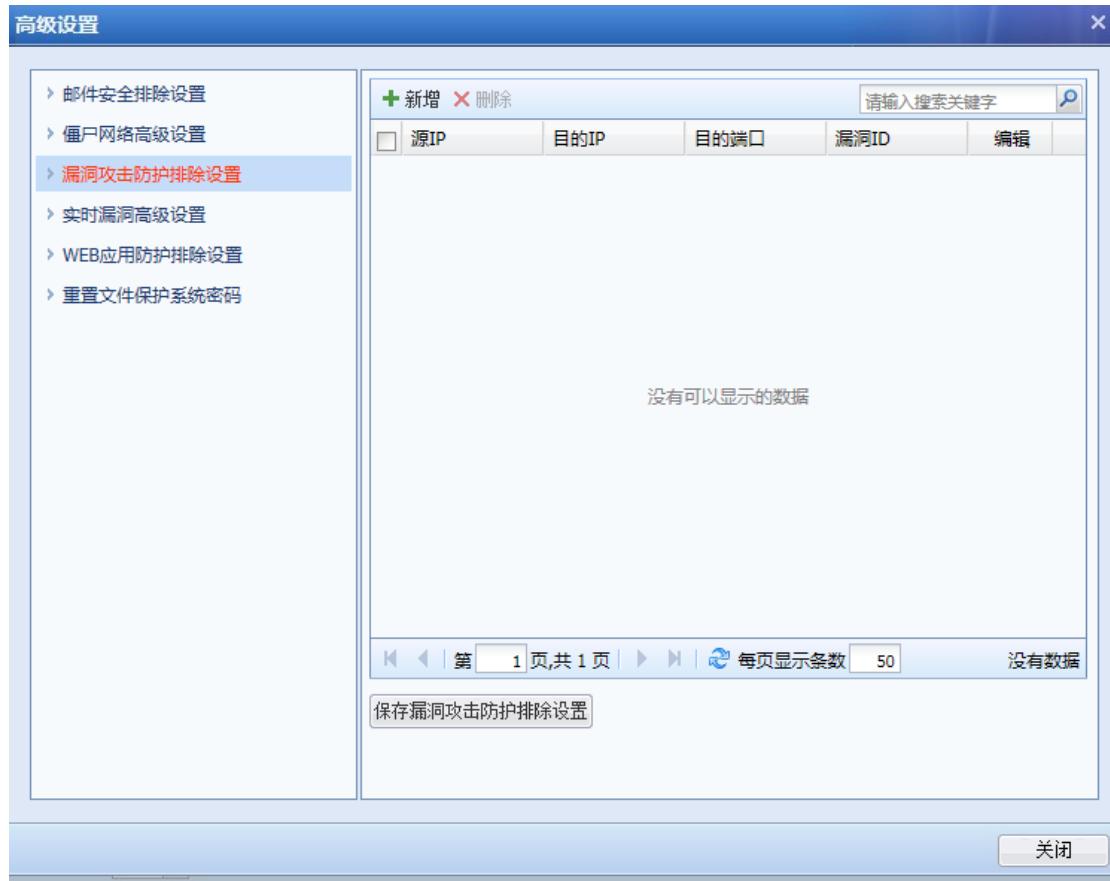
[漏洞攻击防护排除设置]：用于设置漏洞攻击防护不需检测的例外排除数据。

如下图所示：

高级设置

邮件安全排除设置  
僵尸网络高级设置  
**漏洞攻击防护排除设置**  
实时漏洞高级设置  
WEB应用防护排除设置  
重置文件保护系统密码

+ 新增 X 删除  
请输入搜索关键字  
源IP 目的IP 目的端口 漏洞ID 编辑  
没有可以显示的数据  
第 1 页,共 1 页 每页显示条数 50 没有数据  
保存漏洞攻击防护排除设置  
关闭



点击**新增**，弹出添加漏洞攻击防护例外排除。如下图所示：



[源 IP] 定义源 IP。可以是单个 IP、子网或者 IP 范围

[目的] 定义目的 IP。

[目的端口] 定义目的端口。

[漏洞 ID] 定义漏洞 ID。

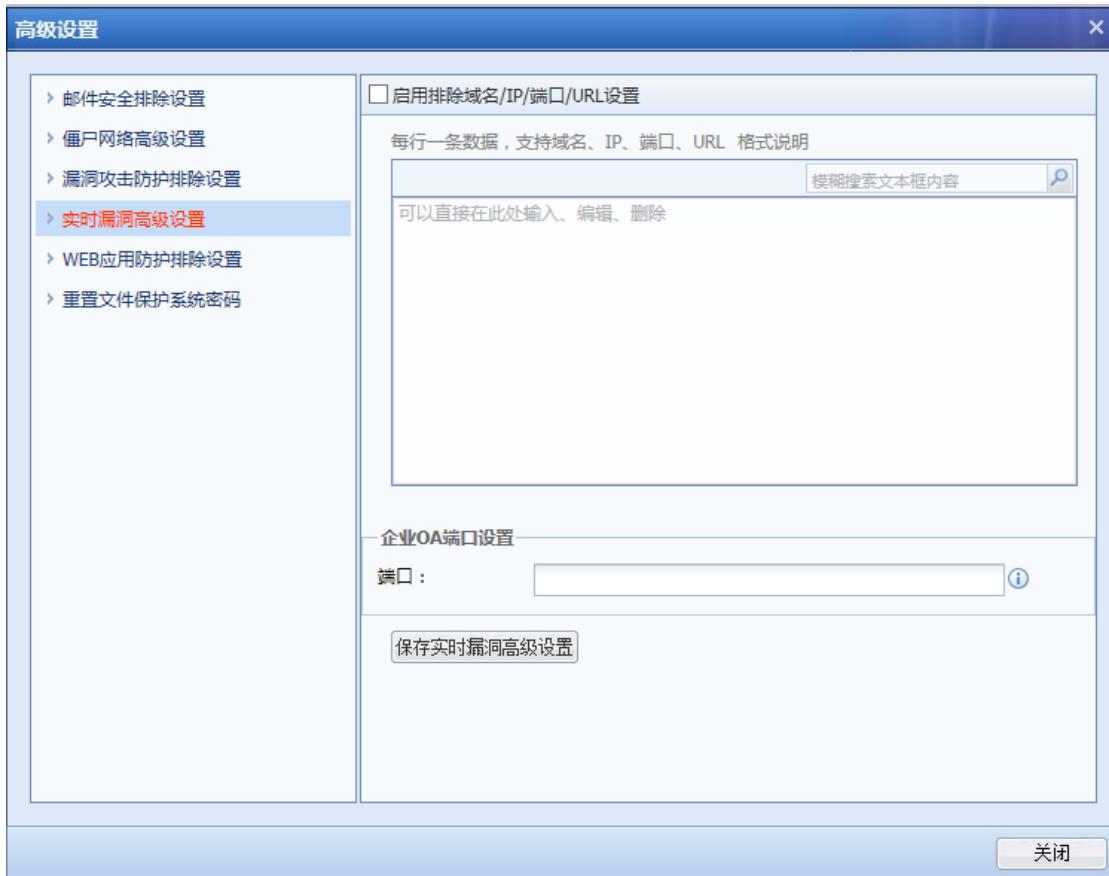
点击**提交**，提交设置

点击**保存漏洞攻击防护排除设置**，对漏洞攻击防护排除设置进行保存。

## 实时漏洞高级设置：

[实时漏洞高级设置]：可以启用排除域名/IP/端口/URL 和企业 OA 端口设置。

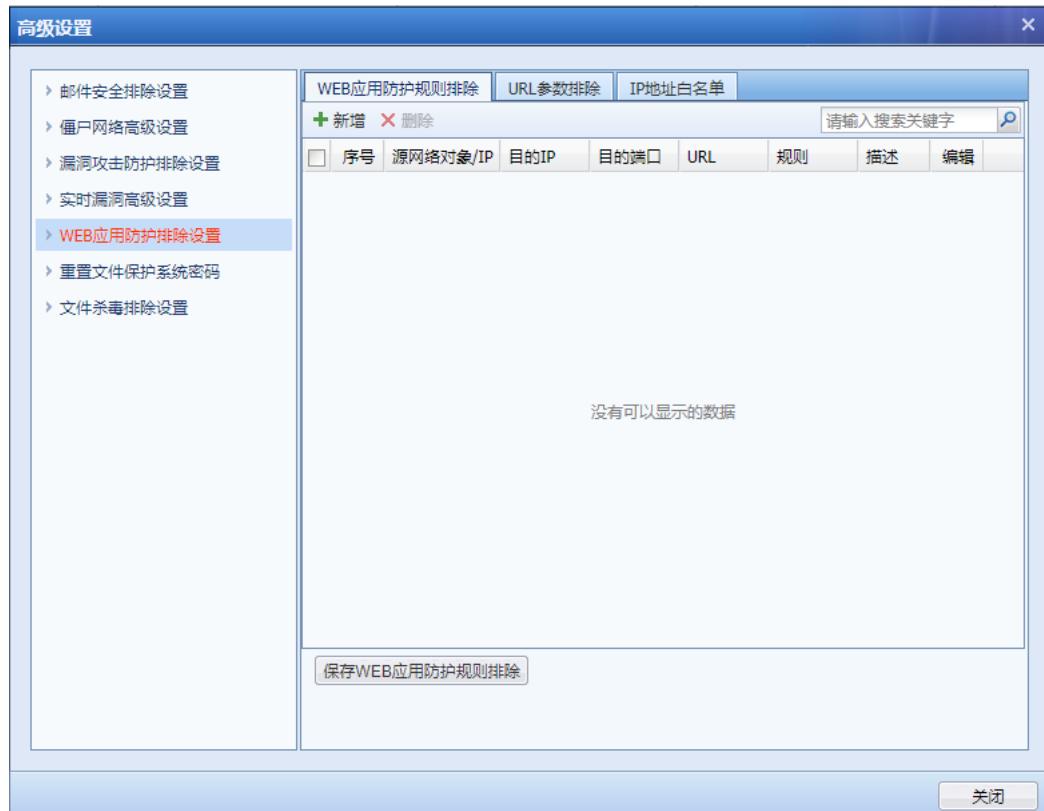
如下图所示：



点击 **保存实时漏洞高级设置**，对实时漏洞高级设置进行保存。

## WEB 应用防护排除设置：

[WEB 应用防护排除设置]：可以自定 WEB 应用防护规则排除。如下图所示：



点击**新增**，弹出 WEB 应用防护规则排除设置。如下图所示：



[源] 定义源 IP。可以是网络对象或者指定 IP。

[目的] 定义目的 IP。

[目的端口] 定义目的端口。

[URL] 定义排除的 URL。

[描述] 定义描述信息。

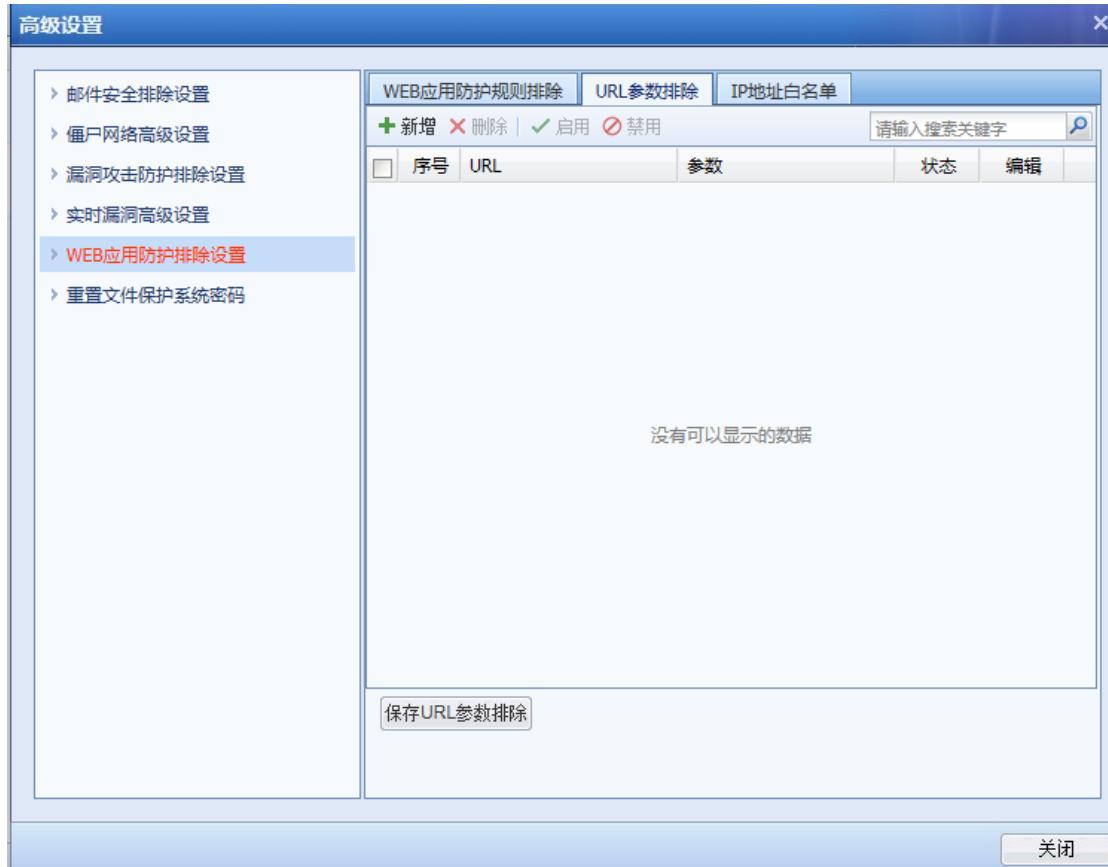
[规则 ID] 定义规则 ID。

[规则类型] 定义规则类型。

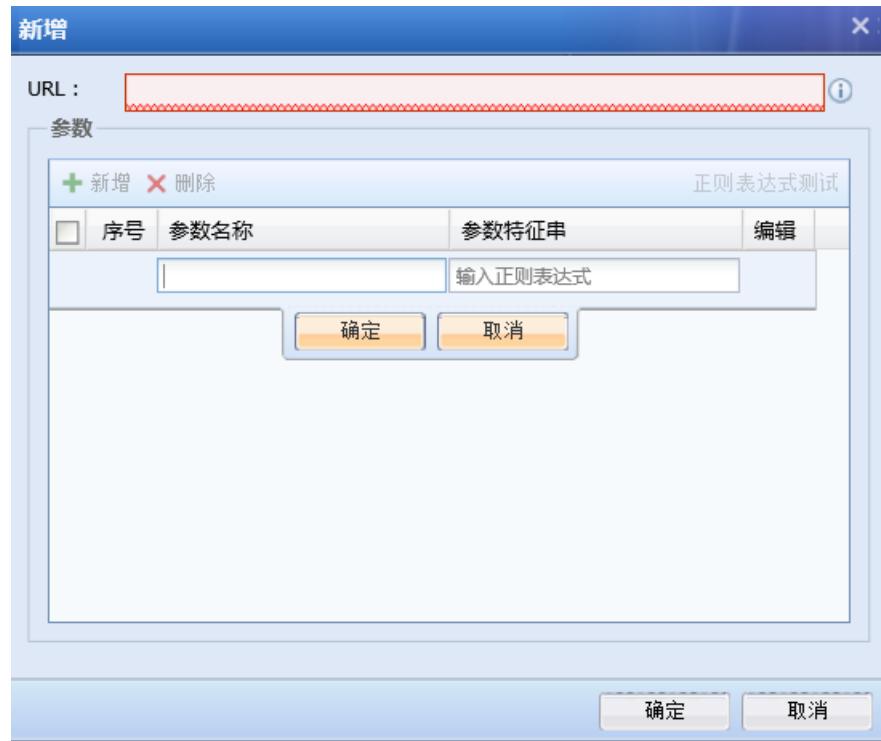
点击**确定**，提交配置

点击**保存WEB应用防护规则排除**，对 WAF 规则排除设置进行保存。

[URL 参数排除]：可以添加 URL 参数进行排除。如下图所示：



点击**新增**，弹出 URL 参数排除设置界面。如下图所示：



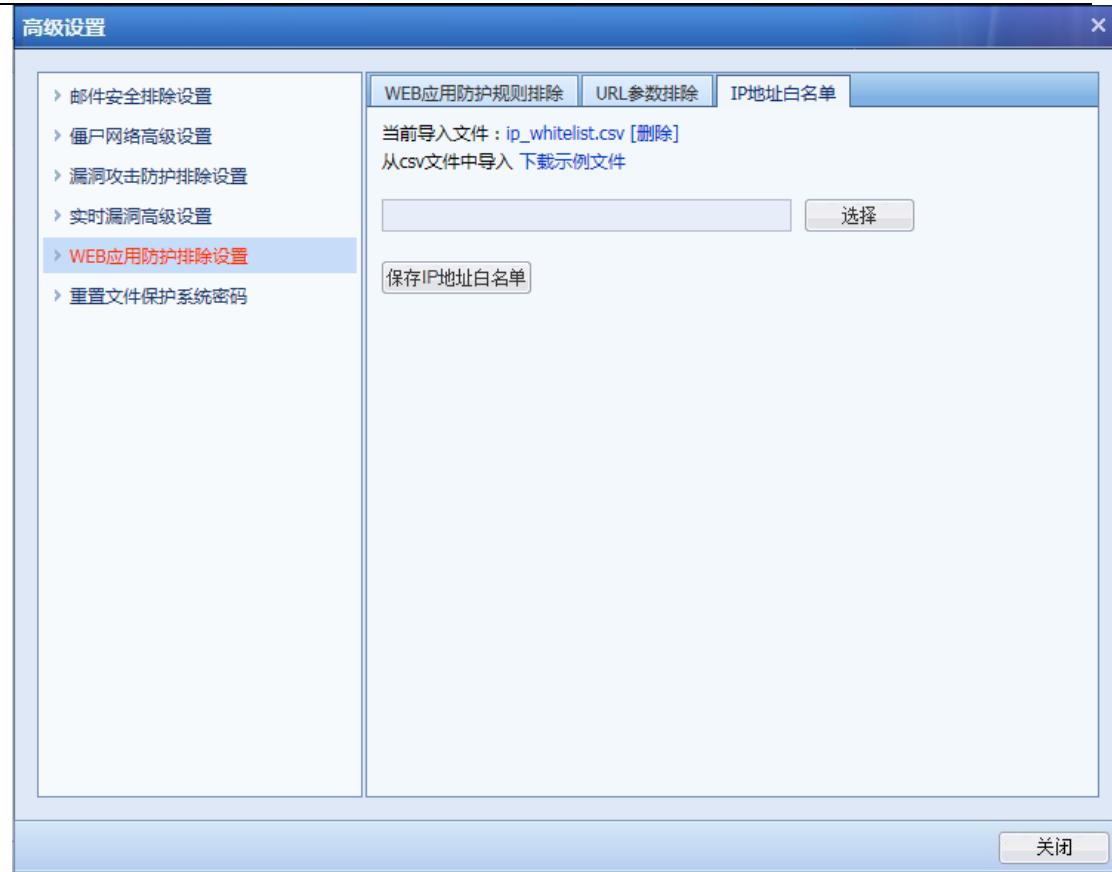
[URL] 定义 URL。

[参数] 定义参数信息。

点击确定，提交配置。

点击 保存URL参数排除，对 URL 参数排除设置进行保存。

[IP 地址白名单]：可对 IP 地址进行排除。如下图所示：

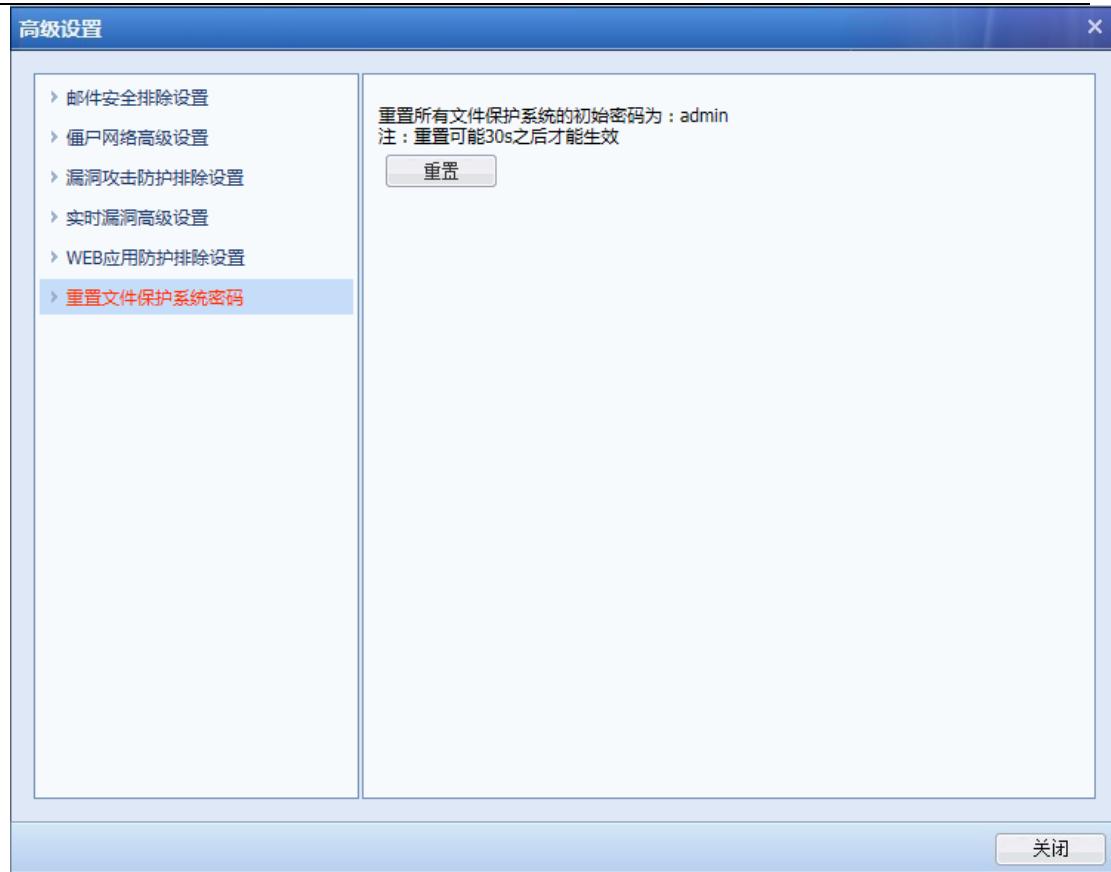


点击[下载示例文件](#)，可下载模板文件，按格式填入要排除的IP，最后导入。

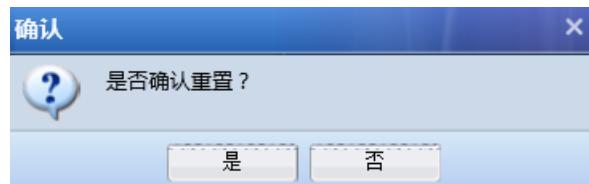
点击[保存IP地址白名单](#)，对IP地址白名单设置进行保存。

#### 重置文件保护系统密码：

[重置文件保护系统密码]：重置所有文件保护系统的初始密码为：admin，重置可能30s之后才能生效。界面如下：



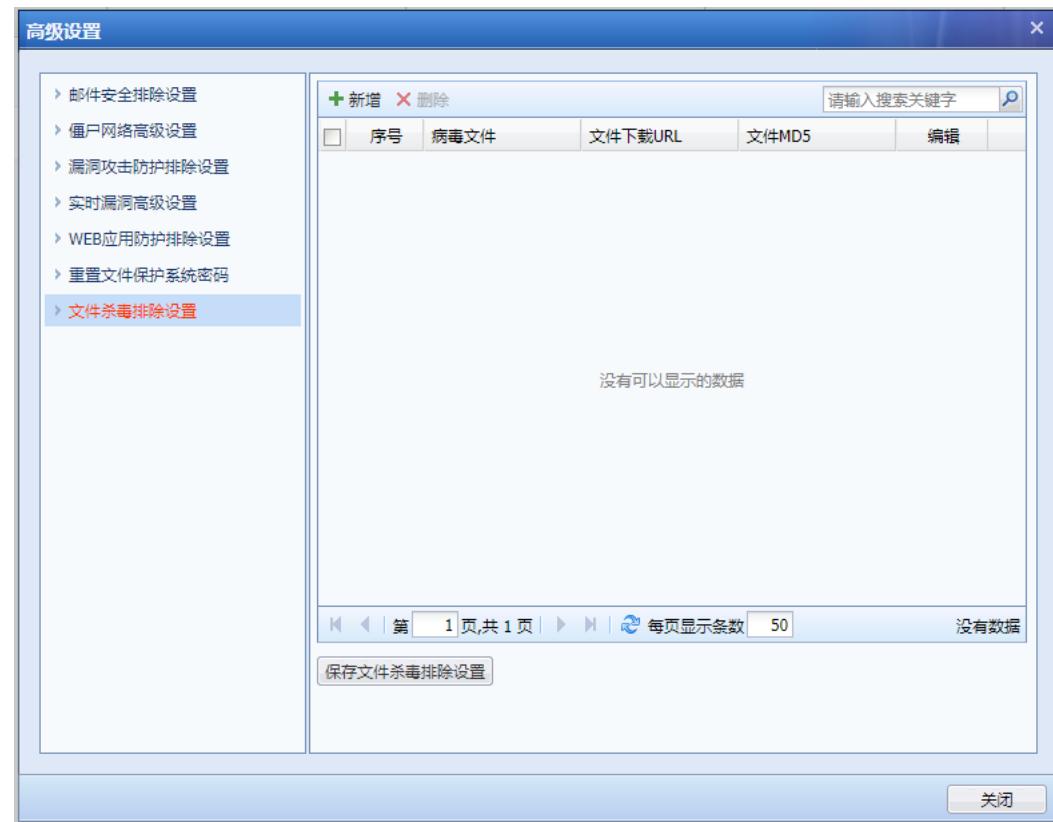
点击**重置**，弹出确认重置页面。如下图所示：



点击**是**，进行重置，点击**否**，不进行重置。

### 文件杀毒排除设置：

[文件杀毒排除设置]：对指定文件或者 URL 不做杀毒处置，如下图所示：



点击**新增**，弹出文件杀毒排除设置页面。如下图所示：



[病毒文件] 定义该排除对象的文件名。

[MD5/URL] 定义该对象的 MD5 值，或者指定 URL 进行排除。MD5 和 URL 两者可选其一。

[描述] 该对象的描述信息。

点击**确定**，提交配置

点击**保存文件杀毒排除设置**，对文件杀毒排除设置进行保存。

### 3.5.3.2. Dos/DDos 防护

DoS 攻击/DDoS 攻击（拒绝服务攻击/分布式拒绝服务攻击），通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的。SANGFOR 设备的防 DOS 攻击功能，按攻击方向可以分为“外网对内网攻击防护策略”和“内网对外网攻击防护策略”两个部分，既可以防止外网对内网的 DOS 攻击，也可以阻止内网的机器中毒或使用攻击工具发起的 DOS 攻击。如下图所示：

DoS/DDoS防护												
新增		删除		启用	禁用	上移	下移	移动	刷新	本机DoS防护	DoS防护辅助工具	查看攻击者IP
序号	名称	防护方向	描述	策略类型		攻击源区域		状态				
1	DOS	外网>内网	扫描防护:开启 DOS/DDoS攻击防护:开启 异常报文侦测:开启	outside		✓						
2	[自动创建]内网	内网>外网	自动创建替换内...	DOS/DDoS攻击防护:开启	inside		✓					

#### 3.5.3.2.1 外网对内网攻击防护策略

外网对内网攻击防护策略默认未启用，需要通过『系统』→『系统配置』→『通用配置』→『网络参数』进行启用，如下图所示：



点击『策略』→『安全策略』→『DoS/DDoS 防护』，新增『外网对内攻击防护策略』，进入外网防护设置，设置界面如下：



[名称]: 设置该防护规则的名称。

[描述]: 设置对该规则的描述

[外网区域]: 设置需要防护的源区域。外网防护的源区域一般是外部区域。

[ARP 洪水攻击防护]: 勾选[ARP 洪水攻击防护]，则启用 ARP 洪水攻击防护，可以设置[每区域阀值]，在每秒单位内如果该区域的接口收到超过阀值的 ARP 包，则会被认为是攻击。如果页面下方勾选了检测攻击后操作为[阻断]，则检测到攻击后，会丢弃超过阀值的 ARP 包。

[扫描防护]: 可开启 IP 地址扫描防护和端口扫描防护。

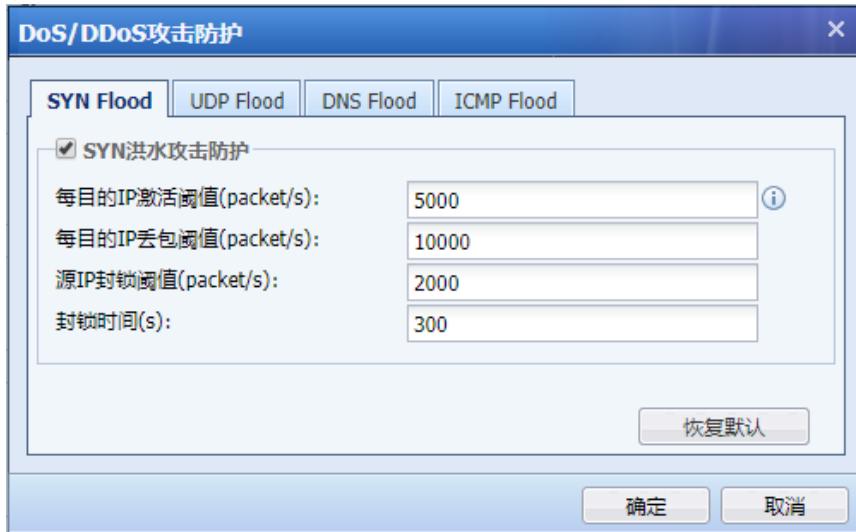


勾选[IP 地址扫描防护]，则启用 IP 地址扫描防护，可以设置[阈值]，在每秒单位内如果收到来自源区域的 IP 地址扫描包个数超过阀值，则会被认为是攻击。如果页面下方勾选了检测攻击后操作为[阻断]，则检测到攻击后，5 分钟之内会阻断该源 IP 的所有数据。5 分钟后解锁，再次计算该 IP 的扫描次数。

[端口扫描防护]: 勾选[端口扫描防护]，则启用端口扫描防护，可以设置[阈值]，在每秒单位内如果收到来自源区域的端口扫描包个数超过阀值，则会被认为是攻击。如果页面下方勾选了检测攻击后操作为[阻断]，则检测到攻击后，5 分钟之内会阻断该源 IP 的所有数据。5 分钟后解锁，再次计算该 IP 的端口扫描次数。

数据包经过上述扫描后，还将进行 [DoS/DDoS 攻击防护]，[基于数据包攻击]，[异常包文侦测]的各种攻击包的过滤。

[DoS/DDoS 攻击防护]: 点击请选择防护类型，分别设置 SYN Flood、UDP Flood、DNS Flood 和 ICMP Flood 的阈值，如下图所示：



### SYN Flood 防护

[每目的 IP 激活阈值(packet/s)]: 统计到达每个目的 IP 的 SYN 包的 PPS (packets per second)，如果超过设定值则触发 NGFW SYN 代理机制，以减少服务器压力，建议比丢包阀值低，最好为其一半。取值范围为 1-100000000。

[每目的 IP 丢包阈值(packet/s)]: 统计到达每个目的 IP 的 SYN 包 PPS(packets per second)，如果超过设定值则触发防护机制。取值范围为 1-100000000。

[源 IP 封锁阈值(packet/s)]: 统计到达每个源 IP 的 SYN 包 PPS (packets per second)，如果超过设定值则触发防护机制。取值范围为 1-100000000。

[封锁时间(s)]: 针对每个源 IP 达到超过设定值后，自动进行封锁时间。取值范围为 0~1800s，在攻击者列表可以查看攻击 IP、封锁时间。

### UDP Flood 防护:

[每目的 IP 丢包阈值(packet/s)]: 统计到达每个目的 IP 的 UDP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[源 IP 封锁阈值(packet/s)]: 统计到达每个源 IP 的 UDP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[封锁时间(s)]：针对每个目的 IP、源 IP 达到超过设定值后，自动进行封锁时间。取值范围为 0~1800s，在攻击者列表可以查看攻击 IP、封锁时间。

### DNS Flood 防护

[每目的 IP 丢包阈值(packet/s)]：统计到达每个目的 IP 的 DNS 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~1000000000。

[源 IP 封锁阈值(packet/s)]：统计到达每个源 IP 的 DNS 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~1000000000。

[封锁时间(s)]：针对每个目的 IP、源 IP 达到超过设定值后，自动进行封锁时间。取值范围 0~1800s，在攻击者列表可以查看攻击 IP、封锁时间。

### ICMP Flood 防护：

[每目的 IP 丢包阈值(packet/s)]：统计到达每个目的 IP 的 ICMP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~1000000000。

[源 IP 封锁阈值(packet/s)]：统计到达每个源 IP 的 ICMP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~1000000000。

[封锁时间(s)]：针对每个目的 IP、源 IP 达到超过设定值后，自动进行封锁时间。取值范围 0~1800s。在攻击者列表可以查看攻击 IP、封锁时间。

『检测攻击后操作』：可以勾选操作[记录日志]和[阻断]。

点击 **高级防御选项**，可基于数据包攻击类型，IP 协议报文选项，TCP 协议报文选项来开启防护，默认不勾选。如下图所示：



[基于数据包攻击]的防护类型如下：

[未知协议类型防护]: 勾选[未知协议类型防护]，则启用未知协议类型防护。当协议 ID 大于 137 时会被认为是未知协议类型。

[TearDrop 攻击防护]: 勾选[TearDrop 攻击防护]，则启用 TearDrop 攻击防护。TearDrop 攻击防御主要是严格控制 IP 头的分片偏移的长度，当 IP 头分片偏移不符合规范时，则认为是 TearDrop 攻击。

[IP 数据块分片传输防护]: 勾选[IP 数据块分片传输防护]，则表示默认不允许 IP 数据块分片传输，若有分片传输则认为是攻击。非特殊情况下，建议不要勾选此项，可能会引起网络中断。

[LAND 攻击防护]: 勾选[LAND 攻击防护]，则启用 LAND 攻击防护。当设备发现数据报文的源地址和目标地址相同时，则认为此报文为 LAND 攻击。

[WinNuke 攻击防护]: 勾选[WinNuke 攻击防护]，则启用 WinNuke 攻击防护。当 TCP 头部标识 URG 位置为 1，且目标端口是 TCP139、TCP445 等，则此报文为 WinNuke 攻击。

[Smurf 攻击防护]: 勾选[Smurf 攻击防护]，则启用 Smurf 攻击防护。当设备

发现数据包的回复地址为网络的广播地址的 ICMP 应答请求包，则认为是 Smurf 攻击。

[超大 ICMP 数据攻击防护]：勾选[超大 ICMP 数据攻击防护]则当 ICMP 报文大于 1024 时，被认为是攻击。

[IP 协议报文选项]配置页面如下：



IP 报文通常可包含 IP 时间戳选项、IP 安全选项、IP 数据流选项、IP 记录路由选项、IP 宽松源路由选项、IP 严格源路由选项等，普通的 IP 报文一般不会携带这些额外的选项，带此类选项的 IP 报文通常以攻击为目的，如果不允许数据报文携带这些选项，则勾选对应的选项即可进行防护。

如果不允许 IP 报文中携带除上述所列选项之外的其他未知 IP 报文选项，则勾选[错误的 IP 报文选项防护]。

[TCP 协议报文选项]配置页面如下：



TCP 协议报文选项的防护支持[SYN 数据分片传输防护]、[TCP 报头标志位全为 0 防护]、[SYN 和 FIN 标志位同时为 1 防护]、[仅 FIN 标志位为 1 防护]。一般情况下，正常的 TCP 报文标识不可能存在这些特征，目标主机可能因无法正常处理这些 TCP 报文而出现异常，勾选对应的选项，则设备对相应的特征报文进行防护。

点击**确定**，保存设置。

最后设置检测攻击后进行的操作，页面如下：



选择[记录日志]则对于检测到的攻击仅记录日志，不进行阻断。如果需要同时阻断攻击数据包，则可以勾选[阻断]。

最后点击**提交**，保存外网防护设置。

可以点击**新增**，继续添加其他的外网防护策略。

如果需要修改已设置的外网防护策略，则可以点击相应的[名称]进行编辑。勾选上需要修改的规则，可以点击删除来删除掉该策略。点击启用可以把规则状态改为启用。点击禁用则把规则状态改为禁用。点击上移或者下移，则可以把规则的序号进行调整。在进行规则匹配的时候，『序号』靠前的规则会先被匹配到。



1.数据包匹配是由上往下匹配的，当匹配到任何一个攻击行为被丢弃之后，都不会往下匹配。如果数据包没有匹配到前面的攻击，则会继续匹配下面设置的攻击行为是否符合。

2.设置了扫描防护，最好再设置 DoS/DDoS 攻击防护里的 ICMP 攻击防护等信息。这个主要是由黑客的攻击行为特征决定的。黑客的入侵一般情况下是首先扫描 IP 地址是否存在，扫描到 IP，然后是扫描端口。当扫描到 IP 和端口之后，则会进行下一步攻击行为。也有一些黑客本来就知道 IP 和端口，不需要扫描，直接发起攻击行为。所以最好是两处都进行设置，才能有效地防范攻击行为。

### 3.5.3.2.2 内网防护

点击『策略』→『安全策略』→『DoS/DDoS 防护』，新增『内网对外攻击防护策略』，设置界面如下：

**新增内网对外攻击防护策略**

启用

注意：如果您的内网到防火墙本机之间是SNAT的部署环境，请勿启用此防护策略！

名称：

描述：

**源**

内网区域： 请选择内网区域

网络对象： 全部

**扫描防护**

扫描攻击类型： 请选择防护类型

**DoS/DDoS 攻击防护**

DoS/DDoS 攻击类型： 已选防护：SYN洪水攻击防护, UDP洪水攻击防护, ...

**检测攻击后操作**

记录日志  阻断

[内网区域]：内网防护的源区域一般是内部区域。

[网络对象]：可以设置哪些网段的 IP 地址允许经过防火墙。

[扫描防护]、[DOS/DDOS 攻击防护]、[检测攻击后操作]与外网攻击防护策略设置相同，点击 **高级防御选项**，可开启基于数据包攻击类型的防御，如下图所示：



点击提交后，保存和生效配置。

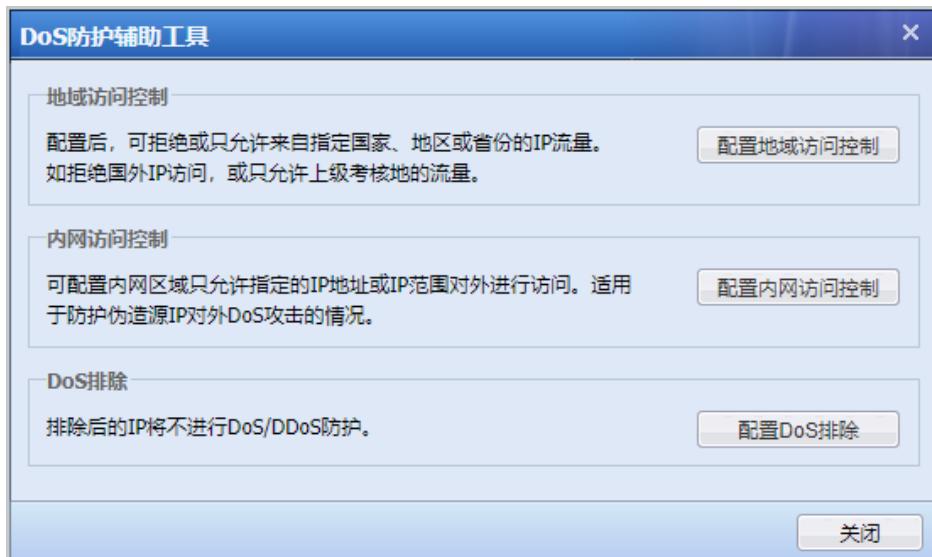
### 3.5.3.2.3 本机 Dos 防护

本机 DOS 防护功能用于防御针对 AF 设备本身的攻击。点击 本机DoS防护，设置防护类型，如下图所示：



### 3.5.3.2.4 Dos 防护辅助工具

DOS 防护辅助工作用于设置地域访问控制、内网访问控制和 DoS 排除，如下图所示：



[地域访问控制]: 可拒绝或允许指定国家或地区的 IP 流量。点击[配置地域访问控制](#)，跳转到『防火墙』→『地域访问控制』的设置页面。

[内网访问控制]: 可配置内网区域只允许指定的 IP 地址或 IP 地址范围对外进行访问。 点击[配置内网访问控制](#)，跳转到内网访问控制页面，如下图所示：

**内网访问控制**

启用

将您内网中的所有IP地址或IP范围配置到“内网网络对象”中，不在配置范围内的IP地址将被拒绝对外访问。可防御伪造源IP对外进行DoS攻击。

**内网配置**

内网区域：

网络对象：

**其它**

放行私有IP网段(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

[DoS 排除]：可配置指定 IP，排除后的 IP 将不进行 DoS/DDoS 防护，如下图所示：

**DoS排除列表配置**

排除列表的IP地址不受DoS/DDoS防护策略的影响。

一行一个IP地址

可以直接在此处输入、编辑、删除

### 3.5.3.2.5 查看攻击者 IP

点击**查看攻击者 IP**，跳转到攻击者列表页面，可以查看正在攻击或者最近 7 天内的攻击者 IP 等相关详情。

序号	攻击时间	攻击者IP	归属地	攻击方向	是否封禁	封禁时间(s)	解除封禁	永久封堵	详情
没有可以显示的数据									

### 3.5.3.3. ARP 欺骗防御

ARP 欺骗是一种常见的内网病毒，中病毒的计算机，不定时地向内网发 ARP 欺骗的广播包，使内网机器的正常通信受到干扰和破坏，严重时会导致整网断网。

设备通过不接受有攻击特征的 ARP 请求或回复来保护设备本身的 ARP 缓存，实现自身的免疫。

如果设备的访问控制用户有绑定 IP/MAC，则设备会以绑定的 IP/MAC 信息为准。

页面设置如下：



[启用]：勾选则启用 ARP 欺骗防御，设备将定时广播自己的 MAC 地址。

[网关 MAC 广播间隔时间 (秒/次)]：设置设备广播 MAC 的间隔时间。

### 3.5.4. 解密

『解密』主要用于内网用户通过设备上网，加密邮件和 HTTPS 数据的解密场

景；以及内网有加密服务器，AF设备通过解密访问服务器的流量，对服务器进行保护的场景。解密功能需要多功能序列号开启。

### 3.5.4.1. 解密内网服务器发布的业务

解密内网服务器发布的业务适用于内网有加密服务器，AF设备通过解密访问服务器的流量，对服务器进行保护的场景。点击**新增**，设置解密的策略，如下图所示：



『名称』：填写易于标识的策略的名称。

『区域』：选择访问服务器的源区域。

『网络对象』：填写访问服务器的网络对象。

『业务类型』：解密内网服务器发布的业务，加密服务器部署在 AF 设备的内网区域。解密访问站点的数据，适用于内网用户上网时邮件和 HTTPS 数据的解密场景。

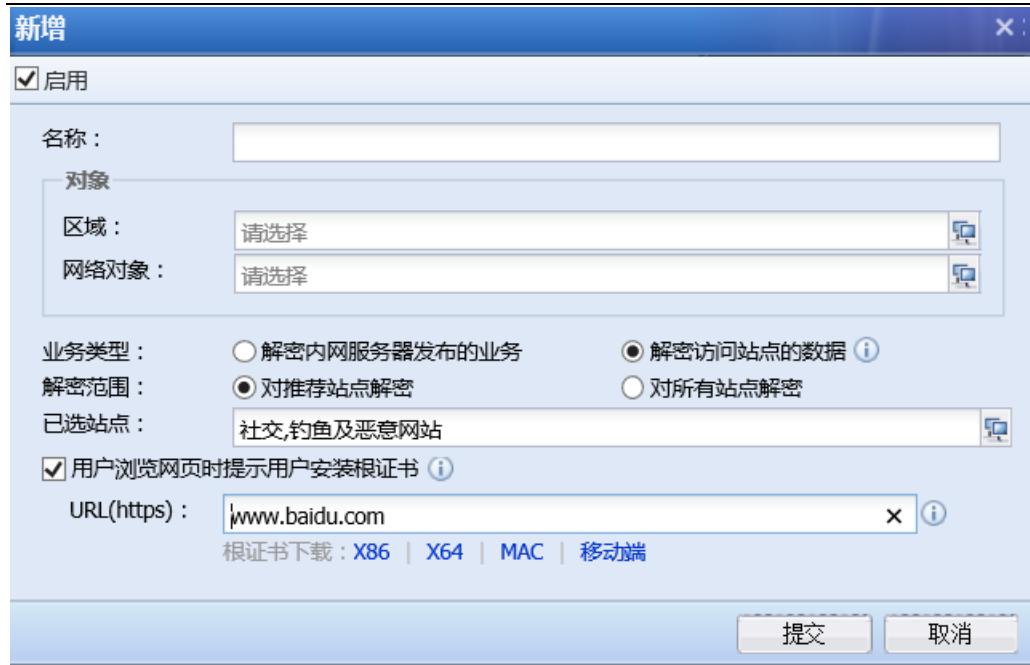
『服务器 IP/端口』：添加需要解密的服务器的 IP 和端口。点击新增，如下所示：



『服务器证书』：选择该加密服务器的证书。需要在『解密』→『服务器证书』页面导入服务器证书。详情参见章节 3.5.3.1.4

### 3.5.4.2. 解密访问站点的数据

解密访问站点的数据适用于内网用户通过设备上网，对加密邮件和 HTTPS 数据的解密场景。如下图所示：



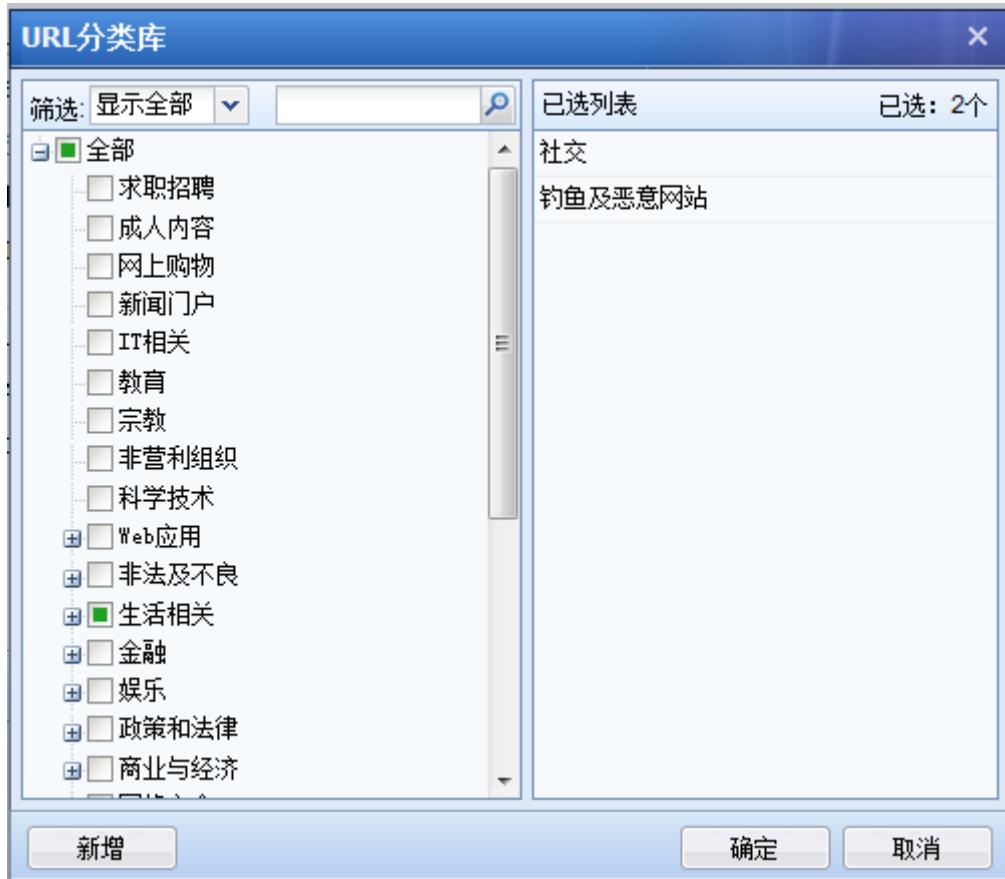
『名称』：填写易于标识的策略的名称。

『区域』：选择访问公网的源区域。

『网络对象』：填写访问服务器的网络对象。

『业务类型』：选择解密访问站点的数据。

『解密范围』：可选择对推荐站点解密和所有站点解密。如果选择对推荐站点解密，点击 ，从 URL 分类库选择需要解密的网站分类：



『用户浏览网页时提示用户安装根证书』：由于解密功能开启后，用户访问 https 网站会出现证书告警的提示，通过配置用户浏览网页时提示用户安装根证书，设置安装根证书下载链接的 URL，可以消除浏览的告警提示。

若 URL 设置为 www.baidu.com，配置后内网用户访问 https://www.baidu.com 会出现如下提示安装证书的页面：



内网用户下载安装受信任的证书后，再访问 https 网站，可消除浏览器的证

书告警。

### 3.5.4.3. 排除列表

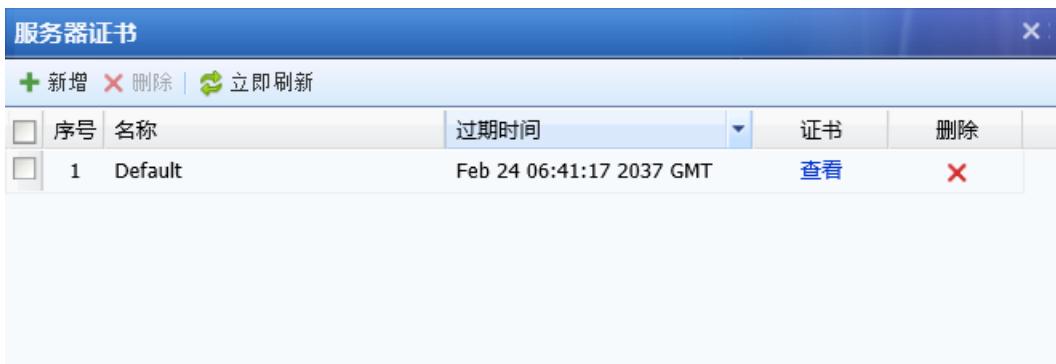
『排除列表』用于设置对特定的 URL、SNI 和 CN 排除不做解密，如下图所示：



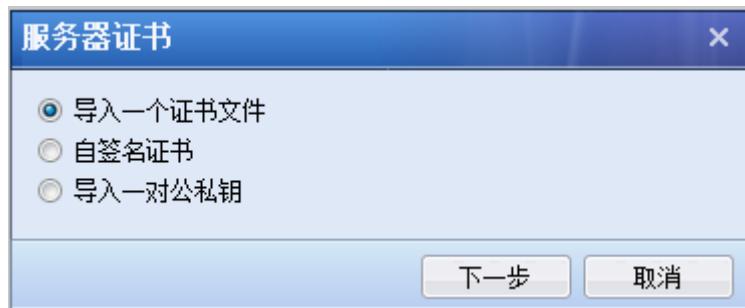
1. 解密功能需要开通多功能序列号开启。
2. 该功能请不要随意开启，会对设备造成一定的性能压力。
3. 内网用户访问外网的加密邮件是默认解密的，只需要有一条启用的解密访问站点数据的规则就行，其余操作只需要在『内容安全』→『内容安全策略』中设置即可。
4. 加密邮件安全、HTTPS 杀毒、HTTPS 网页过滤、HTTPS 的上传和下载过滤功能依赖于解密访问站点的数据。

### 3.5.4.4. 服务器证书

『服务器证书』用于导入需要解密的内网服务器证书。如下图所示：



点击**新增**，可导入一个证书文件、自签名证书或导入一对公私钥，如下图：



点击**查看**，可查看到证书详细信息：



### 3.5.5. 流量管理

#### 3.5.5.1. 概述

流量管理是通过建立流量管理通道对各种上网应用的流量大小进行控制。

流量管理系统提供了带宽保证和带宽限制功能，通过带宽保证可以保证重要应用的访问带宽，通过带宽限制可以做到限制用户组/用户上下行总带宽、各种应用的带宽等。

流量管理系统同时提供流量子通道的功能，可以根据需求建立流量子通道，对通道流量做更为细化的分配。

基本概念：

**流量通道：**我们根据服务类型，访问控制用户组，把整个线路带宽按百分比，分解成若干份，这样的每一份，为一个流量通道。根据流量通道的作用可以分为：带宽保证通道和带宽限制通道

**带宽限制通道：**对此通道的最大流速进行设置。网络繁忙时，该通道占用带宽不会超过我们设置的最大带宽值。

**带宽保证通道：**不仅设置此通道的最大带宽，而且设置最小带宽。当网络繁忙时，保证该通道的带宽不小于设置的最小带宽值。

**虚拟线路：**用于将设备物理网络接口和流量通道中的“生效线路”对应，指明从哪个接口出去的数据，才匹配该流控通道。

### 3.5.5.2. 流量通道匹配及优先级

当流量管理系统处于[启用]状态时，数据经过设备时，会根据数据的相关信息，匹配流量通道，匹配的条件包括：用户组/用户、IP 地址、应用类型、生效时间、目标 IP 组，当数据包的所有条件满足时，即匹配到通道。

相同的数据只会匹配一条流控策略，流量通道的匹配顺序是从上到下匹配的，所以设置的时候需要把具有更细化匹配条件的通道放在上面。

### 3.5.5.3. 通道配置

#### 3.5.5.3.1 保证通道

用于保证重要应用的使用，通过设置最小带宽值，保证特定类型的数据占用带宽不小于某个值，从而保证在线路比较繁忙的时候，重要应用可以有带宽能正常使用。

##### 3.5.5.3.1.1 保证通道设置学习

举例如下：公司租用了一条 10Mb/s 电信线路，内网有 1000 名上网用户，保证财务部访问网上银行网站和收发邮件的数据在线路繁忙时占用带宽也不小于 2Mb/s，但是最大不能超过 5Mb/s。

第一步：进入『流量管理』→『通道配置』，先启用流量管理系统。

勾选[启用流量管理系统]，启用流量管理。



第二步：进入『流量管理』→『虚拟线路配置』，配置虚拟线路列表和虚拟线路规则，设置方法见 3.14.4 虚拟线路配置。

第三步：配置保证通道

本例中是对财务部人员的访问网上银行类别的网站以及收发邮件的数据做带宽保证。



在【带宽分配】中点击**新增通道**，选择**添加通道**，出现【新增一级通道】  
页面



勾选[启用通道]，表示该通道是启用状态，不勾选则为禁用状态，流控功能暂时不生效。

在『通道名称』中输入该通道的名称。

在【通道编辑菜单】中选择[带宽通道设置]，在右边窗口中设置通道的相关属性。



**【带宽通道设置】：**用于设置生效线路、通道类型、限制或保证的带宽、单个用户带宽等。

[生效线路]用于选择通道适用的线路，也就是当数据走此条线路时才会匹配到此通道。生效线路中所列线路，需要事先在虚通道设置中设置，关于虚通道设置参见 3.12.4 小节。

[带宽通道类型]用于选择通道类型并定义带宽值，此例中需要对财务部人员的访问网上银行类别的网站以及收发邮件的数据做带宽保证，保证至少 2Mb/s，最高不超过 5Mb/s，则此处勾选[保证通道]，设置[上行带宽]、[下行带宽]的[保证]和[最大]分别为 20% 和 50% 的总带宽，总带宽是 10Mb/s，则保证带宽为 2Mb/s，最大带宽为 5Mb/s。[优先级]分为高、中、低三类，指其他通道空闲时此通道占用空闲带宽的优先级。

启用限制单IP最大带宽

上行： Kbps ▾

下行： Kbps ▾

**高级选项设置**

把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽以及单用户最高带宽属性对外网IP有效（此选项通常用于对外提供服务的服务器，请慎重选择）。

[启用限制单 IP 最大带宽]用于限制匹配到此通道的单个 IP 占用的带宽值，此例中不需要对单个用户做最大带宽的限制，则此处不勾选。

[高级选项设置]勾选此项表示把每一个外网 IP 作为通道内的用户，使得通道的用户间公平分配带宽以及单用户最高带宽属性对外网 IP 有效（此选项通常用于对外提供服务的服务器，请慎重选择）。

**【通道使用范围】：**用于设置哪些类型的数据会匹配到此通道，即通道的使用范围，此处设置的范围包括：应用类型、适用对象、生效时间、目标 IP 组、子接口、VLAN，这些条件需要全部满足才能匹配到此通道。

新增一级通道

启用通道

通道名称：

**通道编辑菜单**

- 带宽通道设置
- 通道适用范围

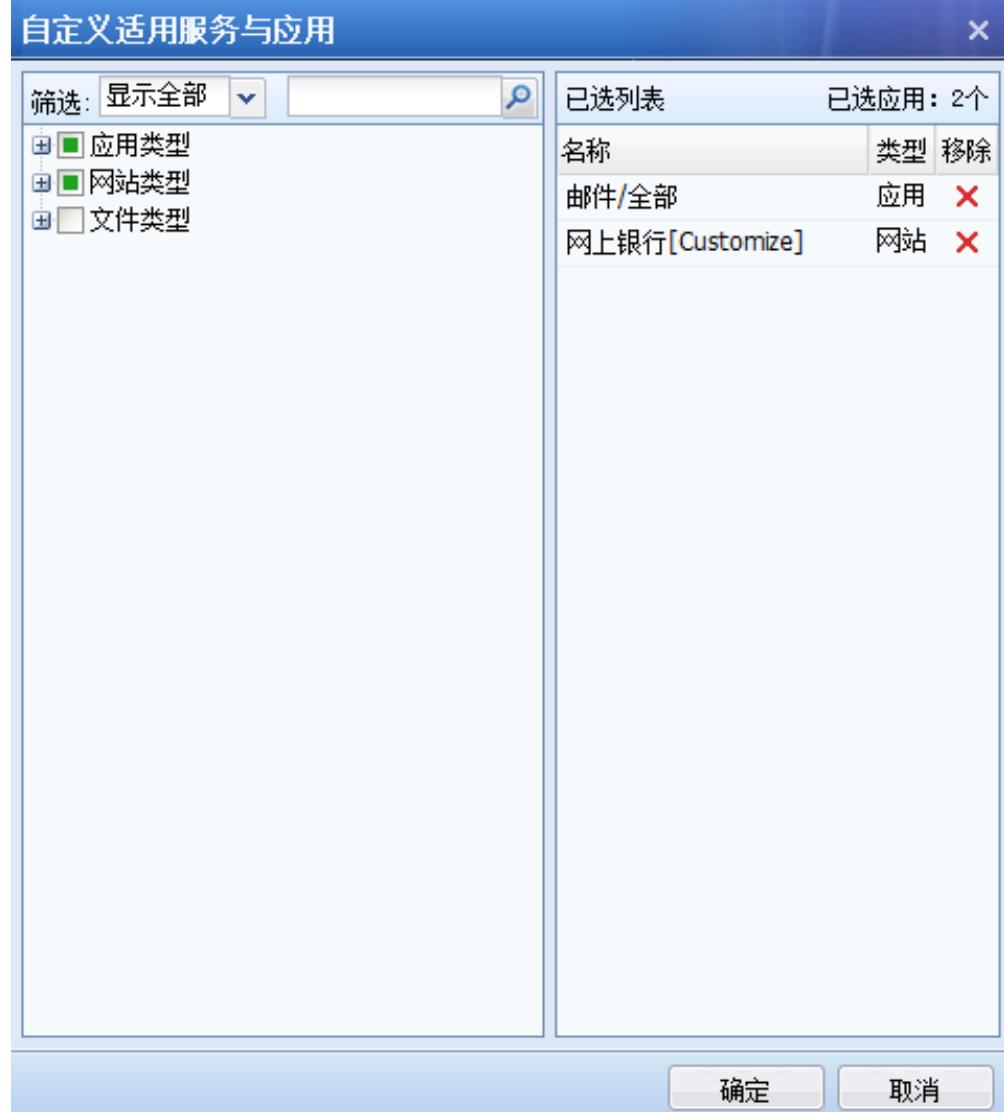
**通道适用范围**

适用应用：  
 所有应用  
 自定义  
[选择自定义应用](#)

适用对象：  
 网络对象  
 全部  
 认证用户/组  
 全天

目标：  
 网络对象  
 全部  
 地区  
 子接口  
 VLAN  
 全部

[适用应用]用于设置应用类型，勾选[所有应用]表示针对所有类型的数据有效，勾选[自定义]选择特定的应用类型，点击[选择自定义应用](#)，在弹出框【自定义适用服务与应用】中选择应用类型和网站类型，此例中需要收发邮件和访问网上银行的网站数据做带宽保证，则此处选择应用：邮件/全部；网站类型选择：网上银行。



另外[文件类型]是用于对通过 HTTP、FTP 协议下载的文件类型做控制。在【已选列表】中确认选择的范围是否正确，点击**确定**，完成适用应用的设置。

[适用对象]用于设置此通道对哪些网络对象和用户组生效，适用对象可以是基于 IP 也可以基于用户。此例中需要对财务部的所有用户做带宽保证，则此处选择“用户”，在【组织结构】中选择需要的组路径；在【当前组路径】中选择用户组和用户；在【已选自定义组和用户】中查看已选的用户、用户组列表。选择好[适用对象]后，点击**确定**，完成设置。

选择用户/组

组织结构

筛选: 显示全部

- /
  - 工程师
  - 市场部
  - 网络部
  - 财务部
  - 默认组

当前组路径: 未选中组

选择 搜索:

名称	类型
没有可以显示的数据	

第 1 页, 共 1 页

已选自定义组和用户

 / 财务部

确定取消

[生效时间]用于设置此通道的生效时间。

[网络对象]用于设置目标 IP 条件。

[地区]用户设置目的地址

[子接口]用于设置流量通道适用的子接口。

[VLAN]设置流量通道适用于的 VLAN。

设置完成后，显示如下：

新增一级通道

启用通道

通道名称： 财务部保障通道 (i)

通道编辑菜单	通道适用范围
➤ 带宽通道设置	通道适用范围
➤ 通道适用范围	通道适用范围

适用应用： 所有应用  自定义  
**已选应用: FTP/ftp或者smtp状态220, 邮件/全部, 网络会议/全部**

适用对象： 网络对象 全部   
 认证用户/组 /财务部/ 

生效时间：全天 

目标： 网络对象 全部   
 地区 请选择国家/地区 

子接口 全部   
 Vlan 请选择Vlan 

设置完成后，点击**确定**，完成保证通道的设置。

第四步：点击确定保存后，【带宽分配】中会出现设置的通道。保证通道配置完成。



1、保证带宽通道百分比之和可能会超过 100%时，当超过 100%时，各保证通道的最小带宽值会按照比例进行缩减。比如，我们设置两条通道，第一条保证带宽设为 30%，第二条设为 90%，则第一条实际分配到  $30 / (90+30) \%$ ，即 25%，第二条实际分配到  $90 / (90+30) \%$ ，即 75%。

2、优先级：当实际带宽有空余，优先级越高越先占用空闲带宽。

### 3.5.5.3.2 限制通道

设置通道的最大带宽，对于匹配到此限制通道的数据进行流量控制，控制占用带宽不得超过设置的最大带宽值。

#### 3.5.5.3.2.1 限制通道设置学习

举例如下：公司租用了一条 10Mb/s 电信线路，内网有 1000 名上网用户，发现很多市场部人员经常使用迅雷下载，P2P 等下载工具进行下载，占用了大部分带宽，影响了其他部门的正常的办公业务，通过流量管理系统将市场部的这部分数据占用的带宽限制在 2Mb/s 之内，并且每个用户这部分数据的占用带宽限制在 30KB/s。

第一步：进入『流量管理』→『通道配置』，先启用流量管理系统。

勾选[启用流量管理系统]，启用流量管理。

第二步：进入『流量管理』→『虚拟线路配置』，配置虚拟线路列表和虚拟线路规则，设置方法见 3.11.4 虚拟线路配置。

第三步：配置限制通道

本例中是对市场部人员的 P2P、下载数据进行流控，限制这些应用占用的总带宽不超过 2Mb/s。

在【带宽分配】中点击**新增通道**，选择**添加通道**，出现【新增一级通道】页面：

勾选[启用通道]，表示该通道是启用状态，不勾选则为禁用状态，通道暂时不生效。

在『通道名称』中输入该通道的名称，『所属通道』用于显示通道级别，“/”表示此通道是一级通道。

在【通道编辑菜单】中选择[带宽通道设置]，在右边窗口中设置通道的相关属性。



**【带宽通道设置】：**用于设置生效线路、通道类型、限制或保证的带宽、单个用户带宽等。

[生效线路]用于选择通道适用的线路，也就是当数据走此条线路时才会匹配到此通道。生效线路配置请见 3.12.4 小节

[带宽通道类型]用于选择通道类型并定义带宽值，此例中需要对市场部的P2P、下载等数据进行带宽限制，则此处勾选[限制通道]，设置[上行带宽]、[下行带宽]分别为20%的总带宽，总带宽是10Mb/s，则限制带宽为2Mb/s。[优先级]分为高、中、低三类，指线路繁忙时通道占用带宽的优先级。



[启用限制单IP最大带宽]用于限制匹配到此通道的单个IP占用的带宽值，此例中需要对市场部每个用户P2P、下载等数据的占用带宽限制在30KB/s，在[上行]、[下行]中分别输入30KB/s。

[用户间带宽分配策略]用于设置匹配到此通道的用户，带宽怎样在用户间进行分配，默认选择的是[平均分配]，即用户间的带宽是平均分配的，注意这里的用户是指有流量匹配到此通道的用户，属于『通道使用范围』内但没有此类应用流量的用户不参与平均分配。[自由竞争]这种分配方式暂时不能设置。

[高级选项设置]勾选此项表示把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽以及单用户最高带宽属性对外网IP有效（此选项通常用

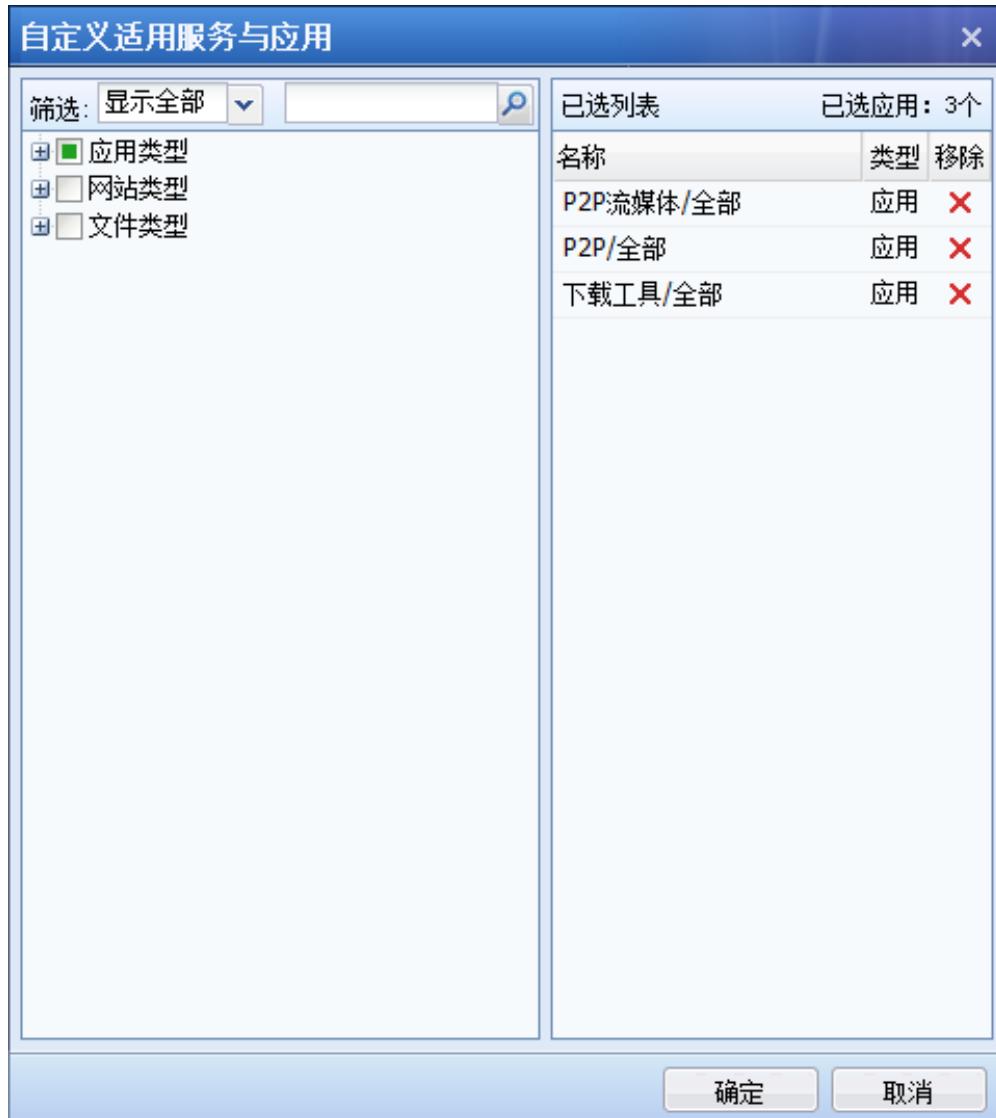
于对外提供服务的服务器，请慎重选择）。

**【带宽使用范围】：**用于设置哪些类型的数据会匹配到此通道，即通道的使用范围，此处设置的范围包括：应用类型、适用对象、生效时间和目标 IP 组，这些条件需要全部满足才能匹配到此通道。



[适用应用]用于设置应用类型，勾选[所有应用]表示针对所有类型的数据有效，勾选[自定义]选择特定的应用类型，点击选择自定义应用，在弹出框【**自定义适用服务与应用**】中选择应用类型，此例中需要对 P2P 相关数据和下载工具下载数据进行流控，则此处选择应用：文件下载/全部、P2P/全部、P2P 流媒体/全部。另外还可以选择[网站类型]和[文件类型]，[网站类型]是用于对访问网站的数据，针对某些类型的网站访问做控制；[文件类型]是用于对通过 HTTP、FTP 协议下载的文件类型做控制。在【已选列表】中确认选择的范围是否正确，点击

确定，完成适用应用的设置。



[适用对象]用于设置此通道对哪些网络对象和用户组，适用对象可以是基于IP 也可以基于用户。此例中需要对市场部门的所有用户做带宽限制，则此处选择“用户”。在【组织结构】中选择需要的组路径；在【当前组路径】中选择用户组和用户；在【已选自定义组和用户】中查看已选的用户、用户组列表。选择好 [适用对象]后，点击**确定**完成设置。



[生效时间]: 用于设置此通道的生效时间。

[目标 IP 组]: 用于设置目标 IP 条件。

[子接口]: 用于设置流量通道适用的子接口。

[VLAN]: 设置流量通道适用于的 VLAN。

设置完成后，显示如下：

新增一级通道

启用通道

通道名称：限制市场部下载    

通道编辑菜单	通道适用范围
<ul style="list-style-type: none"><li>带宽通道设置</li><li><b>通道适用范围</b></li></ul>	<p>通道适用范围</p> <p>适用应用：<input type="radio"/> 所有应用 <input checked="" type="radio"/> 自定义 <b>已选应用: P2P流媒体/全部, P2P/全部</b></p> <p>适用对象：<input type="radio"/> 网络对象 <input checked="" type="radio"/> 认证用户/组 <span style="border: 1px solid #ccc; padding: 2px;">全部</span> <span style="border: 1px solid #ccc; padding: 2px;"> </span> <input checked="" type="radio"/> /市场部/ <span style="border: 1px solid #ccc; padding: 2px;">全部</span> <span style="border: 1px solid #ccc; padding: 2px;"> </span></p> <p>生效时间：<input checked="" type="radio"/> 全天 <span style="border: 1px solid #ccc; padding: 2px;">全天</span> <span style="border: 1px solid #ccc; padding: 2px;"> </span></p> <p>目标：<input checked="" type="radio"/> 网络对象 <input type="radio"/> 全部 <span style="border: 1px solid #ccc; padding: 2px;">全部</span> <span style="border: 1px solid #ccc; padding: 2px;"> </span> <input type="radio"/> 地区 <span style="border: 1px solid #ccc; padding: 2px;">请选择国家/地区</span> <span style="border: 1px solid #ccc; padding: 2px;"> </span></p> <p><input checked="" type="radio"/> 子接口 <input type="radio"/> 全部 <span style="border: 1px solid #ccc; padding: 2px;">全部</span> <span style="border: 1px solid #ccc; padding: 2px;"> </span> <input type="radio"/> Vlan <span style="border: 1px solid #ccc; padding: 2px;"> </span></p>

设置完成后，点击**确定**，完成限制通道的设置。

第四步：点击确定保存后，【带宽分配】中会出现设置的通道。限制通道配置完成。

### 3.5.5.3.3 排除策略

排除策略用于设置某些类型的数据不匹配任何流量管理通道，设置排除策略的目的在于排除部分数据不受流量管理策略的限制，比如设备做网桥模式部署，前置防火墙的 DMZ 区接了部分服务器，内网访问这部分服务器的数据不需要走流量管理，因为数据不经过公网，不需要受公网带宽的限制，此时对这部分服务器的应用或者 IP 做排除策略。

### 3.5.5.3.3.1 排除策略用户设置

举例如下：设备做网桥模式部署，前置防火墙的 DMZ 区接了部分服务器，要对访问这些服务器的数据做排除。

第一步：在『对象』→『网络对象』新增 IP 组，将需要排除的 IP 地址添加进去。



第二步：点击进入『流量管理』→『通道配置』→『排除策略』，点击新增，添加排除策略。



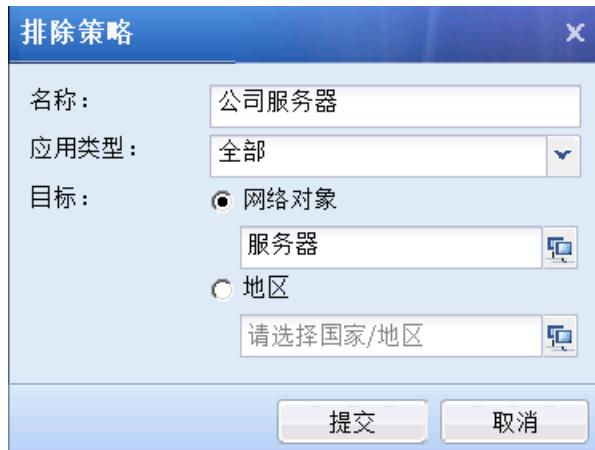
第三步：设置排除策略：

填写[策略名称]；选择[应用类型]，如果应用类型不固定，那么可以选择[全

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

部]；选择[目标 IP 组]，此处选择第一步中设置的[服务器]组。



第四步：点击提交设置完成。

排除策略也可以对去往某些地区的不进行流量控制

### 3.5.5.4. 虚拟线路配置

#### 3.5.5.4.1 虚拟线路列表

虚拟线路列表，显示当前的虚拟线路，此处用于将设备的物理网络接口和通道配置中需要调用的生效线路对应起来，指明数据从哪个接口（哪条生效线路）出去时才匹配流控通道，点击新增，弹出【新增虚拟线路】的设置页面，设置如下：



[外出接口]: 指明数据从哪个接口出去时才匹配此虚拟线路，只能选择属性是 WAN 口的接口。

[上行]: 配置该物理线路的上行带宽，此处一定要按照出口的实际带宽设置，否则可能导致流控效果不理想。

[下行]: 配置该物理线路的下行带宽，此处一定要按照出口的实际带宽设置，否则可能导致流控效果不理想。

如果有多个外网接口都需要做流控，则需要定义多条虚拟线路，点击**新增**继续添加其他的虚拟线路。



定义好虚拟线路之后，一定要设置对应的虚拟线路规则，引用该虚拟线路，否则流控通道设置是无效的。

### 3.5.5.4.2 虚拟线路规则

虚拟线路规则是流控通道生效的必要设置，可以根据不同的协议、内网范围和外网范围、出接口来匹配不同的虚拟线路规则。

在『策略』→『流量管理』→『虚拟线路配置』→『虚拟线路规则』中，点击**新增**，弹出【虚拟线路规则编辑】页面，设置页面如下：

## 新增虚拟线路规则 &gt;

## 协议设置

协议类型: 全部

协议号: 0



## 内网范围

IP地址:  所有IP 指定IP或范围 内网端口:  所有端口 指定端口或范围

## 外网范围

IP地址:  所有IP 指定IP或范围 外网端口:  所有端口 指定端口或范围

## 线路设置

目标线路: 线路1



[协定设置]用于指定数据包的协定；

[内网范围]用于设置数据包的源 IP 和源端口条件；

[外网范围]用于设置数据包的目标 IP 和目标端口条件；

[目标线路]: 指定匹配该虚拟线路规则的数据包匹配哪条虚拟线路，即哪

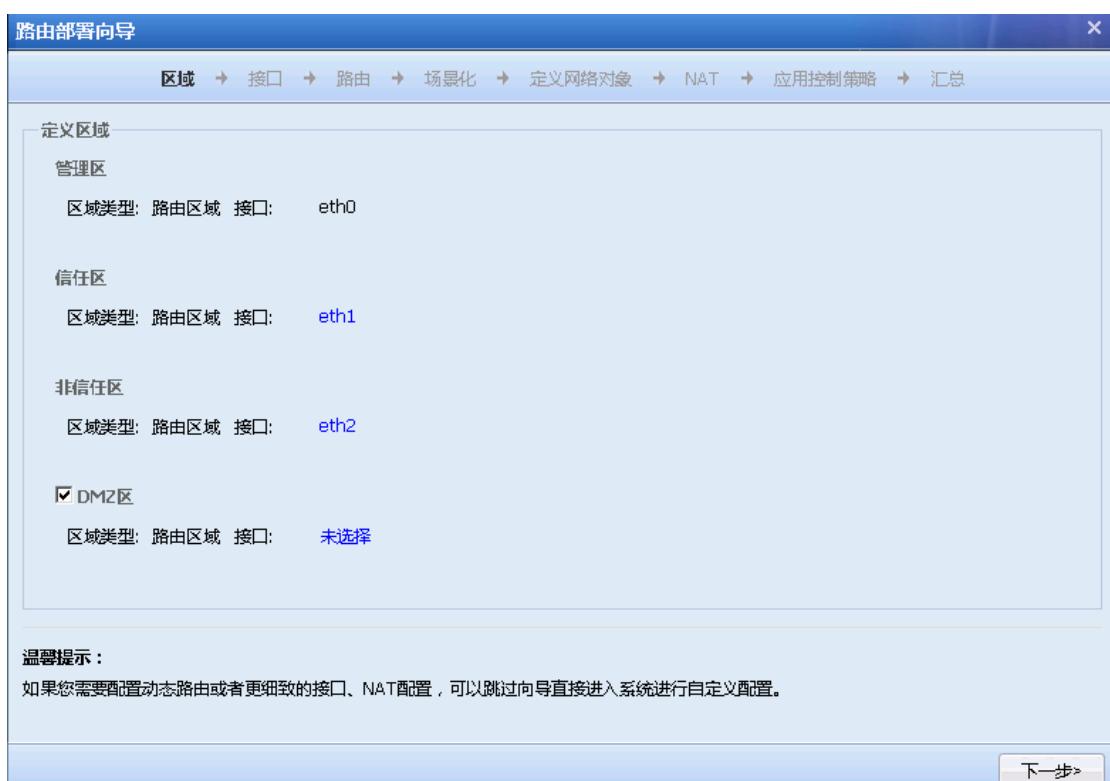
个接口转发。

当虚拟线路成为某条虚拟线路规则的目标线路后，针对该线路作的流控通道才生效。

### 3.5.6. 配置向导

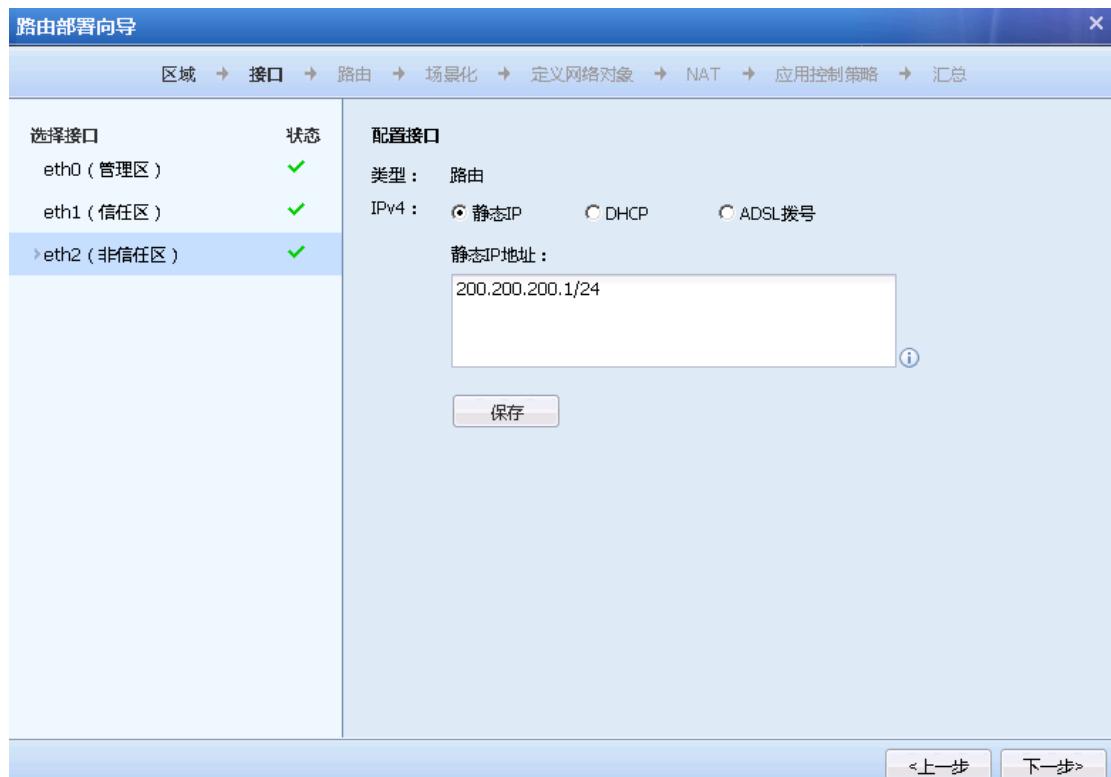
#### 3.5.6.1. 设备作为网关（路由模式）

如果 AF 设备需要作为网关部署在网络环境中，请按照如下图所示步骤进行配置：

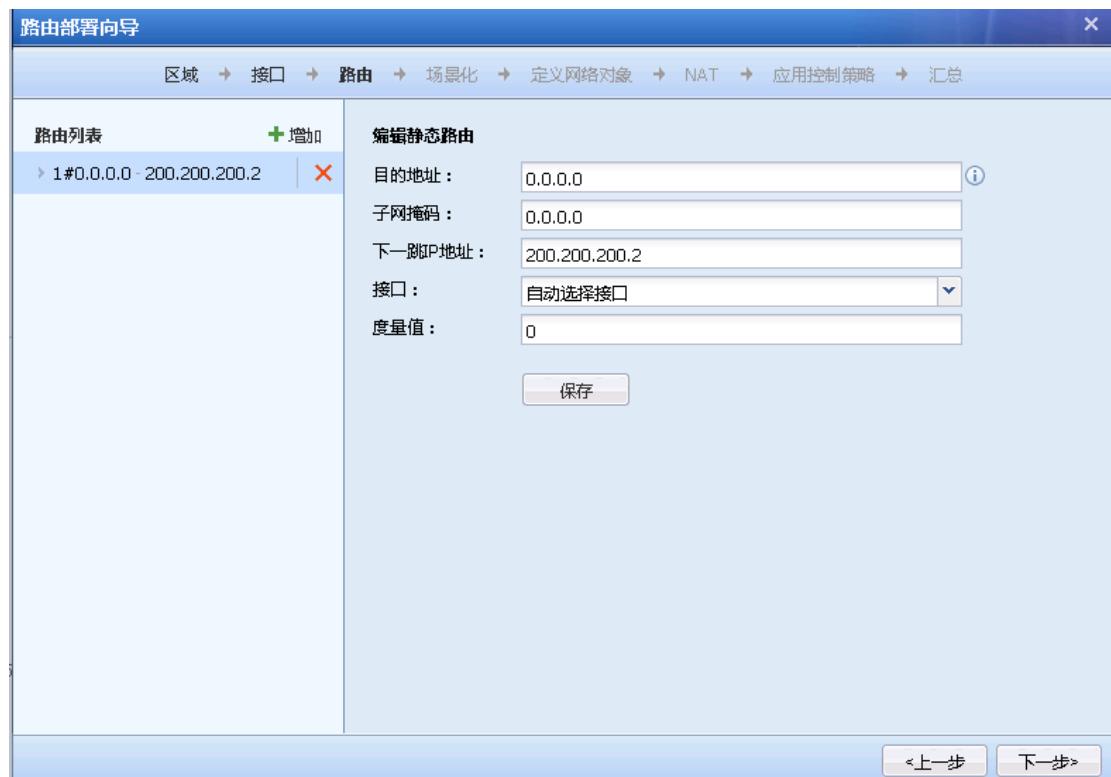


选择信任区和非信任区的接口，DMZ 区为可选项

点击**下一步**，页面将会打开『接口』的配置页面，配置路由接口，接口地址和属性。



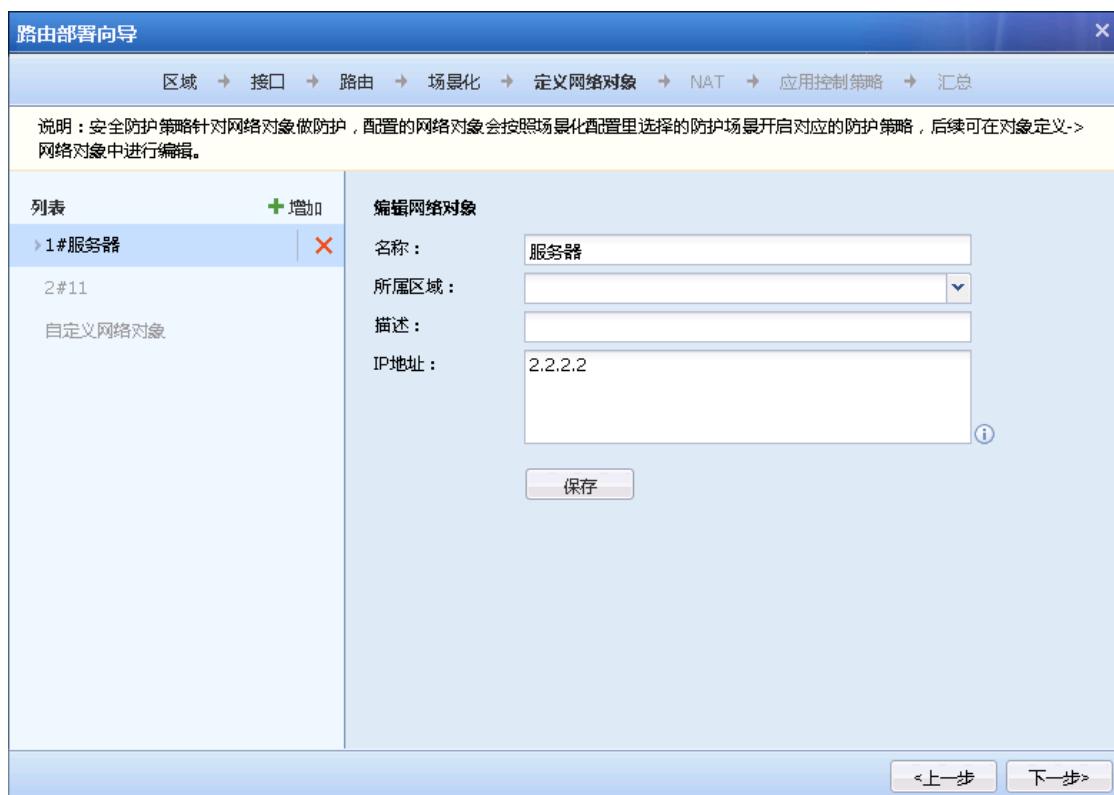
点击**下一步**，将会打开『路由』的配置页面，根据网络环境配置静态路由，保证网络的连通。



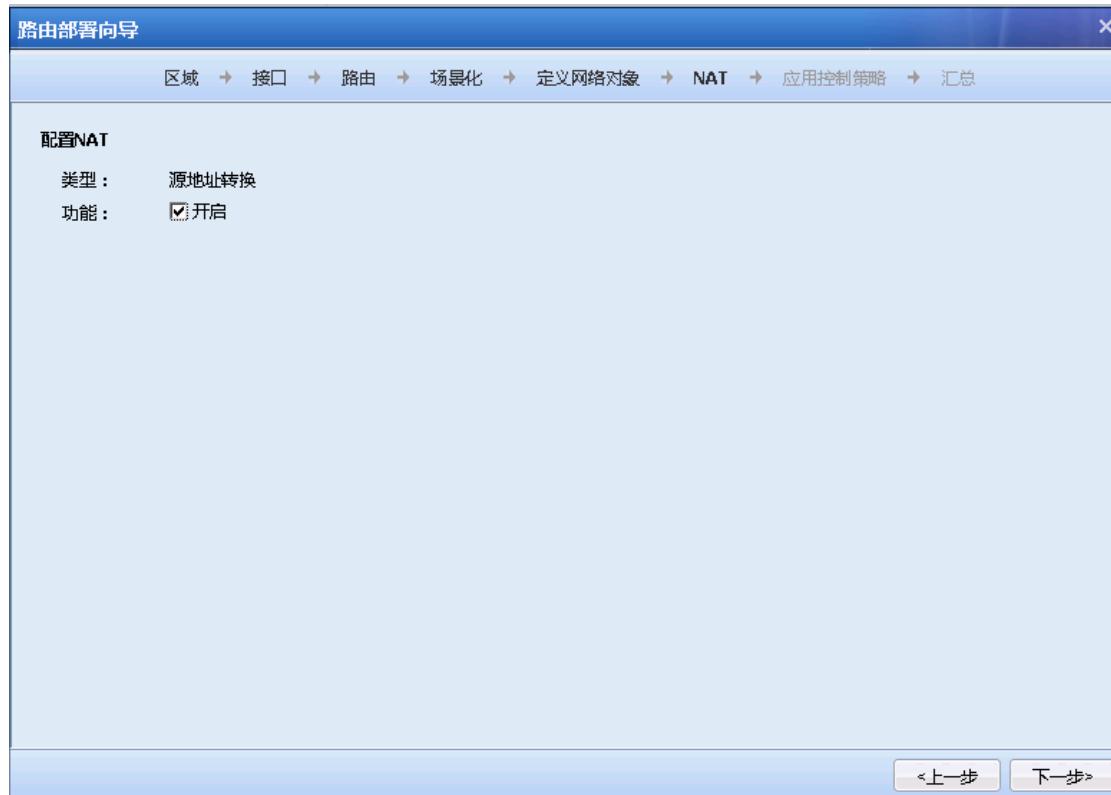
点击**下一步**，将会打开『场景化』，可以根据场景来选择防护策略



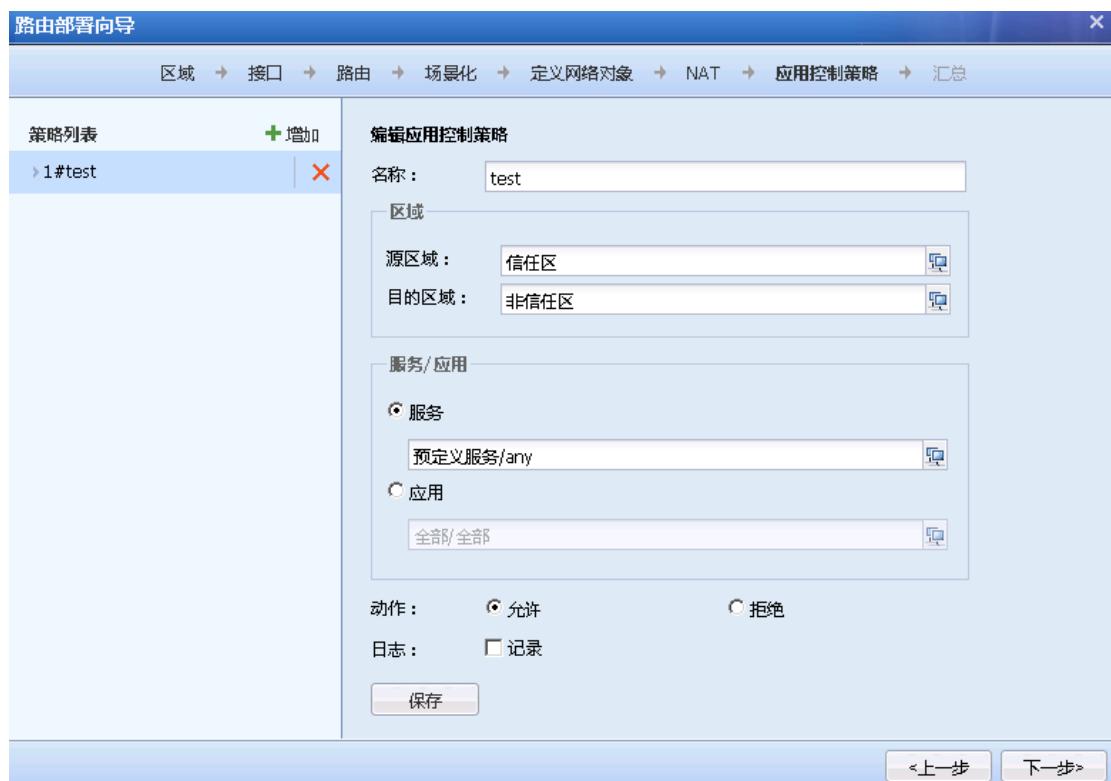
点击**下一步**，将会打开『定义网络对象』，可以自定义网络对象



点击**下一步**，将会打开『NAT』，在这里开启 nat 代理上网



点击**下一步**，将会打开『应用控制策略』，配置应用控制策略



点击**下一步**，将会打开『汇总』，这里展示配置的汇总信息

路由部署向导

区域 → 接口 → 路由 → 场景化 → 定义网络对象 → NAT → 应用控制策略 → 汇总

部署模式：路由部署 场景化配置：上网管控场景

管理区

接口：eth0

信任区

接口：eth1

非信任区

接口：eth2

订阅安全报表

多个邮箱请用“;”隔开，最多支持5个邮箱

系统将定期推送综合网络安全分析报告到以上邮箱！

已配置的防护策略

✓ 入侵防御系统  
✓ 僵尸网络  
✓ 内容安全 (Web、文件、邮件)

NAT

源地址转换：开启

应用控制策略

test

<上一步 提交

点击**提交**，保存配置信息，完成向导



确认后，仅生效向导中配置的策略，原有策略将会被清空

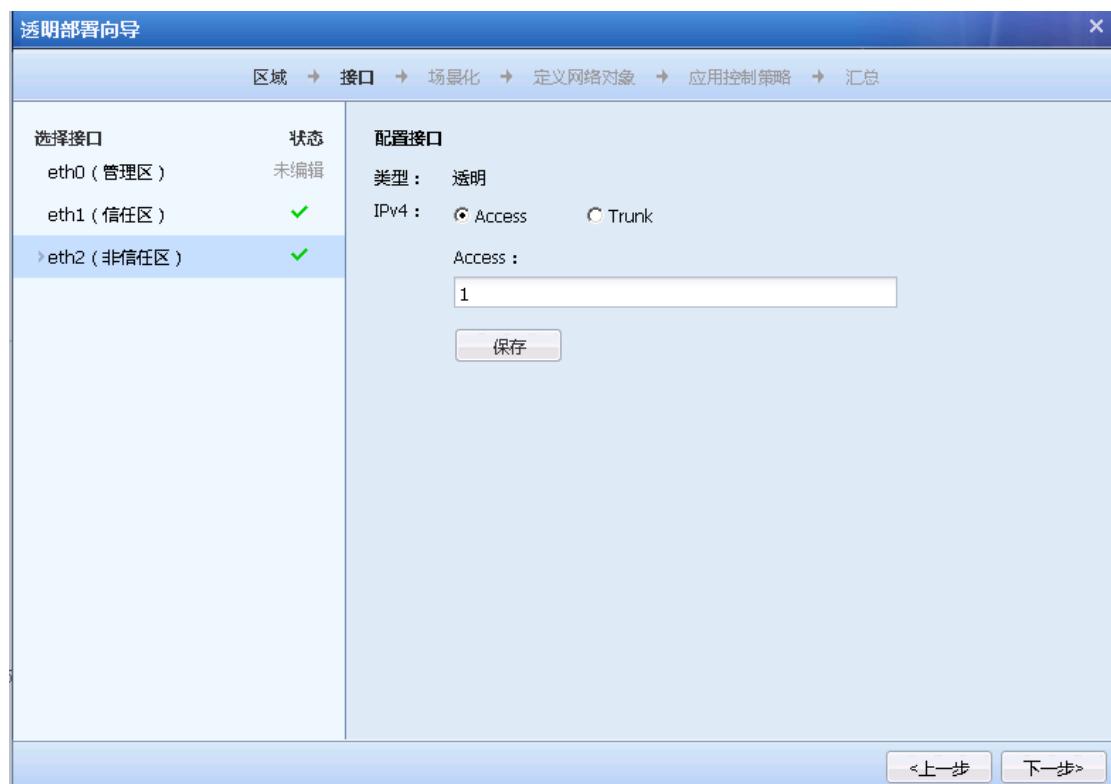
### 3.5.6.2. 不改变原有网络（网桥透明模式）

在不改变原有的网络环境，AF设备作为网桥透明部署在网络中，请按照如下图所示步骤进行配置：



选择信任区和非信任区的接口，DMZ 区为可选项

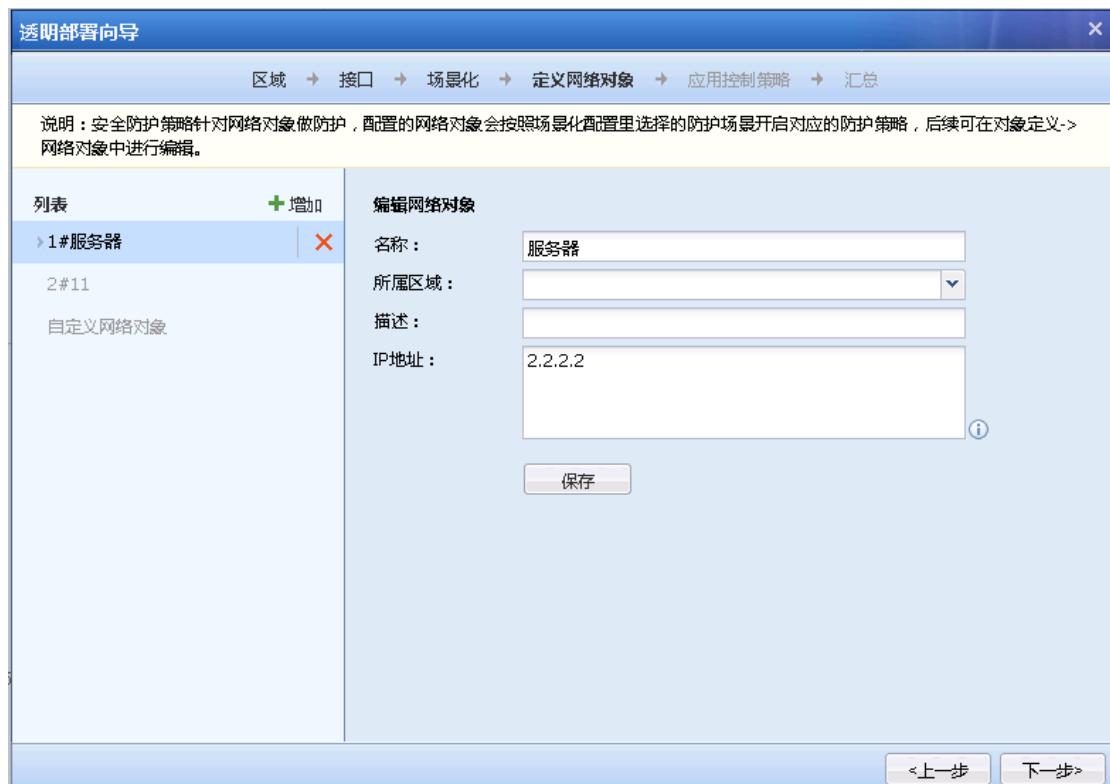
点击**下一步**，页面将会打开『接口』的配置页面，定义网桥



点击**下一步**，将会打开『场景化』，可以根据场景来选择防护策略



点击**下一步**，将会打开『定义网络对象』，可以自定义网络对象



点击**下一步**，将会打开『应用控制策略』，配置应用控制策略

透明部署向导

区域 → 接口 → 场景化 → 定义网络对象 → 应用控制策略 → 汇总

策略列表	增加
> 1#test	X

编辑应用控制策略

名称： test

区域

源区域： 信任区

目的区域： 非信任区

服务/应用

服务 (radio) 预定义服务/any

应用 (radio) 全部/全部

动作： 允许 (radio) 拒绝 (radio)

日志： 记录 (checkbox)

保存

«上一步 下一步»

点击**下一步**，将会打开『汇总』，这里展示配置的汇总信息

透明部署向导

区域 → 接口 → 场景化 → 定义网络对象 → 应用控制策略 → 汇总

部署模式：透明部署 场景化配置：上网管控场景

管理区

接口： eth0

信任区

接口： eth1

非信任区

接口： eth2

已配置的防护策略

✓ 入侵防御系统

✓ 僵尸网络

✓ 内容安全 (Web、文件、邮件)

应用控制策略

test

订阅安全报表

多个邮箱请用“;”隔开，最多支持5个邮箱

系统将定期推送综合网络安全分析报告到以上邮箱！

«上一步 提交»

点击**提交**，保存配置信息，完成向导



确认后，仅生效向导中配置的策略，原有策略将会被清空

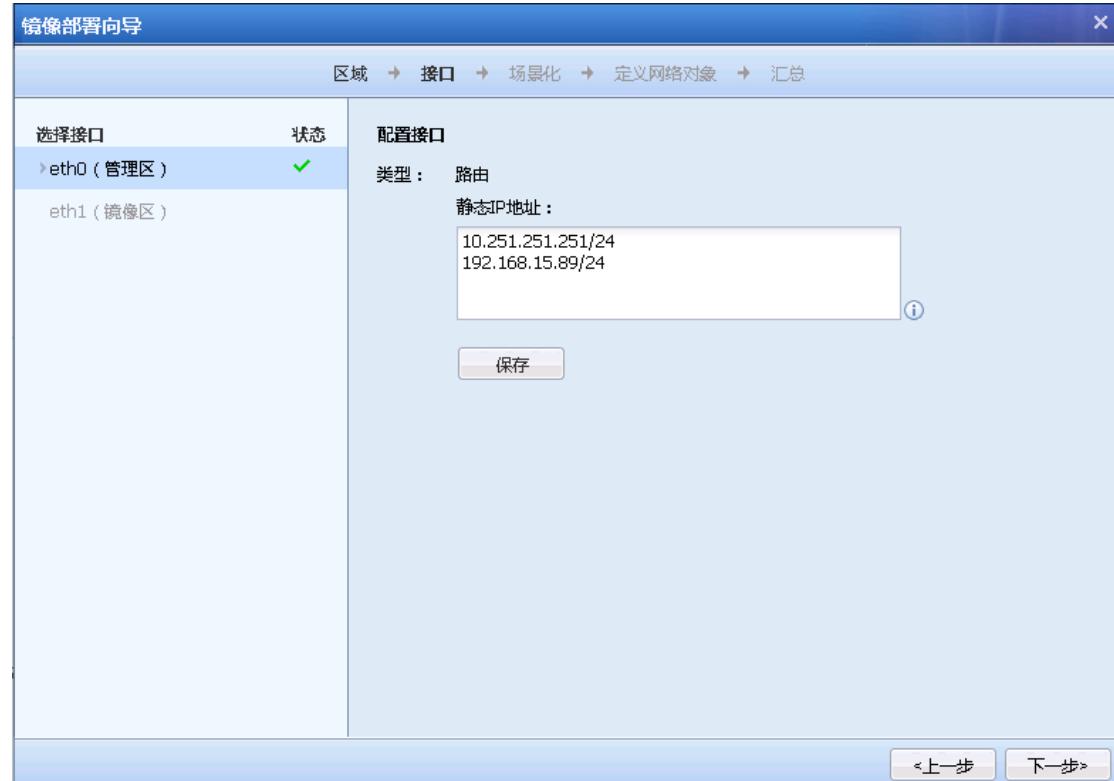
### 3.5.6.3. 数据镜像（旁路模式）

AF 设备以旁路模式部署，在旁路模式下实现漏洞攻击防护、WAF 和数据防泄密功能。



选择镜像区配置接口信息

点击**下一步**，页面将会打开『接口』的配置页面，配置镜像接口。



点击**下一步**，将会打开『场景化』，可以根据场景来选择防护策略



点击**下一步**，将会打开『定义网络对象』，可以自定义网络对象

**镜像部署向导**

区域 → 接口 → 场景化 → 定义网络对象 → 汇总

说明：安全防护策略针对网络对象做防护，配置的网络对象会按照场景化配置里选择的防护场景开启对应的防护策略，后续可在对象定义->网络对象中进行编辑。

<b>列表</b> <span style="color: green;">+ 增加</span> > 1#服务器   <span style="color: red;">X</span> 2#11 自定义网络对象	<b>编辑网络对象</b> 名称： <input type="text" value="服务器"/> 所属区域： <input type="text"/> 描述： <input type="text"/> IP地址： <input type="text" value="2.2.2.2"/> <span style="color: blue;">(i)</span> <input type="button" value="保存"/>
---	---

<上一步 下一步>

点击**下一步**，将会打开『汇总』，这里展示配置的汇总信息

**镜像部署向导**

区域 → 接口 → 场景化 → 定义网络对象 → 汇总

<b>部署模式：镜像部署</b> <b>场景化配置：全场景保护（上网+业务）</b> 管理区 接口： <input type="text" value="eth0"/>  镜像区 接口： <input type="text" value="eth1"/>	<b>已配置的防护策略</b> ✓ 入侵防御系统 ✓ 僵尸网络 ✓ WEB应用防护 ✓ 内容安全（Web、文件、邮件） ✓ 实时漏洞分析
--	---

**订阅安全报表**  
  
 系统将定期推送综合网络安全分析报告到以上邮箱！

<上一步 提交

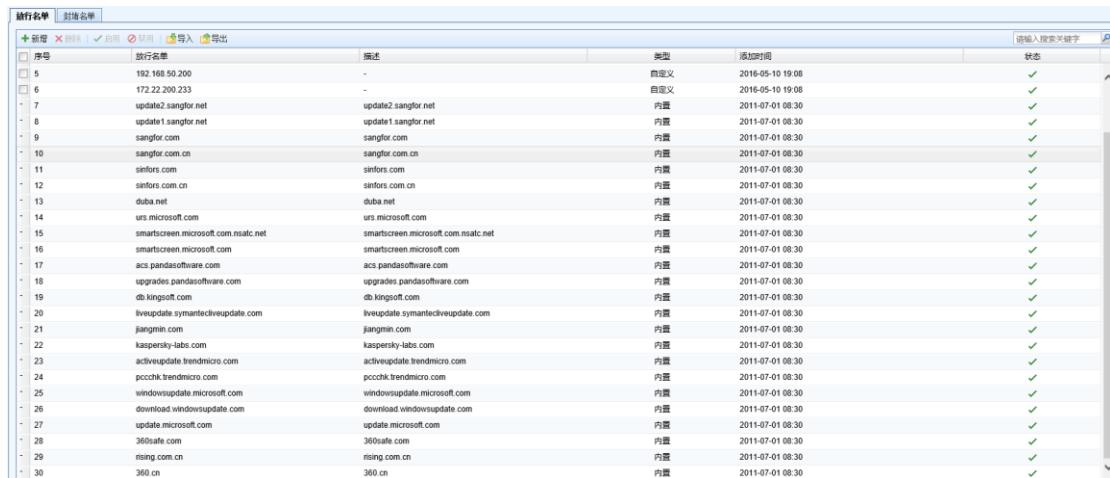
点击**提交**，保存配置信息，完成向导



确认后，仅生效向导中配置的策略，原有策略将会被清空

### 3.5.7. 黑白名单

『放行名单』用于设置当内网用户 IP 或访问的目标服务器的 IP 属于『放行名单』列表中的 IP 时，内网用户上网或访问目标服务器，不受任何监控和控制，直接放行，支持排除域名。



序号	放行名单	描述	类型	添加时间	状态
5	192.168.50.200	-	自定义	2016-05-10 19:08	✓
6	172.22.200.233	-	自定义	2016-05-10 19:08	✓
7	update2.sangfor.net	update2.sangfor.net	内置	2011-07-01 08:30	✓
8	update1.sangfor.net	update1.sangfor.net	内置	2011-07-01 08:30	✓
9	sangfor.com	sangfor.com	内置	2011-07-01 08:30	✓
10	sangfor.com.cn	sangfor.com.cn	内置	2011-07-01 08:30	✓
11	sefors.com	sefors.com	内置	2011-07-01 08:30	✓
12	sfors.com.cn	sfors.com.cn	内置	2011-07-01 08:30	✓
13	duba.net	duba.net	内置	2011-07-01 08:30	✓
14	urs.microsoft.com	urs.microsoft.com	内置	2011-07-01 08:30	✓
15	smartscreen.microsoft.com.msatc.net	smartscreen.microsoft.com.msatc.net	内置	2011-07-01 08:30	✓
16	smartscreen.microsoft.com	smartscreen.microsoft.com	内置	2011-07-01 08:30	✓
17	acs.pandasoftware.com	acs.pandasoftware.com	内置	2011-07-01 08:30	✓
18	upgrades.pandasoftware.com	upgrades.pandasoftware.com	内置	2011-07-01 08:30	✓
19	db.kingssoft.com	db.kingssoft.com	内置	2011-07-01 08:30	✓
20	liveupdate.symantecliveupdate.com	liveupdate.symantecliveupdate.com	内置	2011-07-01 08:30	✓
21	jiangmin.com	jiangmin.com	内置	2011-07-01 08:30	✓
22	kaspersky-labs.com	kaspersky-labs.com	内置	2011-07-01 08:30	✓
23	activeupdate.trendmicro.com	activeupdate.trendmicro.com	内置	2011-07-01 08:30	✓
24	pccchik.trendmicro.com	pccchik.trendmicro.com	内置	2011-07-01 08:30	✓
25	windowsupdate.microsoft.com	windowsupdate.microsoft.com	内置	2011-07-01 08:30	✓
26	download.windowsupdate.com	download.windowsupdate.com	内置	2011-07-01 08:30	✓
27	update.microsoft.com	update.microsoft.com	内置	2011-07-01 08:30	✓
28	360safe.com	360safe.com	内置	2011-07-01 08:30	✓
29	rising.com.cn	rising.com.cn	内置	2011-07-01 08:30	✓
30	360.cn	360.cn	内置	2011-07-01 08:30	✓

默认设备内置的一些地址，包括各种杀毒软件和防火墙的更新升级连接的服务器，避免更新升级时因为和用户策略冲突导致无法更新的问题。内置排除地址可以禁用但不能删除。

点击**新增**，弹出**添加放行白名单页面**，填上便于理解的描述文字，然后在下面的方框里填上需要放行的地址，点击**提交**生效。



『封堵名单』用于封堵一些需要禁止访问外网的内网 IP 或一些攻击服务器的公网 IP。『放行名单』和『封堵名单』都支持导入、导出。



### 3.5.8. 页面定制

『页面定制』用于对设备重定向到终端的页面进行自定义，可以定义的页面包括：认证结果页面、禁止访问页面、发现病毒页面、修改密码页面、公告文件、Web 认证页面、用户冻结提示页面。

定制页面列表

认证结果

> 禁止访问  
> 发现病毒  
> 修改密码  
> 公告文件  
> Web认证  
> 用户冻结提示  
> 提示安装根证书

启用该提示页面 用户web认证成功后,将显示该页面

页面编辑 : ①

预览 恢复上次 恢复默认

```
<html>
<head>
<meta http-equiv="expires" content="0">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="robots" content="noindex"> <!---限制索引首页面-->
<meta name="robots" content="nofollow"> <!---限制索引首页面-->
<meta name="robots" content="noarchive"> <!---限制建立网页快照-->
<title></title>
<link href="/images/style.css" rel="stylesheet" type="text/css">
<style type="text/css">
<!--
.style1 { color: #FFFFFF; }
-->
</style>
<script src="/scripts/authresult.js"></script>
</head>

<body bgcolor="#C1E0FD" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0" onload="onl
<br>
<br>
<table width="505" border="0" align="center" cellpadding="0" cellspacing="0">
<tr>
<td width="64" height="54" rowspan="2" align="center" background="/images/top-bj.jpg" class="new
<td width="372" rowspan="2" align="center" background="/images/top-bj.jpg" class="newtitle" id="tit
<td width="63" rowspan="2" align="right" valign="bottom" background="/images/top-bj.jpg"></td>
<td width="5" height="4" class="line"></td>
</tr>
<tr>
<
```

上传图片及Javascript文件 : ①

+ 新增一个文件

保存

『启用该提示页面』：建议启用，如果禁用，此页面将无法显示。注意：认证结果和 WEB 认证页面无法禁用。

『页面编辑』：通过更改网页源代码来改变显示的页面，建议只改变文字和图片部分，其它的修改可能会导致页面上一些正常的链接丢失。

点击 **预览** 可以预览当前客户自定义的页面，点击 **保存** 可以保存客户当前自定义的页面，点击 **恢复默认** 可以恢复到设备初始的页面，点击 **恢复上次** 页面可以恢复到客户最近一次自定义的页面。

## 3.6. 系统

### 3.6.1. 系统配置

#### 3.6.1.1. 通用配置

『通用配置』设置包括系统时间、网络参数、本机访问控制、控制台配置、邮件服务器、序列号和隐私设置。

### 3.6.1.1.1 系统时间

『系统时间』用于设定 SANGFOR 设备的系统时间。可以直接在页面上修改时间，也可以选择与[时间服务器]进行同步。



『日期和时间设置』用于查看系统的当前时间，也可以在此处手动设置系统时间。点击获取本地时间，则设备的系统时间会和登录控制面板的计算机时间一致，点击获取系统时间，可实时刷新设备系统本身的时间。

设备的系统时间也可以设置成和时间服务器同步，在『时区设置』中选择设备所在的时区，在『与 Internet 时间服务器同步』中设置公网的时间服务器地址，则设备会自动与此时间服务器的时间进行同步。

### 3.6.1.1.2 网络参数

网络参数用于配置全局网络相关参数，页面如下：



[TCP 连接超时]、[UDP 连接超时]、[ICMP 超时]用于指定 TCP、UDP、ICMP 连接超时时间，当指定时间内该连接没有新的数据包产生时，则认为连接超时而断开连接。

[SSH 端口]、[FTP 端口]、[RTSP 端口]、[SIP 端口]、[SQLNET 端口]、[TFTP 端口]、[PPTP 端口]、[H.323 端口]等用于设置协议端口，如果网络中有这些协议需要设备作应用层代理，并且端口不是默认端口时需更改端口信息。

[免费 ARP]用于是否开启免费 ARP 广播和设置设备定期发送免费 ARP 广播

的时间间隔，此项建议开启。现在改为 30s，是为了减少免费 ARP 过多的问题。

[管理口访问控制]勾选后，对访问设备超级管理 IP：10.251.251.251 的源 IP 进行限制，只允许配置源 IP 为：10.251.251.250 的地址才允许访问。

[TCP reset]用于设置当设备策略拒绝数据连接之后，是否发送 reset 报文断开连接。

[异常包检测]开启此功能将会丢弃不符合正常状态的 TCP 报文，对非对称路由等不关注 TCP 状态的部署请勿开启此功能，以防丢弃正常的 TCP 报文。

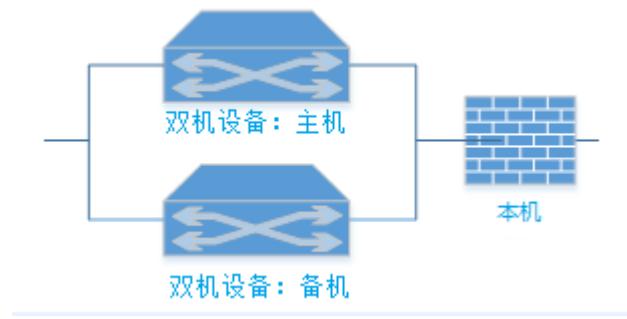
[旁路 RST]设定在旁路模式下是否允许设备发送 TCP RST 报文

[BASE64 解码]设定 web 应用防护是否对 base64 数据进行安全检查

[深度 16 进制解码]设定 WEB 应用防护是否对经过 2 次以上 16 进制编码的数据包进行解码

[上网场景高性能模式]仅限于上网场景用户使用，当遇到性能瓶颈的情况下选择开启，能够提升系统吞吐处理能力。

[与其他双机对接]当本机直接与其他双机对接在同一网络上时，需要开启该选项以确保网络正常。场景拓扑图如下：



[网关为追踪路由可见]Windows 系统已默认支持。此项只针对 Linux 系统，开启后，网关在 Linux 下的追踪路由可见。出于网关安全考虑，默认关闭此项。

[网卡支持软件负载分发] 流量中存在大量相同的五元组数据（源 IP 地址，源端口，目的 IP 地址，目的端口和传输层协议相同）可以进行软件负载分发，提升设备整机性能

[开启外网防 DOS 功能]勾选启用『策略』→『安全策略』→『DoS/DDoS 防护』→『外网对内攻击防护策略』具体配置见 3.5.2.2.1 章节。

[高级配置] 勾选后，将改变防火墙现在的配置流程，使配置变得复杂，若需开启请联系深信服人员进行操作。

### 3.6.1.1.3 本机访问控制

『本机访问控制』主要是设置针对访问本机的数据，进行访问控制。功能默认带有两条策略，优先级低的为拦截所有的访问行为，优先级高的为允许访问设备开启的部分服务端口，页面如下：



优先级	名称	源区域	源网络对象	源端口	目的网络对象	服务	更新时间	动作	状态	操作	
- 1	默认放通策略	全部	全部	全部	全部	预定义服务/本地服务,预定义...	-	允许	√		
- 2	默认拦截策略	全部	全部	全部	全部	全部/ALL	-	拒绝	√		

点击新增按钮，弹出本机访问控制配置界面，如下图：



[名称]设置新增策略名称。

[优先级]: 新增策略在哪个优先级位置。

**源:**

[网络对象]: 用于设置访问的源 IP，配置相应的网络对象。

[区域]: 用于设置访问的源区域，配置相应的区域。

[端口]: 用于设置访问的源端口，一般保持默认的“全部”即可。

**目的:**

[网络对象]: 用于设置访问的目标 IP，配置相应的网络对象。

**服务:**

[服务]: 设置需要访问本机的某个服务。

[动作]: 对匹配到上述条件的数据，进行允许或者拦截的操作。

[日志选项]: 对匹配到上述条件的数据进行相应允许或者拦截操作后，是否需要记录日志。

[备注]: 填写相应的备注信息。

最后点击**确定**保存配置生效。

#### 3.6.1.1.4 控制台配置

『控制面板配置』包括 WEBUI 选项和认证参数设置。

WEBUI 选项下可以设定[设备名称]、[WEBUI 端口]、[控制超时]，配置页面如下所示：



[语言设置]支持中英文互切，但中英文切换回丢掉配置例如：原中文切英文：丢配置。原英文切中文：丢配置。原中文切英文再切中文：会恢复成原中文配置。

[设备名称]: 可以设置设备的显示名称。

[WEB UI 端口]: 用于设置登陆控制台的端口，默认是 TCP 443 端口，在启用 SSL VPN 序列号后登陆控制台端口默认为 4430。

[控制超时]: 设置的是控制台超时时间，如果管理员在设定时间内控制面板无操作，系统会自动断开连接。

[最大并发管理数]: 设置最大允许多少个人同时登录设备控制台。

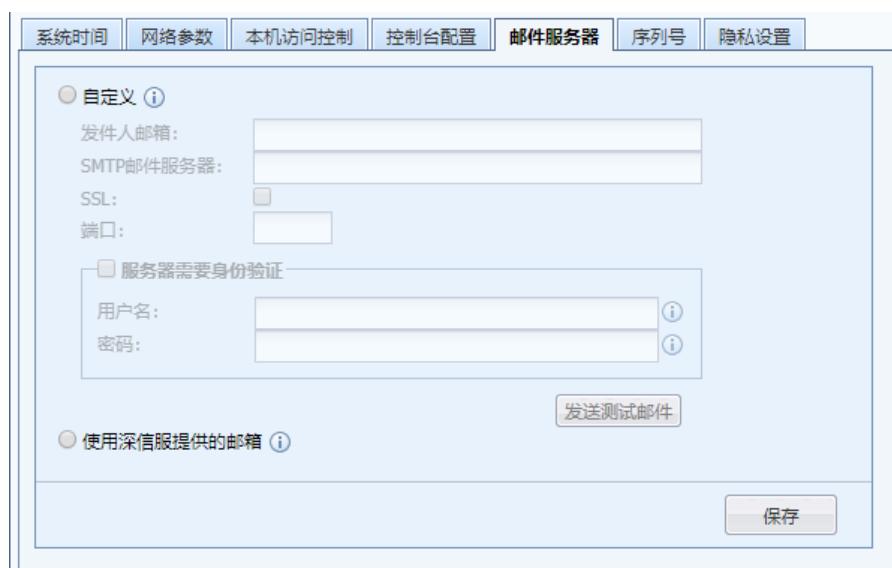
[单用户限制]: 设置允许从多少个不同的地址使用同一管理员账号登录设备控制台。

[登录失败重试]: 设置同一管理员账号允许的登录失败次数。

点击提交保存配置生效。

### 3.6.1.1.5 邮件服务器

『邮件服务器』用于设置设备发送告警邮件的时候使用的 SMTP 服务器信息。界面如下：



The screenshot shows the 'Email Server' configuration page. At the top, there is a navigation bar with tabs: 系统时间, 网络参数, 本机访问控制, 控制台配置, 邮件服务器 (highlighted in blue), 序列号, and 隐私设置. The main form has two sections:

- 自定义 (Custom):** Contains fields for 发件人邮箱 (From Email), SMTP邮件服务器 (SMTP Server), SSL (SSL), and 端口 (Port).
- 服务器需要身份验证 (Server needs authentication):** Contains fields for 用户名 (Username) and 密码 (Password).

At the bottom of the form are two radio buttons:

- 使用深信服提供的邮箱 (Use Sangfor's provided email)
- 自定义 (Custom)

Below the radio buttons are two buttons: **发送测试邮件** (Send Test Email) and **保存** (Save).

[发件人邮箱]: 填写设备发送告警邮件的时候使用的邮箱，例如[test@domain.com](mailto:test@domain.com)。

[SMTP 邮件服务器]: 填写发件箱对应的 SMTP 邮件服务器的域名或者 IP 地址。如 SMTP 邮件服务器需要验证用户名和密码则勾选“需要验证服务器用户名和密码”。

[SSL]: 勾选则采用 SSL 协议进行传输。

[端口]: 定义 SMTP 服务器端口。

填写了地址后点击[发送测试邮件](#)可以检测是否可以发送成功。

[使用深信服提供的邮箱]: 使用深信服科技提供的发件人邮箱和 SMTP 邮件服务器，邮件默认使用 SSL 加密，端口为 465（SMTPS）。



**3.7.3 章节的网站篡改防护设置了篡改后邮件通知管理员，会使用此处设置的 SMTP 服务器信息发送邮件。**

**3.6.1.3.章节设置的邮件告警，会使用此处设置的 SMTP 服务器信息发送邮件。**

### 3.6.1.1.6 序列号

序号包括：网关序列号、跨运营商序列号、功能模块序列号、升级序列号和服务有效期，页面如下：



The screenshot shows the '通用配置' (General Configuration) page with several tabs at the top: 系统时间 (System Time), 网络参数 (Network Parameters), 本机访问控制 (Local Access Control), 控制台配置 (Console Configuration), 邮件服务器 (Mail Server), 序列号 (Serial Number), and 隐私设置 (Privacy Settings). The '序列号' tab is selected.

**网关序列号**:  
用作网关设备，可以连接外网线路与分支。  
**网关序号:** 1710CB63  
**当前序列号:** QA94FW4XFCDCCGEY  
**状态:** 有效  
1. 分支机构: 5  
2. 线路数: 2  
3. 移动用户数: 10  
[修改序列号](#)

**跨运营商序列号**:  
提升不同运营商之间的访问体验性。  
**当前序列号:** -  
**状态:** 未激活  
[修改序列号](#)

**功能模块序列号**:  
根据业务需求开启对应的功能模块。  
1. SSL VPN: 10个用户数  
2. SAVE安全智能文件检测  
3. SSL解密  
4. 增强功能  
[修改序列号](#)

**升级序列号**:  
保持设备处于最新状态。  
1.URL/应用识别库:有效日期: 2019-08-08  
2.软件升级:有效日期: 2019-08-15  
3.安全规则库:有效日期: 2019-08-08  
4.SAVE安全智能文件检测模型库:有效日期: 2019-08-08  
[修改序列号](#)

**云端增值服务序列号**:  
根据业务需求开启对应的增值服务。  
云端增值服务序列号未激活，为了保证更好的使用本产品，请及时购买序列号。  
[修改序列号](#)

**服务有效期**:  
硬件质保: ---  
电话咨询和网络远程支持: ---  
**连接服务器失败，请确保网络畅通!**

[网关序列号]中的【当前序列号】用于启动设备，并授权设备的线路数、分支数和移动用户数。

[跨运营商序列号]用于启动设备的跨运营商功能。

[功能模块序号]用于启动设备各功能模块，需要序号授权启动的功能模块包括 SSL VPN、SAVE 安全智能文件检测、SSL 解密、增强功能。其中增强功能包括：Web 防篡改、WEB 应用防护、数据泄密防护、实时漏洞分析。

[升级序列号]用于启动设备各规则库的升级更新，包括 URL/应用识别库、软件升级、安全规则库、SAVE 安全智能文件检测模型库。其中安全规则库包括：漏洞攻击防护特征库、WEB 应用防护库、实时漏洞分析识别库、数据泄密防护库和热门威胁库。

[云端增值服务序列号]用于启动设备云脑功能的序列号，包括“未知威胁防御”和“高级威胁对抗”两部分。

点击各条目的修改序列号，填入序号，即可启动相应功能的授权。

[服务有效期]显示设备的硬件质保、电话咨询和网络远程支持的有效期。

### 3.6.1.1.7 隐私设置

隐私设置主要用于是否允许上报产品的用户体验改进内容。以进行产品的持续改进，给用户带来体验的提升。



[参与用户体验改进计划]勾选后，允许产品上报相应的体验改进内容。

点击确定，完成功能生效。

### 3.6.1.2. 日志设置

日志设置用于设置设备日志的相关选项，包括日志功能开启、Syslog 设置、内置数据中心设置、外置数据中心设置以及同步到安全感知平台。界面如下：

日志设置

日志功能开启

安全日志	应用控制日志	流量审计日志	NAT日志	用户认证日志	SSL VPN 用户日志	本机访问控制	高可用异常日志
<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭
日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置
Syslog <input checked="" type="checkbox"/> 内置数据中心 (推荐) 外置数据中心 安全策略和系统	Syslog <input checked="" type="checkbox"/> 内置数据中心 外置数据中心 (推荐) 安全策略和系统	Syslog <input checked="" type="checkbox"/> 内置数据中心 外置数据中心 (推荐)	Syslog <input checked="" type="checkbox"/> 内置数据中心	Syslog (推荐) <input checked="" type="checkbox"/> 内置数据中心	Syslog (推荐) <input checked="" type="checkbox"/> 内置数据中心	Syslog <input checked="" type="checkbox"/> 内置数据中心	Syslog <input checked="" type="checkbox"/> 内置数据中心

Syslog设置

地址: 192.200.244.88  
端口: 514

内置数据中心设置

自动清除日志设置:  
 自动删除 30 天数据的日志  
 最长保存天数: 70  
 磁盘占用空间超过此比例则自动删除最早一天的日志, 设置  
 最大占用磁盘比例: 80  
 启用日志归并

外置数据中心设置

安全策略和系统设置

服务器地址: 200.200.5.228  
测试  
通讯端口: 4430  
用户名: sangfor  
密码: \*\*\*\*\*

如何选择?

应用

### 3.6.1.2.1 日志功能开启

『日志功能开启』：安全日志、应用控制日志、流量审计日志、NAT 日志、用户认证日志、SSL 用户日志、本机访问控制日志和高可用异常日志这八种日志。个别默认是关闭的，如果需要开启，请在【日志设置】→【日志功能开启】页面勾选相应的选项开启。页面如下：

日志功能开启

安全日志	应用控制日志	流量审计日志	NAT日志	用户认证日志	SSL VPN 用户日志	本机访问控制	高可用异常日志
<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭	<input checked="" type="checkbox"/> 开启 <input type="checkbox"/> 关闭
日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置	日志存储位置
Syslog <input checked="" type="checkbox"/> 内置数据中心 (推荐) 外置数据中心 安全策略和系统	Syslog <input checked="" type="checkbox"/> 内置数据中心 外置数据中心 (推荐) 安全策略和系统	Syslog <input checked="" type="checkbox"/> 内置数据中心 外置数据中心 (推荐)	Syslog <input checked="" type="checkbox"/> 内置数据中心	Syslog (推荐) <input checked="" type="checkbox"/> 内置数据中心	Syslog (推荐) <input checked="" type="checkbox"/> 内置数据中心	Syslog <input checked="" type="checkbox"/> 内置数据中心	Syslog <input checked="" type="checkbox"/> 内置数据中心

### 3.6.1.2.2 Syslog 设置

Syslog 设置用于将设备日志同步存储到远程的 Syslog 服务器，需要设置 Syslog 服务器的 IP 和端口信息，页面如下：

**Syslog设置** 

地址 :

10.10.10.10

端口 :

514

**1.SYSLOG 仅支持 UDP 方式连接。****2.SYSLOG 不能同步系统日志，只能同步数据中心日志。****3.6.1.2.3 内置数据中心设置**

『内置数据中心』：用于设置设备内置数据中心存储日志的自动删除选项，页面如下：

**内置数据中心设置**

自动删除日志设置：

 自动删除此天数前的日志 

最长保存天数：

60

 磁盘占用空间超过此比例则自动删除最早一天的日志

最大占用磁盘比例：

80

 启用日志归并 

勾选[启用内置数据中心]，用于启用设备的内置数据中心。

[自动删除日志设置]用于设置是否需要系统自动删除已记录的访问控制日志，选择[自动删除此天数前的日志]用于设置按天数来保存日志，选择[磁盘占用空间超过此比例则自动删除最早一天的日志]用于设置按磁盘占用率来保存日志。

[启用日志归并]：勾选上此选项后，对于访问同一域名的行为，在内置数据中心里只会记录一次，用于节省设备的磁盘空间。



不勾选“启用内置数据中心”，则内置数据中心不会记录日志，但配置了

Syslog 服务器，会将日志发送到 Syslog 服务器上。

### 3.6.1.2.4 外置数据中心设置

『外置数据中心』：用于设置设备与外置数据中心服务器同步的相关信息，页面如下：



外置数据中心设置

服务器地址：	<input type="text"/>	<input type="button" value="测试"/>
通讯端口：	810	
WEB访问端口：	80	<input type="button" value="立即访问"/>
同步帐号：	<input type="text"/>	
密码：	<input type="password"/>	

[服务器地址]是指安装了外置数据中心程序的服务器。

[WEB 访问端口]填写外置数据中心程序安装过程中填写的外置数据中心访问端口。

[同步账号/密码]填写外置数据中心配置端上设置好的同步账号密码。

### 3.6.1.2.5 安全感知系统设置

『安全感知系统设置』：用于设置设备与安全感知系统同步的相关信息，页面如下：



安全感知系统设置

服务器地址：	<input type="text" value="200.200.5.228"/>	<input type="button" value="测试"/>
通讯端口：	4430	
同步帐号：	sangfor	
密码：	<input type="password" value="*****"/>	

[服务器地址]是指安全感知系统的地址。

[通讯端口]默认 4430 端口。

[用户账号]接入安全感知系统的账号信息。

[通讯端口]接入安全感知系统的密码信息。

### 3.6.1.3. 告警设置

『告警设置』设置包括邮件告警和短信告警。

#### 3.6.1.3.1 邮件告警

『邮件告警』用于设置将告警信息以邮件的形式发送到管理员邮箱。例如当内网有病毒，或磁盘空间存储到一定比例的时候，设备会自动发送告警邮件到管理员邮箱，达到提醒告警的目的。页面设置如下：

告警设置

邮件告警 短信告警

启用邮件告警 邮件服务器设置

配置邮件告警

》 告警事件设置

》 告警邮件设置

告警事件设置

告警事件

告警值： 60 %

流量超限告警 ①

eth0 上行 80 Mbps 下行 80 Mbps

安全

邮件安全

高  中  低

漏洞攻击防护

致命  高  中  低  信息

WEB应用防护

高  中  低

僵尸主机

确认感染  高可能感染  中可能感染  低可能感染

Dos/DDoS防护

对外DoS攻击

内置数据中心日志

磁盘空间使用率

告警值： 80 %

日志读写繁忙程度

告警值： 80 %

日志数量

应用控制日志： 12000000 条/天

流量审计日志： 1500000 条/天

序列号过期告警

日志合规提醒 ①

点击 邮件服务器设置，跳转到邮件服务器设置，详见 3.6.1 章节中邮件服务器设置。

[告警事件设置]：用于指定哪些情况下需要进行邮件告警。可以同时选择多个告警事件，那么其中任何一个满足条件，都会发送告警。



邮件告警 短信告警

启用邮件告警 [邮件服务器设置](#)

配置邮件告警

› 告警事件设置

› **告警邮件设置**

告警邮件设置

邮件标题 : 有告警邮件

最短发送间隔 : 20

收件箱 : support@sangfor.com

提交

[告警邮件设置]: 用于设置邮件标题以及最短发送间隔等信息。

### 3.6.1.3.2 短信告警

『短信告警』用于设置将告警信息以短信的形式发送到管理员手机上。短信告警只对数据防泄密模块有效，当 AF 设备检测到有敏感信息泄露时，会自动发送告警信息到手机上。页面设置如下：



邮件告警 短信告警

短信猫状态 : 未检测到短信猫

发送到手机 :

发送测试短信

保存

[短信猫状态]: 用于显示检测到的短信猫状态。

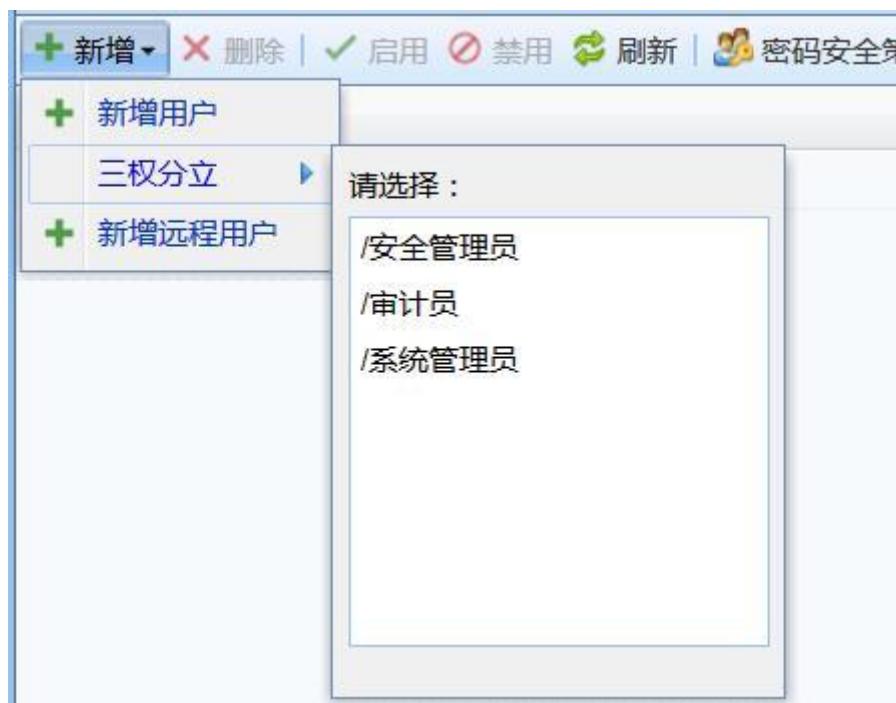
[发送到手机]: 用于设置将告警信息发送到哪些手机号码上，最多支持 5 个手机号码。

点击 **发送测试短信**，发送测试短信，测试短信猫是否能把短信正常的发送到手机上。

### 3.6.2. 管理员账号

『管理员账户』用来设置能够通过控制台管理设备的登录用户。【管理员账号】编辑页面如图所示：

点击**新增**添加管理员帐户，如下图所示：



『三权分立』包括三种管理员可以选择，分别是：安全管理员、审计员、系统管理员。

系统管理员：具有基础网络配置，用户管理等其他非安全策略的管理权限。

安全管理员：具有查看和修改安全策略的权限，日志查看权限。

审计员：只具有查看和修改内置数据中心的权限。

这三种管理员是系统内置的三种分类，可以根据这三种分类创建管理员，如果这种分类不能满足需求，也可以自定义用户权限，点击**新增用户**，用于新增自定义权限的管理员：



[用户名]: 设置管理员账户名称。

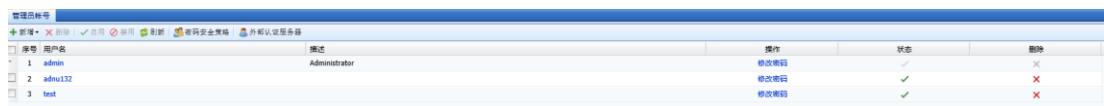
[描述]: 设置对该账户的描述。

[新密码]、[确认新密码]: 设置管理员账户密码。

[页面权限设置]: 用于设置对控制台和数据中心各个模块是否有可查看或可

编辑权限。

点击**提交**，完成管理员的添加：



[新增远程用户]可以在外部认证服务器中选择用户作为管理员账号



如需要编辑已经建立的管理员，可以点击用户名进入编辑页面。点击**删除**用于删除已有的管理员账户，点击**启用**用于将管理员账户状态设置为启用，点击**禁用**用于将管理员账户状态设置为禁用。

点击**密码安全策略**，用于设置控制台管理员密码的安全策略，注意：只有admin管理员可以设置此功能：

### 密码安全策略

安全密码格式必须为：

1、密码不包含用户名  
2、密码长度大于等于8位  
3、必须同时包含字母、数字和特殊字符中两者

下次登录必须修改密码  
 密码最长使用天数：

点击外部认证服务器，弹出如下界面：

### 外部认证服务器

启用

服务器名称：

认证方式  
 TACACS  RADIUS

认证服务器配置

服务器地址：

认证端口：

共享密钥：

采用协议：

登陆优先设置  
 认证服务器优先  本地优先

在这里可以添加 TACACS 和 RADIUS 服务器

### 3.6.3. 系统维护

#### 3.6.3.1. 备份与恢复

『备份与恢复』用于将设备的配置下载到本地保存，或者是将原有的备份的配置文件恢复到设备中。



『备份配置』：用于备份下载设备中已有的配置，点击[点击下载配置](#)，就可以对当前的配置进行备份。

『恢复配置』：用于恢复已备份的配置文件。恢复配置文件有两种方式：

方式一：从自动备份中恢复，设备会在每日凌晨自动备份一次配置，默认保存一周的配置文件，选择要恢复的配置文件，点击[恢复](#)即可。

方式二：从本地文件中恢复，点击**浏览**，并打开备份文件，点击**恢复**即可恢复备份配置。

方式三：从默认配置中恢复，点击**一键恢复**，可以将设备恢复到出厂状态。



**AF6.8** 版本开始支持低版本的备份配置导入，中文版设备支持从 **AF6.6** 版本-**AF8.0.6** 版本的配置导入，英文版设备支持从 **AF6.4** 版本-**AF8.0.6** 版本的配置导入。具体导入时还需要注意的事项，请咨询深信服技术人员。

### 3.6.3.2. 系统更新

#### 3.6.3.2.1 库升级

『库升级』用于对设备的补丁和内置库（SAVE 安全智能文件检测模型库、URL 库、IPS 漏洞特征识别库、软件优化、应用识别库、WEB 应用防护库、数据泄密防护库、实时漏洞分析识别库、IP 地址库、威胁情报预警与处置库、热门威胁库、热点事件库）进行升级管理。界面如下：

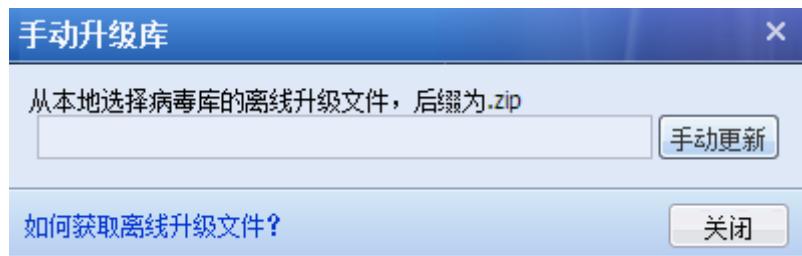


序号	相关库	当前版本	最新版本	升级服务有效期	自动升级	操作
1	SAVE安全智能文件检测模型库	2018-10-20 日志详情	2018-11-15	2019-08-08	✓	
2	URL库	2018-09-17 日志详情	2018-11-12	2019-08-08	✓	
3	IPS漏洞特征识别库	2018-09-12 日志详情	2018-11-14	2019-08-08	✓	
4	软件优化	...	2018-10-23	永不过期	✓	
5	应用识别库	2018-09-10 日志详情	2018-11-12	2019-08-08	✓	
6	WEB应用防护库	2018-09-12 日志详情	2018-11-14	2019-08-08	✓	
7	数据泄密防护库	2018-02-16 日志详情	2018-02-16	2019-08-08	✓	
8	实时漏洞分析识别库	2018-08-29 日志详情	2018-10-31	2019-08-08	✓	
9	IP地址库	2018-09-12 日志详情	2018-11-12	永不过期	✓	
10	威胁情报预警与处置库	2018-08-29 日志详情	2018-10-31	永不过期	✓	
11	热门威胁库	2018-07-27 日志详情	2018-07-27	2019-08-08	✓	
12	热点事件库	2018-07-31 日志详情	2018-07-31	2019-08-08	✓	

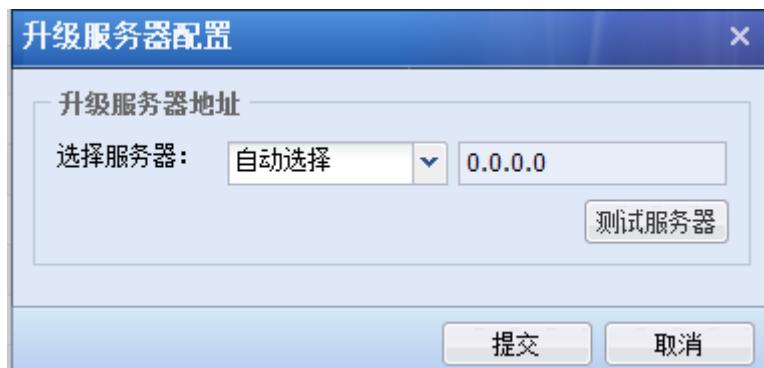
首先勾选序号前面的框 ，通过点击**启用**可开启内置库的自动升级，点击**禁用**可关闭内置库的自动升级，点击**刷新列表**用于看到内置库版本的实时信息。

通过点击 可以配置在升级服务有效期内的规则库的手动升级。界

面如下：

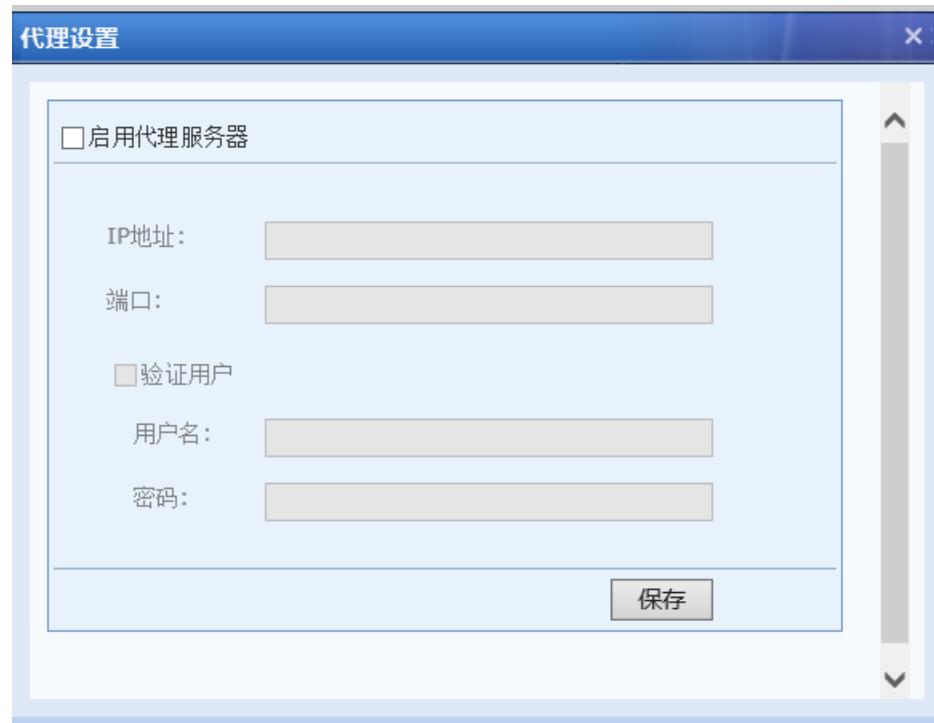


点击  升级服务器配置，进入【升级服务器配置】页面，『服务器设置』用于配置设备需要连接的升级服务器，可以根据客户外网的线路进行选择，也可以[自动选择服务器]让设备自动检测可以连接的更新服务器。



点击  代理设置，进入代理设置页面。

『代理设置』内置库升级需要设备本身可以上网，或者网络中有 HTTP 代理服务器时，可以通过设置代理服务器，使设备可以通过代理服务器上网更新内置库。勾选[启用 HTTP 代理服务器]，填写代理服务器的 IP 地址、端口，勾选[验证用户]输入代理服务器需要验证的用户名和密码。界面如下：



### 3.6.3.2.2 系统升级

『系统升级』支持从设备界面加载升级包升级系统版本。新版本发布后，判断升级条件满足，需要版本更新时，点击【升级到其他版本】，显示【上传本地升级包】，加载本地升级包升级即可。页面如下：



点击【查看升级历史】，可以查看历史的升级记录。页面如下：

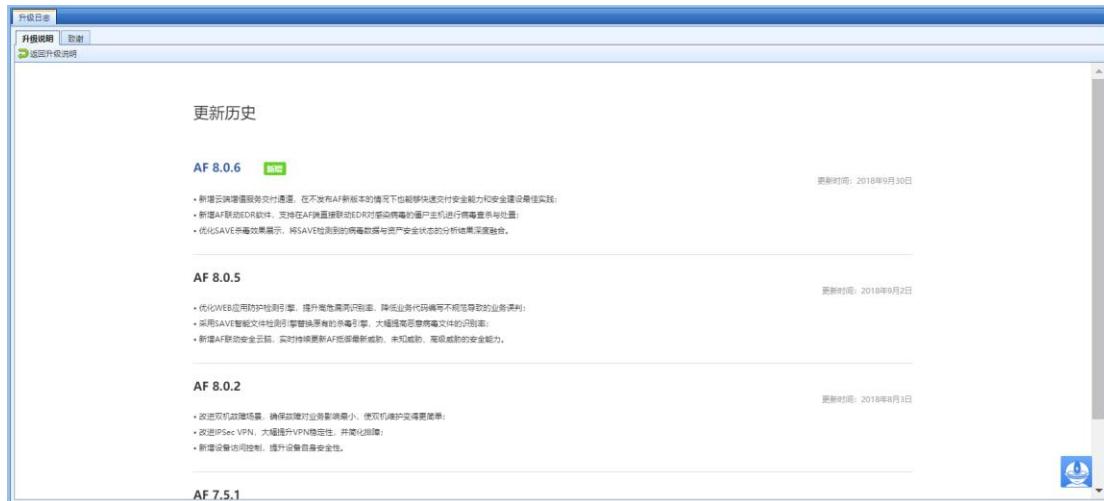


### 3.6.3.2.3 升级日志

『升级日志』展示当前版本较上一个版本，在功能上面有哪些方面的新增、优先及删减等。页面如下：



点击【查看更新历史】，可以查看历史的升级记录。页面如下：



### 3.6.3.3. 重启网关/服务

『重启网关/服务』页面提供重启设备、重启所有服务和启动 SSLVPN 服务三个功能按钮，页面如下图所示：



### 3.6.4. 排障

『排障』主要用于排查网络当中出现的故障。包括数据包拦截日志与直通、命令行控制台、抓包取证、系统故障日志和技术支持工具。

### 3.6.4.1. 数据包拦截日志与直通

『数据包拦截日志与直通』用于查询一个数据包在通过设备时是被哪个模块拒绝，是什么原因被拒绝，以便快速定位配置错误，也可用来测试一些规则是否生效。点击【开启】，点击【设置开启条件】，出现【设置开启条件】页面，可设置各种条件进行过滤，包括[IP 地址]、[排除 IP 地址]、[协议类型]和[端口]等，如下图：



[指定 IP 地址]用于设置对指定的 IP 地址开启拒绝列表，默认包括所有网段。

[排除 IP 地址]用于排除包含在[指定 IP 地址]中的指定地址不开启实时拦截日志并且不开启直通。

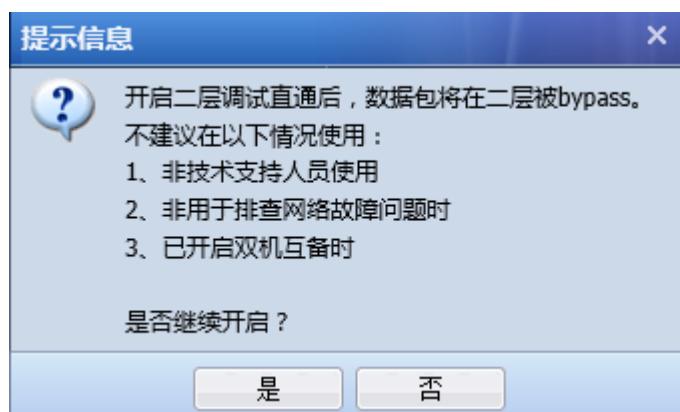
[协议类型]和[端口]设置对符合指定协议类型、端口的数据包的拒绝情况才输出到访问控制列表中。

点击**开启实时拦截日志**将打开拒绝列表，此时设备所有的策略依然生效，符合策略设置应该拒绝的数据包会被设备拒绝掉，同时会将符合策略设置应该拒绝数据包的情况显示出来，可以点击刷新实时查看数据包被拒绝的情况。

点击**开启实时拦截日志并直通**可以打开拒绝列表同时开启直通。此时设置的上网策略将不生效，符合策略设置应该拒绝的数据包会被设备放行，同时会将符合策略设置应该拒绝数据包的情况显示出来，可以点击**刷新**实时查看数据包被拒绝的情况。通过该功能可以快速排除是否因为设备的上网行为管理模块配置错误而导致网络中断等错误并快速恢复策略配置错误带来的网络故障。

**关闭实时拦截日志**用于关闭拒绝列表输出，并关闭直通。

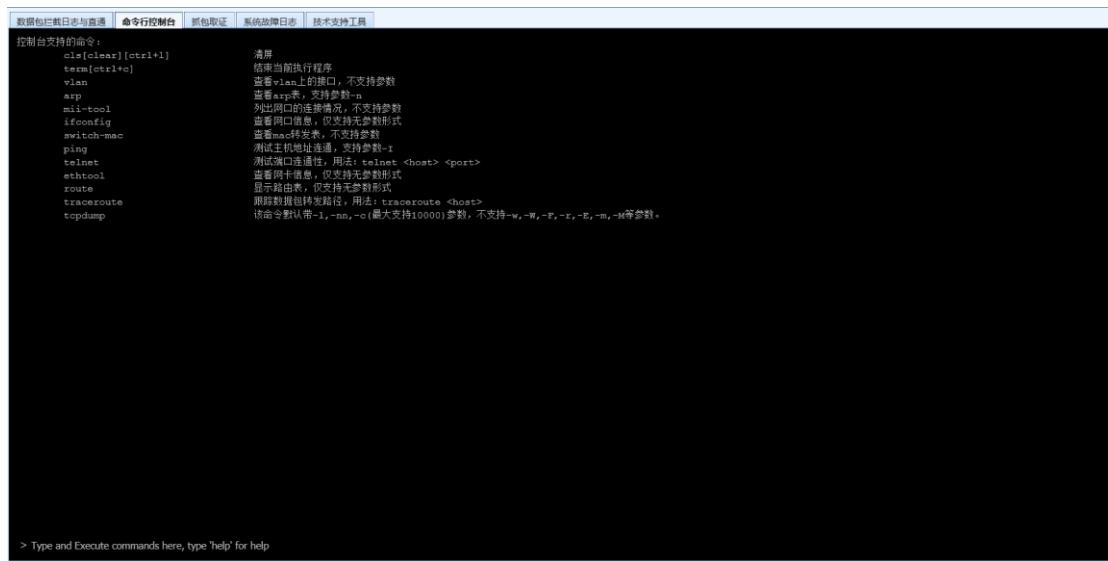
**【开启二层调试直通】**开启后数据包将在二层被 bypass，开启时需要注意以下情况：



### 3.6.4.2. 命令行控制台

『命令行控制台』提供一个简单的控制台命令行，可用于对设备的一些简单信息进行查看，支持的命令包括：cls（清屏）、term（结束当前执行程序）、vlan

(查看 vlan 上的接口)、arp (查看 arp 表)、mii-tool (列出网口的连接情况)、ifconfig (查看网口信息)、switch-mac (查看 mac 转发表)、ping (测试主机地址连通)、telnet (测试端口连通性)、ethtool (查看网卡信息)、route (显示路由表) 和 traceroute (跟踪数据包转发路径)，tcpdump (该命令默认带-l,-nn,-c 参数，抓包用) 在命令行页面直接输入命令人回车即可，如下图：



### 3.6.4.3. 抓包取证

『抓包取证』用于对经过设备的数据包进行抓取，以便快速定位问题，可以作为排错的辅助工具，点击**抓包选项**，出现【抓包选项】界面，如下图：



[抓取包数]用于设置抓取的数据包的总个数。

[高级（TCPDUMP）]：通过指定网口，可以同时选择多个网口，设备会抓取指定网口的数据包；IP 地址，设备会抓取指定 IP 的数据包；端口，设备会抓取指定端口的数据包；过滤表达式用来设置抓取数据包的条件（过滤表达式使用的是 linux 下的标准 TCPDUMP 格式）。

点击**开始抓包**即开始进行数据包的抓取。



点击**停止抓包**即停止数据包的抓取，此时可以看到生成了一个后缀名为 pcap 的文件，如下图：

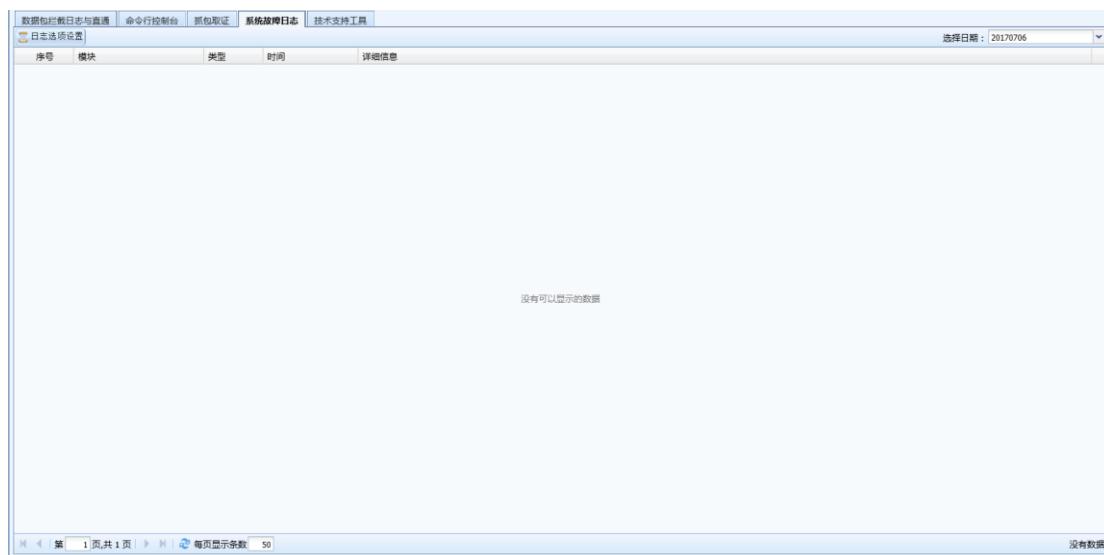


点击【删除】删除指定文件，点击【下载】可将此文件保存在指定路径下，此文件可用 Sniffer 或 Ethereal、Wireshark 等抓包软件进行查看，点击【刷新】可查看抓包结果的实时信息。

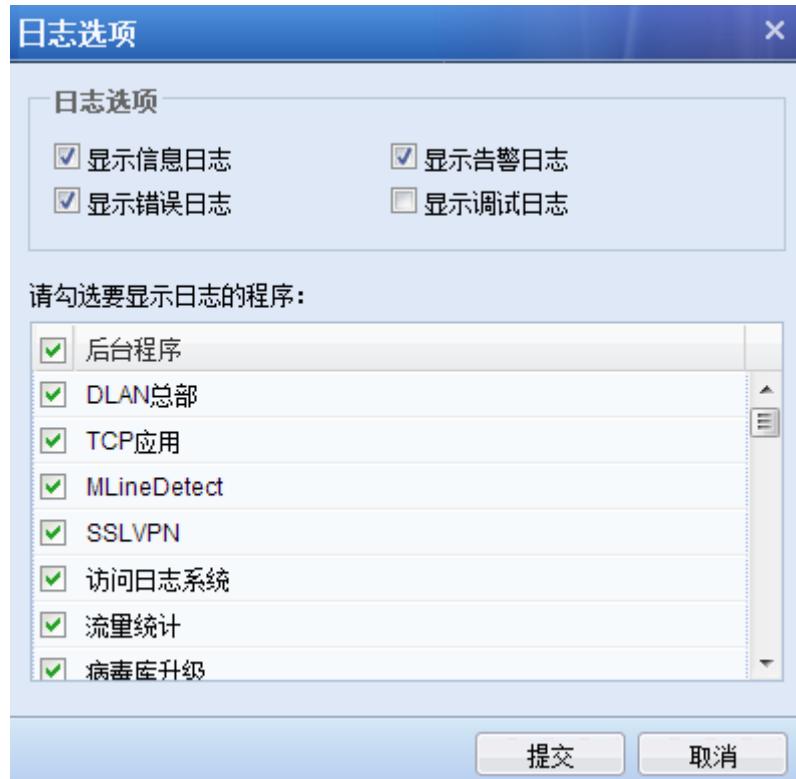


### 3.6.4.4. 系统故障日志

『系统故障日志』用于查看设备各模块运行状态日志，可通过日志判断设备各模块是否正常运行，如下图：



点击【日志选项设置】，出现【日志选项】页面，选择要查看的日志类型，如下图：



点击**提交**后，即显示所选日志信息。

在**选择日期:**  中选择日期，查询相应日期的系统日志。

### 3.6.4.5. 技术支持工具

[获取黑盒信息]该功能主要是获取黑盒信息，可以下载黑盒信息，方便技术支持人员排查问题



[重置数据库]该功能主要用来重置数据库，重置数据库将清空内置数据中心的所有数据，请谨慎操作！

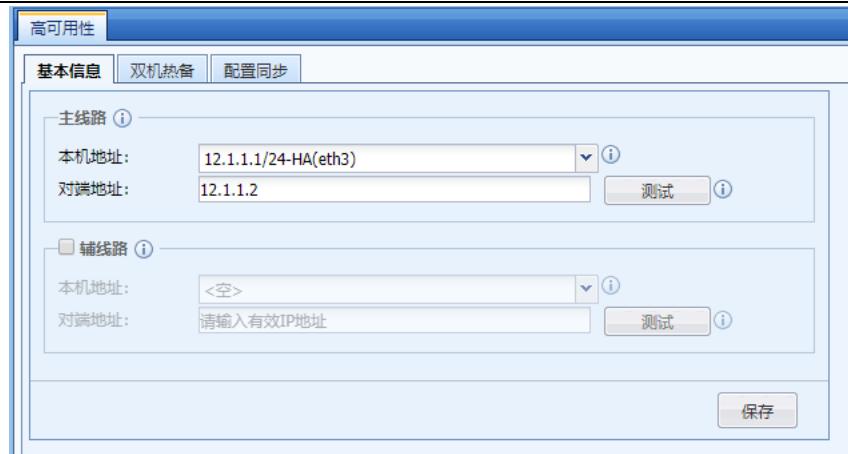


[获取远程技术支持]该功能主要是为解决在某些环境下无法通过端口映射来连接设备的情况下使用的。只要将供货商提供的编码填入，启用后，技术支持人员可以远程连接到此设备及你的内部网络。



### 3.6.5. 高可用性

高可用性主要是在防火墙双机工作，或者两台设备并行工作等场景使用。进入『系统配置』->『高可用性』配置页面，如下：

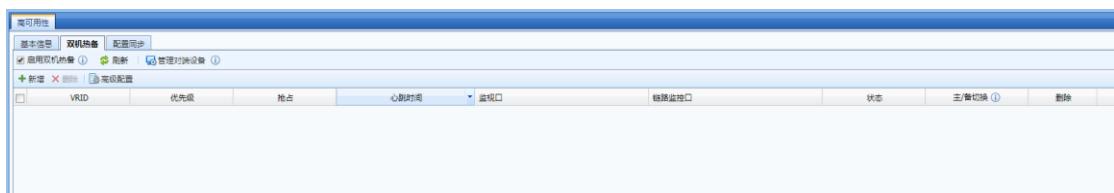


『基本信息』：用于设置本机与对端的心跳地址。本机地址只能选择配置里带有 HA 标识的接口。并且该接口只能与做高可用的其他 AF 设备接口通信，用于收发心跳包信息、交互配置信息等。

[主线路]：设置主心跳地址，负责同步双会话、配置、用户认证及心跳信息等。

[辅线路]：设置辅心跳地址，作为心跳冗余，只负责同步心跳信息。

『双机热备』：勾选启用双机热备，点击新增，界面如下：



**新增虚拟路由组**

虚拟组：	100 (1-255)
优先级：	100 (1-255)
抢占：	<input type="radio"/> 是 <input checked="" type="radio"/> 否
心跳时间：	1 (1-60)s
网口监视：	<a href="#">i</a>

**+ 新增 X 删除**

<input type="checkbox"/>	组序号	网口	编辑
没有可以显示的数据			

**接口链路监控： [i](#)**

**+ 新增 X 删除**

<input type="checkbox"/>	组序号	网口	编辑
没有可以显示的数据			

**提交 取消**

[虚拟组]：用于定义 VRRP 工作时，接口所属的组。两台设备不同的接口可以定义成同一个虚拟组。一台设备的多个接口也可以定义成一个虚拟组。两台设备的同一个虚拟组之间是互为主备的关系。

[优先级]：用于设置网口列表中选中接口的优先级。值越高，优先级越高。一定要设置抢占为是，则优先级的设置才有意义。如果两台设备是双机热备工作方式（即一台工作，另外一台完全作为备机，不工作），那么可以设置 A 设备优先级为 90 抢占，B 设备设置为优先级 80（抢占或不抢占都行）。90 优先级的设备故障，那么 80 优先级的设备工作，90 优先级的设备恢复，那么 90 优先级的设备会抢占成为主机，80 优先级的设备成为备机。

[抢占]：设置是否抢占成为主机。需要与优先级配合使用。

[心跳时间]：两台设备交互数据的时间，在这个设定的间隔时间发包通信。告知对方本端的网口状态以及链路监控状态。如果其中一台异常，则进行切换。如果两台设备都收不到心跳包，则会将自己置为主机，两台设备同时工作。

[网口监视]：设置需要监控的网口，可设置多个网口组，每个网口组中可设置多个网口。当同一组网口中所有网口断开时，才判定该组网口故障，才会进行双机切换。

[接口链路监控]：该设置依赖于接口/区域设置中定义的接口检测方式，即接口的链路故障检测功能。此处选择相应的接口，则会进行探测，检测接口的好坏以及链路是否有问题，如果不选择链路监控，则双机工作的时候只检测[网口监视]中的网口是否 DOWN 掉，物理网口 DOWN 掉才进行切换。可以设置多个监控组，每个监控组里面可以添加多个链路监测网口，每种链路监视可以选择不同的故障判定方式。只有当同一组中所有网口都链路故障时，才判断该组链路监控组故障，才会进行双机切换。

[主/备切换]：支持主机切换到备机，但是备机不能切换成主机。

点击上方的  管理对端设备 ①，可以通过心跳代理，从主机直接访问到备机的控制台界面。

『配置同步』：配置同步有主备控状态，并不是一定是主机向备机同步配置。只要哪端的配置做了修改，那么就从哪台设备同步配置。勾选“启用配置同步”，页面如下：

基本信息 双机热备 配置同步

启用同步 [i](#)

自动同步 [i](#)

同步对象：

待选	已选
用户认证	
会话表	
配置同步	

增加  移除 

配置同步角色： 主控 [设置](#) [i](#)

手动同步 [i](#)

手动同步配置

[查看同步报告](#)



[同步对象]：用于选择两台设备的同步对象。包括[用户认证]、[会话表]、[配置同步]。设备每 10 秒检测一次配置是否改变。

[配置同步角色]：用于设置配置同步角色包括主控和备控。注意：主控角色配置会同步给备控角色，备控角色无法修改配置，主、备控角色与双机状态无关。



1. 主备设备的监控网口必须要设置成一致，HA 口建议设置成一致。只
2. 虚拟组设置的优先级一样，那么无论开启抢占与否，都不会进行抢占。
3. 路由模式下，如果设置了链路监控，则主备切换条件有三个：没有收到心跳包、物理接口 DOWN 状态、链路检测检测到链路失效。以上任意一个条件符合即进行主备切换。
4. 配置同步分为两种：批量同步和增量同步。只有主控设备会向对端发送配

置同步请求，要求将对方的配置同步到本端，此时会进行批量同步。当主控设备批量同步完成后，设备每隔 10 秒检查一次配置是否改变，如改变，则同步主控修改的配置到备控设备，此时会进行增量同步。备控设备无权修改配置，如需自行修改先修改同步角色，否则提交无权修改。

5.如果设备 A 的规则库序号没有过期，设备 B 规则库序号过期了。那么设备 A 升级规则库后，设备 A 的规则库同步给对端会失败，但是不影响其他配置的同步。

6.双机热备的两台设备硬件型号必须一致。不同型号的设备网口数不同，作为双机的设备进行配置同步时，也会同步网口的配置，会导致主备设备工作不正常。

7.配置同步不会同步带 HA 接口的 IP 地址信息和『高可用性』配置。

8、当设备作为双机工作时，双机的状态可以在首页运行状态-今日系统状态中查看。

### 3.7. 用户认证

『用户认证』主要用于设置内网用户的认证方式和服务器访问认证，设备上定义的用户针对的是内网的终端上网用户，用户是网络权限分配的基本单元。管理员可以通过『用户管理』页面来对上网用户进行统一管理，通过『用户认证』页面来对内网的上网用户设置认证策略。通过服务器访问认证对服务器的登录进行认证。

## 3.7.1. 用户管理

### 3.7.1.1. 概述

防火墙所管理的对象是终端的上网用户，因此用户是网络权限分配的基本单元。管理员可以通过【组/用户】页面来对上网用户进行统一管理。

### 3.7.1.2. 原理

#### 3.7.1.2.1 用户认证

传统网络设备，管理的基本单位是 IP 地址，而 AF 设备管理的基本单位是用户，相比基于 IP 地址的管理来说更直观，也更精确。

要实现基于用户的管理，本系统必须要知道某个 IP 地址上某个时刻是哪个用户在使用的信息，因此需要对上网用户的身份进行认证，从而实现基于用户的上网行为管理。

根据认证方式，可以分为以下几种类型：

##### 1、用户名/密码

指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。密码认证包括本地密码认证以及外部服务器密码认证两种形式。

上网用户输入用户名，密码后，系统会首先在本地用户中检查输入的用户名，密码是否正确。如果本地查找不到该用户名，并且配置了外部的认证服务器，则会尝试到外部的认证服务器上检查用户名，密码是否正确。

注意：只有用户账号上勾选了“本地密码”的账号才属于本地密码认证账号，没有勾选“本地密码”的情况下，用户名和密码会发送到外部认证服务器进行认

---

证。

## 2、单点登录

**单点登录：**如果组织的网络中已经部署有身份认证系统，则本系统可以跟这些身份认证系统进行结合，以识别出某个 IP 地址上目前正在使用的用户，用户上网时不会再要求先输入用户名/密码，降低对上网用户的影响。

单点登录功能目前支持的类型有：

[结合微软 Active Directory 域的单点登录](#)（参见章节 3.7.2.2.1.1）

[结合代理服务器的单点登录](#)（参见章节 3.7.2.2.1.2）

[结合 POP3 邮件服务器的单点登录](#)（参见章节 3.7.2.2.1.3）

[结合 WEB 表单认证的单点登录](#)（参见章节 3.7.2.2.1.4）

## 3、基于 IP 地址、MAC 地址、计算机名的识别

根据数据包的源 IP 地址/源 MAC 地址，上网计算机的计算机名来识别用户。此种识别方式，优点是上网用户访问网络前不会在浏览器中弹出认证框要求输入用户名，密码。因此上网用户不会感知到设备的存在；缺点是无法识别出上网用户具体的用户名，特别是在地址动态分配的环境中，无法把上网行为对应到具体的用户，因此策略就无法针对具体的用户进行精确控制。

### 3.7.1.2.2 用户类型

根据用户来源，可以分为以下几个类型：

设备自动发现并创建；管理员手动创建；从 csv 表格文件中导入；从外部的 LDAP 服务器上导入；扫描网络上的计算机，并导入。

根据用户上网时的认证方式，可以分为以下几个类型：

不需要认证（绑定 IP/MAC）；本地密码认证；外部密码认证；单点登录（结合外部认证系统做身份识别）

### 3.7.1.3. 组/用户

#### 3.7.1.3.1 查看用户/组

查看设备中已经存在的用户和组信息，在【组织结构】中选择需要查看的用户组，右边的【组织成员】页面显示对应用户组的信息，包括：所属组、描述信息、组信息等。

**【组织成员】：**在【组织成员】页面中可以查看到各个子组以及用户的详细信息，包括：所属组、绑定信息（用户绑定的 IP、MAC 信息）、过期时间（用户）、描述信息、状态（启用或禁用）等。您还可以通过选择列来选择需要显示的信息。

The screenshot shows the Sangfor Management Interface. On the left, there's a sidebar titled 'Group Management' with a search bar and a tree view showing a single node labeled 'Default Group'. The main area has a title 'Organization Members' with sub-sections for 'Group Path', 'Description Information', and 'Group Information' (showing 1 child group, 0 direct users, and 0 total users). Below this is a 'Member Management' section with a toolbar for 'Add', 'Delete', 'Refresh', 'Batch Edit', 'Select', 'Import', 'Export', 'Move', 'Advanced Search', and 'Search by Content'. A table lists one member: '1 零 默认组'. At the bottom, there are navigation buttons for pages and a status bar indicating 'Current display: 1-1 of 1'.

选择功能：此功能用于快速选择当前页和全部页的用户、用户组，点击

选择弹出如下页面：



搜索功能：用于快速查找用户或用户组，点击搜索，选择搜索的方式：[搜索名称]、[搜索 IP 地址]、[搜索 MAC 地址]，在后面的输入框中输入内容，按回车键进行搜索。



高级搜索：仅适用于搜索用户，当需要通过多个搜索条件查询用户时，可以进行高级搜索。搜索条件包括：『基本搜索条件』和『其他选项』，当设置多个搜索条件时，搜索条件是与的关系，也就是需要所有条件都满足。

『基本搜索条件』包括[按用户名]、[按 IP 址址]和[按 MAC 地址]三种可选条件，只能三选一，如图所示：



『其他选项』包括[账号过期时间]、[用户状态]和[允许多人同时使用该账号登录的用户]三个选项。



### 3.7.1.3.2 新增用户/组

#### 3.7.1.3.2.1 新增子组

设备默认自带的组为根组（接口用“/”表示），根组不能删除，组名不能修改，用户自建的组都是根组的子组。设备中将用户组进行分级，根组是一级组，根组的子组是二级组，依次类推。这样设计更符合一个企业或者单位的组织结构，方便管理。

##### 3.7.1.3.2.1.1 新增子组配置案例

以在根组下新增一个工程师子组为例，介绍新增子组的步骤：

第一步：在【组织结构】中选择需要添加子组的用户组，右边进入管理页面，在【成员管理】窗口中，点击新增按钮，然后选择新增类型[组]

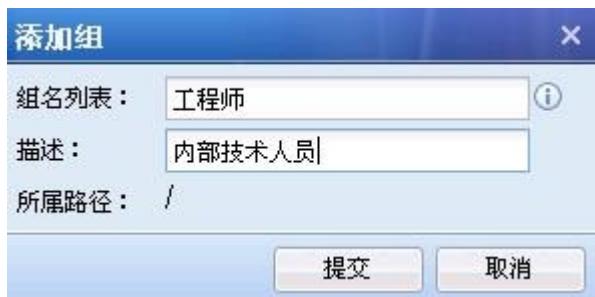


组织结构 <>  
搜索：输入关键字模糊搜索组  
组路径： / 修改组名与描述  
描述信息：  
组信息： 子组个数：1，直属用户个数：0，总用户个数(包含子组)：0

成员管理  
+ 新增 | X 删除 | 刷新 | 批量编辑 | 选择 | 导入 | 导出 | 移动 | 高级搜索 | 搜索名称 | 输入内容按回车键搜索  
序号 名称 地址绑定 过期时间 状态  
1 默认组 -

第 1 页 共 1 页 每页显示条数 20 当前显示1-1条 共1条

第二步：进入【添加组】窗口。设置[组名列表]即用户组的名称；设置[描述]即用户组的描述信息。点击添加策略，可以添加该组策略。



第三步：点击提交，完成子组添加



设备最多支持 16 级组织结构，包括根组。

### 3.7.1.3.2.2 新增用户

新增用户分为两类：新增用户和新增多用户。

此处新增的用户包括用户名、所属组、用户名密码、绑定 IP/MAC 等用户属性，但不包括指定用户的认证方式。内网用户的认证方式由『用户认证』→『认

证策略』设置，通过设置 IP 或者 MAC 条件，用于设备判断用户的认证方式。

### 3.7.1.3.2.2.1 新增用户配置案例 1

客户内网 192.168.1.0/255.255.255.0 网段的计算机全部采用用户名密码的认证方式，并在工程师组中新增一个用户：公共用户，此用户的认证方式是用户名密码认证，并且单向绑定 IP 范围（即限制登录的 IP 范围）为 192.168.1.2-192.168.1.100，可以多人同时登陆。

第一步：客户需求是：192.168.1.0/255.255.255.0 网段的计算机全部采用用户名密码的认证方式。所以首先需要设置这个网段用户的认证方式。

在『用户认证』→『认证策略』中设置认证策略，设置此用户的 IP 或者 MAC 范围，勾选认证方式为[本地密码认证/外部密码认证/单点登录]。设置认证策略前首先需要设置认证区域。如图，本例用以选择内网区做认证为例。区域设置请参考章节 3.3.1.5。



**认证策略**

名称：

描述：

策略适用 [?](#)  
IP/MAC范围：

**认证方式**

不需要认证/单点登录

把IP作为用户名

把MAC作为用户名

把计算机名字作为用户名

备注：如果配置了单点登录，则通过单点登录功能识别出该计算机上用户的用户名后，会优先使用该用户名。

本地密码认证/外部密码认证/单点登录 [?](#)

备注：密码认证指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。  
[点击配置外部认证服务器](#)

必须使用单点登录 [?](#)

例外的用户：

**提交** **取消**

第二步：在【组织结构】中选择需要添加用户的用户组，右边进入管理页面，在【成员管理】窗口中，点击**新增**按钮，然后选择新增类型[用户]

第三步：进入【添加用户】窗口。勾选[启用该用户]，填写[登录名]，[描述]，[显示名]和[当前所属组]。

**添加用户**

启用该用户

登录名：

描述：

显示名：

当前所属组： [...](#)

第四步：设置『用户属性』，用户属性设置包括：用户的认证方式、公用账

号和过期时间。

勾选[本地密码]，在[密码]的输入框中输入用户登录认证的密码。



The screenshot shows a configuration interface for a user account. A checkbox labeled "本地密码" (Local Password) is checked. Below it are two input fields: "密码" (Password) containing a series of asterisks, and "确认密码" (Confirm Password) also containing a series of asterisks.

[绑定 IP/MAC 地址]用于将该用户和 IP/MAC 地址绑定。此例中需要：单向绑定 IP 范围（即限制登录的 IP 范围）为 192.168.1.2-192.168.1.100。

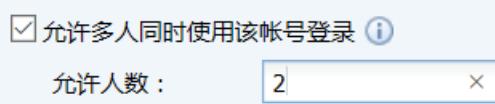
点击[绑定方式]，在弹出的页面中选择[用户和地址单向绑定]

勾选[绑定 IP]，在输入框中填入 192.168.1.2-192.168.1.100。



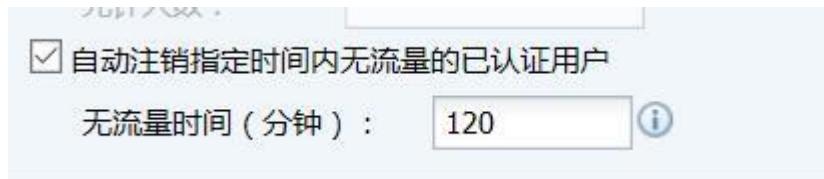
The screenshot shows a configuration interface for binding methods. A checkbox labeled "绑定IP/MAC地址" (Bind IP/MAC Address) is checked. Below it are three radio buttons: "绑定IP" (Bind IP) is selected, "绑定MAC" (Bind MAC) and "绑定IP和MAC" (Bind IP and MAC) are not selected. A note below says "一行一个条目，格式见绑定类型描述。#"为注释符号，例如："#200.200.0.1"。 An input field contains the IP range "192.168.1.2-192.168.1.100". At the bottom are two buttons: "从IP组获取" (Get from IP group) and "扫描MAC地址" (Scan MAC address).

[允许多人同时使用该账号登录]用于设置用户名密码认证的用户，是否可以多人同时用此账号登陆，勾选则表示允许多人同时登录。此例中该用户允许 2 人同时登陆，需要勾选。



The screenshot shows a configuration interface for account login settings. A checkbox labeled "允许多人同时使用该帐号登录" (Allow many people to log in with this account) is checked. Below it is a numeric input field set to "2".

勾选[自动注销指定时间内无流量的已认证用户]用来设置一个超时时间，用户超过此超时时间没有流量则自动注销该用户。



勾选[密码认证成功后弹出注销窗口]，此选项是针对用户名密码认证的用户，在成功登陆后弹出注销页面。



[过期时间]用于设置该用户的过期时间。



第五步：完成用户属性的编辑后，点击**提交**，完成用户的添加。

第七步：对应网段的用户上网时，打开网页，页面重定向到设备的认证页面。输入用户名和密码，点击**登录**。如果用户名密码验证正确并且符合绑定的IP条件，则认证通过。



如果用户名密码正确，但登录使用的 IP 地址不属于绑定的 IP 范围，则认证不通过，提示页面如下：



[绑定 IP/MAC 地址]分两种[绑定方式]：单向绑定和双向绑定。

**单向绑定：**用户只能使用指定的地址认证，但其它用户也允许使用该地址进行认证。

**双向绑定：**用户只能使用指定的地址认证，并且指定的地址仅供该用户使用。

上例中是创建一个用户名密码认证并且做单向绑定 IP 的用户，下面的例子说明的是双向绑定的用户设置：

### 3.7.1.3.2.2.2 新增用户配置案例 2

客户内网 192.168.1.0/255.255.255.0 网段的计算机全部采用用户名密码的认证方式，并在工程师组中新增一个用户：工程李，此用户的认证方式是用户名密码认证，并且双向绑定 IP/MAC 为 192.168.1.117/00-1C-25-AC-4C-44（即此用户认证时必须使用此 IP/MAC，并且其他用户不能使用此 IP/MAC）。

第一步：客户需求是：192.168.1.0/255.255.255.0 网段的计算机全部采用用户名密码的认证方式。所以首先需要设置这个网段用户的认证方式。

在『用户认证』→『认证策略』中设置认证策略，设置此用户的 IP 或者 MAC 范围，勾选认证方式为[本地密码认证/外部密码认证/单点登录]。设置认证策略前首先需要设置认证区域。如图，本例用以选择内网区做认证为例。



**认证策略**

名称：

描述：

策略适用  
IP/MAC范  
围：  
i 192.168.1.0/255.255.255.0

**认证方式**

不需要认证/单点登录

把IP作为用户名

把MAC作为用户名

把计算机名字作为用户名

备注：如果配置了单点登录，则通过单点登录功能识别出该计算机上用户的用户名后，会优先使用该用户名

本地密码认证/外部密码认证/单点登录 i

备注：密码认证指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。

[点击配置外部认证服务器](#)

必须使用单点登录 i

例外的用户：

**提交** **取消**

第二步：在【组织结构】中选择需要添加用户的用户组，右边进入管理页面，在【组织成员】窗口中，点击**新增**按钮，然后选择新增类型[用户]

第三步：进入【添加用户】窗口。勾选[启用该用户]，填写[登录名]，[描述]，[显示名]和[当前所属组]。

**添加用户**

启用该用户

登录名：

描述：

显示名：

当前所属组： 

第四步：设置『用户属性』，勾选[本地密码]，在[密码]的输入框中输入用

户登录认证的密码。



本地密码 [i](#)

密码：  
\*\*\*\*\*

确认密码：  
\*\*\*\*\*

[绑定 IP/MAC 地址]用于将该用户和 IP/MAC 地址绑定。此例中需要：双向绑定 IP/MAC 为 192.168.1.117/ 00-1C-25-AC-4C-44（即此用户认证时必须使用此 IP/MAC，并且其他用户不能使用此 IP/MAC）。

点击[绑定方式]，在弹出的页面中选择[用户和地址双向绑定]

勾选[绑定 IP 和 MAC]，在输入框中填入 192.168.1.117(00-1C-25-AC-4C-44)。



绑定IP/MAC地址：[绑定方式](#)

绑定IP [i](#)     绑定MAC [i](#)     绑定IP和MAC [i](#)

一行一个条目，格式见绑定类型描述。“#”为注释符号，例如：“#200.200.0.1”。

192.168.1.117(00-1c-25-ac-4c-44)

[从IP组获取](#) [扫描MAC地址](#)

由于此用户只绑定了一个 IP/MAC 地址，所以此用户默认是私有账号。

勾选[登陆成功后弹出注销窗口]，此选项是针对用户名密码认证的用户，在成功登陆后弹出注销页面。



登录成功后弹出注销窗口

[过期时间]用于设置该用户的过期时间。

帐号过期时间： 永不过期  
 过期时间（在此日期之后过期）  
\_\_\_\_\_

第五步：完成用户属性的编辑后，点击提交，完成单用户添加。

第六步：对应网段的用户上网时，打开网页，页面重定向到设备的认证页面。输入用户名和密码，点击登录。如果用户名密码验证正确并且符合绑定的IP条件，则认证通过。

如果用户名密码正确，但登录使用的IP/MAC地址和绑定的IP/MAC不符，则认证不通过，提示页面如下：



其他用户在此IP/MAC认证，也会提示认证不通过：



当「用户认证」→「认证策略」中设置了某些地址的用户采用不需要认证的认证方式时，用户可以不用输入用户名密码直接上网，此时设备是以 IP 地址、MAC 地址或者计算机名识别用户的。常见的设置是：

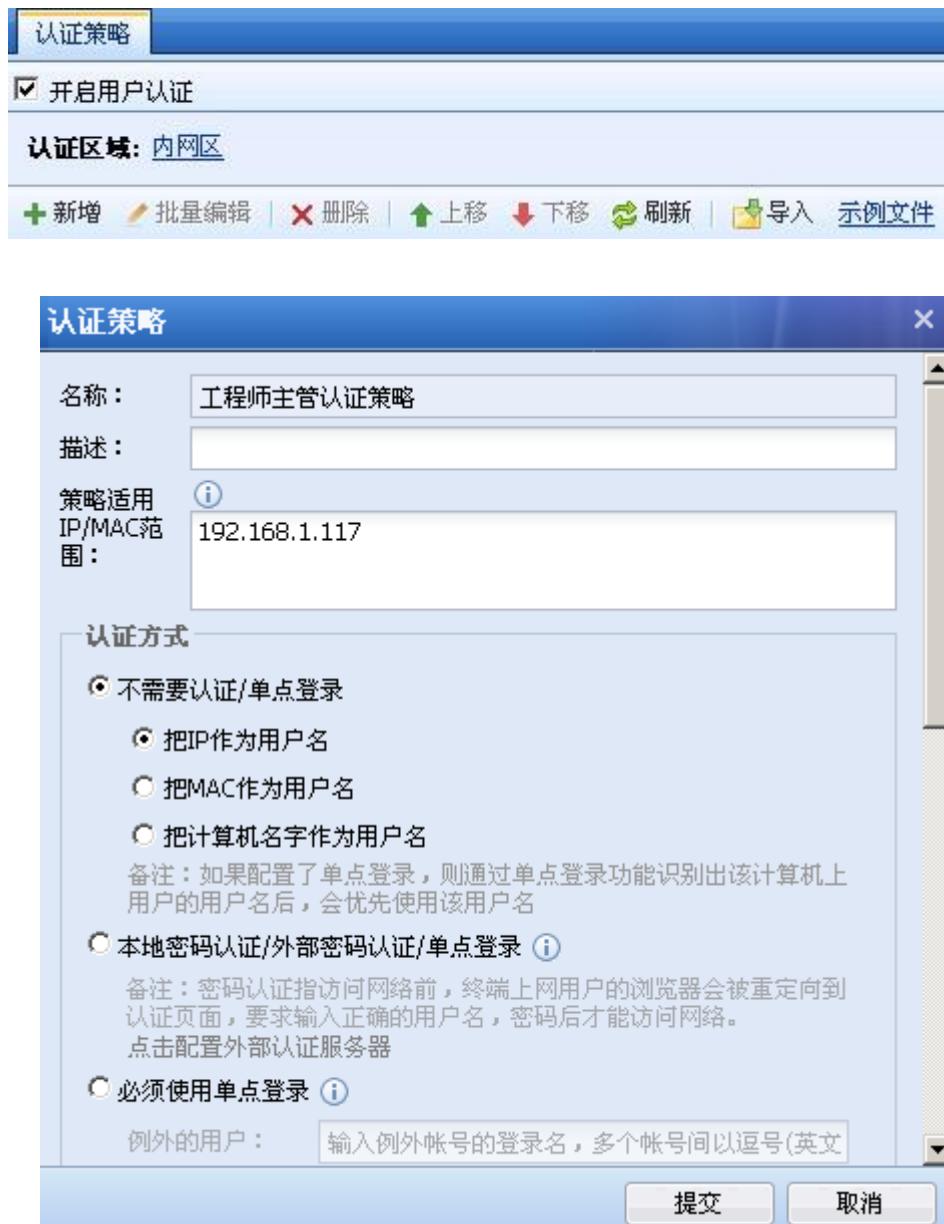
1、创建用户时将用户和 IP/MAC 地址进行双向绑定，因为双向绑定时 IP/MAC 和用户是一对一的关系，此时可以根据 IP/MAC 识别到对应的用户。

2、「用户认证」→「认证策略」中设置不需要认证，并以 IP 地址或者 MAC 地址或者计算机名做为用户名。内网用户认证时则根据 IP 地址或者 MAC 地址或者计算机名，匹配到对应的用户名。

### 3.7.1.3.2.2.3 新增用户配置案例 3

在“/工程师”组设置一个用户：主管，此用户不需要认证，并且将此用户和主管计算机的 IP/MAC 进行双向绑定，即只有主管的计算机才可以使用此账号上网。主管计算机的 IP/MAC 是：192.168.1.117(00-1C-25-AC-4C-44)。

第一步：在『用户认证』→『认证策略』中设置认证策略，设置此用户的IP或者MAC范围，勾选认证方式为[不需要认证/单点登录]。设置认证策略前首先需要设置认证区域。如图，本例以选择内网区做认证为例。



第二步：在【组织结构】中选择需要添加用户的用户组，右边进入管理页面，在【组织成员】窗口中，点击新增按钮，然后选择新增类型[用户]

第三步：进入【添加用户】窗口。勾选[启用该用户]，填写[登录名]，[描述]，[显示名]和[当前所属组]。

添加用户

启用该用户

登录名：

描述：

显示名：

当前所属组： 

第四步：设置『用户属性』，勾选[绑定 IP/MAC 地址]用于将该用户和 IP/MAC 地址绑定。此例中需要：双向绑定 IP/MAC 为 192.168.1.117/00-1C-25-AC-4C-44。

点击[绑定方式]，在弹出的页面中选择[用户和地址双向绑定]

勾选[绑定 IP 和 MAC]，在输入框中填入 192.168.1.117(00-1C-25-AC-4C-44)。

绑定IP/MAC地址：[绑定方式](#)

绑定IP   绑定MAC   绑定IP和MAC 

一行一个条目，格式见绑定类型描述。“#”为注释符号，例如：“#200.200.0.1”。

[过期时间]用于设置该用户的过期时间。

帐号过期时间：

永不过期

过期时间（在此日期之后过期）

第五步：完成用户属性的编辑后，点击[提交](#)，完成单用户添加。

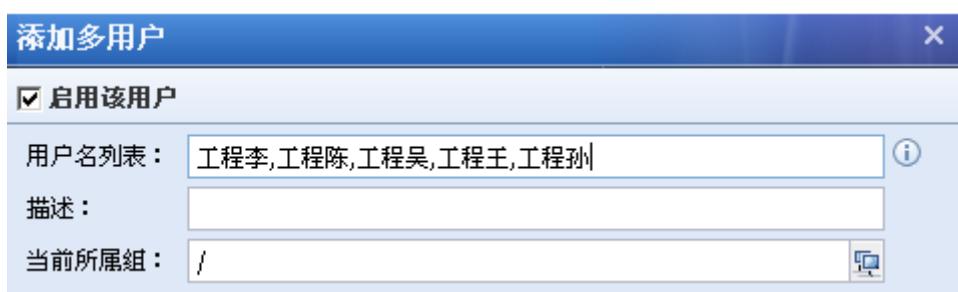
第六步：通过设备上网时，验证 IP 和 MAC 是否正确，如果正确则认证通过，客户端不会弹出认证页面。

如果 IP/MAC 地址和绑定的 IP/MAC 不符，则认证不通过，此时没有提示页面，但客户端的现象是上不了网。

### 3.7.1.3.2.3 新增多用户

[新增多用户]用于同时新增多个用户，与[新增用户]不同的是，新增多用户时用户属性不能 [绑定 IP/MAC 地址]的双向绑定，因为这项设置具有唯一性，不能在添加多用户时设置。

[新增多用户]设置的多个用户的属性和策略时完全相同的，除了用户名。在[用户名列表]中配置多个用户名，用户名之间用英文逗号隔开，其他配置和[新增单用户]相同，请参见上一节的内容。



### 3.7.1.3.3 删 除 用户/组

删除『组/用户』功能，作用是把不需要的用户或者用户组删除。

第一步：选择需要删除的组和用户。



组织成员

组路径： / 修改组名与描述

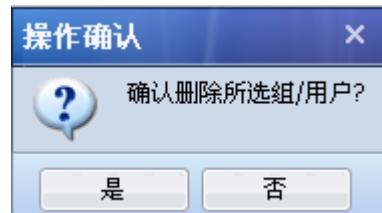
描述信息：

组信息： 子组个数：2，直属用户个数：0，总用户个数(包含子组)：1

序号	名称	地址绑定	过期时间	状态
1	工程师	-	-	-
2	默认组	-	-	-

第 1 页共 1 页 每页显示条数 20 当前显示1-2条 共2条

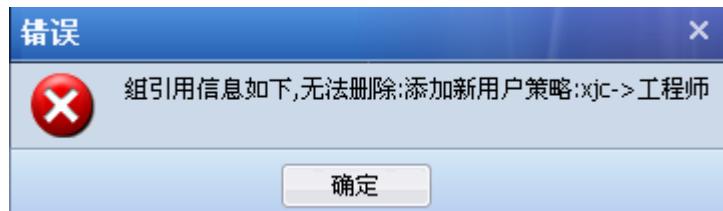
第二步：点击**删除**按钮



第三步：点击**是**后，删除对应的组和用户。控制面板上会有成功删除的信息。



如果「认证策略」中有策略关联了此处需要删除的用户组，则此用户组将无法直接删除，会提示删除失败，如下图。此时需要将「认证策略」中相关的策略删掉，才能将该组删除。（「认证策略」设置请参见章节 3.7.2.1）



### 3.7.1.3.4 批量编辑用户/组

批量编辑与单用户编辑的不同在于可编辑的属性不同。批量编辑，可以针对多个用户或多个组进行编辑，批量编辑用户时不能设置 [绑定 IP/MAC 地址]的双向绑定，因为这两项设置具有唯一性。

#### 3.7.1.3.4.1 批量编辑用户/组配置案例

把“网管 4, master, 网管 3, 网管 2, 网管, 工程张”这六个用户的描述都写为工程部；设置同样的用户名认证密码；单向绑定 IP 地址范围：192.168.1.1-192.168.1.255；用户有效期到 2012 年 1 月 1 号。

第一步：选择“网管 4, master, 网管 3, 网管 2, 网管, 工程张”六个用户，然后点击**批量编辑**按钮。

### 编辑多用户

启用IP/MAC绑定  
 用户和地址双向绑定  
 用户和地址单向绑定

修改IP/MAC地址  
 指定IP       指定MAC       指定IP和MAC

格式：不能为空，一行输入一个IP段，用户只能在这些IP段上登录  
可以直接在此处输入、编辑、删除

公用帐号  
 允许多人同时使用该帐号登录 i  
允许人数：  
 自动注销指定时间内无流量的已认证用户  
无流量时间（分钟）： i

注销窗口  
 密码认证成功后弹出注销窗口

帐号过期时间  
 永不过期  
 过期时间（在此日期之后过期）

第二步：勾选[描述]，填上工程师。勾选[密码设置]和[本地密码]，填上密码。

**用户属性**

用户名： master,工程张,网管,网管2,网管3,网管4 (i)

**用户状态**

启用  
 禁用

**描述**

工程师

**密码设置**

**本地密码** (i)

密码：  
\*\*\*\*\*

确认密码：  
\*\*\*\*\*

第三步：勾选[绑定 IP/MAC 地址]和[启用 IP/MAC 绑定]，选择[修改 IP/MAC 地址]，填上 192.168.1.1-192.168.1.255。勾选[账号过期时间]，选择[过期日期]，选择时间为 2012-01-01 00:00。

第四步：点击**提交**，完成批量编辑。

### 3.7.1.3.5 导入导出用户/组

导出导入用户/组的作用是将用户/组批量的导入导出设备。

在页面上点击  **导入**  **导出** 按钮，选择“导入”页面链接到【用户导入】页面，在此页面进行用户的导入，详细配置请参见章节 3.7.1.5

#### 3.7.1.3.5.1 导出用户/组配置案例

导出“工程部”组及用户

第一步，在【成员管理】窗口中找到“工程部”，勾选“工程部”，然后点击

导出按钮，选择导出。

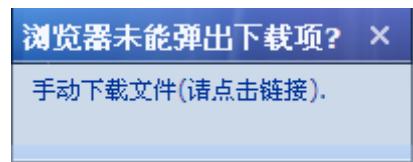


组织结构 <>  
搜索：输入关键字模糊搜索组  
/ 工程师  
默认组

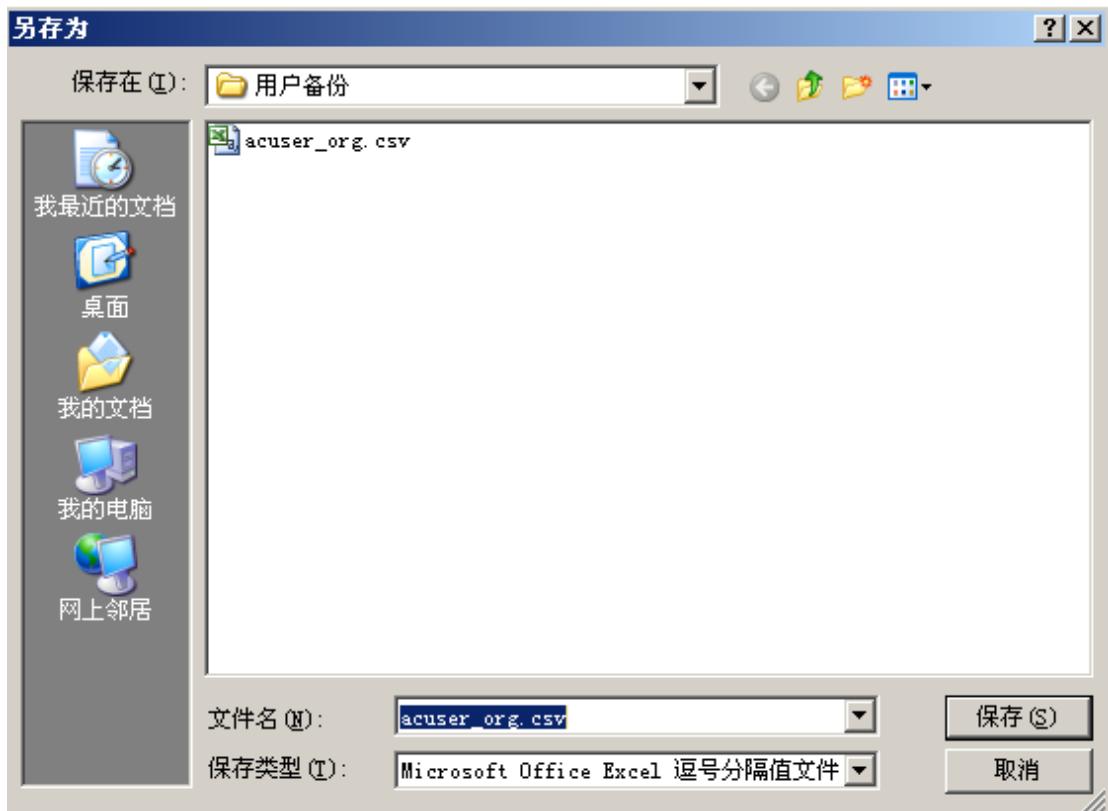
组织成员  
组路径： / 修改组名与描述  
描述信息：  
组信息： 子组个数：2，直属用户个数：0，总用户个数（包含子组）：2

成员管理  
+ 新增 | - 删除 | 刷新 | 批量编辑 | 选择 | 导入 | 导出 | 移动 | 高级搜索 | 搜索名称 | 输入内容按回车键搜索  
序号 名称 地址绑定 过期时间 状态  
1 变更工程师 - -  
2 变更默认组 - -

第二步：控制台上有提示“导出成功”，然后弹出下载对话框。点击链接下载导出的文件。



第三步：保存好导出文件。完成“工程部”组及用户的导出。



另存为

保存在(I):

我最近的文档  
桌面  
我的文档  
我的电脑  
网上邻居

文件名(N): acuser\_org.csv

保存类型(T): Microsoft Office Excel 逗号分隔值文件

保存(S) 取消



- 当某个用户组中没有用户时，此用户组是不支持单独导出的。

### 3.7.1.3.6 移动用户/组

把现有的用户或者组，移动到其他组下。成功移动后，用户会从原来的组中移动到目标组中。

#### 3.7.1.3.6.1 移动用户/组配置案例

将用户 support-xwb 与 support-pc 移动到“/默认组”组里面。

第一步：选择用户 support-xwb 和 support-pc 用户。点击**移动**按钮，然后选择移动的目标组织结构。

点击**移动**按钮成功移动 support-xwb。

The screenshot shows the 'Organization Member Management' interface. At the top, it displays group path: '/修改组名与描述', description information, and group details: 子组个数: 2, 直属用户个数: 2, 总用户个数(包含子组): 4. Below this is a table titled 'Member Management' with columns: 序号 (Index), 名称 (Name), 地址绑定 (Address Binding), 过期时间 (Expiration Time), and 状态 (Status). The table lists four items: 1. 工程师 (Engineer), 2. 默认组 (Default Group), 3. support-pc, and 4. support-xwb. Item 3 and 4 have checkboxes checked. A modal window titled 'Move Group/User' is open over the table, showing the 'Move to Target Group:' field set to '/默认组/'. At the bottom of the modal are 'Move' and 'Cancel' buttons.

第二步：点击**移动**按钮成功移动 support-pc 和 support-xwb。完成用户移动。



The screenshot shows the Sangfor Management Platform interface. On the left, there is a tree view of the organizational structure with nodes like '工程师' (Engineers) and '默认组' (Default Group). The main panel is titled '组织成员' (Organizational Members) and displays group information: '组路径: /默认组' (Group Path: /Default Group), '描述信息: /默认组' (Description: /Default Group), '组信息: 子组个数: 0, 直属用户个数: 2, 总用户个数(包含子组): 2' (Group Information: Subgroup count: 0, Direct user count: 2, Total user count (including subgroups): 2). Below this is a '成员管理' (Member Management) section with a table showing two users:

序号	名称	地址绑定	过期时间	状态
1	support-pc	没有绑定信息	永不过期	√
2	support-xwb	没有绑定信息	永不过期	√



1、对于普通管理员而言，可能只有管理某些组的权限，所以普通管理员在移动用户/组的时候，无法将用户/组移动到没有权限管理的用户组。

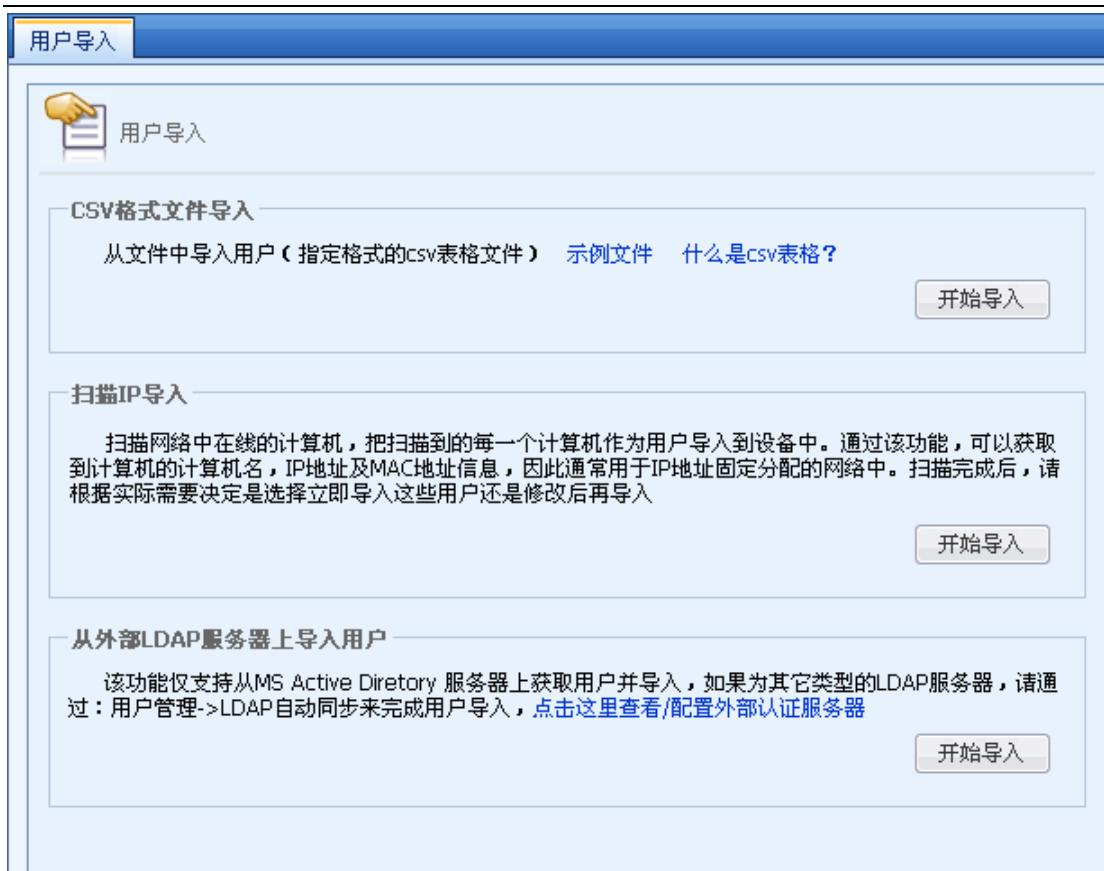
### 3.7.1.4. 用户导入

『用户导入』用于把用户批量导入，它提供三种方式：

『CSV 格式文件导入』：是通过一个 CSV 的文件导入用户，导入时可以同时导入显示名、认证方式、绑定 IP/MAC 信息、密码等。同时如果导入用户时指定的所属组不存在，那么同时也可自动创建对应的用户组。

『扫描 IP 导入』：当导入 IP/MAC 绑定的用户时，可以通过[扫描 IP 导入]扫描内网用户的 MAC 地址，方便此类用户的导入。通过此方法导入的用户默认都属于根组，并且认证方式是不需要认证，绑定 IP/MAC，用户名是通过扫描得到的机器名。当导入的用户 IP 和已有的用户绑定的 IP 有冲突时，无法导入此用户。

『从外部 LDAP 服务器上导入用户』：用于将 LDAP 服务器中的用户同步到设备中，支持从 MS Active Directory 服务器上导入用户。此处的域用户导入时，域服务器中的安全组会以用户组的形式导入设备，用户会导入到对应的安全组。



用户导入

CSV格式文件导入  
从文件中导入用户（指定格式的csv表格文件）[示例文件](#) [什么是csv表格？](#)

开始导入

扫描IP导入  
扫描网络中在线的计算机，把扫描到的每一个计算机作为用户导入到设备中。通过该功能，可以获取到计算机的计算机名，IP地址及MAC地址信息，因此通常用于IP地址固定分配的网络中。扫描完成后，请根据实际需要决定是选择立即导入这些用户还是修改后再导入

开始导入

从外部LDAP服务器上导入用户  
该功能仅支持从MS Active Directory 服务器上获取用户并导入，如果为其它类型的LDAP服务器，请通过：[用户管理->LDAP自动同步](#)来完成用户导入，[点击这里查看/配置外部认证服务器](#)

开始导入

### 3.7.1.4.1 CSV 格式文件导入

通过一个 CSV 的文件导入用户，导入的用户时可以同时导入显示名、认证方式、绑定 IP/MAC 信息、密码等。同时也如果导入用户时指定的所属组不存在，那么可以同时也可以建立用户组。

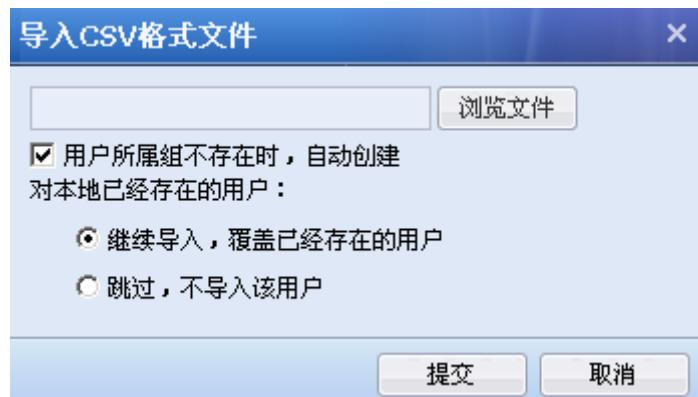
什么是 CSV 表格？CSV 表格文件格式非常简单，几乎所有的电子表格软件都可以编辑，保存该格式的表格文件，例如常见的微软 EXCEL 电子表格软件就可以编辑该类型的文件，而且可以非常方便地把 XLS 表格文件转换为 CSV 表格。技巧：因为 csv 文件格式很简单，不支持设置列宽，字体，颜色等属性，因此为了方便编辑，管理用户，平时可以先通过普通的 xls 表格中编辑用户信息，导入时，再转换成 csv 格式后导入。



第一步：导入用户的格式示例，可以点击[示例文件](#)进行下载。根据示例文件中的格式，设置需要导入的用户信息。

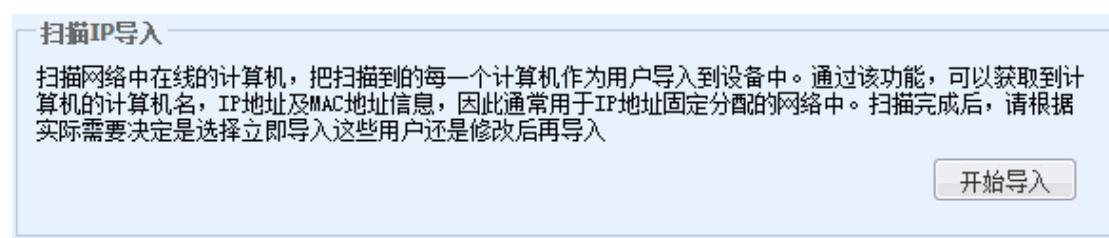
	A	B	C	D	E	F	G	H	I	J
1	#以#开头的行代表该行是注释行，而不是需导入的数据									
2	#请参考下面的示例添加需导入的用户帐号，带*的字段为必填项，注意不要删除列以及不要修改列的顺序									
3	#本地密码(留空代表空密码, N/A代表没有此用户不使用本地密码，因此无法使用本地认证的认证方式){xxx..}是导出用户时，经过加密后的本地密码(导入时，									
4	#单向绑定地址(留空则允许从任意地址上登录，多个地址间用英文逗号分隔，支持的详细格式可以参考新增用户页面)									
5	#双向绑定地址(留空则允许从任意地址上登录，多个地址间用英文逗号分隔，支持的详细格式可以参考新增用户页面)									
6	#是否允许多人同时使用该帐号登录(取值范围: Y/N, 留空代表: N)									
7	#帐号是否启用(取值范围: Y/N, 留空代表: Y)									
8	#帐号过期时间(格式: yy-mm-dd hh:mm, 留空代表永不过期)									
9	登录名(*) 显示名 所属组路径(*) 用户描述			本地密码	绑定地址（单向绑定）	绑定地址（双向绑定）	是否允许多人同时	帐号是否启用	帐号过期时间	
10	张三 /总部/市场部/研发部新同事			password			N	N		
11	李四 /总部/研发/	本地密码为空			10.0.10.10					
12	ID_95471 王五 /默认组/	一个到外部服务N/A			10.0.1.0-10.0.1.255, 192.168.1.0/24		Y	Y		
13	赵六 /默认组/			password	00-A1-B2-C3-D4-E5, 00-a1-b2-c3-d4-e6		Y	Y		
14	钱七 /默认组/				123 10.0.0.2 (00-A1-B2-C3-D4-E5)			Y	#####	#####
15	邮件服务器	/服务器		N/A		10.0.0.1	N		#####	#####

第二步：将设置好的 CSV 文件导入，点击[开始导入](#)，在【导入 CSV 格式文件】页面中选择需要导入的文件，勾选[用户所属组不存在时，自动创建]表示导入用户指定的用户组不存在时，设备会自动新建该组，反之不勾选则不会新建该组，用户会默认导入到根组。在[对本地已经存在的用户]中选择[继续导入，覆盖已经存在的用户]表示如果用户列表中已经有相同的用户名的用户，则更新此用户的属性；选择[跳过，不导入该用户]表示如果用户列表中已经有相同用户名的用户，则不更改用户属性，跳过此用户的导入。



### 3.7.1.4.2 扫描 IP 导入

用于扫描对应 IP 的 MAC 地址，并且支持将扫描出的用户导入设备，用户名是用扫描到的机器名做用户名，这些用户将默认导入到根组，认证方式是不需要认证，绑定 IP 和 MAC。



#### 3.7.1.4.2.1 扫描 IP 配置案例

扫描内网 192.200.200.1-192.200.200.100 范围内的计算机，并导入到用户列表中。

第一步：选择『扫描 IP 导入』，点击【开始导入】按钮，填写需要扫描的 IP 范围。



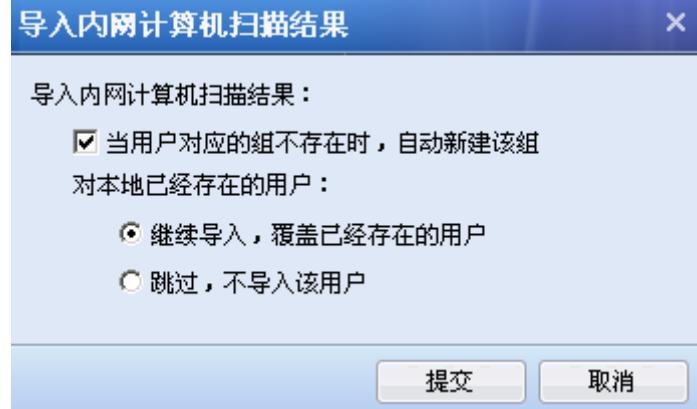
第二步：点击**开始扫描**，扫描出 192.200.200.1-192.200.200.100 范围内的计算机出来的结果。只能扫描出目前存活的计算机。[用户名]是以扫描到的计算机名作为用户名。

**扫描结果预览**

序号	用户名	IP地址	MAC地址
1	unknow0	192.200.200.2	00-02-B6-36-0A-FC
2	unknow1	192.200.200.4	00-E0-A0-0D-CA-76
3	unknow2	192.200.200.9	00-0A-DB-01-22-D0
4	SINFOR-LAB	192.200.200.19	00-19-e0-29-cb-d3
5	BACKUPSERVER	192.200.200.20	00-0b-2f-16-a8-ba
6	SERVER	192.200.200.40	00-0c-29-a8-86-63
7	unknow3	192.200.200.44	00-0C-29-55-C2-D8
8	SUPPORT-RTX	192.200.200.66	00-01-6c-b1-76-c3
9	SINFOR-CTI	192.200.200.72	00-90-30-03-12-af
10	SINFOR-SINFOR	192.200.200.84	00-e0-4c-c1-95-a0
11	SVRBAK	192.200.200.86	00-0c-76-3b-0b-86
12	SUPPORT-87	192.200.200.87	00-f0-cf-82-5d-1f
13	SUPPORT-88	192.200.200.88	00-0a-eb-94-fc-b7

**上一步** **直接导入扫描结果** **下载编辑扫描结果** **取消**

第三步：点击**直接导入扫描结果**按钮，将上面扫描出的用户直接导入设备。  
在弹出的导入选项中，勾选[当用户对应的组不存在时，自动新建该组]表示导入用户指定的用户组不存在时，设备会自动新建该组，反之不勾选则不会新建该组，用户会默认导入到根组。在[对本地已经存在的用户]中选择[继续导入，覆盖已经存在的用户]表示如果用户列表中已经有相同的用户名的用户，则更新此用户的属性；选择[跳过，不导入该用户]表示如果用户列表中已经有相同用户名的用户，则不更改用户属性，跳过此用户的导入。



点击[下载编辑扫描结果](#)，用于将扫描出来的用户信息以 CSV 格式的文件保存在本地，如果您需要对扫描的结果和用户属性做修改，则通过修改文件实现。修改完的文件可以通过『CSV 格式文件导入』进行导入。

第四步：点击[提交](#)按钮，用户将被导入到根组中。



1、扫描用户名显示为 **unknow** 表示机器名没有获取到，机器名是通过登录控制面板的计算机使用 **netbios** 协议获取的，扫描不到机器名，请确认以下几点：目标计算机上是否开启了 **netbios** 协议；目标计算机上是否配置了多 IP；目标计算机上是否有防火墙过滤了 **netbios** 协议；网络路径中是否有设备做了 **netbios** 协议的过滤。

#### 3.7.1.4.3 从外部 LDAP 服务器上导入用户

用于将 LDAP 服务器中的用户同步到设备中，该功能仅支持从 MS Active Directory 服务器上导入用户，如果是其他类型的 LDAP 服务器，请通过『用户管理』→『LDAP 自动同步』来完成用户的导入（参见章节 3.7.1.6）。

实现从 LDAP 服务器上导入用户，首先需要配置 LDAP 服务器（具体设置参见：『功能说明』→『用户与策略管理』→『用户认证』→『外部认证服务器』，章节 3.7.2.3）

**从外部LDAP服务器上导入用户**

该功能仅支持从MS Active Directory 服务器上获取用户并导入，如果为其它类型的LDAP服务器，请通过：用户管理->LDAP自动同步来完成用户导入，[点击这里查看/配置外部认证服务器](#)

**开始导入**

**1、LDAP 用户导入需要安装控件，所以进行 LDAP 导入的操作时请使用 IE 浏览器登陆控制台。**

**2、LDAP 导入时需要设备能够正常连接到 LDAP 服务器的 TCP389 端口，保证可以正常读取到和导入 LDAP 服务器中的用户信息。**

### 3.7.1.5. LDAP 自动同步

『LDAP 自动同步』用于将域服务器中的用户、组织结构、安全组同步到设备上，并且可以进行自动同步，设备每天会和域服务器自动同步一次，同步时间是凌晨 0 点-6 点的一个随机时间。

『LDAP 自动同步』分为两种类型的同步：[按组织结构(OU)同步]和[按安全组同步（仅 AD 域）]。

[按组织结构(OU)同步]：适用于所有类型的 LDAP 服务器，按照这种方式同步时 LDAP 服务器中的 OU 会以用户组的形式同步到设备，并且 OU 的组织结构也会以相同的形式同步到设备，用户同步到设备仍然属于对应的 OU 组。

[按安全组同步（仅 AD 域）]：仅适用于微软的 LDAP 服务器，即 AD 域。按照这种方式同步时，AD 域服务器中的安全组会以用户组的形式同步到设备，安全组没有组织结构，设备会以平级的方式把安全组同步过来，即同步的安全组都是同一级别的组。

### 3.7.1.5.1 新增同步策略

同步策略用于设置同步的相关参数，设置进行 LDAP 同步时，是根据同步策略中的设置进行同步的。

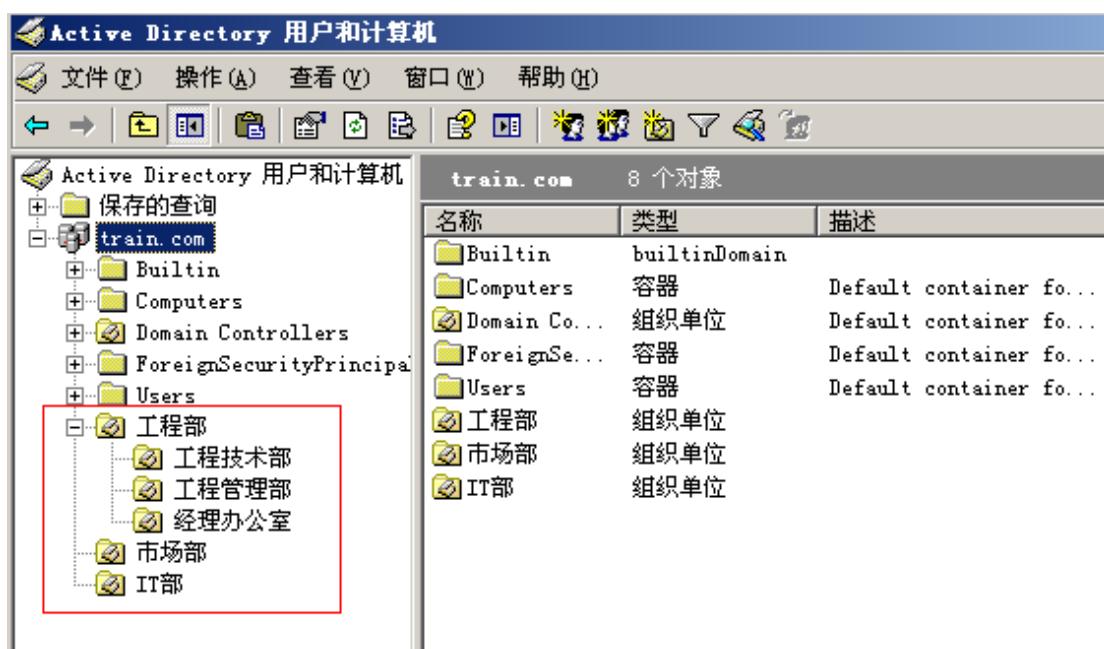
#### 3.7.1.5.1.1 按组织结构（OU）同步

适用于所有类型的 LDAP 服务器，按照这种方式同步时 LDAP 服务器中的 OU 会以用户组的形式同步到设备，并且 OU 的组织结构也会以相同的形式同步到设备，用户同步到设备仍然属于对应的 OU 组。

##### 3.7.1.5.1.1.1 按 OU 同步配置案例

将 LDAP 服务器中的 OU=工程部，OU=市场部，OU=IT 部同步到设备中，同时同步这些 OU 对应的子 OU 和用户。

LDAP 服务器中的组织结构如下：



配置步骤：

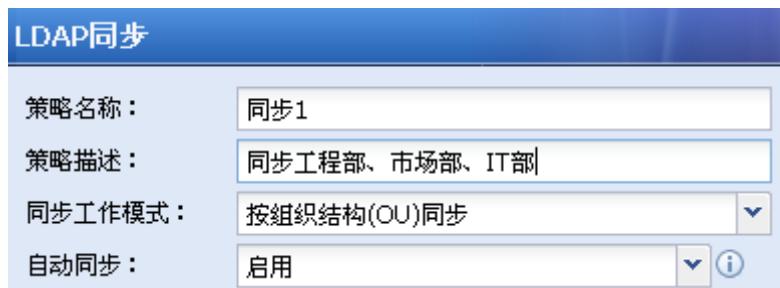
第一步：设置需要同步的 LDAP 服务器，设置 IP、端口、登陆用户名密码

等信息，具体请参见『用户认证』→『外部认证服务器』（参见章节 3.7.2.3）

第二步：进入『用户认证』→『LDAP 自动同步』，点击**新增**，在弹出的【LDAP 同步】窗口中设置同步参数。



第三步：在【LDAP 同步】窗口中，设置[策略名称]、[策略描述]、[同步工作模式]、[自动同步]。[同步工作模式]选择按组织结构（OU）同步，[自动同步]选择启用，自动同步一天同步一次。



策略名称：	同步1
策略描述：	同步工程部、市场部、IT部
同步工作模式：	按组织结构(OU)同步
自动同步：	启用

第四步：[同步来源配置]用于设置需要同步的 LDAP 服务器的 OU 的相关信息。

## LDAP同步

### 同步来源配置(远程)

LDAP服务器：  
LDAP1

从以下远程目标同步：

选择

OU=IT部,DC=train,DC=com  
OU=工程部,DC=train,DC=com  
OU=市场部,DC=train,DC=com

从远程目标的根节点开始创建本地组织结构 i

从远程目标的当前选中节点开始创建本地组织结构 i

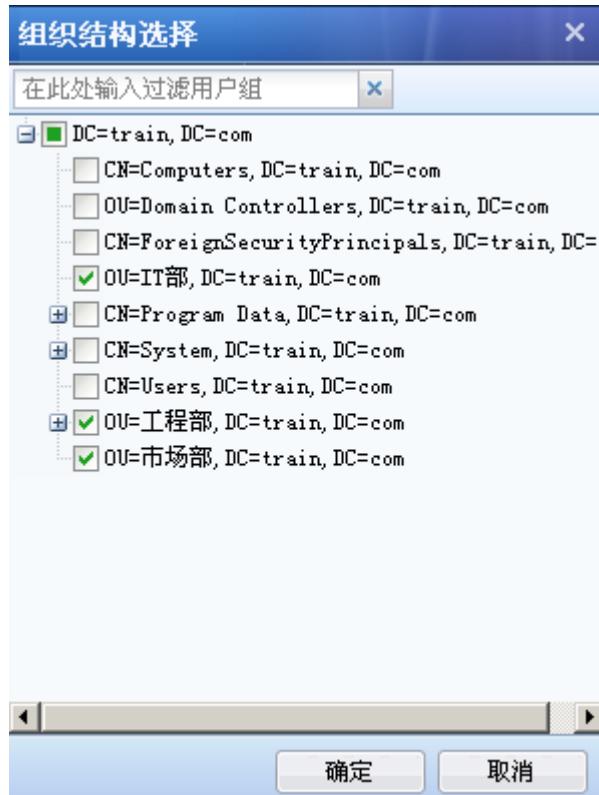
从远程目标的当前选中节点的子节点开始创建本地组织结构 i

导入OU的最大深度：  
10

过滤参数：

[LDAP服务器]用于设置需要同步的 LDAP 服务器，此处选择的服务器即为步骤一中设置的服务器。

[从以下远程目标同步]用于指定需要同步 LDAP 服务器中哪些 OU，点击[选择](#)，在窗口【组织结构选择】中选择需要同步的 OU：OU=工程部，OU=市场部，OU=IT 部。选择完成后点击[确定](#)。



勾选[从远程目标的根节点开始创建本地组织结构]表示 LDAP 中的根域名也会以组的形式同步过来，且同步的 OU 都是它的子组。

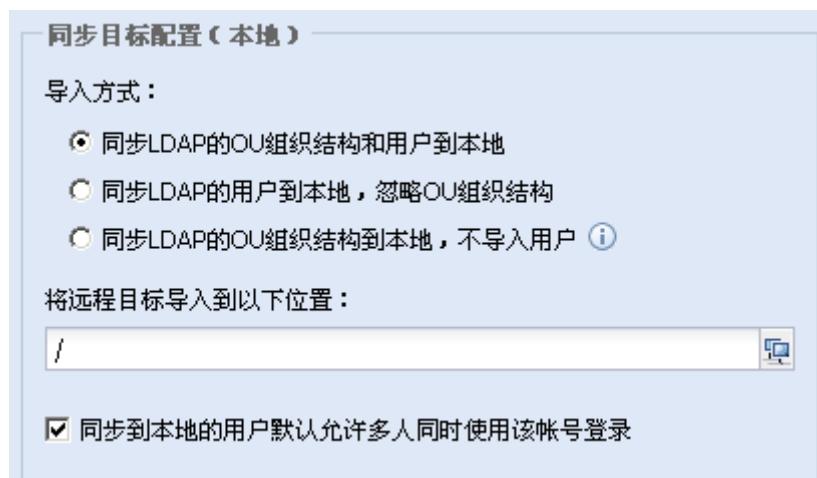
勾选[从远程目标的当前选中节点开始创建本地组织结构]表示同步从所选的 OU 开始同步。

勾选[从远程目标的当前选中节点的子节点开始创建本地组织结构]表示同步从所选 OU 的子 OU 开始同步，所选 OU 和所选 OU 的直属用户此时都不会同步到设备上。

[导入 OU 的最大深度]: 用于设置导入的 OU 深度，此处设置的是 10，表示从所选 OU 开始同步的话，它的 9 级子 OU 都能以用户组同步到设备，但是 9 级以下的 OU 不会以用户组同步到设备了，9 级以下 OU 的用户还是可以同步到设备的，这些用户同步过来是属于第 9 级 OU 的。

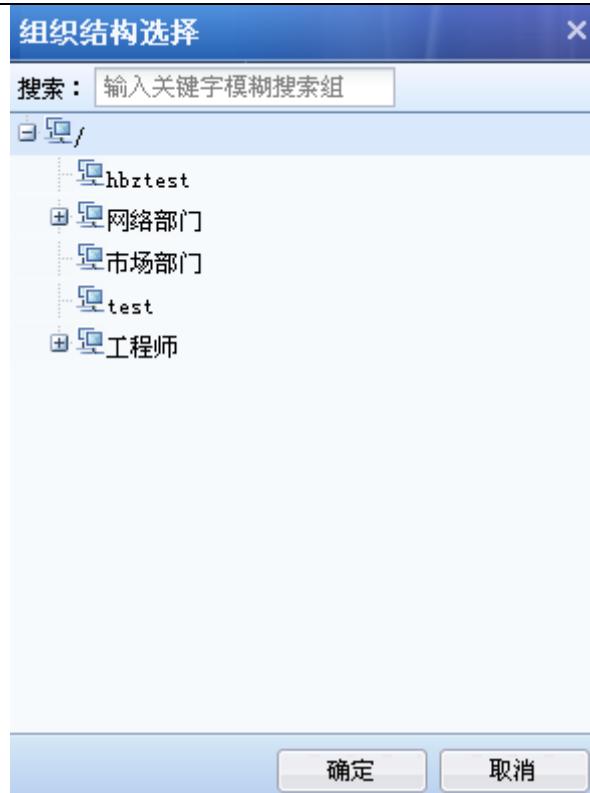
[过滤参数]: 用于设置同步的过滤参数。

第五步：[同步目标配置]用于设置导入方式、同步的 OU 和用户被放置在设备组织结构的什么位置，并且可以设置同步用户的属性。



[导入方式]用于选择同步时是否同步 OU 和用户。勾选[同步 LDAP 的 OU 组织结构和用户到本地]表示将 OU 做为用户组同步到设备上，同时将 OU 中的用户同步到 OU 对应的用户组下。勾选[同步 LDAP 的用户到本地，忽略 OU 组织结构]表示将 OU 中的用户同步到设备上，但不同步 OU。勾选[同步 LDAP 的 OU 组织结构到本地，不导入用户]表示只将 OU 做为用户组同步到设备上，但不同步 OU 中的用户。此例中应该选择第一项，即同时同步 OU 和用户。

[将远程目标导入到以下位置]用于指定设备中已有的一个组，同步过来的 OU 都会成为此处所选组的子组。点击 ，在【组织结构选择】窗口选择相应的组，选择完成点击 。



勾选[同步到本地的用户默认允许多人同时使用该账号登录]表示同步到设备的域账号默认是公用账号，即同一账号能够在多台计算机上登录，不勾选此项则表示用户是私有账号，只能同时在一台计算机上登录。

第六步：设置完同步策略，点击提交，添加策略完成。在【LDAP 自动同步】页面查看添加的同步策略，点击 可以立即进行同步，不点击则可以等到自动一天一次进行同步。

LDAP 自动同步						
操作		策略名		描述	包含组或用户	自动同步
序号	策略名	描述	包含组或用户	自动同步	最后同步状态	立即同步
1	同步1	同步工程部、市场部、IT部	OU	是	同步失败	

第七步：点击立即同步后，查看同步的结果：『用户管理』→『组/用户』中查看【组织结构】，如下图：此时导入的 OU 和用户同 LDAP 服务器中的完全一致。



组织结构

搜索 : 输入关键字模糊搜索组

/

- IT部
- 工程部
  - 工程技术部
  - 工程管理部
  - 经理办公室
- 市场部



1、当同步的 OU 或者用户同设备中已有的用户组或者用户同名时，  
LDAP 中的 OU 或用户无法同步到设备。

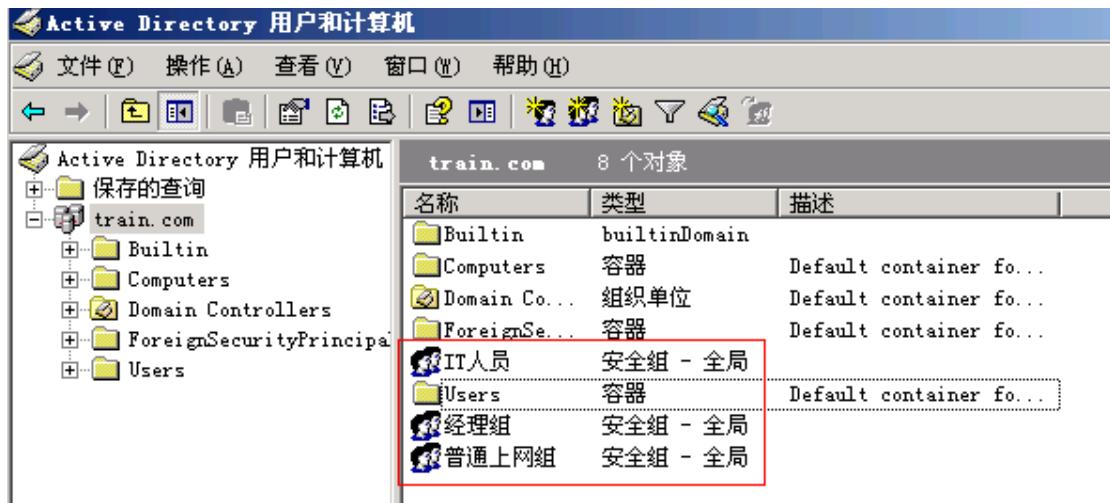
#### 3.7.1.5.1.2 按安全组同步（仅 AD 域）

仅适用于 MS Active Directory 服务器，即 AD 域。按照这种方式同步时，AD 域服务器中的安全组会以用户组的形式同步到设备，在 LDAP 中安全组没有组织结构的概念，设备会以平级的方式把安全组同步过来，即同步的安全组都是同级别的组。

##### 3.7.1.5.1.2.1 按安全组同步配置案例

将 LDAP 服务器中的 CN=IT 人员，CN=经理组，CN=普通上网组同步到设备中，同时同步这些安全组中的用户。

LDAP 服务器中的安全组如下：



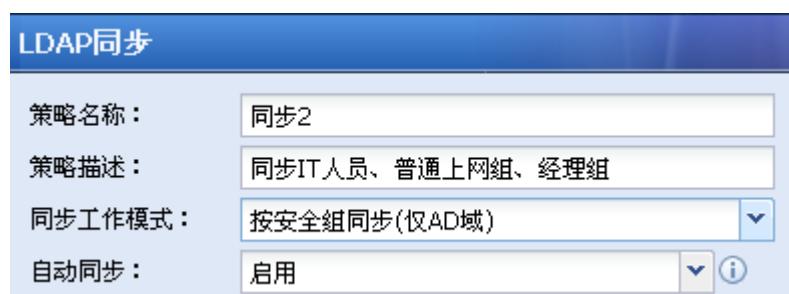
配置步骤：

第一步：设置需要同步的 LDAP 服务器，设置 IP、端口、登陆用户名密码等信息，具体请参见『用户认证』→『外部认证服务器』（参见章节 3.7.2.3）

第二步：进入『用户认证』→『LDAP 自动同步』，点击【新增】，在弹出的【LDAP 同步】窗口中设置同步参数。

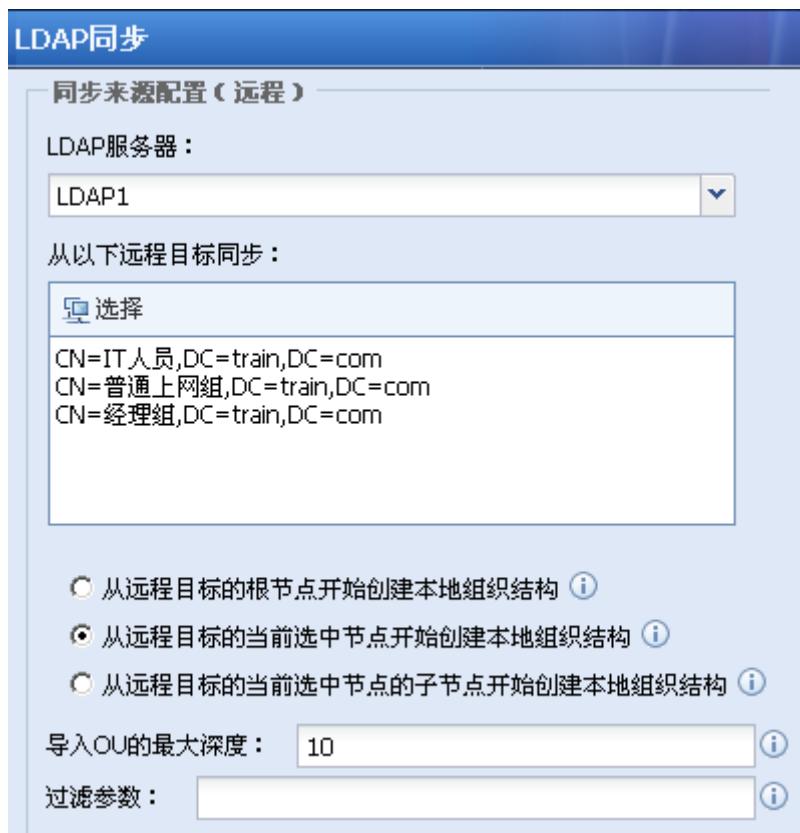


第三步：在【LDAP 同步】窗口中，设置[策略名称]、[策略描述]、[同步工作模式]、[自动同步]。[同步工作模式]选择按安全组同步，[自动同步]选择启用，自动同步一天同步一次。



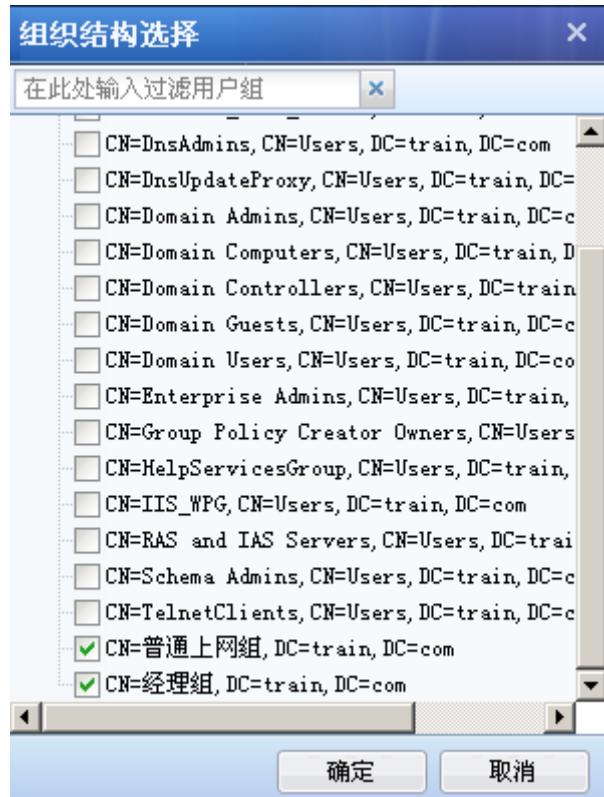
第四步：[同步来源配置]用于设置需要同步的 LDAP 服务器的安全组相关信息

息。



[LDAP 服务器]用于设置需要同步的 LDAP 服务器，此处选择的服务器即为步骤一中设置的服务器。

[从以下远程目标同步]用于指定需要同步 LDAP 服务器中哪些安全组，点击 **选择**，在窗口【组织结构选择】中选择需要同步的安全组：CN=IT 人员，CN=经理组，CN=普通上网组。选择完成后点击**确定**。



勾选[从远程目标的根节点开始创建本地组织结构]表示 LDAP 中的根域名也会以组的形式同步过来，且同步的 OU 都是它的子组。

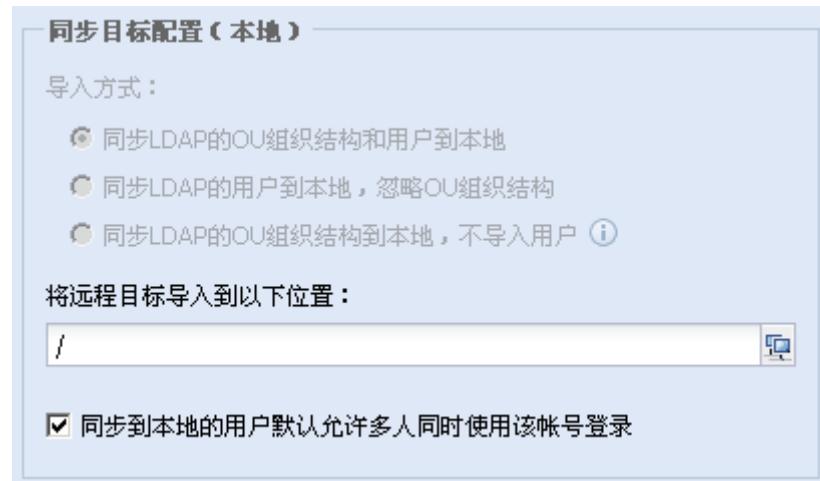
勾选[从远程目标的当前选中节点开始创建本地组织结构]表示同步从所选的 OU 开始同步。

勾选[从远程目标的当前选中节点的子节点开始创建本地组织结构]表示同步从所选 OU 的子 OU 开始同步，所选 OU 和所选 OU 的直属用户此时都不会同步到设备上。

[导入 OU 的最大深度]在按照安全组同步时是没有作用的，可以忽略不设置。

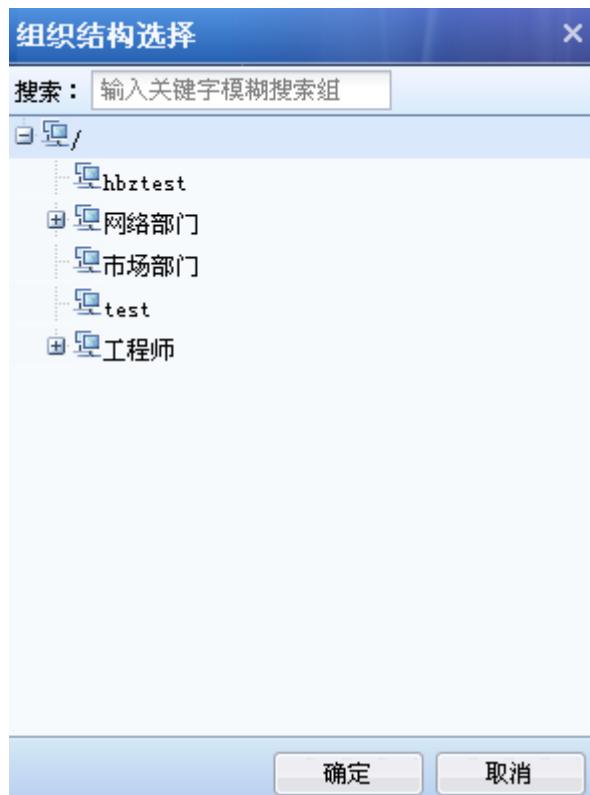
[过滤参数]：用于设置同步的过滤参数。

第五步：[同步目标配置]用于设置同步的安全组和用户被放置在设备组织结构的什么位置，并且可以设置同步用户的属性。



[导入方式]在选择按照安全组同步时不可选择，默认是将安全组和用户都同步到设备中。

[将远程目标导入到以下位置]用于指定设备中已有的一个组，同步过来的安全组都会成为此处所选组的子组。点击 ，在【组织结构选择】窗口选择相应的组，选择完成点击 。



勾选[同步到本地的用户默认允许多人同时使用该账号登录]表示同步到设备的域账号默认是公用账号，即同一账号能够在多台计算机上登录，不勾选此项则表示用户是私有账号，只能同时在一台计算机上登录。

第六步：设置完同步策略，点击提交，添加策略完成。在【LDAP 自动同步】页面查看添加的同步策略，点击立即同步可以立即进行同步，不点击则可以等到自动一天一次进行同步。

LDAP 自动同步							
<span style="color: green;">+</span> 新增 <span style="color: red;">-</span> 删除   <span style="color: blue;">=</span> 查看同步报告   <span style="color: green;">↻</span> 刷新							
序号	策略名	描述	包含组或用户	自动同步	最后同步状态	<span style="color: green;">↻</span> 立即同步	<span style="color: red;">X</span> 删除
<input type="checkbox"/>	同步1	同步工程部、市场部、IT部	OU	是	同步成功	<span style="color: green;">↻</span>	<span style="color: red;">X</span>
<input type="checkbox"/>	同步2	同步IT人员、普通上网组、经理组	GROUP	是	同步失败	<span style="color: green;">↻</span>	<span style="color: red;">X</span>

第七步：点击立即同步后，查看同步的结果：『用户管理』→『组/用户』中查看【组织结构】，如下图：此时导入的安全组和用户同 LDAP 服务器中的完全一致。



当同步的安全组或者用户同设备中已有的用户组或者用户同名时，LDAP 中的安全组或用户无法同步到设备。

### 3.7.1.5.2 删除同步策略

当某些同步策略没用的时候，可以将同步策略删除，点击进入【LDAP 同步】页面：勾选需要删除的同步策略，点击删除即可。同步策略删除不会影响之前已经同步到设备上的组和用户。

LDAP 自动同步							
<span style="color: green;">+</span> 新增 <span style="color: red;">-</span> 删除   <span style="color: blue;">=</span> 查看同步报告   <span style="color: green;">↻</span> 刷新							
序号	策略名	描述	包含组或用户	自动同步	最后同步状态	<span style="color: green;">↻</span> 立即同步	<span style="color: red;">X</span> 删除
<input checked="" type="checkbox"/>	同步1	同步工程部、市场部、IT部	OU	是	同步成功	<span style="color: green;">↻</span>	<span style="color: red;">X</span>
<input type="checkbox"/>	同步2	同步IT人员、普通上网组、经理组	GROUP	是	同步失败	<span style="color: green;">↻</span>	<span style="color: red;">X</span>

### 3.7.1.5.3 查看同步报告

设备在每一次进行 LDAP 同步时，都会产生一份同步报告，便于您查看同步的情况。点击 **查看同步报告**，在【同步报告】页面选择需要查看的同步报告，下载后即可查看。

同步报告				
<b>✖ 清空同步报告</b>				
序号	同步报告名	同步方式	同步时间	同步状态
2	1320088331-2011-11...	自动同步	2011-11-01 03:12:11	失败
3	1320001932-2011-10...	自动同步	2011-10-31 03:12:12	失败
4	1319915531-2011-10...	自动同步	2011-10-30 03:12:11	失败
5	1319829131-2011-10...	自动同步	2011-10-29 03:12:11	失败
6	1319742731-2011-10...	自动同步	2011-10-28 03:12:11	失败
7	1319656331-2011-10...	自动同步	2011-10-27 03:12:11	失败
8	1319569931-2011-10...	自动同步	2011-10-26 03:12:11	失败
9	1319483531-2011-10...	自动同步	2011-10-25 03:12:11	失败
10	1319397131-2011-10...	自动同步	2011-10-24 03:12:11	失败
11	1319310731-2011-10...	自动同步	2011-10-23 03:12:11	失败
12	1319224331-2011-10...	自动同步	2011-10-22 03:12:11	失败
13	1319137931-2011-10...	自动同步	2011-10-21 03:12:11	失败
14	1319051531-2011-10...	自动同步	2011-10-20 03:12:11	失败
15	1318965131-2011-10...	自动同步	2011-10-19 03:12:11	失败
16	1318878731-2011-10...	自动同步	2011-10-18 03:12:11	失败
17	1318792331-2011-10...	自动同步	2011-10-17 03:12:11	失败
18	1318705931-2011-10...	自动同步	2011-10-16 03:12:11	失败
19	1318819531-2011-10...	自动同步	2011-10-15 03:12:11	失败
20	1318533132-2011-10...	自动同步	2011-10-14 03:12:12	失败

关闭

### 3.7.2. 用户认证

『用户认证』用于设置用户认证的相关设置，包括『认证策略』、『认证选项』、『外部认证服务器』。需要注意的是设备不启用用户认证，内网用户也是可以上网的。此时可以通过对象中定义 IP 来实现对内网 PC 的各种保护，此时用户排名以及记录日志均以 IP 地址的方式显示。

### 3.7.2.1. 认证策略

#### 3.7.2.1.1 概述

开启了用户认证，则认证区域的所有计算机上网前，都必须经过用户认证，以识别上网计算机的身份。『认证策略』决定了某个 IP/网段/MAC 地址上计算机的认证方式。通过『认证策略』设置内网用户的认证方式，以及新用户添加的策略。

认证策略是从上往下逐条匹配的，可以通过页面上的移动按钮来调整认证策略优先级。通过认证策略可以为不同的网段配置不同的认证方式。

#### 认证方式：

设备的认证方式有以下几种：

1、不需要认证；2、密码认证（包括本地密码认证和外部服务器认证）；3、单点登录；以上几种认证方式是由『认证策略』设置决定的，其中单点登录还需要在『认证选项』中进行设置。

『认证策略』的认证方式有三种选择：[不需要认证/单点登录]、[本地密码认证/外部密码认证/单点登录]、[必须使用单点登录]。



这三种认证方式中都包含有单点登录的认证方式，如果在『认证选项』中配置了单点登录，则通过单点登录功能识别出某计算机上用户的用户名后，会优先使用该用户名上网。

#### 1、[不需要认证/单点登录]

选择此种认证方式：如果『认证选项』中配置了单点登录，则通过单点登录功能识别出某计算机上用户的用户名后，会优先使用该用户名上网。

没有单点登录认证的情况下，设备根据数据包的源 IP 地址、源 MAC 地址、上网计算机的计算机名来识别用户。不需要认证的识别方式，优点是用户上网前浏览器中不会弹出认证框，要求输入用户名，密码才能上网。因此上网用户不会感知到设备的存在。

### 如何创建一个不需要认证的用户？

一种做法是：在『认证策略』中设置不需要认证，创建用户时将用户和 IP/MAC 地址进行双向绑定，因为双向绑定时 IP/MAC 和用户是一对一的关系，此时可以根据 IP/MAC 识别到对应的用户。（注意『认证策略』中设置的 IP/MAC 范围需要包含绑定的 IP/MAC）。

另一种做法是：在『认证策略』中设置不需要认证，并以 IP 地址或者 MAC 地址或者计算机名做为用户名。内网用户认证时则根据 IP 地址或者 MAC 地址或者计算机名，匹配到对应的用户名。

## 2、[本地密码认证/外部密码认证/单点登录]

开启了用户认证，并选择此种认证方式：

没有单点登录认证或者单点登录不成功的情况下，用户上网时的认证流程如下：

第一步：浏览器会被重定向到用户名，密码输入页面，要求用户输入正确的用户名密码后才能上网。假设输入的用户名为：test，密码为：password。

第二步：系统尝试从本地用户中查找是否有 test 这个用户，如果存在该用户，并且该用户具有本地密码（也就是用户属性中，勾选了“本地密码”），则检查该用户的本地密码是否为 password，如果密码正确，则认证成功，否则，认证失败。

第三步：如果本地用户不存在 test 用户，或者虽然存在该用户，但该用户并没有设定本地密码。则系统会尝试到外部认证服务器上去检查用户名，密码是否正确。如果用户名密码正确，则认证成功，否则，认证失败。

概括来讲就是先本地认证，再外部认证。

### 3、[必须使用单点登录]

勾选此项时，强制要求策略中指定的地址范围必须使用单点登录才能通过上网认证。

配置步骤：

第一步：对指定的网段设置认证策略为：必须使用单点登录

第二步：在『认证选项』中，开启单点登录，如果是域单点登录的话还需要在域服务器上进行设置（参见章节 3.7.2.2.1）。

通过设置[例外的用户]，排除一部分用户无需使用单点登录认证，通过手动输入用户名，密码的方式完成上网认证。

新用户处理方式：

新用户是指设备中不存在的用户。对于这些新用户，设备会以 IP 或 MAC 地址匹配到『认证策略』，根据『认证策略』→『新用户选项』判断是否自动添加新用户。

通过设备认证的用户可以自动添加。包括：1、『认证策略』选择不需要认证，新用户选择以 IP 地址做为用户名或者以 MAC 地址做为用户名或者以计算机名作为用户名；2、单点登录用户；3、外部密码认证用户。

根据需要管理员可以设置三种新用户处理方式：[添加到指定的本地组中]、[仅作为临时账号，不添加到本地用户列表中]、[不允许新用户认证]。

#### 3.7.2.1.2 选择认证区域

在设置认证策略前，首选需要设置针对哪些区域开启认证。关于区域的设置，

请参考 3.3.1.5 章节。

第一步：勾选【开启用户认证】按钮；



第二步：选择需要认证的区域；



点击确定，即完成认证区域的选择



一般情况下，选择内网口所在的区域作为认证区域即可。定义区域的时候也按内网口，外网口区域定义。例如 ETH2 口为 WAN 口，ETH1 口为非 WAN 口。那么就可以定义 ETH2 口为外网区，ETH1 口为内网区。

### 3.7.2.1.3 新增认证策略

#### 3.7.2.1.3.1 新增认证策略配置案例 1

设置工程部 192.168.1.0/255.255.255.0 网段的计算机结合 LDAP 服务器做第三方密码认证，新用户自动添加到“/工程师”组，同时用户名要和 IP 绑定做双向绑定，即用户名要和 IP 一一对应。内网其他网段的用户不需要认证，以 IP 作为用户名，新用户自动添加到“/默认组”。（此例中以外部服务器 LDAP 为例，其

他类型的外部认证服务器设置步骤类似)

第一步：设置『外部认证服务器』，设置 LDAP 认证服务器(参见章节 3.7.2.3)

第二步：设置『用户认证』→『认证策略』，点击新增，弹出【认证策略】窗口。

在[名称]中填写认证策略的名称，必填项。

在[描述]中填写对策略的描述，补充说明，可选项。

在[策略适用 IP/MAC 范围]中填写 IP、IP 段或者 MAC 地址，这里填写的地  
址是匹配条件，当未通过认证的用户通过设备上网时，设备会根据数据包的 IP  
或 MAC 匹配用户对应的『认证策略』。此例中需要设置：  
192.168.1.0/255.255.255.0。



第三步：设置『认证策略』→『认证方式』，用于设置匹配条件的用户采用  
何种认证方式。

『认证策略』的认证方式有三种选择：[不需要认证/单点登录]、[本地密码  
认证/外部密码认证/单点登录]、[必须使用单点登录]（三种认证方式的说明请参  
见本章概述部分）。

本例中需要做第三方服务器密码认证，所以勾选[本地密码认证/外部密码认  
证/单点登录]。

## 认证策略

### 认证方式

不需要认证/单点登录  
 把IP作为用户名  
 把MAC作为用户名  
 把计算机名字作为用户名  
备注：如果配置了单点登录，则通过单点登录功能识别出该计算机上用户的用户名后，会优先使用该用户名

本地密码认证/外部密码认证/单点登录 [i](#)

备注：密码认证指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。  
[点击配置外部认证服务器](#)

必须使用单点登录 [i](#)

例外的用户：

第四步：设置『认证策略』→『新用户选项』，设置对新用户的处理方式：

## 认证策略

### 新用户选项(新用户指本地不存在的账号)

添加到指定的本地组中  
选择组： [...](#)  
 到外部LDAP上认证的新用户，不添加到选择的本地组，而是自动触发该用户的同步，添加到相应的组中。  
[点击配置LDAP同步策略](#)

添加用户其它属性设置

账号公共属性：[i](#)

允许多人同时使用  
 仅允许一人使用  
 绑定IP/MAC地址：[绑定方式](#)

绑定第一次登录的IP地址，MAC地址不绑定  
 绑定第一次登录的MAC地址，IP地址不绑定  
 绑定第一次登录的IP和MAC地址

仅作为临时账号，不添加到本地用户列表中  
使用该组的上网权限： [...](#)

不允许新用户认证

[提交](#) [取消](#)

勾选[添加到指定的本地组中]表示用户可以自动添加到设备的用户列表中，在[选择组]中选择新加用户需要加入的用户组，用户将自动添加到此组中。此例中将第三方认证自动添加的用户加到/工程师组，所以此处选择“/工程师”。

勾选[到外部 LDAP 上认证的新用户，不添加到选择的本地组，而是自动触发该用户的同步，添加到相应的组中]此项勾选表示用户如果是 LDAP 第三方认证或者是单点登录的用户，并且设备上设置了相关的 LDAP 同步策略，那么此时会根据 LDAP 同步的策略将用户同步过来，并且加入相应的组中，上一步[选择组]则不生效了。

[添加用户其他属性设置]包括[账号公共属性]和[绑定 IP/MAC 地址]

[账号公共属性]可以选择[允许多人同时使用]和[仅允许一人使用]，此选择对认证用户有效，对不需要认证的用户无效。

[绑定 IP/MAC 地址]分两种[绑定方式]：单向绑定和双向绑定。

单向绑定：用户只能使用指定的地址认证，但其它用户也允许使用该地址进行认证。

双向绑定：用户只能使用指定的地址认证，并且指定的地址仅供该用户使用。

此例中需要选择[双向绑定]的绑定方式，并且勾选第一项[绑定第一次登录的 IP 地址，MAC 地址不绑定]。

勾选[仅作为临时账号，不添加到本地用户列表中]表示新用户不添加到用户列表，仅以临时用户的权限进行上网，在[使用该组的上网权限]中选择某个组，则临时用户以选择的指定组的权限进行上网。

勾选[不允许新用户上网]，则不允许添加新用户，不在用户列表中的用户认证不通过，不允许上网，只能使用『用户认证』→『认证选项』→『其他认证选项』中设置的未通过认证用户权限。

第五步：如果需要手动新增用户，如下图设置：[登录名]填写外部认证服务器上对应的用户名；此处不需要勾选[本地密码]，因为勾选本地密码后，此用户就拥有本地密码认证的属性，用户认证时不再到外部服务器上认证；勾选[绑定IP/MAC地址]设置需要绑定的IP地址。



第六步：设置其他网段用户的认证策略：

需求：内网其他网段的用户不需要认证，以 IP 作为用户名，新用户自动添

加到“/默认组”。

编辑『认证策略』中的『默认策略』：

『认证方式』：勾选[不需要认证/单点登录]中的[以 IP 作为用户名]

**认证策略**

名称：	默认策略
描述：	默认策略
策略适用 IP/MAC范 围：	<input type="button" value="i"/> 0.0.0.0-255.255.255.255

**认证方式**

不需要认证/单点登录

把IP作为用户名

把MAC作为用户名

把计算机名字作为用户名

备注：如果配置了单点登录，则通过单点登录功能识别出该计算机上用户的用户名后，会优先使用该用户名

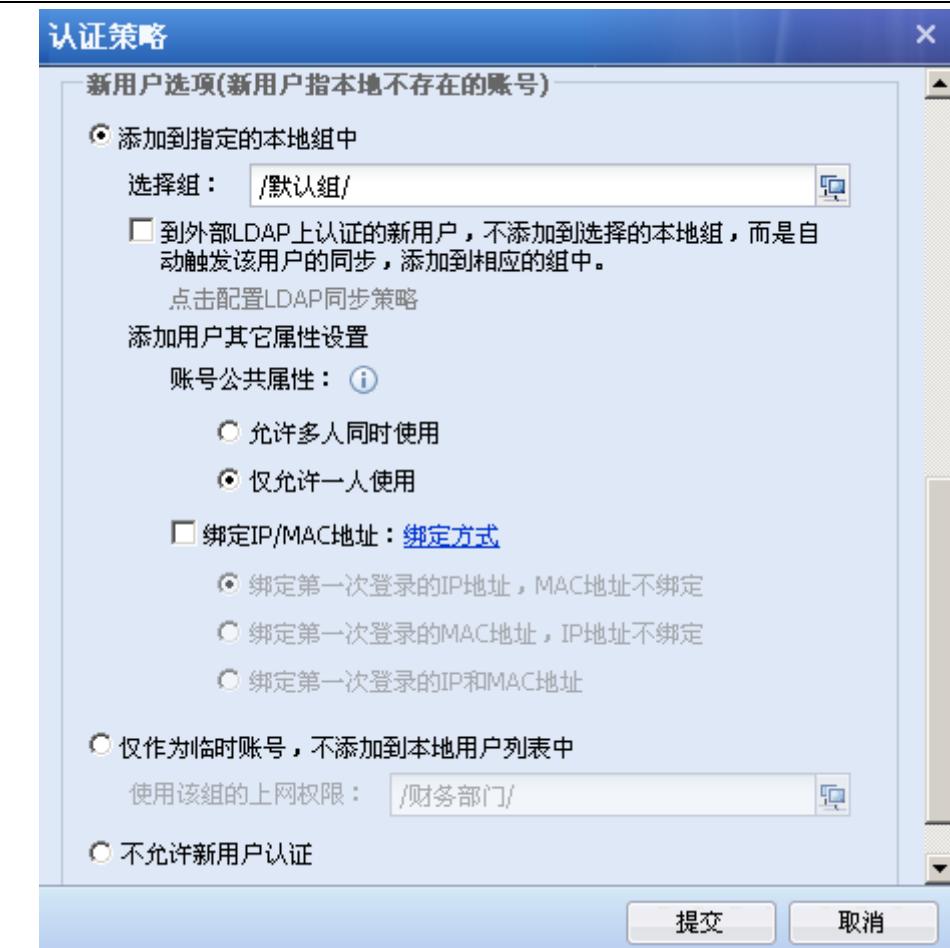
本地密码认证/外部密码认证/单点登录

备注：密码认证指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。  
[点击配置外部认证服务器](#)

必须使用单点登录

例外的用户：

『新用户选项』：勾选[添加到指定的本地组中]，并选择“/默认组/”。



认证策略是从上往下匹配的，所以本例中设置的两条认证策略，设置顺序应如下图所示：

认证策略						
<input checked="" type="checkbox"/> 开启用户认证 认证区域: 内网区						
<a href="#">新增</a> <a href="#">批量编辑</a>   <a href="#">删除</a>   <a href="#">上移</a> <a href="#">下移</a> <a href="#">刷新</a>   <a href="#">导入</a> <a href="#">导出</a>						
序号	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移
1	内网认证策略	192.168.1.0/255.255.255.0	密码认证	添加到组: /工程师/		<a href="#">↑</a> <a href="#">↓</a> <a href="#">X</a>
2	默认策略	0.0.0.0~255.255.255.255	不需要认证(把IP作为用户名)	添加到组: /默认组/	默认策略	<a href="#">↑</a> <a href="#">↓</a> <a href="#">X</a>

### 3.7.2.1.3.2 新增认证策略配置案例 2

内网 IP 范围为 192.168.2.1-192.168.2.255 的计算机，自动以新用户添加，认证方式是不需要认证，以计算机名作为用户名并双向绑定 MAC 地址，新用户自动添加到“/市场部门”组。

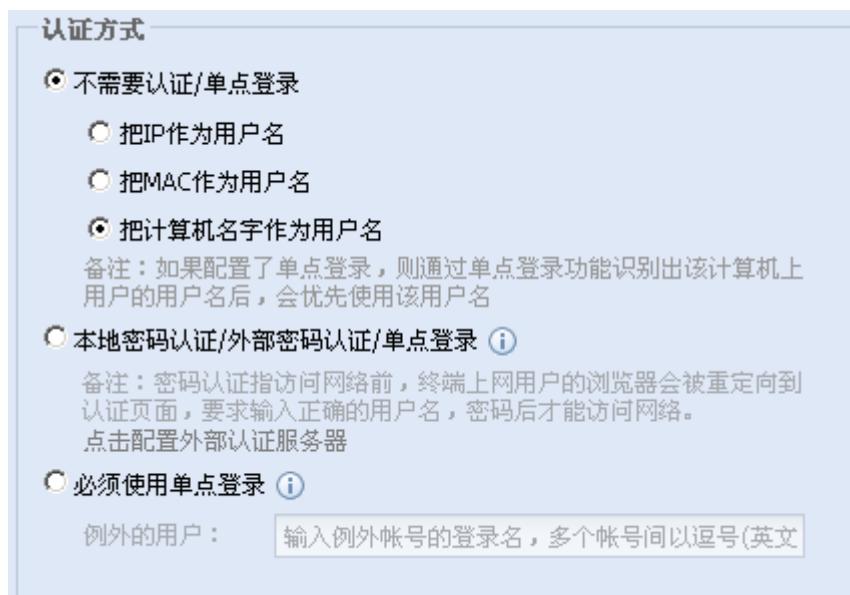
第一步：在『用户认证』→『认证选项』→『跨三层 MAC 识别』中设置 SNMP

跨三层获取 MAC 的选项。（参见章节 3.7.2.2.4）

第二步：在【认证策略】窗口中，点击新增按钮。进入【认证策略】的新增窗口。填写上名称描述。



第三步：『认证方式』选择[不需要认证/单点登录]，勾选[把计算机名字作为用户名]。



第四步：[新用户选项]中，勾选[添加到指定的本地组中]并选择用户组“/市场部门/”。

勾选[绑定 IP/MAC 地址] 和[绑定第一次登录的 MAC 地址，IP 不绑定]，此例中因为内网是跨三层的，所以需要通过 SNMP 协议从交换机上获取到 MAC 地址，在『用户认证』→『认证选项』→『跨三层 MAC 识别』中设置。

新用户选项(新用户指本地不存在的账号)

添加到指定的本地组中

选择组： /市场部门/

到外部LDAP上认证的新用户，不添加到选择的本地组，而是自动触发该用户的同步，添加到相应的组中。  
[点击配置LDAP同步策略](#)

添加用户其它属性设置

账号公共属性：[i](#)

允许多人同时使用  
 仅允许一人使用

绑定IP/MAC地址：[绑定方式](#)

绑定第一次登录的IP地址，MAC地址不绑定  
 绑定第一次登录的MAC地址，IP地址不绑定  
 绑定第一次登录的IP和MAC地址

仅作为临时账号，不添加到本地用户列表中

使用该组的上网权限：

不允许新用户认证

第五步：点击提交按钮，完成策略编辑。

认证策略						
<input checked="" type="checkbox"/> 启用用户认证 认证区域：内网区						
<a href="#">新增</a> <a href="#">批量编辑</a> <a href="#">删除</a> <a href="#">上移</a> <a href="#">下移</a> <a href="#">刷新</a> <a href="#">导入</a> <a href="#">示例文件</a>						
...	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移
<input type="checkbox"/>	1 市场部	192.168.2.1-192.168.2.255	不需要认证(把计算机名作为用户)	添加到组：/市场部/ 市场部认证策略		
<input type="checkbox"/>	2 网段认证策略	192.168.1.0/255.255.255.0	密码认证	添加到组：/工程师/		
<input type="checkbox"/>	3 默认策略	0.0.0.0-255.255.255.255	不需要认证(把IP作为用户)	添加到组：/默认组/ 默认策略		



1、设备是通过 NETBIOS 协议来获取上网计算机的计算机名，可能会出现获取不到计算机名的情况，遇到这种情况请查看一下几点：计算机上是否开启了 NETBIOS 协议；计算机上是否配置了多 IP；计算机上是否有防火墙过滤了 NETBIOS 协议；网络路径中是否有设备做了 NETBIOS 协议的过滤。如果获取不到计算机名，则系统会把该计算机当成临时用户，用户名为：Unknown Computer，且只会在在线用户列表中查找到，不会加到指定的本地组中。

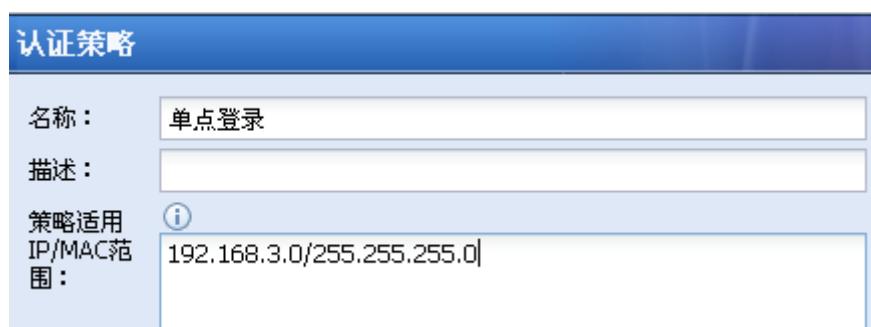
2、如果上网用户的计算机到设备间，穿越了一台/多台三层交换设备，则因为上网用户的计算机源 MAC 地址已经被改变，因此无法获取到真正的源 MAC 地址，此种情况下，可以有以下方式识别出真正的源 MAC 地址。方法：通过 SNMP 协议，获取离上网计算机最近的三层交换机（也就是上网计算机指向的网关设备）的 ARP 表，以获得某个 IP 地址上真正的源 MAC 地址。

### 3.7.2.1.3.3 新增认证策略配置案例 3

内网网段 192.168.3.0/255.255.255.0 的计算机使用 AD 域单点登录进行认证，即用户在登录系统通过 AD 域认证时，同时通过设备的认证，AD 域中的用户可以同步到设备上。要求如果这个网段的计算机单点登录失败或者是没有登录域的时候，以 IP 地址做用户名，不需要认证上网，并自动添加“/默认组”。

第一步：设置『外部认证服务器』和『LDAP 自动同步』（参见章节 3.7.2.3 和 3.7.1.6）

第二步：在【认证策略】窗口中，点击新增按钮。进入【认证策略】的新增窗口。填写上名称描述。



第三步：『认证方式』选择[不需要认证/单点登录]，勾选[把 IP 作为用户名]。

**认证方式**

不需要认证/单点登录

把IP作为用户名

把MAC作为用户名

把计算机名字作为用户名

备注：如果配置了单点登录，则通过单点登录功能识别出该计算机上用户的用户名后，会优先使用该用户名

本地密码认证/外部密码认证/单点登录 i

备注：密码认证指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。  
点击配置外部认证服务器

必须使用单点登录 i

例外的用户：

第四步：[新用户选项]中，勾选[添加到指定的本地组中]并选择用户组“/默认组/”，此时未做单点登录的用户会添加到默认组，使用默认组的上网策略。

勾选[到外部 LDAP 上认证的新用户，不添加到选择的本地组，而是自动触发该用户的同步，添加到相应的组中]，使域单点登录的用户添加到同步规则中设置的组。

注意此处不能设置[绑定 IP/MAC 地址]进行双向绑定，因为未做单点登录的用户自动添加新用户并双向绑定 IP/MAC 后，此 IP/MAC 只能给此用户使用，不能再使用单点登录认证了。设置单向绑定没有问题。

新用户选项(新用户指本地不存在的账号)

添加到指定的本地组中

选择组： /默认组/

到外部LDAP上认证的新用户，不添加到选择的本地组，而是自动触发该用户的同步，添加到相应的组中。  
[点击配置LDAP同步策略](#)

添加用户其它属性设置

账号公共属性：[i](#)

允许多人同时使用  
 仅允许一人使用

绑定IP/MAC地址：[绑定方式](#)

绑定第一次登录的IP地址，MAC地址不绑定  
 绑定第一次登录的MAC地址，IP地址不绑定  
 绑定第一次登录的IP和MAC地址

仅作为临时账号，不添加到本地用户列表中

使用该组的上网权限：

不允许新用户认证

第五步：点击提交按钮，完成策略编辑。

认证策略							
<input checked="" type="checkbox"/> 开启用户认证 认证区域：内网区							
<a href="#">新增</a> <a href="#">批量编辑</a> <a href="#">删除</a> <a href="#">上移</a> <a href="#">下移</a> <a href="#">刷新</a> <a href="#">导入</a> <a href="#">示例文件</a>							
...	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...
<input type="checkbox"/>	1 单点登录	192.168.3.0/255.255.255.0	不需要认证 (把IP作为用户)	添加到组：/默认组/			
<input type="checkbox"/>	2 市场部	192.168.2.1-192.168.2.255	不需要认证 (把计算机名作为用户)	添加到组：/市场部/ 市场部认证策略			
<input type="checkbox"/>	3 1网投认证策略	192.168.1.0/255.255.255.0	密码认证	添加到组：/工程师/			
<input type="checkbox"/>	4 默认策略	0.0.0.0-255.255.255.255	不需要认证 (把IP作为用户)	添加到组：/默认组/ 默认策略			

### 3.7.2.1.4 删除认证策略

举例：删除新用户认证策略 test。

第一步：选择策略 test。

认证策略

开启用户认证

认证区域: 内网区

+ 新增 | 批量编辑 |  删除 |   | 刷新 | 导入 | 云例文件

名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...
1 单点登录	192.168.3.0/255.255.255.0	不需要认证(把IP作为用户名)	添加到组: /默...		<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	
2 市场部	192.168.2.1-192.168.2.255	不需要认证(把计算机名作为用户名)	添加到组: /市...	市场部认证策略	<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	
3 1网段认证策略	192.168.1.0/255.255.255.0	密码认证	添加到组: /工...		<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	
4 默认策略	0.0.0.0-255.255.255.255	不需要认证(把IP作为用户名)	添加到组: /默...	默认策略	<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	

第二步：点击**删除**，并且进行操作确认。完成策略删除。

信息  
操作成功  
删除策略: 单点登录 成功！

### 3.7.2.1.5 批量编辑认证策略

批量编辑认证策略，可以对除了对[名称]、[描述]外的所有属性进行批量编辑。

举例：把市场部，1网段用户的认证方式改为不需要认证，新用户认证选项都改为以计算机名作为新用户。

第一步：勾选上“市场部”，“1网段认证策略”两个认证策略。

认证策略

开启用户认证

认证区域: 内网区

+ 新增 | 批量编辑 |  删除 |   | 刷新 | 导入 | 云例文件

名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...
1 单点登录	192.168.3.0/255.255.255.0	不需要认证(把IP作为用户名)	添加到组: /默...		<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	
2 市场部	192.168.2.1-192.168.2.255	不需要认证(把计算机名作为用户名)	添加到组: /市...	市场部认证策略	<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	
3 1网段认证策略	192.168.1.0/255.255.255.0	密码认证	添加到组: /工...		<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	
4 默认策略	0.0.0.0-255.255.255.255	不需要认证(把IP作为用户名)	添加到组: /默...	默认策略	<input type="button" value="上移"/> <input type="button" value="下移"/> <input type="button" value="删除"/>	

第二步：，点击**批量编辑**，进入批量编辑页面。勾选上[认证方式]，选择[不需要认证]，接着选择[把计算机名作为用户名]。

**批量编辑认证策略**

名称： 市场部,1网段认证策略

认证方式

不需要认证/单点登录

把IP作为用户名

把MAC作为用户名

把计算机名字作为用户名

备注：如果配置了单点登录，则通过单点登录功能识别出该计算机上的用户名后，会优先使用该用户名

本地密码认证/外部密码认证/单点登录 i

备注：密码认证指访问网络前，终端上网用户的浏览器会被重定向到认证页面，要求输入正确的用户名，密码后才能访问网络。  
点击配置外部认证服务器

必须使用单点登录 i

例外的用户：

新用户选项(新用户指本地不存在的账号)

添加到指定的本地组中

选择组：

**提交** **取消**

第三步：点击**提交**按钮，完成批量编辑。

**认证策略**

开启用户认证

认证区域：内网区

**+ 新增** **批量编辑** **删除** **上移** **下移** **刷新** **导入** **示例文件**

	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...
<input type="checkbox"/>	1 单点登录	192.168.3.0/255.255.255.0	不需要认证(把IP作为用户名)	添加到组: /默...		<span style="color: green;">↑</span> <span style="color: red;">↓</span> <span style="color: red;">X</span>	
<input type="checkbox"/>	2 市场部	192.168.2.1~192.168.2.255	不需要认证(把计算机名作为用户名)	添加到组: /市...	市场部认证策略	<span style="color: green;">↑</span> <span style="color: red;">↓</span> <span style="color: red;">X</span>	
<input type="checkbox"/>	3 1网段认证策略	192.168.1.0/255.255.255.0	不需要认证(把计算机名作为用户名)	添加到组: /工...		<span style="color: green;">↑</span> <span style="color: red;">↓</span> <span style="color: red;">X</span>	
<input type="checkbox"/>	4 默认策略	0.0.0.0~255.255.255.255	不需要认证(把IP作为用户名)	添加到组: /默...	默认策略	<span style="color: green;">↑</span> <span style="color: red;">↓</span> <span style="color: red;">X</span>	



批量编辑时，如果只勾选上[认证方式]进行编辑。则批量编辑后，原来策略中[新用户选项]的相关策略不会变化，仍然是原来的策略。相反，只编辑[新用户选项]，批量编辑后，[认证方式]不会变化。

### 3.7.2.1.6 认证策略优先级调整

认证策略的优先级别与上网策略一样，也是从上往下进行匹配，序号越低的优先级越高。用户认证时，从上往下进行匹配。一旦 IP 或 MAC 符合该策略，则执行该策略的认证方式。

如下，“市场部小组一”策略的条件为 192.168.2.1-192.168.2.10，而“市场部”策略的条件 192.168.2.1-192.168.2.255。很明显“市场部”条件包含了“市场部小组一”，会导致 192.168.2.1-192.168.2.10 的用户匹配到“市场部”的认证策略。

认证策略								
<input checked="" type="checkbox"/> 开启用户认证								
认证区域: 内网区								
	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...	
<input type="checkbox"/>	1 市场部	192.168.2.1-192.168.2.255	不需要认证(…)	添加到组: /市场部/				
<input type="checkbox"/>	2 市场部小组一	192.168.2.1-192.168.2.10	不需要认证(…)	添加到组: /市场部/市场部小组一/				
<input type="checkbox"/>	3 工程部	192.168.3.0/255.255.255.0	不需要认证(…)	添加到组: /				
<input type="checkbox"/>	4 网络部	192.168.1.1-192.168.1.255	不需要认证(…)	添加到组: /网络部/				
<input type="checkbox"/>	5 默认策略	0.0.0.0-255.255.255.255	不需要认证(…)	添加到组: /默认组/	默认策略			

勾选“市场部小组一”策略，点击上移，向上移动到“市场部”策略上面，让“市场部小组一”策略优先级别更高，192.168.2.1-192.168.2.10 的用户可以优先认证到“市场部小组一”的策略。

认证策略								
<input checked="" type="checkbox"/> 开启用户认证								
认证区域: 内网区								
	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...	
<input checked="" type="checkbox"/>	1 市场部小组一	192.168.2.1-192.168.2.10	不需要认证(…)	添加到组: /市场部/市场部小组一/				
<input type="checkbox"/>	2 市场部	192.168.2.1-192.168.2.255	不需要认证(…)	添加到组: /市场部/				
<input type="checkbox"/>	3 工程部	192.168.3.0/255.255.255.0	不需要认证(…)	添加到组: /				
<input type="checkbox"/>	4 网络部	192.168.1.1-192.168.1.255	不需要认证(…)	添加到组: /网络部/				
<input type="checkbox"/>	5 默认策略	0.0.0.0-255.255.255.255	不需要认证(…)	添加到组: /默认组/	默认策略			

### 3.7.2.1.7 导入认证策略

『认证策略』较多的情况下，可以通过导入 CSV 表的方式将『认证策略』统

一导入，如下图所示：导入文件的格式可以通过点击**示例文件**，按照示例文件的格式编辑『认证策略』。

认证策略								
<input checked="" type="checkbox"/> 开启用户认证 <b>认证区域:</b> 内网区								
	名称	IP/MAC	认证方式	新用户选项	描述	上移/下移	...	
<input checked="" type="checkbox"/>	1 市场部小组一	192.168.2.1-192.168.2.10	不需要认证(...	添加到组: /市场部/市场部小组一/				
<input type="checkbox"/>	2 市场部	192.168.2.1-192.168.2.255	不需要认证(...	添加到组: /市场部/				
<input type="checkbox"/>	3 工程部	192.168.3.0/255.255.255.0	不需要认证(...	添加到组: /				
<input type="checkbox"/>	4 网络部	192.168.1.1-192.168.1.255	不需要认证(...	添加到组: /网络部/				
<input type="checkbox"/>	5 默认策略	0.0.0.0-255.255.255.255	不需要认证(...	添加到组: /默认组/	默认策略			

示例文件：

A	B	C	D	E	F	G	H	I	J	K	L
1	#IP段/MAC地址（不允许留空，多个条目间用英文逗号分隔，支持如下所列的格式：单个IP地址，如：“200.200.0.1”；IP范围，格式为“起始IP-结束IP”）										
2	#认证方式（取值范围：IP认证、密码认证，留空代表：IP认证）										
3	#新用户选项（取值范围：添加到本地列表、不允许上网、临时账号，留空代表：添加到本地列表）										
4	策略名称 策略描述 IP段/MAC地址	认证方式	新用户选项	组							
5	policy1 policy1 200.200.20.0-200.2 IP认证	临时账号	/								
6	policy1.ipolicy1.1200.200.20.24 IP认证	临时账号	/								
7	policy1.ipolicy1.2200.200.20.126-200 IP认证	临时账号									
8	policy2 policy2 00-1C-F1-09-50-1A 不允许上网	/默认组									
9	policy2.ipolicy2.1200.200.20.245,200.200.20.5 不允许上网	默认组/									
10	policy3 policy3 200.200.20.0/255.2 密码认证	默认组									
11	policy4 policy4 00-1C-F1-09-69-1A, 密码认证 添加到本地列表	/									
12	policy5 policy5 00-1c-f1-09-69-1b 密码认证 添加到本地列表	/									

根据示例文件编辑好需要导入的策略文件后，点击**导入**，选择需要导入的文件导入即可。

### 3.7.2.2. 认证选项

『认证选项设置』主要是用来设置设备上用户认证的相关配置信息，包括『单点登录选项』、『认证通过跳转』、『认证冲突』、『跨三层 MAC 识别』『其他认证选项』。

#### 3.7.2.2.1 单点登录选项

当客户有自己的第三方认证服务器对内网用户进行认证时，单点登录可以实现在内网用户通过第三方认证服务器认证时同时通过设备的认证，并且获取到相关的权限上网。设备上使用和第三方认证服务器同一套用户名密码。目前设备支

持的单点登录类型包括：AD 域单点登录、Proxy 单点登录、POP3 单点登录和 Web 单点登录。此处设置的是只是实现单点登录的基本方法，完成单点登录的配置还需要配置用户、认证服务器以及用户的认证方式，分别在『用户管理』、『外部认证服务器』、『认证策略』中设置（参见章节 3.7.1.、3.7.2.3、3.7.2.1）。

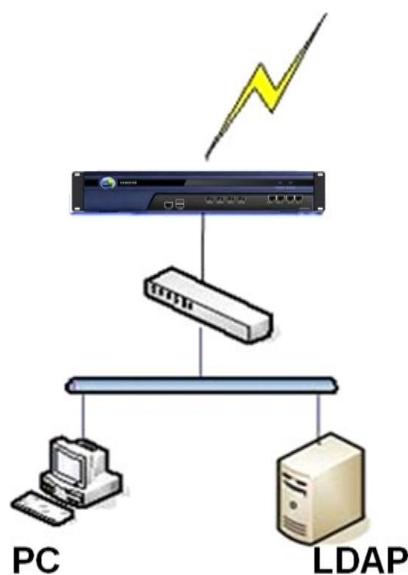
### 3.7.2.2.1.1 域单点登录

如果客户的网络中已有一台微软 AD 域服务器做用户管理，并且客户内网用户登录计算机系统都是使用域账号登录的，那么可以采用域单点登录的方式，在内网用户登录到域之后就通过设备的认证，即终端用户登陆域即可上网，无需通过设备再次认证。域单点登录可以采用域脚本下发或监听登录域的数据包两种方式实现。域单点登录只适用于微软 AD 域（MS Active Directory）。

#### 3.7.2.2.1.1.1 域脚本下发模式配置：

通过配置域服务器登录（logon.exe）和注销（logoff.exe）脚本，在用户登陆或注销域时通过下发的域策略执行登录或注销脚本，执行脚本的同时完成用户在设备上的登录和注销。

如图所示：



数据流的过程大致如下：

1、PC 请求登陆域

2、域返回成功登陆信息给 PC

3、PC 运行 logon.exe 并上报 成功登陆域的信息给设备

设置方法：

第一步：设置认证 AD 域服务，点击进入『用户认证』→『认证选项』→『外部认证服务器』进行设置（参见章节 3.7.2.3）

第二步：在设备上启用单点登录，选择单点登录模式并设置共享密钥。点击进入『用户认证』→『认证选项』→『单点登录选项』→『域单点登录』编辑页面。

勾选[启用单点登录]启用域单点登录功能；

勾选[通过域自动下发。执行指定的登录脚本，获取登录信息]，表示使用域脚本下发模式实现单点登录。在[请输入共享密钥]中输入共享密钥，如下图所示：



共享密钥用于 AD 域服务器和设备的加密通讯，需要在登录脚本中设置相同的共享密钥。在[域单点登录程序]处[点击此处下载](#)按钮用于下载登录注销脚本，下载脚本用于第三四步的设置。



1、此处支持 AC11.0R2 及以上版本，同步认证信息到 AF，端口为 1775。

第三步：在 AD 域服务器上配置登录脚本程序。

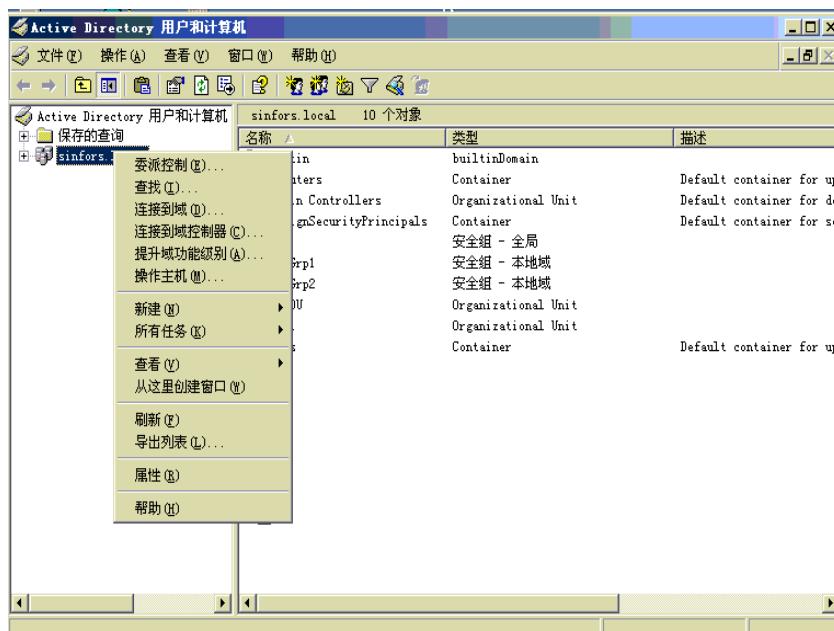
1. 登陆域服务器后，打开“管理您的服务器”菜单，如下图：



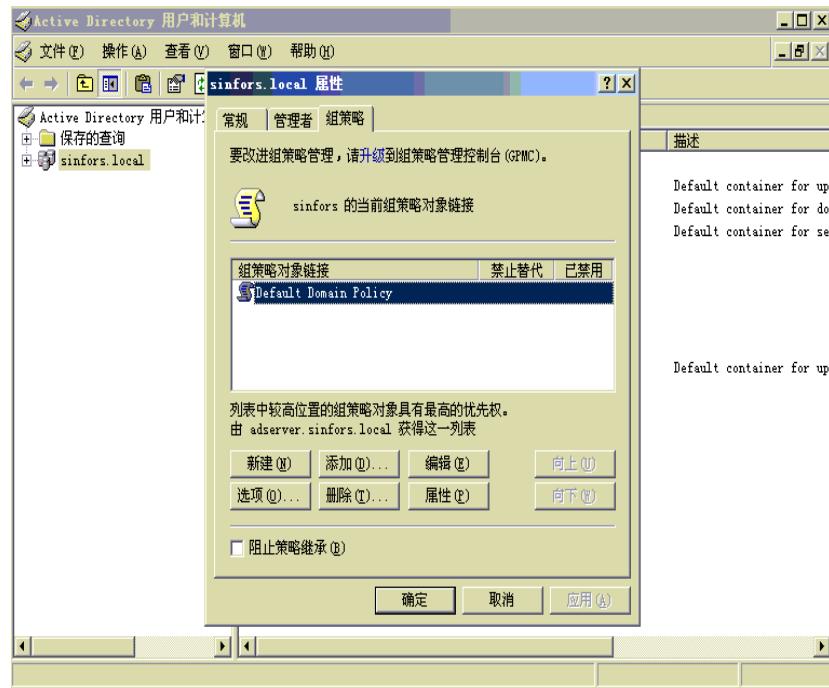
2. 选择“管理 Active Directory 中的用户和计算机”选项，如图：



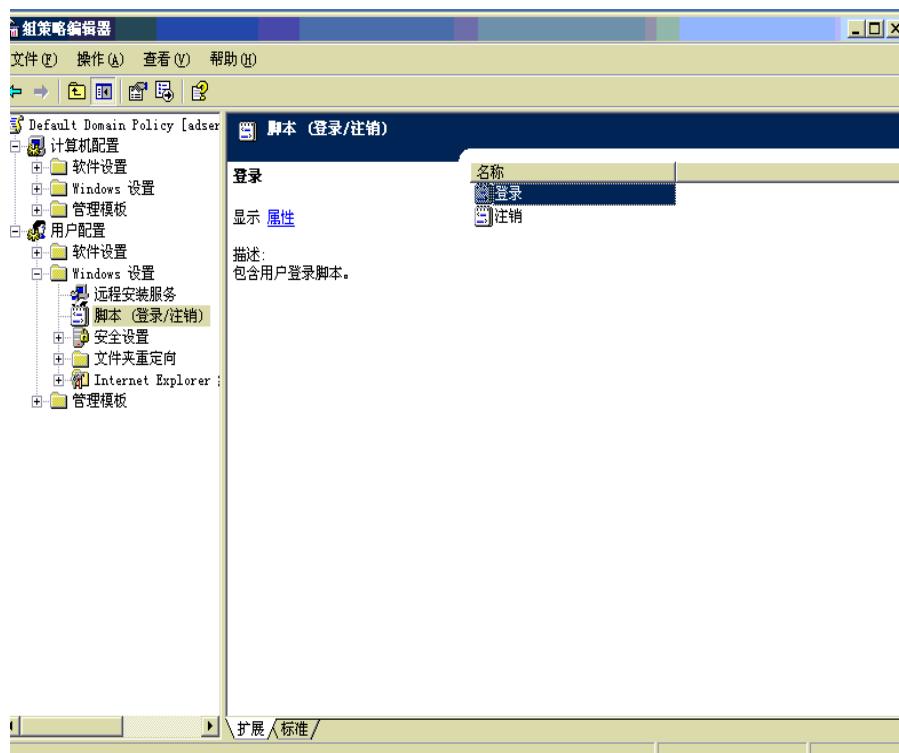
3.在弹出的窗口中右键所要监控的域，选择属性：



4.在弹出的窗口中，点击组策略选项，在组策略窗口中，双击其中的组策略“Default Domain Policy”

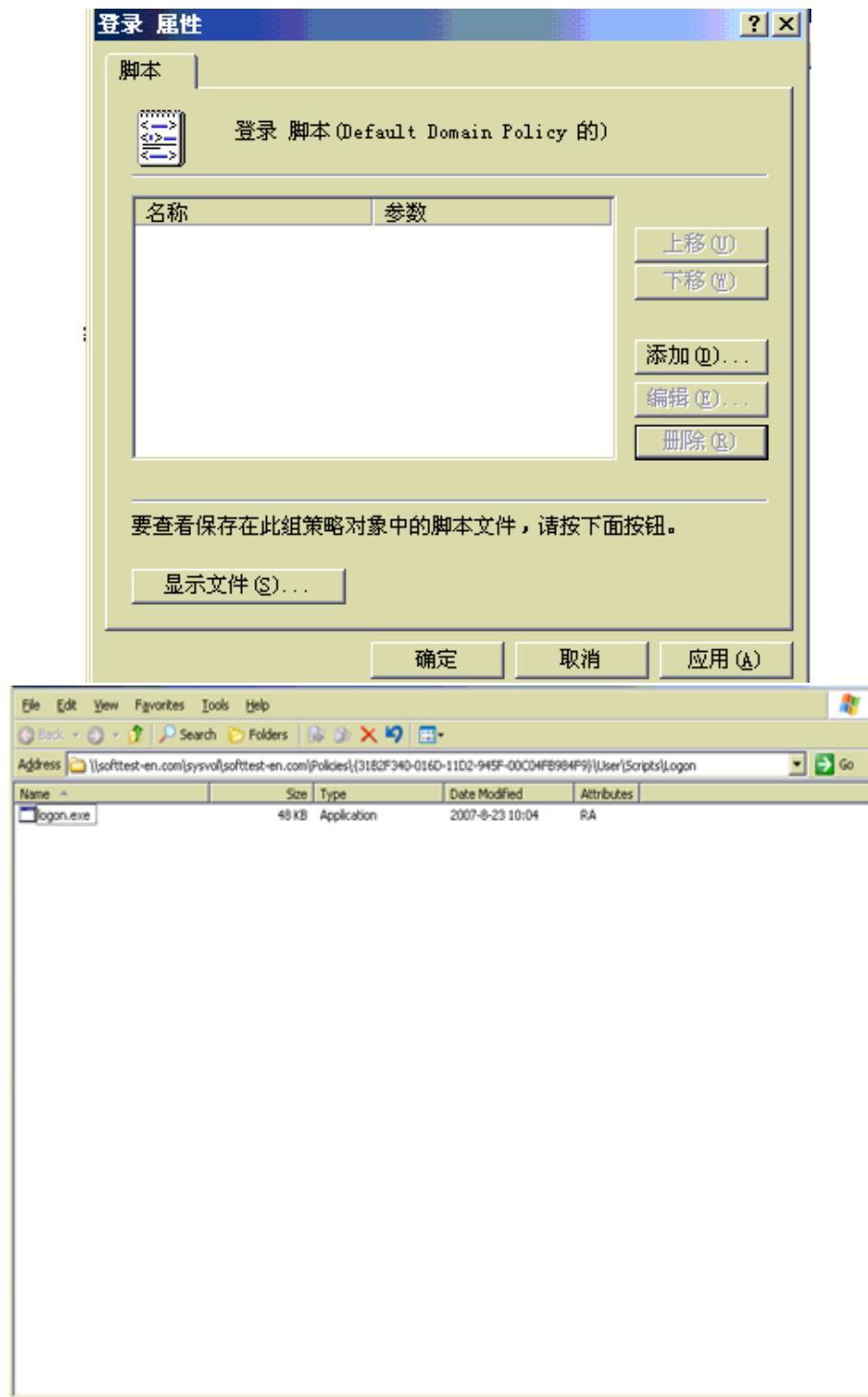


5.在弹出的组策略编辑器中依次点击“用户配置-Windows 设置-脚本(登录/注销)”



6.双击右边的“登录”选项，在弹出的登陆脚本编辑窗口左下脚点击“显示文

件”，将打开一个目录然后将登陆脚本文件保存在该目录下，关闭该目录。



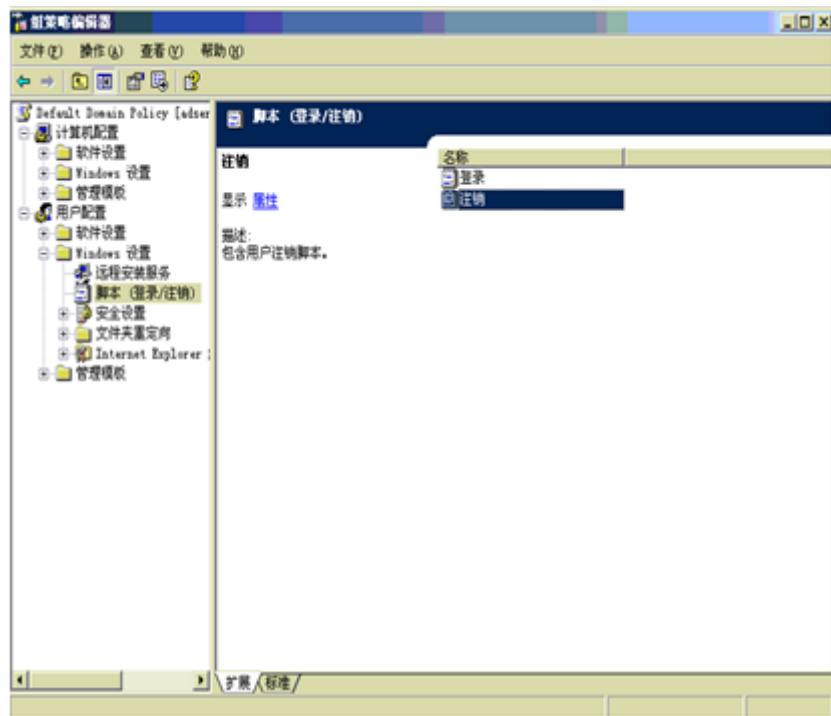
7.在弹出的登陆脚本编辑窗口中单击添加按钮，在添加脚本窗口中，点击浏览，选择保存的登陆脚本文件(即 logon.exe)，并在脚本参数中输入 IP(IP 是属于设备端的 IP)，端口号(固定是 1775)，密钥(必须与设备端设置的密码一致)。注意

每个参数以空格分隔，后点击应用后点击确定，依次关闭所有组策略属性页面布局。

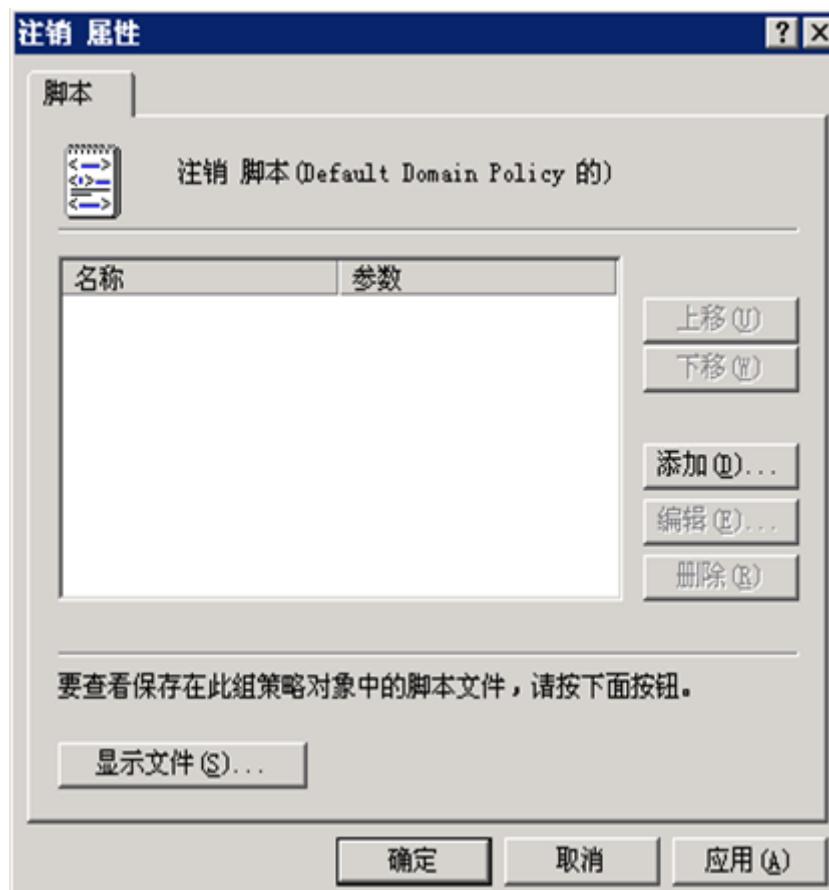


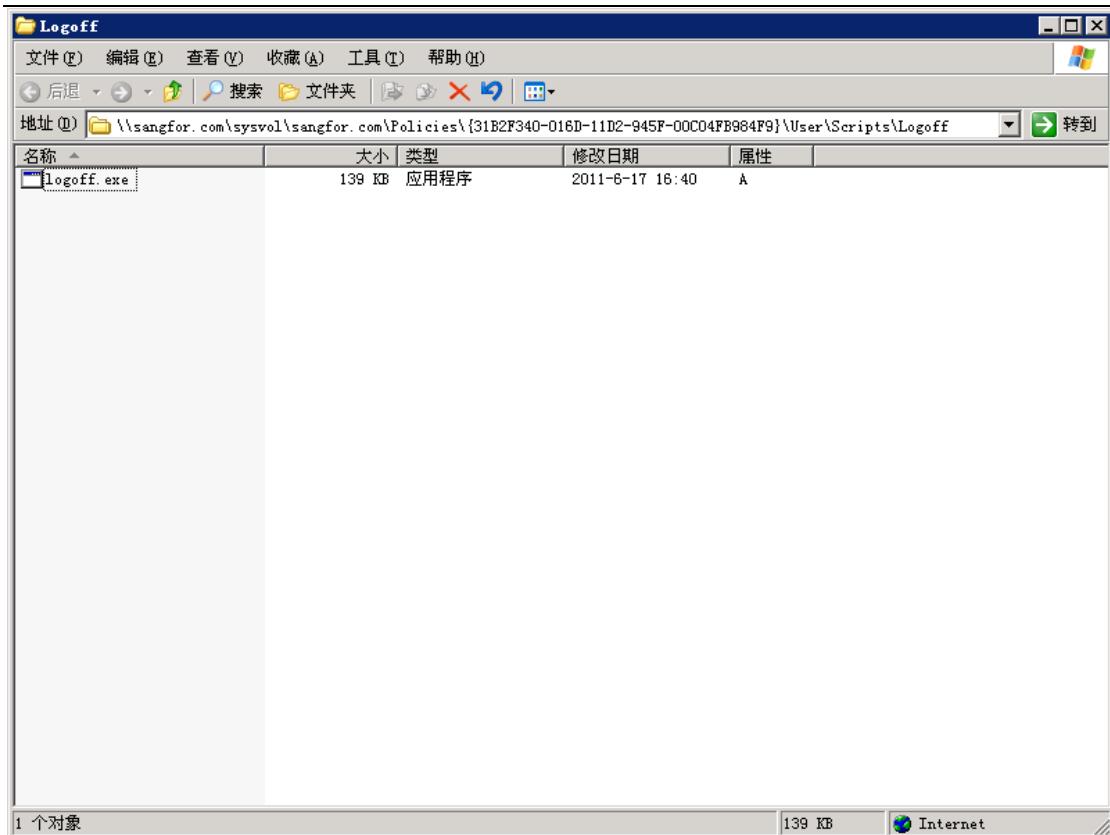
第四步：在 LDAP 上配置注销脚本程序。设置注销脚本的目的是在用户注销域的时候同时注销在设备上的登录账号。

#### 1. 依次操作配置登陆脚本程序的步骤，在第六步时双击“注销”选项

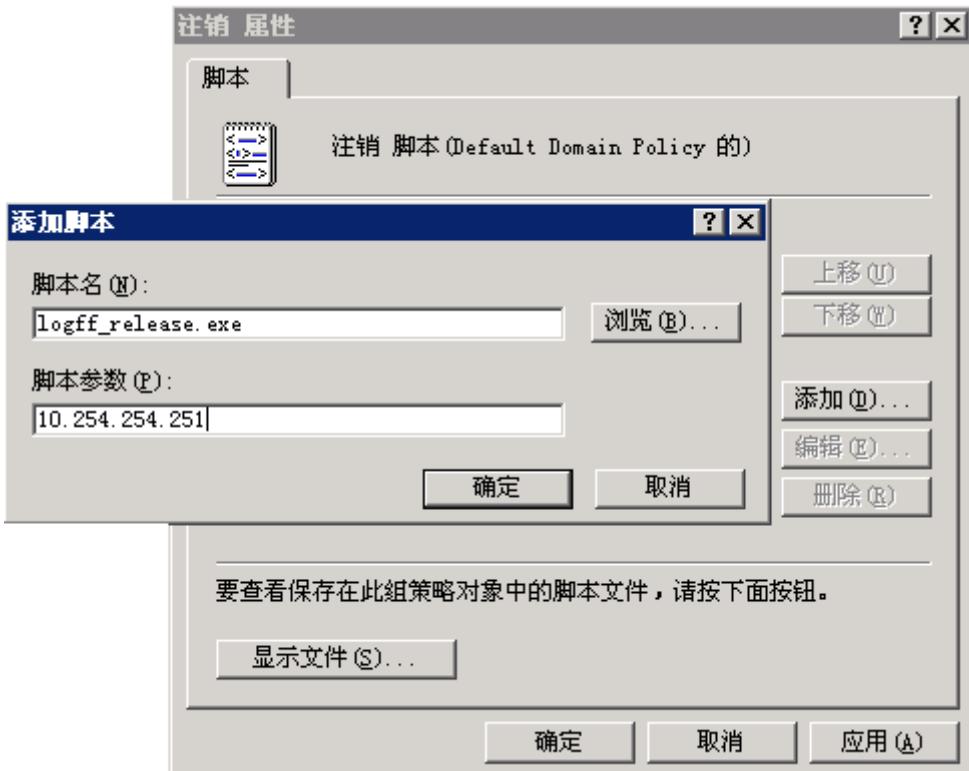


2.在弹出的注销脚本编辑窗口左下脚点击“显示文件”(在此为 Show File)，将打开一个目录然后将注销脚本(即 logoff.exe)文件保存在该目录下，关闭该目录。





3.在弹出的注销脚本编辑窗口中单击添加按钮，在添加脚本窗口中，点击浏览，选择保存的AD注销脚本文件（即 logff.exe），并在脚本参数中输入在配置登陆脚本参数时输入的AF的IP，依次关闭所有的组策略属性页面布局。



4.配置完脚本后，依次点击桌面左下角的“开始”，点击“运行”，在弹出的运行窗口中输入：“gpupdate”并点击确定，生效配置完的组策略。

第五步：设置认证策略，根据需要使用单点登录的用户的 IP 或 MAC 设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节 3.7.2.1.3）。

第六步：用 PC 登录域，登录域成功后即可上网。



1、要求用户 PC 的第一 DNS 填写为域服务器的 IP 地址，否则会因无法解析域的 IP 而导致登录不了域服务器。

2、如果第一次用户登录域成功后，修改了 DNS 或者 IP 地址，此时可以用正确的密码登陆到域，可以进入 windows，但实际上没有登录到域，此时单点登录无效，用户上网时仍会弹出认证框要求输入用户名和密码，这个主要是因为 windows 可以记住上次输入的正确密码，没有登录到域也可以进入 windows。

### 3、要求域服务器 IP，设备 IP 以及用户 PC 能够相互通信。

### 4、AF 和与服务器通信使用的是 1775 端口

#### 3.7.2.2.1.1.2 域监控单点登录配置：

通过 AF 设备本身的程序自动获取登录信息：AF 设备内置一个单点登录客户端程序 ADSSO。启用这种方式时，程序会定时从域服务器上获取 PC 登录域成功的状态，并将获取的信息上报 AF 设备来实现单点登录。

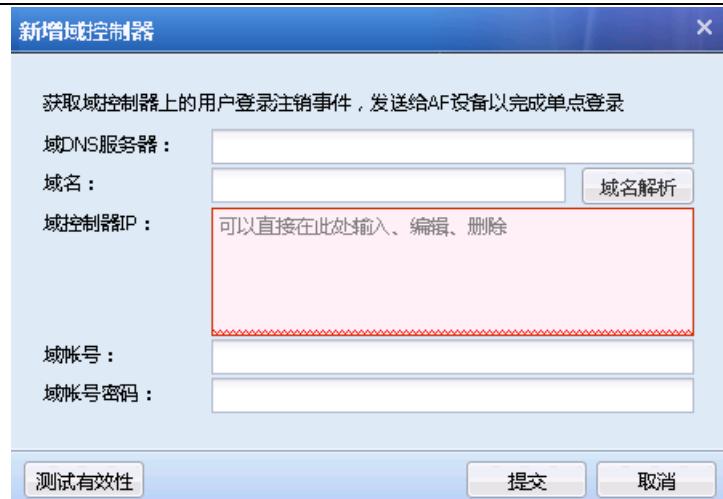
AF 上需要做的单点登录配置：

勾选[启用域单点登录]

勾选[域监控单点登录]



点击新增，添加域服务器：



[域 DNS 服务器]: 填写域 DNS 服务器和域名，域 DNS 服务器要能解析域名，点击域名解析按钮，可自动解析出所有的域控制器的 IP 地址。

[域名]: 填写域服务器对应的域名

[域控制器 IP]: 填写域服务器对应的 IP 地址

[域账号]: 填写具有域管理员权限的账号（本身是管理员，或者加入管理员组）

[域账号密码]: 填写对应域账号的密码

点击**测试有效性**，提示域控制器测试的结果。

点击**提交**，保存配置。

### 3.7.2.2.1.1.3 集成 windows 身份验证配置：

[集成 windows 身份验证]: 简称 IWA 认证，是在 windows 域环境下普遍支持的一种认证方式。通过这种方式实现的单点登录，需要先将 AF 设备和内网电脑都加入到域，当内网电脑打开网页时会自动访问 AF 并提交身份凭证，从而实

现单点登录。

AF 上需要做的单点登录配置：

勾选[启用域单点登录]

勾选[启用集成 windows 身份验证]



启用集成windows身份验证 [帮助文档](#)

计算机名：

域名：

域DNS服务器：

域帐号：

任意可以加入域的域帐户，例如：Administrator

域帐号密码： 测试有效性

高级选项： [配置...](#)

[计算机名]: 设置 AF 设备加入域的计算机名，后四位固定为网关序号的后四位，前面的字段可以用户自己定义，只支持字母，数字以及连接符“-”，最多支持 10 个字节。

[域名]: 设置 AF 需要加入域的域名。

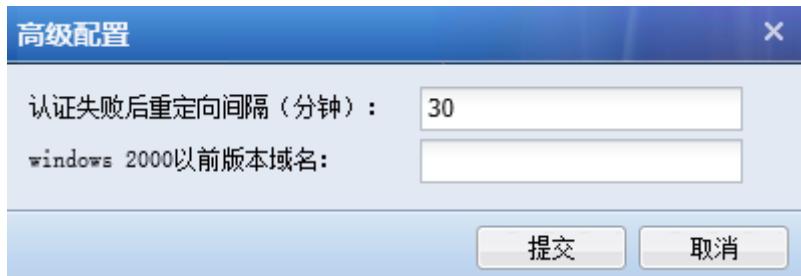
[域 DNS 服务器]: 设置域对应的 DNS 服务器 IP 地址。

[域账号]: 设置 AF 加入域时使用的域账号。

[域账号密码]: 设置域账号密码。

点击[测试有效性](#)，检测各个参数是否有效，测试通过后点击[提交](#)。

高级选项：



[认证失败后的重定向间隔]: 设置 IWA 单点登录失败后隔多久再做重定向，重新认证

[windows 2000 以前版本域名]: 如果域服务器是 windows server 2000 以前的版本，还需要在这里设置下域名。



1、在域上使域账户过期或者禁用，已登录的 PC 还是可以 kerberos 认证成功攻击展示 UI 优化

2、手机代理上网不支持 iwa 认证(启用 iwa 认证后，手机设置代理不会弹认

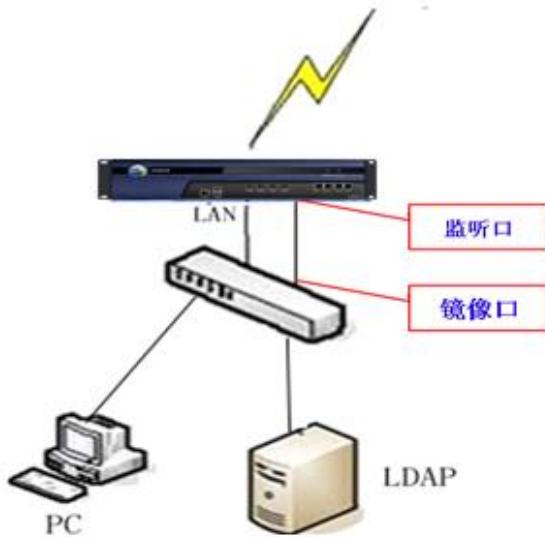
3、kerberos 认证不会踢密码认证的用户

4、含有`~!#\$%^&\*+|\{};：“‘，/,<>?等特殊字符的域账号登陆时，不支持认

#### 3.7.2.2.1.1.4 监听模式配置：

监听模式是通过监听 PC 登录域服务器的数据，从监听到的数据中获取用户登录的信息，从而实现的单点登录。监听模式的单点登陆无需在域服务器上安装任何组件，但要求内网计算机登陆域的数据经过设备或者是通过监听口镜像到设备。设备通过监听 UDP 88 端口的登陆信息，如果用户成功登陆域，则上网时无法再次通过我们设备的认证，可以直接上网。适用于域服务器在外网和内网情况。下面分两种情况介绍单点登录的设置。

第一种情况：域服务器在内网环境：



数据流过程如下

- 1、PC 登陆域整个过程被设备监听到
- 2、如果用户登陆域成功，则自动通过设备认证。

设置方法：

第一步：设置认证 AD 域服务，点击进入『用户认证』→『认证选项』→『外部认证服务器』进行设置（参见章节 3.7.2.3）

第二步：在设备上启用单点登录，选择监听模式并设置域服务器的 IP 地址。点击进入『用户认证』→『认证选项』→『单点登录选项』→『域单点登录』页面进行配置。

勾选[启用单点登录]启用域单点登录功能；

勾选[监听计算机登录域的数据，获取登录信息]，表示使用监听模式实现单点登录。在[监听的域控制器地址列表]中输入域服务器的 IP 和监听端口，如果有多个域服务器，则一行一个 IP 和端口，如下图所示：



第三步：如果登录数据不经过设备，需要通过设置镜像口，并将镜像口连接到转发登录数据的交换机镜像口上，点击**其他选项**，设置设备的镜像口。镜像口需要设置空闲网口，已经在使用的网口请不要设置成镜像网口。

**单点登录选项**

域单点登录 Proxy单点登录 Pop3单点登录 Web单点登录 Radius 其它选项

如果需要结合外部认证服务器做单点登录，并且用户登录到这些外部认证服务器的数据并没有经过本设备，则需要把用户登录的数据镜像到本设备空闲的网口上，在这里指定镜像网口。

启用镜像网口

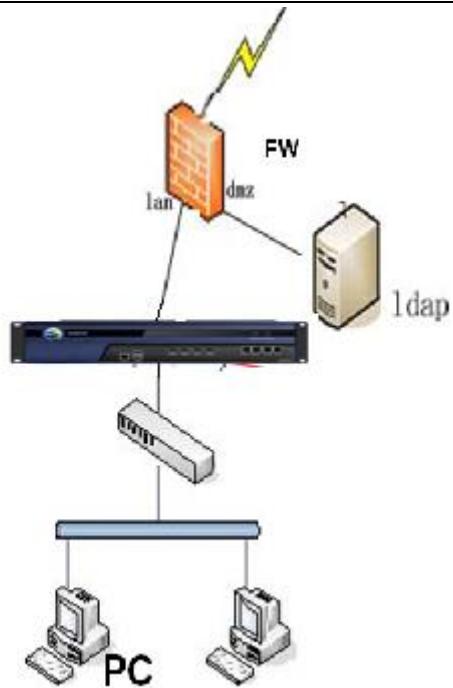
监听的镜像网口列表（选中代表监听该网口）：

eth0  
 eth1  
 eth2  
 eth3  
 eth4  
 eth5

第四步：设置认证策略，根据需要使用单点登录的用户的IP或MAC设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节3.7.2.1.3）。

第五步：PC登录域，登录成功后即可上网。

第二种情况：域服务器在外网：



数据流过程如下：

1、PC 登陆域是穿透设备的

2、设备的内网接口同时作为监听口，无需再设置监听口。

设置方法：

第一步：设置认证 AD 域服务，点击进入『用户认证』→『认证选项』→『外部认证服务器』进行设置（参见章节 3.7.2.3）

第二步：在设备上启用单点登录，选择监听模式并设置域服务器的 IP 地址。点击进入『用户认证』→『认证选项』→『单点登录选项』→『域单点登录』页面进行配置。

勾选[启用单点登录]启用域单点登录功能；

勾选[监听计算机登录域的数据，获取登录信息]，表示使用监听模式实现单点登录。在[监听的域控制器地址列表]中输入域服务器的 IP 和监听端口，如果有多个域服务器，则一行一个 IP 和端口，如下图所示：



第三步：设置认证策略，根据需要使用单点登录的用户的 IP 或 MAC 设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节 3.7.2.1.3）。

第四步：PC 登录域，登录成功后即可上网。

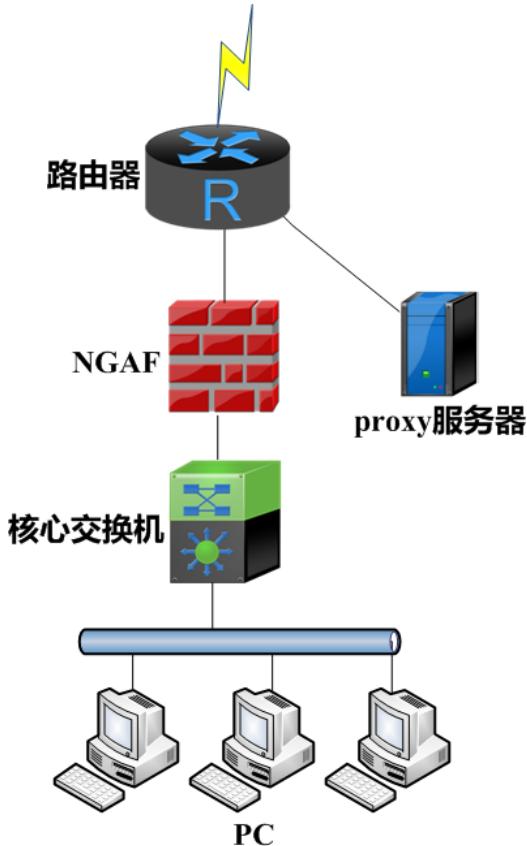


1、监听模式只能监听到用户登录的信息，用户注销时没有数据，故无法监听到注销的状态，所以可能会出现 PC 已经注销了，但设备的在线用户列表中还没有注销此用户。

### 3.7.2.2.1.2 PROXY 单点登录

一般适用于用户使用 Proxy 代理上网的环境，并且每个用户均分配了代理服务器的账号。使用 Proxy 单点登录的认证方式时，当用户通过 Proxy 服务器的验证时，同时通过设备的认证。Proxy 单点登录使用的是监听模式，也是通过监听登录数据完成单点登录的。

第一种情况：Proxy 服务器在外网方向，如图所示：



数据流过程如下：

- 1、用户通过 Proxy 服务器代理上网，设备监听 PC 和 Proxy 服务器的交互
- 2、PC 成功经过 Proxy 服务器认证的同时也经过设备的认证。

设置步骤：

第一步：在设备上启用单点登录，选择监听模式并设置域服务器的 IP 地址。  
点击进入『用户认证』→『认证选项』→『单点登录选项』→『Proxy 单点登录』  
页面进行配置。

勾选[启用 PROXY 单点登录]启用 PROXY 单点登录功能；

在[Proxy 代理服务器地址列表]中输入 Proxy 服务器的 IP 和监听端口，如果有多个 Proxy 服务器，则一行一个 IP 和端口，此处的端口设置 Proxy 认证的端口即可，如下图所示：

**单点登录选项**[域单点登录](#) [Proxy单点登录](#) [Pop3单点登录](#) [Web单点登录](#) [Radius](#) [其它选项](#) 启用Proxy单点登录(如果登录域的数据不经过本设备)

如果内网用户登录Proxy服务器(代理服务器)的数据包不经过本设备，则需要把登录的数据包镜像到本设备，并且到“[其它选项](#)”中启用镜像功能。

Proxy代理服务器地址列表：一行一个IP和端口，IP和端口用“:”分隔，如果端口为空则使用默认端口。

1.2.3.4

第二步：如果登录数据不经过设备，需要通过设置镜像口，并将镜像口连接到转发登录数据的交换机镜像口上，点击[其他选项](#)，设置设备的镜像口。镜像口需要设置空闲网口，已经在使用的网口请不要设置成镜像网口。

**单点登录选项**[域单点登录](#) [Proxy单点登录](#) [Pop3单点登录](#) [Web单点登录](#) [Radius](#) [其它选项](#)

如果需要结合外部认证服务器做单点登录，并且用户登录到这些外部认证服务器的数据并没有经过本设备，则需要把用户登录的数据镜像到本设备空闲的网口上，在这里指定镜像网口。

 启用镜像网口

监听的镜像网口列表（选中代表监听该网口）：

- eth0
- eth1
- eth2
- eth3
- eth4
- eth5

第三步：设置认证策略，根据需要使用 Proxy 单点登录的用户的 IP 或 MAC 设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节 3.7.2.1.3）。

第四步：PC 登录 Proxy 服务器，登录成功后即可上网。



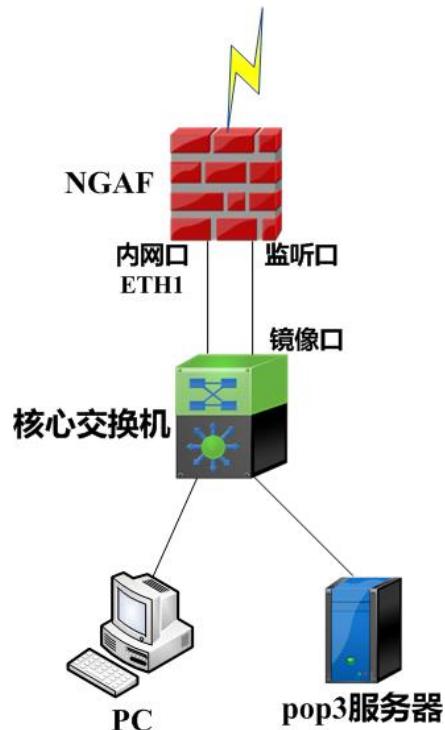
1、如果 Proxy 服务器在外网，要启用自动认证，则必须在根组中开放访问 Proxy 这个服务器的权限，并在【认证选项】→【其它认证选项】中勾选[未通过认证用户可以访问基本服务（HTTP 除外）]如图所示：

选项设置菜单	<<	其它认证选项
<p>单点登录选项</p> <p>认证通过跳转</p> <p>认证冲突</p> <p>跨三层MAC识别</p> <p><b>其它认证选项</b></p>		
<p><input checked="" type="checkbox"/> 自动注销指定时间内无流量的已认证用户 无流量时间（分钟）： <input type="text" value="120"/> <span>(i)</span></p> <p><input type="checkbox"/> 采用SSL方式加密提交用户名和密码</p> <p><input checked="" type="checkbox"/> 用户未通过认证前，允许访问DNS服务</p> <p><input checked="" type="checkbox"/> 未通过认证用户可以访问基本服务（HTTP/HTTPS除外）</p> <p><input type="checkbox"/> mac地址发生变动时，需要重新认证</p> <p><input checked="" type="checkbox"/> 冻结认证失败次数超过最大值的用户 <span>(i)</span> 认证失败最大值（次）：<input type="text" value="2"/> 冻结时间（分钟）：<input type="text" value="1"/> <span>(i)</span></p> <p><input type="checkbox"/> 登录页面需要安装根证书后，才允许用户登录</p>		
<input type="button" value="提交"/>		

### 3.7.2.2.1.3 POP3 单点登录

客户网络中有邮件服务器，用户信息存放在 POP3 服务器上，在上网之前，用户使用 Outlook、Foxmail 之类的客户端登陆 POP3 服务器收发一次邮件，设备通过监听模式监听到用户登录的信息，则设备会自动识别并认证通过该用户，此时用户可以直接上网，而不需再次输入用户名密码。同时适用 POP3 服务器在内网和外网情况。下面分两种情况讲述 POP3 单点登录的设置。

#### 第一种情况：POP3 服务器在内网



数据流过程如下：

- 1、用户通过邮件客户端和 POP3 服务器通讯，设备监听整个通信过程
- 2、邮件客户端成功登陆 POP3 服务器的同时，设备自动认证用户，上网不需要再次输入密码。
- 3、由于数据交互是在内网，内网登录 POP3 服务器的数据不经过设备，需要在设备上设置监听口。

设置方法：

第一步：设置认证 POP3 服务器，点击进入『用户认证』→『认证选项』→『外部认证服务器』进行设置（参见章节 3.7.2.3）

第二步：在设备上启用单点登录，选择监听模式并设置域服务器的 IP 地址。点击进入『用户认证』→『认证选项』→『单点登录选项』→『POP3 单点登录』页面进行配置。

勾选[启用 POP3 单点登录]启用 POP3 单点登录功能；

在[邮件服务器地址列表]中输入 POP3 服务器的 IP 和监听端口，如果有多个 POP3 服务器，则一行一个 IP 和端口，此处的端口设置 POP3 认证的端口（一般默认是 TCP110），如下图所示：

**单点登录选项**

域单点登录     Proxy单点登录     **Pop3单点登录**     Web单点登录     Radius     其它选项

启用Pop3单点登录

如果内网用户登录Pop3服务器(邮件服务器)的数据包不经过本设备，则需要把登录的数据包镜像到本设备，并且到“其它选项”中启用镜像功能。

邮件服务器地址列表：一行一个IP和端口，IP和端口用":分隔，如果端口为空则使用默认端口。  
可以直接在此处输入、编辑、删除

第三步：如果登录数据不经过设备，需要通过设置镜像口，并将镜像口连接到转发登录数据的交换机镜像口上，点击其他选项，设置设备的镜像口。镜像口需要设置空闲网口，已经在使用的网口请不要设置成镜像网口。

**单点登录选项**

域单点登录     Proxy单点登录     Pop3单点登录     Web单点登录     Radius     **其它选项**

如果需要结合外部认证服务器做单点登录，并且用户登录到这些外部认证服务器的数据并没有经过本设备，则需要把用户登录的数据镜像到本设备空闲的网口上，在这里指定镜像网口。

启用镜像网口

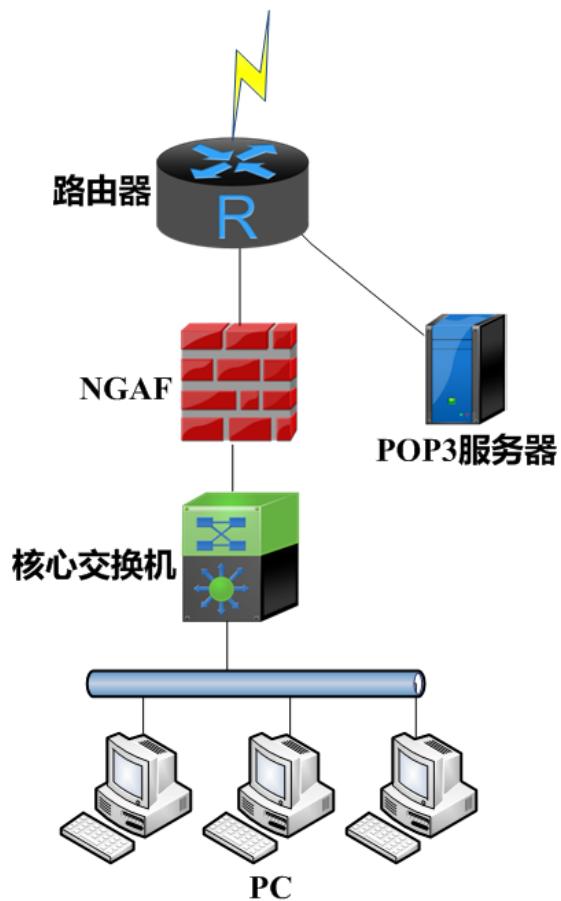
监听的镜像网口列表 ( 选中代表监听该网口 ) :

eth0  
 eth1  
 eth2  
 eth3  
 eth4  
 eth5

第四步：设置认证策略，根据需要使用 POP3 单点登录的用户的 IP 或 MAC 设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节 3.7.2.1.3）。

第五步：PC 通过邮件客户端收发一次邮件，登录 POP3 成功后即可上网。

第二种情况：POP3 服务器在外网：



数据流过程如下：

- 1、PC 登陆 POP3 服务器是穿透设备的
- 2、设备的内网接口同时作为监听口，无需再设置监听口。

设置方法：

第一步：设置认证 POP3 服务器，点击进入『用户认证』→『认证选项』→『外部认证服务器』进行设置（参见章节 3.7.2.3）

第二步：在设备上启用单点登录，选择监听模式并设置域服务器的 IP 地址。点击进入『用户认证』→『认证选项』→『单点登录选项』→『POP3 单点登录』页面进行配置。

勾选[启用 POP3 单点登录]启用 POP3 单点登录功能；

在[邮件服务器地址列表]中输入 POP3 服务器的 IP 和监听端口，如果有多个 POP3 服务器，则一行一个 IP 和端口，此处的端口设置 POP3 认证的端口（一般默认是 TCP110），如下图所示：



第三步：设置认证策略，根据需要使用 POP3 单点登录的用户的 IP 或 MAC 设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节 3.7.2.1.3）。

第四步：PC 通过邮件客户端收发一次邮件，登录 POP3 成功后即可上网。



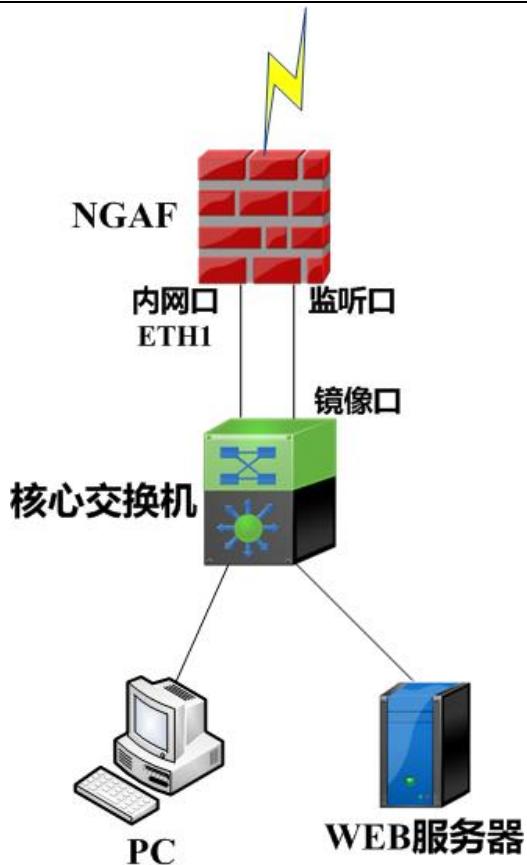
1、如果 POP3 服务器在外网，要启用自动认证，则必须在根组中开放访问 POP3 这个服务器的权限，并在【认证选项】→【其它认证选项】中勾选[未通过认证用户可以访问基本服务（HTTP 除外）]如图所示：

选项设置菜单	<<	其它认证选项
<p>单点登录选项</p> <p>认证通过跳转</p> <p>认证冲突</p> <p>跨三层MAC识别</p> <p><b>其它认证选项</b></p>		
<p><input checked="" type="checkbox"/> 自动注销指定时间内无流量的已认证用户 无流量时间（分钟）： <input type="text" value="120"/> <span>(i)</span></p> <p><input type="checkbox"/> 采用SSL方式加密提交用户名和密码</p> <p><input checked="" type="checkbox"/> 用户未通过认证前，允许访问DNS服务</p> <p><input checked="" type="checkbox"/> 未通过认证用户可以访问基本服务（HTTP/HTTPS除外）</p> <p><input type="checkbox"/> mac地址发生变动时，需要重新认证</p> <p><input checked="" type="checkbox"/> 冻结认证失败次数超过最大值的用户 <span>(i)</span></p> <p>认证失败最大值（次）：<input type="text" value="2"/></p> <p>冻结时间（分钟）：<input type="text" value="1"/> <span>(i)</span></p> <p><input type="checkbox"/> 登录页面需要安装根证书后，才允许用户登录</p>		
<input type="button" value="提交"/>		

#### 3.7.2.2.1.4 Web 单点登录

Web 单点登陆一般适用于用户有自己的 web 服务器，且帐户信息均保存在 web 服务器上，客户想要实现，用户上网前通过自己 Web 服务器的认证同时也通过设备的认证。适用于 Web 服务器在内网或外网的环境。

第一种情况：Web 服务器在内网：



数据流过程如下：

- 1、用户登陆 Web 服务器，整个过程是明文的，设备监听整个通信过程
- 2、通过用户认证后服务器回馈的关键词来判断认证成功与否，从而决定 Web 单点登陆成功或失败。

设置方法：

第一步：在设备上启用单点登录，选择单点登录模式并设置共享密钥。勾选上【策略导航】页面中的『用户与策略管理』→『用户认证』→『认证选项』，右边进入【认证选项】编辑页面。然后点『单点登录选项设置』→『Web 单点登录』进入 Web 单点登录配置页面，先勾选『启用 Web 单点登录』。

**单点登录选项**[域单点登录](#) [Proxy单点登录](#) [Pop3单点登录](#) **Web单点登录** [Radius](#) [其它选项](#) 启用Web单点登录

如果内网用户登录Web认证服务器的数据包不经过本设备，则需要把登录的数据包镜像到本设备，并且到“[其它选项](#)”中启用镜像功能。

Web认证服务器：ip或者ip:port或者服务器域名url，如果端口为空则使用默认端口。

 200.200.0.20 用户未认证前，把浏览器重定向到此Web认证服务器

用户表单名称：Web认证页面中用户名所对应的表单名称。

 pwuser 认证成功关键字 新员工 认证失败关键字 提交

第二步：在[Web 认证服务器]中填写 Web 认证服务器地址

第三步：勾选[用户未认证前，把浏览器重定向到此 Web 认证服务器]，当用户未通过认证前，进行访问网页都会重定向到此页面上进行 Web 单点登录。

第四步：填写[用户表单名称]，用来填写 Web 认证时，向服务器提交用户名表单名称

第五步：选择[认证成功关键词]或者[认证失败关键词]，用来识别 Web 登录是否成功的关键词。比如选了[认证成功关键词]，则在 POST 的返回结果中，如果包含了设定的关键词，则判断为 Web 单点登录成功，选择了[认证失败关键词]，则在 POST 的返回结果中，如果包含了设定的关键词，则判断为 Web 单点登录失败，反之单点登录成功。

第六步：设置监听口，点『其他选项』，勾选『设置监听镜像网口』，选择

地址:深圳市南山区学苑大道1001号南山智园A1栋

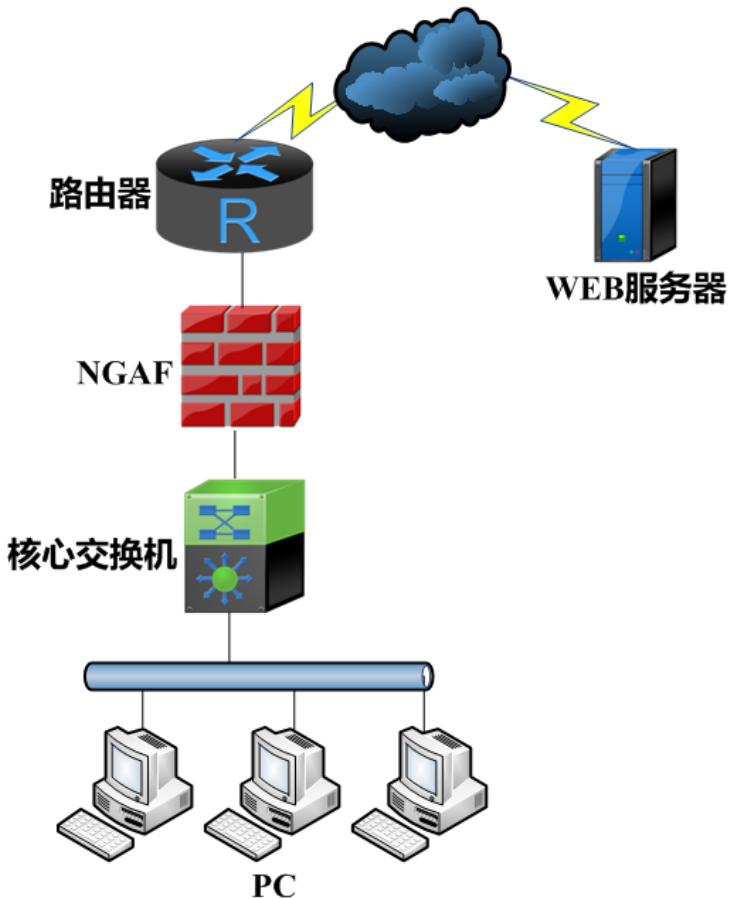
咨询热线 : 400-806-6868 | 服务热线 : 400-630-6430 | 邮箱: market@sangfor.com.cn | 网址 : www.sangfor.com.cn

监听口。

<b>选项设置菜单</b> <<	<b>其它认证选项</b>  <input checked="" type="checkbox"/> 自动注销指定时间内无流量的已认证用户 无流量时间（分钟）： <input type="text" value="120"/>  <input type="checkbox"/> 采用SSL方式加密提交用户名和密码 <input checked="" type="checkbox"/> 用户未通过认证前，允许访问DNS服务 <input checked="" type="checkbox"/> 未通过认证用户可以访问基本服务（HTTP/HTTPS除外） <input type="checkbox"/> mac地址发生变动时，需要重新认证 <input checked="" type="checkbox"/> 冻结认证失败次数超过最大值的用户  认证失败最大值（次）： <input type="text" value="2"/> 冻结时间（分钟）： <input type="text" value="1"/>  <input type="checkbox"/> 登录页面需要安装根证书后，才允许用户登录
提交 	

第七步：PC 上网先登录设置的网站，如例子中的 bbs，登录成功后即可上网。

第二种情况：Web 服务器在外网：



数据流过程如下：

- 1、PC 登陆 web 服务器是穿透设备的
- 2、设备的内网接口同时作为监听口，无需再设置监听口，Web 登录成功后则 Web 单点登录成功。

设置方法：

第一步：在设备上启用单点登录，选择单点登录模式并设置共享密钥。勾选上【策略导航】页面中的『用户认证』→『认证选项』，右边进入【认证选项】编辑页面。然后点『单点登录选项设置』→『Web 单点登录』进入 Web 单点登录配置页面，先勾选『启用 Web 单点登录』。

**单点登录选项**[域单点登录](#) [Proxy单点登录](#) [Pop3单点登录](#) **Web单点登录** [Radius](#) [其它选项](#) 启用Web单点登录

如果内网用户登录Web认证服务器的数据包不经过本设备，则需要把登录的数据包镜像到本设备，并且到“[其它选项](#)”中启用镜像功能。

Web认证服务器：ip或者ip:port或者服务器域名url，如果端口为空则使用默认端口。

 200.200.0.20 用户未认证前，把浏览器重定向到此Web认证服务器

用户表单名称：Web认证页面中用户名所对应的表单名称。

 pwuser 认证成功关键字 新员工 认证失败关键字 提交

第二步：在[Web 认证服务器]中填写 Web 认证服务器地址

第三步：勾选[用户未认证前，把浏览器重定向到此 Web 认证服务器]，当用户未通过认证前，进行访问网页都会重定向到此页面上进行 web 单点登录。

第四步：填写[用户表单名称]，用来填写 Web 认证时，向服务器提交用户名表单名称

第五步：选择[认证成功关键词]或者[认证失败关键词]，用来识别 Web 登录是否成功的关键词。比如选了[认证成功关键词]，则在 POST 的返回结果中，如果包含了设定的关键词，则判断为 Web 单点登录成功，选择了[认证失败关键词]，则在 POST 的返回结果中，如果包含了设定的关键词，则判断为 Web 单点登录失败，反之单点登录成功。

第六步：PC 上网先登录设置的网站，如例子中的 bbs，登录成功后即可上

网。

### 3.7.2.2.1.5 Radius 单点登录

当用户环境中存在 Radius 服务器，并且 Radius 认证和计费的数据包经过 AF 设备时，可以启用 Radius 单点登录，认证成功后以 Radius 的用户名在 AF 上上线。

勾选[启用 Radius 单点登录]，在[Radius 服务器地址列表]中填写 Radius 服务器的地址，如下图所示：

**单点登录选项**

域单点登录	Proxy单点登录	Pop3单点登录	Web单点登录	<b>Radius</b>	其它选项
-------	-----------	----------	---------	---------------	------

启用Radius单点登录

Radius服务器地址列表：一行一个IP

192.200.200.1

**提交**

如果 Radius 认证和计费的数据包不经过 AF，则需要在 AF 上设置镜像口，并把这部分数据通过镜像口镜像到 AF 上。

**单点登录选项**

域单点登录 | Proxy单点登录 | Pop3单点登录 | Web单点登录 | Radius | 其它选项

如果需要结合外部认证服务器做单点登录，并且用户登录到这些外部认证服务器的数据并没有经过本设备，则需要把用户登录的数据镜像到本设备空闲的网口上，在这里指定镜像网口。

启用镜像网口

监听的镜像网口列表（选中代表监听该网口）：

eth0  
 eth1  
 eth2  
 eth3  
 eth4  
 eth5

### 3.7.2.2.1.6 其他选项

『其他选项』用于登录服务器的数据不经过网关，则需要设定监听镜像网口，监听登录的数据，勾选一个空闲接口进行监听。这个监听口在域单点登录监听模式、POP3 单点登录以及 Web 单点登录等实现时均需要设置。

**单点登录选项**

域单点登录 | Proxy单点登录 | Pop3单点登录 | Web单点登录 | Radius | 其它选项

如果需要结合外部认证服务器做单点登录，并且用户登录到这些外部认证服务器的数据并没有经过本设备，则需要把用户登录的数据镜像到本设备空闲的网口上，在这里指定镜像网口。

启用镜像网口

监听的镜像网口列表（选中代表监听该网口）：

eth0  
 eth1  
 eth2  
 eth3  
 eth4  
 eth5

### 3.7.2.2.2 认证通过跳转

『认证通过跳转设置』用于设置 Web 认证用户在认证成功后的跳转页面。

配置接口如下：

选项设置菜单 < 认证通过跳转

用户认证通过后，页面跳转到：

最近请求的页面  
 注销页面  
 自定义页面URL  
 HTTPS请求跳转到认证页面

提交

[最近请求的页面]勾选此项，则内网用户在认证成功后 Web 页面跳转到用户认证前请求的页面。

[注销页面]勾选此项，则用户在认证成功后 Web 页面跳转到用户手动注销页面。

[自定义页面 URL]勾选此项，则用户在认证成功后跳转到用户自定义的页面。

[HTTPS 请求跳转到认证页面]勾选此项，则会将未认证通过前访问 HTTPS 的请求，重定向到认证页面。

### 3.7.2.2.3 认证冲突

『认证冲突』用于不允许许多人同时登陆的账号，如果认证时发现该账号已登

陆，则设备的处理方式有两种，分别为[强制注销以前的登录，在当前 IP 上认证通过]、[提示账号在其他 IP 上登录，不注销以前的登录]。页面如下：



### 3.7.2.2.4 跨三层 IP/MAC 识别

内网用户采用绑定 MAC 或者是限定 MAC 的认证方式，并且内网是跨三层的环境下，需要启用『跨三层 MAC 识别』的功能，用于获取内网用户的 MAC 地址。使用此功能的前提是内网交换机支持 SNMP 功能。

原理：设备上的会定期发 snmp request 到三层交换机请求交换机的 MAC 表，并保存在设备内存中。此时如果三层交换机其它网段的计算机经过设备上网时，如一台 PC 192.168.1.2（和设备 lan 口不在同一网段）经过设备上网，该 PC 数据包经过设备时，设备校验此数据包的 MAC 是三层的 MAC，则对此 MAC 不做处理，而根据 192.168.1.2 这个 IP 去内存中查找其真实的 MAC 地址，实现对用户真正 MAC 的验证。

设置方法如下：

第一步：在三层交换机上开启 SNMP 功能。

第二步：点击进入『用户认证』→『认证选项』→『跨三层 MAC 识别』进行设置，在设备接口上勾选『启用 SNMP 设置』，启用 SNMP 功能。

认证选项

选项设置菜单 <<	<b>跨三层MAC识别</b>
> 单点登录选项	<input checked="" type="checkbox"/> 启用SNMP设置
> 认证通过跳转	访问SNMP服务器超时设置(秒) : <input type="text" value="1"/>
> 认证冲突	访问SNMP服务器时间间隔(秒) : <input type="text" value="5"/>
<b>&gt; 跨三层MAC识别</b>	SNMP服务器列表 : <input type="button" value="添加服务器"/>
> 其它认证选项	可以直接在此处输入、编辑、删除

第三步：设置[访问 SNMP 服务器超时时间设置]和[访问 SNMP 服务器时间间隔]，一般保持默认设置。

第四步：在[SNMP 服务器列表]添加服务器，点击添加服务器，会弹出【添加 SNMP 服务器】的编辑窗口，输入 SNMP 的 IP 地址，再点击搜索服务器，勾选下面的搜索到的服务器，点击添加即可。如图：



第五步：设置认证策略，根据需要使用 MAC 验证的用户的 IP 或 MAC 设置认证策略，点击『用户认证』→『认证策略』→『新增认证策略』进行配置（参见章节 3.7.2.1.3）。

第六步：前面五步配置好后，三层交换机下的计算机就可以直接以认证新用户的方式通过设备认证上网了。



填入服务器的 IP 搜索 SNMP 服务器时，要求服务器必须开启 SNMP 功能，且 COMMUNITY 设置为 public，否则将搜索服务器失败，需要手动设置 SNMP 服务器信息。

### 3.7.2.2.5 其他认证选项

『其他认证选项』用于配置跟认证相关的一些选项，配置页面如下图：

<b>选项设置菜单</b>  <input type="checkbox"/> 单点登录选项 <input type="checkbox"/> 认证通过跳转 <input type="checkbox"/> 认证冲突 <input type="checkbox"/> 跨三层MAC识别 <input checked="" type="checkbox"/> 其它认证选项	<b>其它认证选项</b>  <input checked="" type="checkbox"/> 自动注销指定时间内无流量的已认证用户 无流量时间（分钟）： <input type="text" value="120"/> <small>(i)</small> <input type="checkbox"/> 采用SSL方式加密提交用户名和密码 <input checked="" type="checkbox"/> 用户未通过认证前，允许访问DNS服务 <input checked="" type="checkbox"/> 未通过认证用户可以访问基本服务（HTTP/HTTPS除外） <input type="checkbox"/> mac地址发生变动时，需要重新认证 <input checked="" type="checkbox"/> 冻结认证失败次数超过最大值的用户 <small>(i)</small> 认证失败最大值（次）： <input type="text" value="2"/> 冻结时间（分钟）： <input type="text" value="1"/> <small>(i)</small> <input type="checkbox"/> 登录页面需要安装根证书后，才允许用户登录
提交	

[自动注销指定时间内无流量的已认证用户]用来设置一个超时时间，用户超过此超时时间没有流量则自动注销该用户

[采用 SSL 加密方式提交用户名和密码]密码认证页面默认是 HTTP 页面，通过这个页面提交用户名是明文的方式，如果客户要求页面采用 SSL 加密的方式，则需要勾选此项。

[用户未通过认证前，允许访问 DNS 服务]用于允许在用户通过认证前访问 DNS 服务。

[未通过认证用户可以访问基本服务（根组权限，HTTP 除外）]用于允许用户在通过认证前能使用除 HTTP 服务外的根组权限。

[mac 地址发生变动时，需要重新认证]原本认证通过的用户，MAC 地址变化了会要求重新认证。比如一个 IP 为 192.168.1.1 的用户，认证方式为用户名和

密码认证，当这个用户下线后，由于有一段时间不会注销该用户，这时另一个用户把 IP 改成 192.168.1.1，这样 MAC 地址就发生了变化，需要重新认证方可上网。

[冻结认证失败次数超过最大值的用户]用来设置超过认证失败次数，则冻结该用户的时间。如图是登陆三次失败后冻结该用户 1 分钟。

[登录页面需要安装根证书后，才允许用户登录]解密功能可以通过此选项安装 ssl 证书。



1、在[用户名/密码]的认证方式下，支持用户自己修改自己的密码，不需要管理员来修改，如果修改密码失败，该用户会被冻结，冻结时间根据[冻结认证失败次数超过最大值的用户]中设置决定。

2、打开修改用户密码的页面，地址为：<http://设备 IP>，进入后点击**修改密码**，进入修改密码页面。





输入要修改的用户名，旧密码，新密码，确认新密码，点击提交即可。

### 3.7.2.3. 外部认证服务器

『外部认证服务器』用来设置第三方认证服务器的信息，设备支持三种外部认证服务器，包括 LDAP，RADIUS，POP3 三种。点新增，出现一个下拉列表：



#### 3.7.2.3.1 新增外部认证服务器

##### 3.7.2.3.1.1 新增 LDAP 服务器

选择【导航菜单】窗口中的『用户认证』。点击『用户认证』选项，选择『外

部认证服务器】。进入【外部认证服务器】的编辑窗口。点击【新增】，选择[LDAP服务器]，会弹出【外部认证服务器（LDAP）】窗口。

在[基本配置]中填写服务器的名称，IP，认证端口，超时时间，BaseDN（即为用户所在服务器的具体路径）。



在[同步配置]中填写域用户的用户名和密码，以及选择域的类型，支持的 LDAP 有以下五种:[MS Active Directory] [OPEN LDAP] [SUN LDAP] [IBM LDAP][OTHER LADAP]。



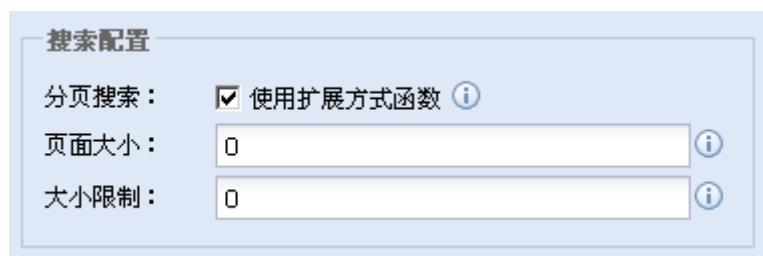
[搜索配置] :

[使用扩展方式函数]如果 ldap 服务器支持分页搜索，可勾用此选项，否则使

用普通 ldap\_search，不支持的情况一般是服务器禁用或 ldap 软件未实现（如较老版本的 openldap）。

[页面大小]指使用扩展方函数搜索时每页指定返回的大小，可咨询 ldap 服务器管理员。（通常配置时会选用 800/400/200 ... 往小的试，直到可以同步为止）

[大小限制]Size Limits 选项，用于设置同步时的 size limit，除非服务端有明确配置，否则请不要配置此选项。



[测试有效性]用于测试连接服务器的 IP、端口以及用户名是否可用。



[搜索配置]默认情况下按照默认即可，不需要设置

### 3.7.2.3.1.2 新增 RADIUS 服务器

选择【导航菜单】窗口中的『用户与策略管理菜单』。点击『用户认证』选项，选择『外部认证服务器』。进入【外部认证服务器】的编辑窗口。点击新增，选择[RADIUS 服务器]，会弹出一个【外部认证服务器（RADIUS）】编辑页面。

外部认证服务器 (RADIUS) ×

服务器名称：

**Radius服务器配置**

IP地址：

认证端口：

超时(秒)：

共享密钥：

采用协议：

填写[服务器名称]

[Radius 服务器配置]用于设置 Radius 服务器的 IP 地址、端口、超时时间、共享密钥以及采用协议。

### 3.7.2.3.1.3 新增 POP3 服务器

选择【导航菜单】窗口中的『用户与策略管理菜单』。点击『用户认证』选项，选择『外部认证服务器』。进入【外部认证服务器】的编辑窗口。点击新增，选择[POP3 服务器]，会弹出一个【外部认证服务器 (POP3)】编辑框。

外部认证服务器 (POP3) ×

服务器名称：

**Pop3服务器配置**

IP地址：

认证端口：

超时(秒)：

填写[服务器名称]，

[POP3 服务器配置]用于设置 POP3 服务器的 IP 地址、认证端口和超时时间。

### 3.7.2.3.2 删除外部认证服务器

第一步：选择【导航菜单】窗口中的『用户认证』。点击『用户认证』选项，选择『外部认证服务器』。进入【外部认证服务器】的编辑窗口。选择要删除的服务器。

外部认证服务器						
+ 新增		×	删除	✓ 启用	✗ 禁用	刷新
序号	名称	认证类型	服务器	端口	状态	删除
<input checked="" type="checkbox"/>	1 域认证服务器	LDAP	192.168.1.240	389	✓	✗
<input type="checkbox"/>	2 radius	RADIUS	192.168.1.23	1812	✓	✗

第二步：点击删除按钮，进行删除。

### 3.7.2.3.3 启用/禁用外部认证服务器

第一步：选择【导航菜单】窗口中的『用户认证』菜单。点击『用户认证』选项，选择『外部认证服务器』。进入【外部认证服务器】的编辑窗口。选择要启用/禁用的服务器。

外部认证服务器						
+ 新增		×	删除	✓ 启用	✗ 禁用	刷新
序号	名称	认证类型	服务器	端口	状态	删除
<input checked="" type="checkbox"/>	1 域认证服务器	LDAP	192.168.1.240	389	✓	✗
<input type="checkbox"/>	2 radius	RADIUS	192.168.1.23	1812	✓	✗

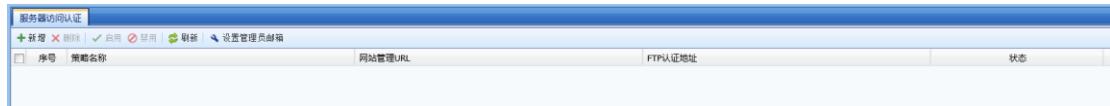
第二步：启用/禁用该服务器。

## 3.7.3. 服务器访问认证

『服务器访问认证』可以对访问服务器后台页面的人进行 IP 认证或者邮件

认证。

在此页面可以对服务器访问认证进行新增、删除、启用、禁用以及刷新。如下图所示：



[设置管理员邮箱]：服务器访问认证策略引用该邮箱地址发送邮件，管理员维护网址收取验证码的邮箱地址。

点击**新增**，弹出新增服务器访问认证页面。如下如所示：



The dialog box contains the following fields:

- 策略名称 :** (Strategy Name) - Input field.
- 服务器IP地址 :** (Server IP Address) - Input field.
- 网站防护方式** (Website Protection Method):
  - 网站后台登录防护 (CMS)**:
    - HTTP端口 :** 80
    - 网站管理URL :** 可以直接在此处输入、编辑、删除
  - FTP登录防护**:
    - FTP端口 :** 21
    - 配置认证URL :** http://www.yoursite.com/ftp.html
      - 管理员登录FTP时，需先在该URL上进行验证码认证，建议格式为：您的网站域名+/ftp.html，如：  
http://www.baidu.com/ftp.html
- 管理员认证方式** (Administrator Authentication Method):
  - IP认证 (以下IP地址维护网站无需邮件认证)**:
    - 请选择** (Select) - Input field.
  - 邮件认证**:
    - 管理员邮箱地址 :** 配置邮箱列表... (Configure Email List) - Input field.
    - 认证通过有效时间 :** 5 分钟 (Authentication Valid Time: 5 minutes) - Input field.

At the bottom right are the **提交** (Submit) and **取消** (Cancel) buttons.

[策略名称]：定义策略名称。

[服务器 IP 地址]: 网站服务器 IP 地址。

[HTTP 端口]: 管理员使用 HTTP 协议登陆网址后台端口，默认是 80。

[网址管理 URL]: 管理员登陆网址后台的 URL。

[FTP 端口]: 管理使用 FTP 协议登陆网址后台端口，默认是 21。

[配置认证 URL]: 管理员登陆网址后台 URL, 管理员登录 FTP 时，需先在该 URL 上进行验证码认证，建议格式为：您的网站域名+/ftp.html，如：  
<http://www.baidu.com/ftp.html>。

[IP 认证]: 选中的 IP 组无需邮件认证。

[管理员邮件地址]: 管理员维护网址收取验证码的邮箱地址。

[认证通过有效时间]: 网站管理员 5min 内使用动态码进行认证，认证成功，直接跳转到 CMS 登录页面；网站管理员 5min 之后，在 10min 内没有任何网站管理员登录请求，需要重新发送邮件验证。

## 3.8. 下一代安全防护体系

『下一代安全防护体系』主要用于设置 AF 产品与云端产品、终端产品进行联动效应，形成更全面的防护体系。深信服下一代安全防护体系通过联动云端、终端、边界进行协同响应，建立全面的事前风险预警、事中防御、事后检测与响应的整套安全防御体系。云端持续风险分析与预警，终端持续检测与响应，边界持续检测与防御。

### 3.8.1. 体系总览

#### 3.8.1.1. 概述

设置目前 AF 可以联动响应的云端/终端产品，包括安全云脑、云守、云眼、

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

云镜、EDR 共五款产品。如下图所示：



### 3.8.1.2. 安全云脑

深信服安全云脑通过不断的自主学习，持续提升识别新威胁、未知威胁和高级威胁的能力；同时保持与设备深度联动，持续提升 AF 的安全能力，保障您的网络安全。

设备可以访问互联网，同时已开通云脑相应的序列号（序列号参考 3.6.1.1.6 章节），设备可以自动完成云脑的接入。此外无需额外设置，如下图：



安全云脑 云守 云眼 云镜 EDR

### 深信服安全云脑

深信服安全云脑通过不断的自主学习，持续提升识别新威胁、未知威胁和高级威胁的能力；同时保持与设备深度联动，持续提升AF的安全能力，保障您的网络安全。

#### 安全云脑服务信息

服务状态：在线

服务时长：已累计为您服务 86 天

#### 服务亮点

- 安全能力持续更新**  
持续收集与分析全网最新威胁特征，实时下发最新的安全能力到设备，使设备具备应对最新威胁的能力。
- 未知威胁检测**  
结合静态与动态沙箱检测技术，识别传统基于规则类无法识别的恶意威胁，让未知威胁原形毕露。
- 高级威胁分析**  
通过对流量、日志、行为等数据进行深度挖掘与关联分析，并结合威胁情报准确识别网络中潜伏的黑客或失陷主机。

### 3.8.1.3. 云守

深信服云守作为您的云端安全专家团队，利用全网威胁情报、行业专家安全最佳实践，协助您更有效利用 AF 保护业务，对抗威胁，实现从被动防御到主动响应的转变。

设备可以访问互联网，同时已开通云守，并在云守平台完成了与设备的绑定。此处可通过所开通的云守账号，完成与云守平台的对接。

绑定后，可以通过右上角  按钮，完成绑定账号的解除。

具体配置效果如下图所示：



The screenshot shows two side-by-side web interfaces for Sangfor Cloud Eye. The left interface is for 'Cloud Eye' and shows a status of '未接入联动' (Not yet connected). It includes fields for account and password, and a '立即接入' (Connect immediately) button. The right interface is also for 'Cloud Eye' and shows a status of '已过期' (Expired). It displays service information such as '服务状态: 在线' (Service status: Online), '云守账号: 273295576@qq.com', '设备别名: SANGFOR AF', '服务时长: 0天', and a checked checkbox for '同意云守联动处置紧急安全事件' (Agree to handle emergency security events via Cloud Guard interconnection).

### 3.8.1.4. 云眼

深信服云眼为互联网业务提供持续的风险评估+实时监测+篡改处置+应急对抗服务，让用户重新获得更加安全的保障。

设备可以访问互联网，同时已开通云眼，并在云眼平台完成了相关监测网站的绑定。此处可通过所开通的云眼账号，完成与云眼平台的对接。

绑定后，可以通过右上角  按钮，完成绑定账号的解除。

具体配置效果如下图所示：



The screenshot shows two side-by-side views of the Sangfor Cloud Mirror (云镜) interface. Both views feature a top navigation bar with tabs: 安全云脑 (Security Cloud Brain), 云守 (Cloud Guard), 云眼 (Cloud Eye), 云镜 (Cloud Mirror), and EDR. The left view displays the 'Cloud Eye' section, which includes a logo, the text '深信服云眼', a brief description of its risk assessment and monitoring features, and a '前往云眼Web端' (Go to Cloud Eye Web End) button. It also has a 'Cloud Eye Access Settings' section with fields for account and password, and a 'Connect Now' button. The right view shows the 'Cloud Eye' section with a similar layout, including a logo, a brief description, a '前往云眼Web端' button, and a 'Cloud Eye Service Information' box containing details like service status (Online), account number (sangfor), service duration (6 days), and expiration date (2018-12-30). Both sections have a 'Cloud Mirror Features' section at the bottom.

### 3.8.1.5. 云镜

深信服云镜结合业界最佳安全实践，聚焦高可利用安全漏洞及紧急安全事件，持续为用户业务系统安全保驾护航。

云镜无需配置，可通过点击 [前往云镜Web端](#) 进行云镜界面操作，如下图：

安全云脑 云守 云眼 云境 EDR

## 深信服云镜

深信服云镜结合业界最佳安全实践，聚焦高可利用安全漏洞及紧急安全事件，持续为用户业务系统安全保驾护航。

[前往云镜Web端](#)

### 服务亮点

-  预防为先  
安全漏洞，提早发现，防患于未然，消灭于摇篮。
-  持续检测  
风险异动，持续检测，过程无死角，异常早发现。
-  资产可视  
业务画像，全面可视，资产了如心，风险去无踪。
-  紧急响应  
紧急漏洞，及时响应，攻与防对抗，时效最优先。
-  即刻处理  
即时检测，处置止损，事前发现早，事后损失少。

### 3.8.1.6. EDR

深信服终端检测响应平台 EDR，通过人工智能 SAVE 引擎、行为引擎、云引擎、信誉库，持续检测发现、快速响应处置，构筑全面有效的终端威胁平台，深信服 EDR 产品可与 AF、SIP、AC 产品进行协同联动、自动处置，形成多层次立体化的威胁防御体系。

设备可以与 EDR 平台进行通信，同时 EDR 平台已完成主机的 EDR 客户端安装与部署。

绑定后，可以通过右上角  按钮，完成绑定平台的解除。

具体配置效果如下图所示：



The screenshot shows the Sangfor EDR Management Platform. At the top, there are two tabs: '联动EDR' (left) and 'EDR' (right). Below the tabs, there are two main sections: 'EDR接入设置' (EDR Connection Settings) and '服务亮点' (Service Features). The 'EDR接入设置' section contains an input field for 'EDR平台IP:' and a button labeled '立即接入' (Connect Now). The '服务亮点' section highlights two features: '人工智能, 精准识别' (AI, Precise Identification) and '协同联动, 快速响应' (Cooperative Interconnection, Quick Response). To the right, there is a summary of EDR service status: '服务状态: 在线' (Status: Online), 'EDR平台IP: 117.48.147.11', and '服务时长: 已累计为您服务219天' (Service Duration: Total service time for you is 219 days). Below this, there are statistics: '接入EDR终端数: 1031 台' (Number of connected EDR terminals: 1031 units) and '已联动处置次数: 0 次' (Number of cooperative handling cases: 0 times).

## 3.8.2. EDR

### 3.8.2.1. 概述

设置 AF 与 EDR 联动的功能，通过此功能，可以查看历史 AF 联动 EDR 处置的记录，同时查看当前 EDR 平台上已接入的相关终端信息。如下图所示：

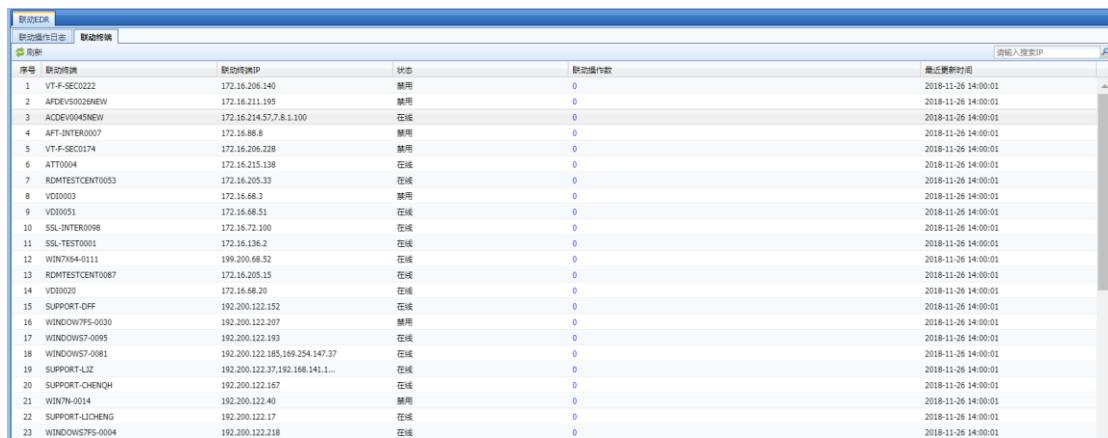


### 3.8.2.2. 联动操作日志

查看 AF 历史联动 EDR 操作的相关日志。可以点击 [前往EDR管理平台](#)，直接打跳转到 EDR 管理平台。

### 3.8.2.3. 联动终端

查看当前 EDR 平台上联动的所有终端，包括在线、离线、禁用状态的均会显示出来，如下图：



序号	联动终端	联动终端IP	状态	联动操作数	最近更新时间
1	VT-F-SEC0222	172.16.206.140	禁用	0	2018-11-26 14:00:01
2	APEV05020NEW	172.16.211.195	禁用	0	2018-11-26 14:00:01
3	ACDEV0045NEW	172.16.214.57.7.8.1.100	在线	0	2018-11-26 14:00:01
4	APT-INTER0007	172.16.88.8	禁用	0	2018-11-26 14:00:01
5	VT-F-SEC0174	172.16.206.228	禁用	0	2018-11-26 14:00:01
6	ATT0004	172.16.215.138	在线	0	2018-11-26 14:00:01
7	RDMTESTCENT0053	172.16.205.33	在线	0	2018-11-26 14:00:01
8	VDD0003	172.16.68.3	禁用	0	2018-11-26 14:00:01
9	VDD0051	172.16.66.51	在线	0	2018-11-26 14:00:01
10	SSL-INTER0098	172.16.72.100	在线	0	2018-11-26 14:00:01
11	SSL-TEST0001	172.16.136.2	在线	0	2018-11-26 14:00:01
12	WIN7X8-0111	199.200.68.52	在线	0	2018-11-26 14:00:01
13	RDMTESTCENT0087	172.16.205.15	在线	0	2018-11-26 14:00:01
14	VDD0020	172.16.68.20	在线	0	2018-11-26 14:00:01
15	SUPPORT-OFF	192.200.122.152	在线	0	2018-11-26 14:00:01
16	WINDOW7FS-0030	192.200.122.207	禁用	0	2018-11-26 14:00:01
17	WINDOW7ST-0095	192.200.122.193	在线	0	2018-11-26 14:00:01
18	WINDOW7ST-0081	192.200.122.185.169.254.147.37	在线	0	2018-11-26 14:00:01
19	SUPPORT-LJZ	192.200.122.37.192.168.141.1...	在线	0	2018-11-26 14:00:01
20	SUPPORT-CHENQH	192.200.122.167	在线	0	2018-11-26 14:00:01
21	WIN7N-0014	192.200.122.40	禁用	0	2018-11-26 14:00:01
22	SUPPORT-LIENGHENG	192.200.122.17	在线	0	2018-11-26 14:00:01
23	WINDOW7PS-0004	192.200.122.218	在线	0	2018-11-26 14:00:01

### 3.8.3. 云端增值服务

#### 3.8.3.1 概述

设置 AF 与云脑、云眼的联动展示。此处无需单独配置，只要在 3.8.1 章节里，完成了云脑与云眼的相关配置即可。如下图所示：



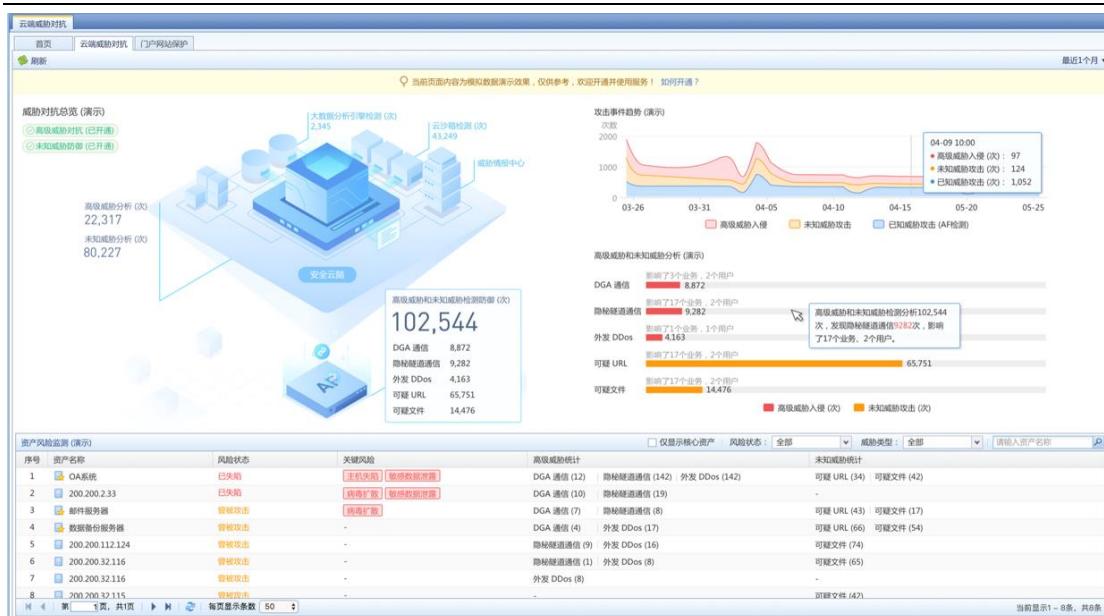
[云端威胁对抗]: 联动云脑功能，持续监测和展示“未知威胁鉴别”和“高级威胁分析”的状态；

[门户网站保护]: 联动云眼功能，持续监测和展示“网站安全状态监测”和“网站风险监测”的状态；

点击进入按钮，可进入对应的功能模块，进行状态查看，具体见3.8.3.2和3.8.3.3章节。

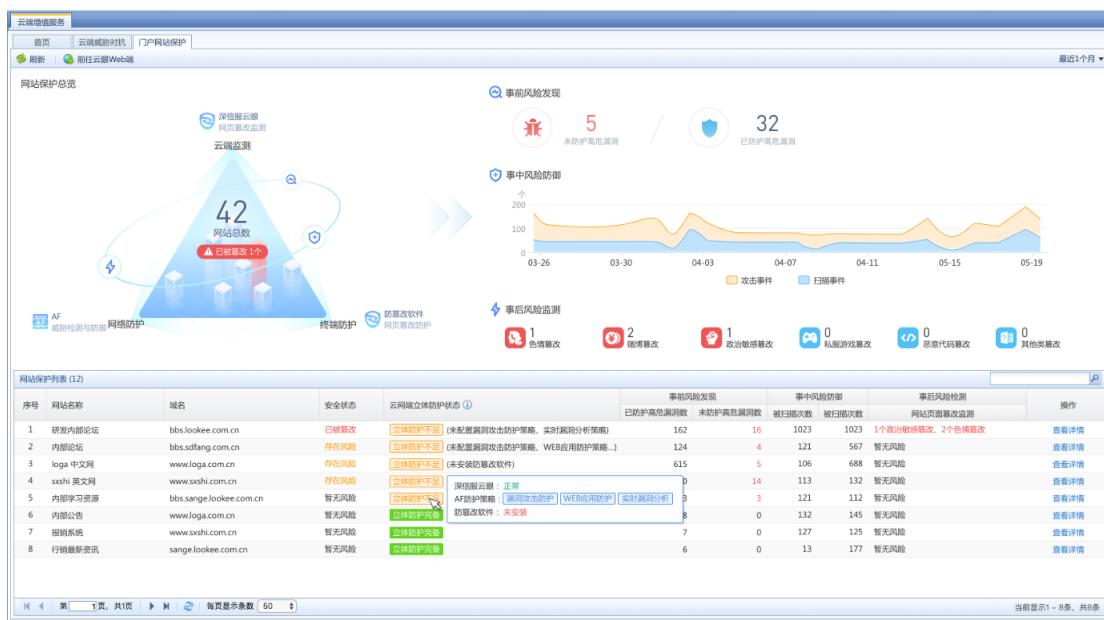
### 3.8.3.2 云端威胁对抗

对云脑功能处置的数据进行统一展示，此界面无需做相关的配置，效果图如下图所示：



### 3.8.3.3 门户网站保护

对云眼功能处置的数据进行统一展示，此界面无需做相关的配置，效果图如下图所示：



### 3.8.4. 安全防护能力

展示深信服科技 AF 的更新能力，包括“安全能力图谱”、“能力更新指标”

和“能力更新日历”三部分内容。如下图所示：



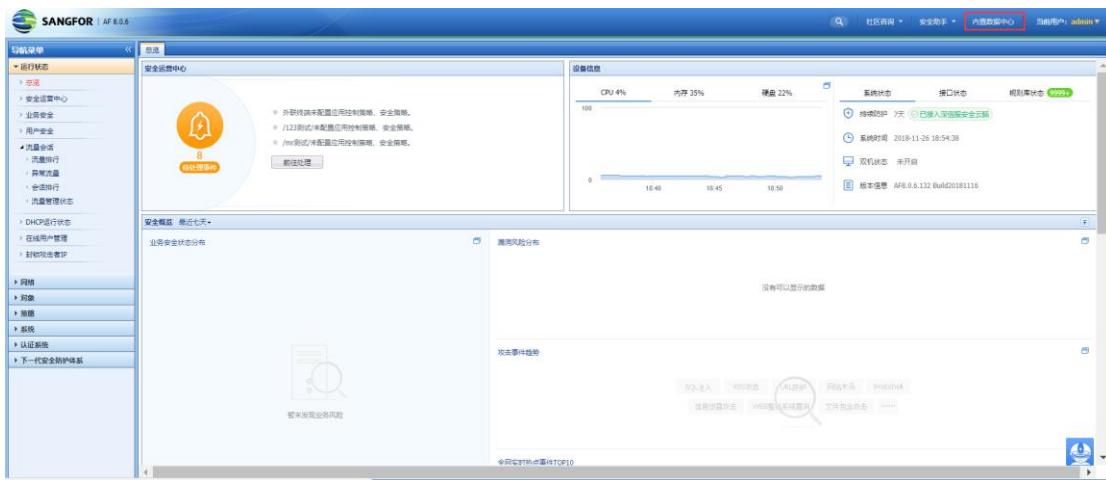
[安全能力图谱]: 以图例方式展示 AF 与其它深信服产品的联动更新过程，完成“事前风险发现能力”、“事中风险防御能力”和“事后风险管理能力”的实时更新；

[能力更新指标]: 以趋势图的方式展示持续更新的能力，以及相关热点事件的实时数据；

[能力更新日历]: 以日历的方式展示每日规则库更新的种类，及其具体的更新数量。

## 第4章 数据中心

数据中心主要用于查询和统计各功能模块产生的日志。例如可以查询出WEB应用防护阻断的攻击行为，以及可以查询到攻击源IP，目标IP等详细信息。可以统计出服务器在指定的时间内受到多少次DOS攻击等。点击页面右上角的**内置数据中心**，可以进入数据中心页面。界面如下：



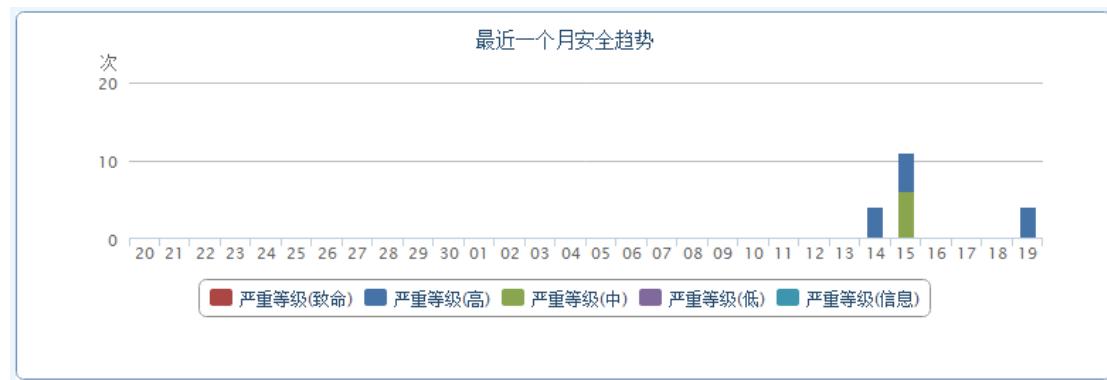
### 4.1. 统计分析

进入数据中心后，首页即显示近一个月的安全趋势。界面如下：



[磁盘信息]: 用于显示当前磁盘的占用比率。图中表示磁盘占用了 3%。

[最近一个月安全趋势]: 显示了近一个月的安全趋势。此安全包括病毒防御、ActiveX 过滤、脚本过滤、DOS 攻击、漏洞攻击防护、WEB 应用防护中检测出来的各种安全威胁。将鼠标移动到相应柱子上，即可显示详细信息。横坐标为时间，纵坐标为次数。界面如下：



### 4.1.1. 业务安全

服务器安全主要用于统计服务器受到外网 DOS 攻击、漏洞攻击防护、WEB

应用防护模块的攻击次数，界面如下：



The screenshot shows the 'Business Security' module with the 'Attack Statistics' tab selected. The configuration includes:

- Time Range: Today (2018-11-26) to Today (2018-11-26)
- Server IP: All
- Attack Type: All
- Severity Level: Critical, High, Medium, Low, Information
- Action: Allow, Reject
- Statistics Method: Target Server (selected), Attack Type, Attack Source
- Statistics Count: 10
- Chart Display: Statistics (selected), Trend, Statistics & Trend

At the bottom are 'Query' and 'New Tab' buttons.

#### 4.1.1.1. 业务安全统计案例

应用场景案例：某用户需要统计 11 月 1 日到 11 月 26 号内网所有服务器受到 WEB 应用攻击的次数以及百分比。只需要统计前 10 名即可。

第一步：设置好统计条件，界面如下：

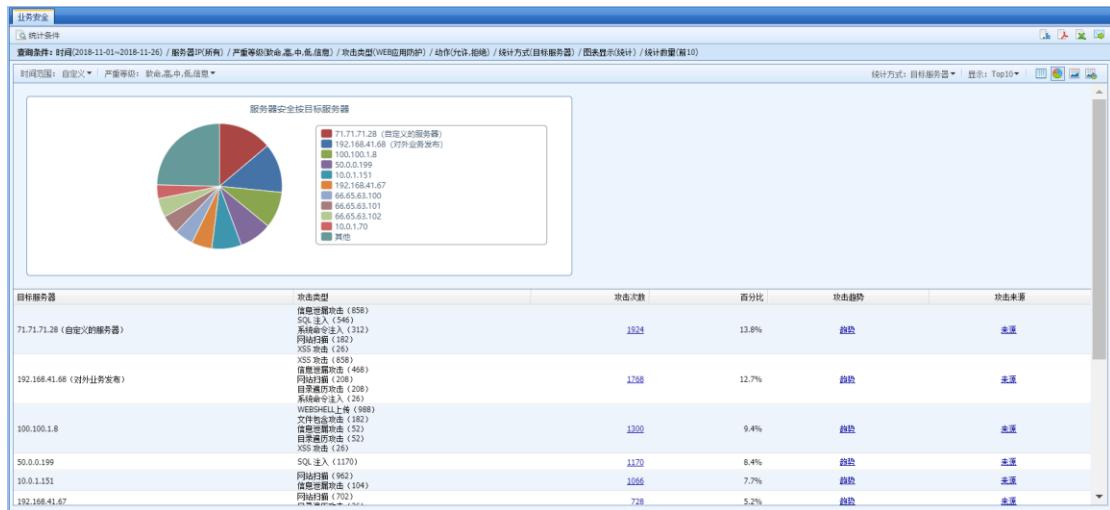


The screenshot shows the 'Business Security' module with the 'Attack Statistics' tab selected. The configuration includes:

- Time Range: Custom (2018-11-01) to (2018-11-26)
- Server IP: All
- Attack Type: WEB Application Defense (selected)
- Severity Level: Critical, High, Medium, Low, Information
- Action: Allow, Reject
- Statistics Method: Target Server, Attack Type (selected), Attack Source
- Statistics Count: 10
- Chart Display: Statistics (selected), Trend, Statistics & Trend

At the bottom are 'Query', 'Close', and 'New Tab' buttons.

第二步：点击 **查询**，会自动生成报表。界面如下：



第三步：上图中如果想查看服务器受 WEB 应用攻击中的哪一种攻击，则可以点击攻击次数，可以链接到详细页面。页面如下：



必须在控制面板的相应规则处勾选了检测后操作日志“记录”，才能在数据中心统计到服务器安全日志。

### 4.1.2. 用户安全

用户安全主要用于统计内网用户发起内网 DOS 攻击、漏洞攻击防护攻击、杀毒、APT 检测的攻击行为次数以及百分比。界面如下：

用户安全

设置统计条件点击“查询”按钮开始统计

统计条件

时间范围：今天 2018-11-26 15 至 2018-11-26 15

IP/用户：所有 IP 用户 组

威胁类型：

严重等级：致命 高 中 低 信息

动作：允许 拒绝

统计选项

统计方式：主机IP 威胁类型

统计数量：10

简单统计↑

从新选项卡打开

#### 4.1.2.1. 用户安全统计案例

典型应用案例：某客户需要统计出 11 月 1 日到 11 月 26 日内网用户受到僵尸网络攻击的次数，统计出前 10 名即可。

第一步：设置好统计条件，界面如下：

用户安全

设置统计条件点击“查询”按钮开始统计

统计条件

时间范围：自定义 2018-11-01 15 至 2018-11-26 15

IP/用户：所有 IP 用户 组

威胁类型：

严重等级：致命 高 中 低 信息

动作：允许 拒绝

统计选项

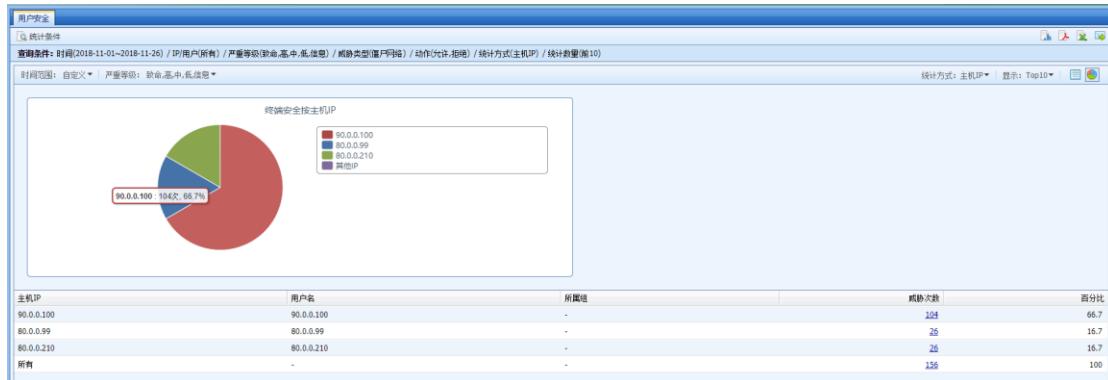
统计方式：主机IP 威胁类型

统计数量：10

简单统计↑

从新选项卡打开

第二步：点击**查询**，设备会生成相应的图标，页面如下：



点击页面右上角的  四个按钮，分别可以对应生成报表、生成 PDF、导出 XLS、发送邮件四个操作。



必须在控制面板相应规则处勾选检测后操作日志“记录”，才能在数据中心统计到日志。

#### 4.1.3. 流量统计

流量统计用于统计内网用户上网的流量，可以根据应用，IP 等各种条件进行统计。界面如下：

流量统计

统计条件

设置统计条件点击“查询”按钮开始统计

统计条件

时间范围：自定义 2016-05-01 至 2016-05-30

时间计划：全天

IP/用户：所有 IP 用户 组

应用/协议：所有应用

统计选项

统计方式：应用类型 应用名称 组 IP/用户

排行依据：总流量 上行流量 下行流量

统计数量：10

图表显示：统计 趋势 统计&趋势

简单统计↑

查询 关闭  从新选项卡打开



#### 4.1.3.1. 流量统计案例

典型应用案例：某客户需要统计出5月30日内网用户哪些IP占用了最多流量，统计出前10名即可。

第一步：设置好统计条件，界面如下：

**流量统计**

 **统计条件**

 设置统计条件点击“查询”按钮开始统计

**统计条件**

时间范围：  至

时间计划：

IP/用户： 所有  IP  用户  组

应用/协议： 

**统计选项**

统计方式： 应用类型  应用名称  组  IP/用户

排行依据： 总流量  上行流量  下行流量

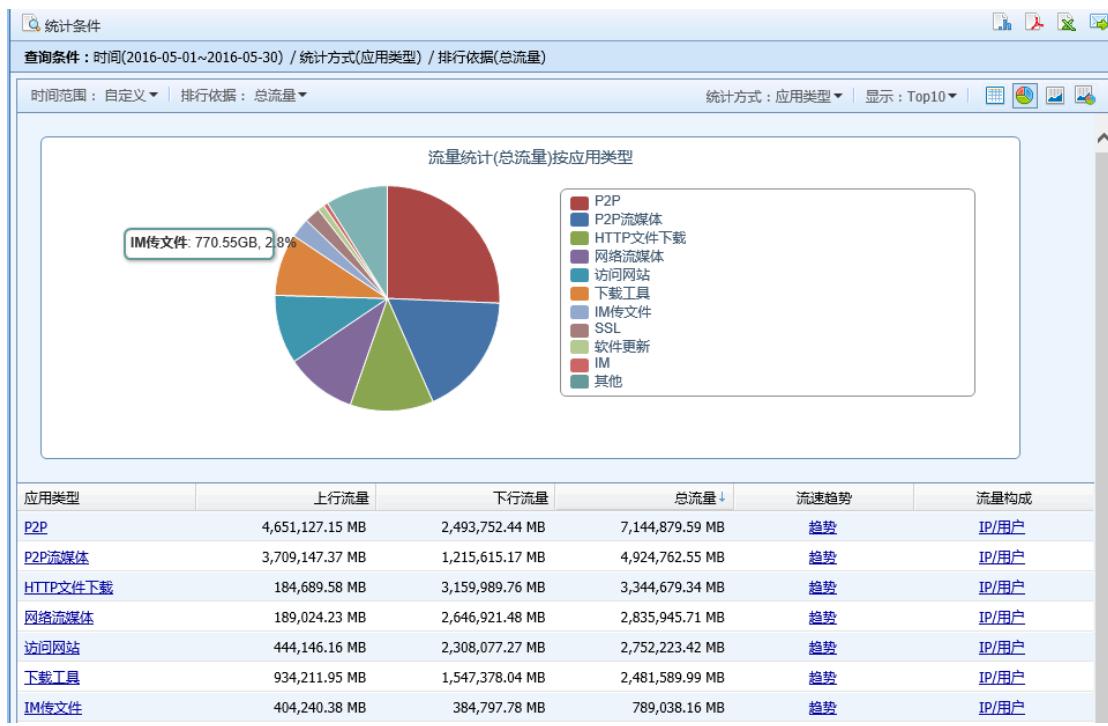
统计数量： 

图表显示： 统计  趋势  统计&趋势

 **简单统计↑**

从新选项卡打开

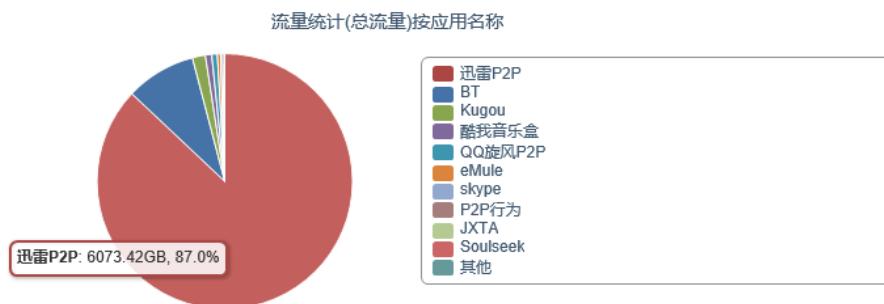
第二步：点击**查询**，设备会生成相应数据，页面如下：



点击趋势，可以查看该IP在5月30日当天的流速趋势。界面如下：



点击应用名称，可以查看该IP的流量构成。界面如下：



点击页面右上角的    四个按钮，分别可以对应生成报表、生成PDF、导出XLS、发送邮件四个操作。



流量统计设备默认已经开启，不需要在控制台做统计流量的操作。

#### 4.1.4. 应用统计

应用统计主要用于统计内网用户上网的时候访问某一种应用的次数。例如可以统计内网用户访问哪些应用最活跃，既访问的次数最多。界面如下：

应用统计

统计条件

设置统计条件点击“查询”按钮开始统计

统计条件

时间范围：自定义 2016-05-01 至 2016-05-30

时间计划：全天

IP/用户： 所有  IP  用户  组

应用：所有应用 

动作： 允许  拒绝

统计选项

统计方式： 应用类型  应用名称  IP/用户

统计数量：10 

简单统计↑

查询 关闭  从新选项卡打开

#### 4.1.4.1. 应用统计案例

典型应用案例：某客户需要统计出 5 月 1 日到 5 月 30 日内网用户哪些应用最多。统计出前 10 名即可。

第一步：设置好统计条件，界面如下：

应用统计

统计条件

设置统计条件点击“查询”按钮开始统计

统计条件

时间范围：自定义 2016-05-01 至 2016-05-30

时间计划：全天

IP/用户：所有

应用：所有应用

动作：允许 拒绝

统计选项

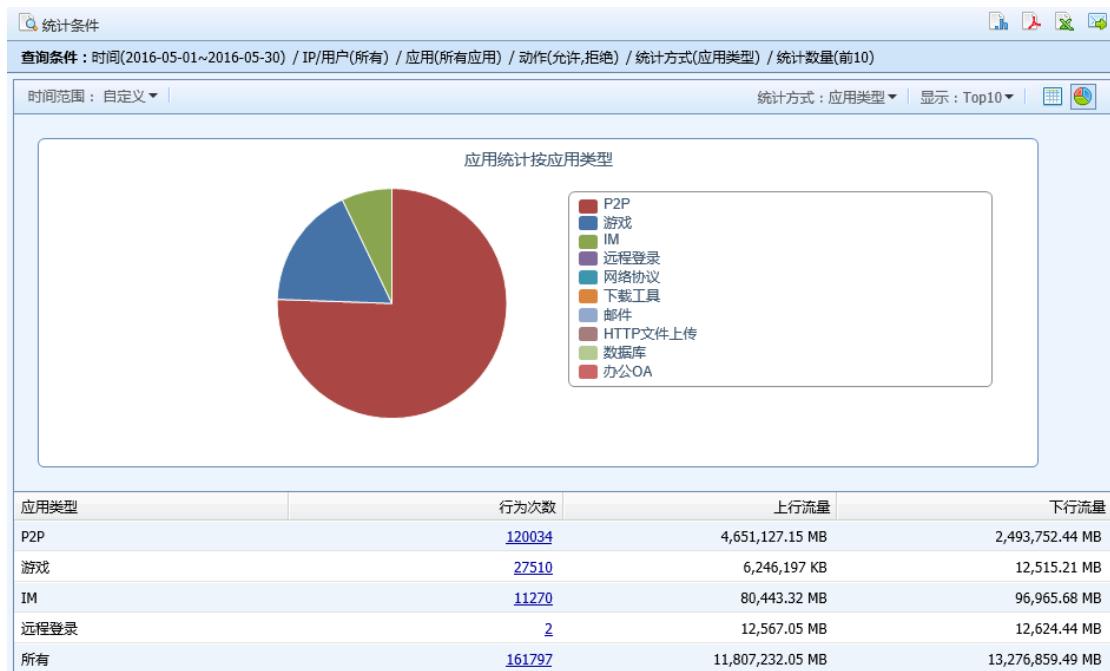
统计方式：应用类型 应用名称 IP/用户

统计数量：10

简单统计↑

查询 关闭  从新选项卡打开

第二步：点击**统计**，即可生成相应的数据，页面如下：



以上可以看出，内网用户上网访问 P2P 的应用次数是最高的。

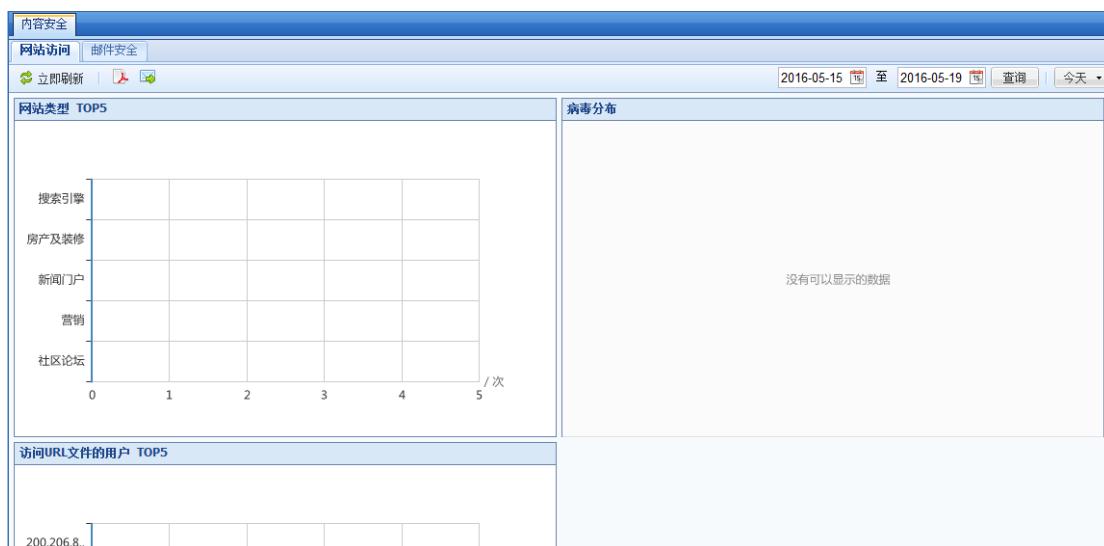


必须在『内网安全』-『应用控制策略』中新建策略，并且日志勾选“记录”，数据中心才能统计到数据。

## 4.1.5. 内容安全

### 4.1.5.1. 网站访问

网站访问主要用于统计内网用户访问网站类型、访问 URL 文件的用户、病毒分布的数据。界面如下：



选择日期点击【查询】就可以统计出 TOP5 的数据，点击【PDF】导出 PDF，可生成 PDF 文档下载。点击【邮件】发送，可生成 PDF 文档发送到指定邮箱，但需要先配置好邮件服务器，配置参考章节 4.4.1 系统设置。

### 4.1.5.2. 邮件安全

邮件安全主要可以统计攻击源地理分布图和被攻击的用户 TOP5 数据。页面配置如下：



选择日期点击  就可以统计出 TOP5 的数据，点击  导出 PDF，可生成 PDF 文档下载。点击  邮件发送，可生成 PDF 文档发送到指定邮箱，但需要先配置好邮件服务器，配置参考章节 4.4.1 系统设置。



必须在「内网安全」-「内容安全策略」中新建规则，并且日志勾选“记录”，才能在数据中心查看到统计信息。

#### 4.1.6. 业务模型学习监督

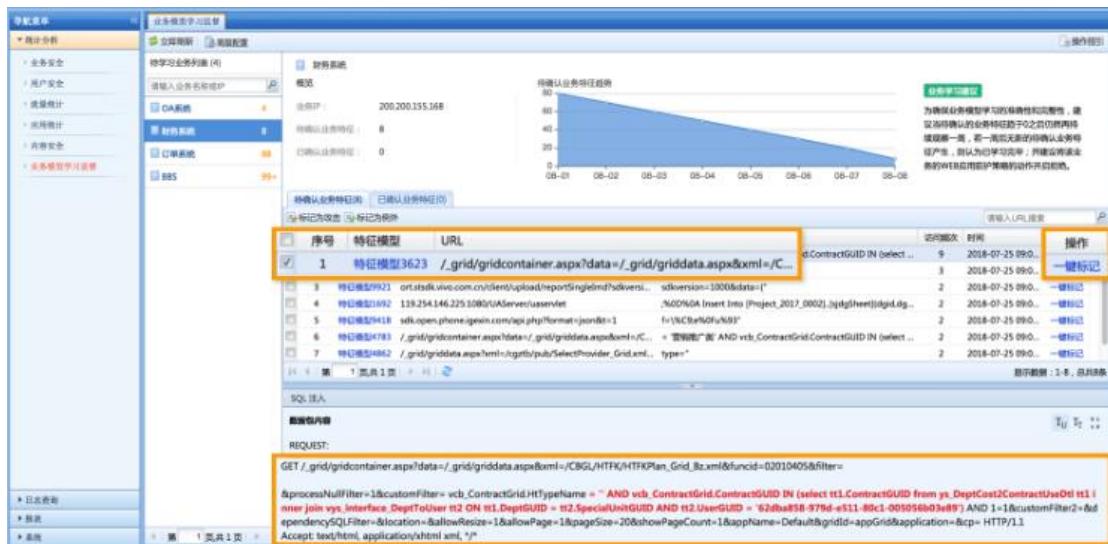
使用 AI 半自动化学习算法(部分需要人工参与)解决 WEB 业务代码编写不规范导致业务误判问题，然后能够将 WEB 应用安全策略开启防御模式，保障业务系统的安全与稳定运行。

AI 半自动化学习算法对 WEB 业务访问的流量进行分析与学习，学习 WEB 业务系统特征；然后将基于攻击特征和业务特征的检测方式进行融合，解决 WEB 业务代码编写不规范导致的误判问题。对于 AI 学习算法无法自动判别的特征，通过人工进行判别与标记；该学习方法需要针对业务系统访问流量持续学习一段时间，直到业务系统的特征全部学习完成，才能将对应业务的 WEB 应用防护策略开启防御。

## 使用指南：

### 第一步：判别与标记业务特征

查看业务特征对应的原始数据包内容(高亮部分为特征)，判别该特征是正常的业务访问特征还是攻击特征，并对其进行标记。



序号	特征模型	URL	操作
1	特征模型3623	/_grid/gridcontainer.aspx?data=/_grid/griddatas.aspx&xml=/C...	一键标记
2			
3			
4			
5			
6			
7			

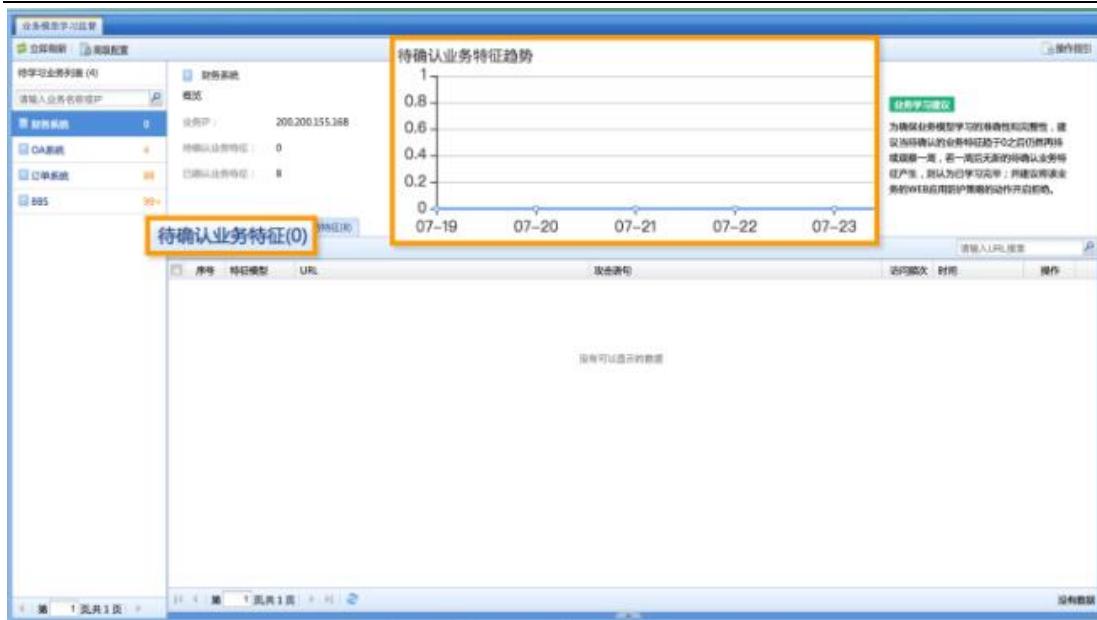
REQUEST:

```

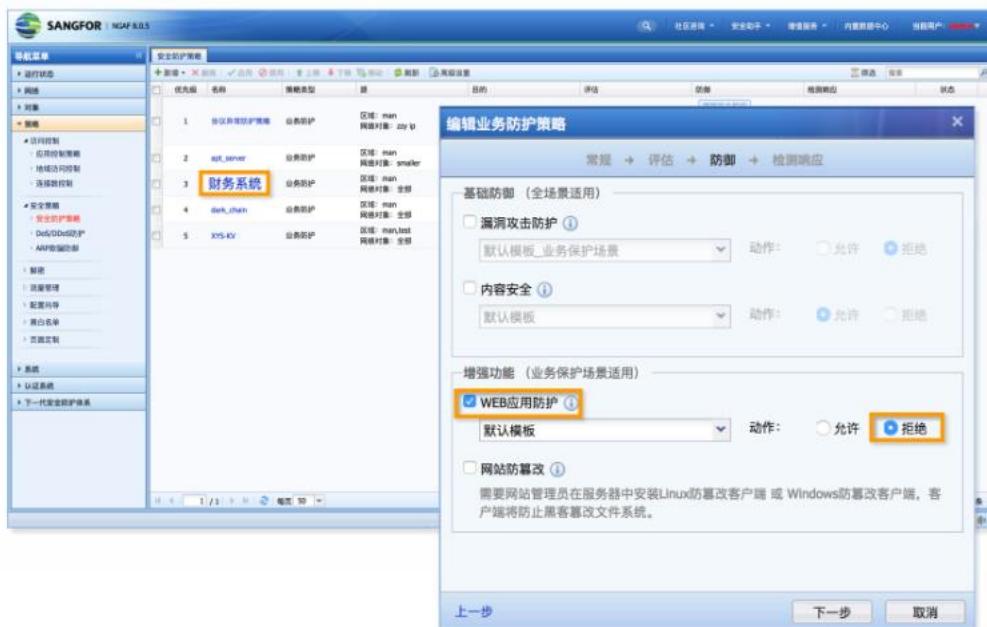
GET /_grid/gridcontainer.aspx?data=/_grid/griddatas.aspx&xml=/CBGL/HTFK/HTFKPten_Grid_Bz.xml&funcid=02010405&filter=
&processNullFilter=1&customFilter= vcb_ContractGrid.Ht?typeName = " AND vcb_ContractGrid.ContractGUID IN (select tt1.ContractGUID from ys_DeptCost2ContractUseDetail tt1
inner join vys_Interface_DeptToUser tt2 ON tt1.DeptGUID = tt2.SpecifyUnitGUID AND tt2.UserId = 62db858-979d-e511-80c1-005056b03e97) AND 1=1&customFilter2=&filter
dependingsSQLFilter=&location=&allowResize=1&allowPage=1&pageCount=1&showPageCount=1&appName=Default&gridId=appGrid&application=Bcp= HTTP/1.1
Accept: text/html,application/xhtml+xml,*/*
    
```

### 第二步：确认业务模型学习趋势

当业务待确认特征趋势趋于 0，且连续两周内无新的待确认特征产生，则表明该业务系统的业务特征已学习完毕，建议将该业务系统的 WEB 应用防护策略的动作开启拒绝。



在“策略 -> 安全策略 -> 安全防护策略”页面找到对应业务的策略，然后在“编辑业务防护策略”弹窗中，点击下一步，到“防御”页面，将“WEB 应用防护”的动作配置为“拒绝”。



## 4.2. 日志查询

日志查询主要用于查询具体的日志情况，例如可以查询到内网哪台服务器受

到了 DOS 攻击，并且查询出攻击的源 IP 和端口等详细信息。界面如下：

#### 4.2.1. DOS 攻击

DOS 攻击用于查询内网->外网 DOS 攻击和外网->内网 DOS 攻击具体信息。例如可以查询出某个时间内所有内网服务器受到 ICMP 洪水攻击的具体情况。DOS 攻击查询界面如下：

DoS攻击

设置查询条件点击"查询"按钮开始查询

起始时间:	2016-05-19	15	00:00
结束时间:	2016-05-19	15	23:59
攻击方向:	<input checked="" type="checkbox"/> 内网->外网	<input checked="" type="checkbox"/> 外网->内网	
攻击者区域:	所有区域		
攻击者IP:	所有		
攻击类型:	所有类型		
严重等级:	<input checked="" type="checkbox"/> 高	<input checked="" type="checkbox"/> 中	<input checked="" type="checkbox"/> 低
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝	

查询结果从新标签页中打开

#### 4.2.1.1. DOS 攻击查询案例

典型应用案例：某客户需要查询出 5 月 30 日当天内网服务器受到的 DOS 攻击具体情况。内网用户的 DOS 攻击不用查询。

第一步：设置好查询条件，界面如下。由于统计内网服务器，所以要选择攻击方向为外网->内网。界面如下：

查询条件 | 导出日志

设置查询条件点击"查询"按钮开始查询

起始时间:	2016-05-30	15	00:00
结束时间:	2016-05-30	15	23:59
攻击方向:	<input type="checkbox"/> 内网->外网	<input checked="" type="checkbox"/> 外网->内网	
攻击者区域:	所有区域		
攻击者IP:	所有		
攻击类型:	所有类型		
严重等级:	<input checked="" type="checkbox"/> 高	<input checked="" type="checkbox"/> 中	<input checked="" type="checkbox"/> 低
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝	

查询结果从新标签页中打开

第二步：点击**查询**，设备会自动查询出相应数据，页面如下：

序号	时间	类型	攻击方向	攻击者IP	攻击者MAC	受害者IP	严重等级	动作	描述	详细
1	2016-05-30 23:03:40	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	严重1			查看
2	2016-05-30 23:55:37	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	严重1		IP数据块分片传输	查看
3	2016-05-30 23:54:31	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	严重1		IP数据块分片传输	查看
4	2016-05-30 23:51:37	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	严重1		IP数据块分片传输	查看
5	2016-05-30 23:49:31	IP数据块分片传输	外网->内网	117.135.156.51	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
6	2016-05-30 23:48:39	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
7	2016-05-30 23:47:39	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
8	2016-05-30 23:46:47	IP数据块分片传输	外网->内网	117.135.156.51	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
9	2016-05-30 23:46:33	IP数据块分片传输	外网->内网	117.135.156.51	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
10	2016-05-30 23:44:31	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
11	2016-05-30 23:44:17	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
12	2016-05-30 23:42:17	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
13	2016-05-30 23:37:17	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
14	2016-05-30 23:26:17	IP数据块分片传输	外网->内网	59.151.36.122	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
15	2016-05-30 23:25:41	IP数据块分片传输	外网->内网	117.135.156.52	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
16	2016-05-30 23:25:27	IP数据块分片传输	外网->内网	117.135.156.52	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
17	2016-05-30 23:25:11	IP数据块分片传输	外网->内网	117.135.156.52	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
18	2016-05-30 22:07:14	IP数据块分片传输	外网->内网	117.135.156.52	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
19	2016-05-30 22:06:46	IP数据块分片传输	外网->内网	182.254.17.102	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
20	2016-05-30 22:06:44	IP数据块分片传输	外网->内网	182.254.17.102	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看
21	2016-05-30 21:50:07	IP数据块分片传输	外网->内网	182.254.17.102	00:30:80:16:9f:9a	211.161.129.69	中	拒绝	WAN	查看

以上数据可以看出内网 211.161.129.69 服务器在 5 月 30 日 16:14 分受到外网 DOS 攻击。攻击类型为 IP 数据块分片传输，攻击源 IP 为 59.151.36.122。

#### 4.2.2. WEB 应用防护

WEB 应用攻击用于查询『服务器保护』中检测到的各种攻击行为。界面如下：

查询条件
导出日志

设置查询条件点击“查询”按钮开始查询

起始时间:	<input type="text" value="2016-05-30"/> <input type="button" value="15"/>	00:00	
结束时间:	<input type="text" value="2016-05-30"/> <input type="button" value="15"/>	23:59	
源区域:	<input type="text" value="所有区域"/>		
源IP:	<input type="text" value="所有"/>		
目的区域:	<input type="text" value="所有区域"/>		
目的IP:	<input type="text" value="所有"/>		
类型:	<input type="text" value="所有类型"/>		
规则ID:	<input type="text" value="所有"/>		
回复状态码:	<input type="text" value="所有"/>		
域名/URL:	<input type="text" value="所有"/>		
严重等级:	<input checked="" type="checkbox"/> 高	<input checked="" type="checkbox"/> 中	<input checked="" type="checkbox"/> 低
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝	
日志归并:	<input checked="" type="checkbox"/> 启用		

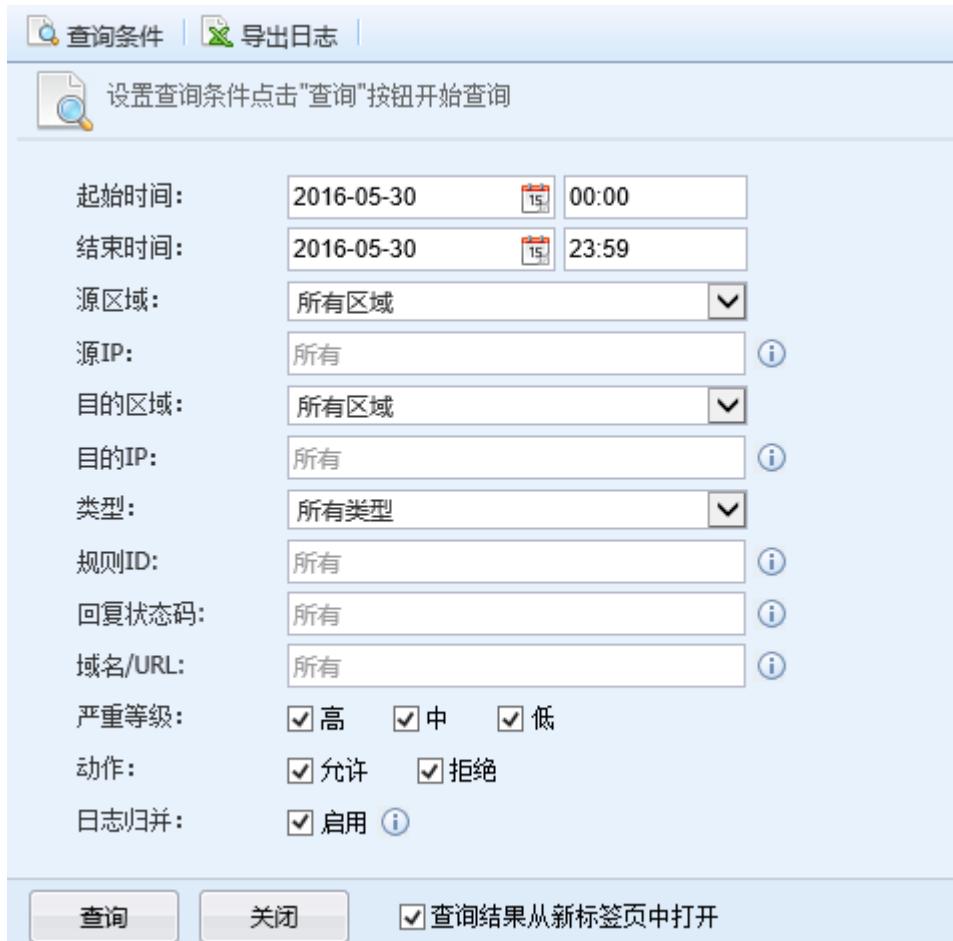
查询
关闭

查询结果从新标签页中打开

### 4.2.2.1. WEB 应用攻击查询案例

典型应用案例：某客户需要查询出 5 月 30 日当天所有的 WAF 应用防护的具体情况。

第一步：设置好查询条件，界面如下：



The screenshot shows the 'Query Conditions' (查询条件) screen of the Sangfor WAF system. The search parameters are set as follows:

- 起始时间 (Start Time): 2016-05-30 00:00
- 结束时间 (End Time): 2016-05-30 23:59
- 源区域 (Source Region): 所有区域 (All Regions)
- 源IP (Source IP): 所有 (All)
- 目的区域 (Destination Region): 所有区域 (All Regions)
- 目的IP (Destination IP): 所有 (All)
- 类型 (Type): 所有类型 (All Types)
- 规则ID (Rule ID): 所有 (All)
- 回复状态码 (Response Status Code): 所有 (All)
- 域名/URL (Domain/URL): 所有 (All)
- 严重等级 (Severity Level): 高 (High), 中 (Medium), 低 (Low) (all checked)
- 动作 (Action): 允许 (Allow), 拒绝 (Deny) (both checked)
- 日志归并 (Log Aggregation): 启用 (Enabled) (checked)

At the bottom, there are 'Query' (查询) and 'Close' (关闭) buttons, and a checked checkbox for opening the results in a new tab.

第二步：点击 **查询**，设备会过滤出相应信息，页面如下：



The screenshot shows the query results table for May 30, 2016. The table lists 10 entries of detected attacks, each with details like time, type, source IP, destination IP, rule ID, severity, action, and a 'View' (查看) link for more details.

序号	时间	类型	URL/目录	源IP	源IP归属地	目的IP	规则ID号	描述	严重等级	动作	详细	白名单
1	2016-05-30 20:57:41	暴力破解FTP口令	-	61.147.121.73	中国江苏	10.1.1.110	-	FTP登录密码尝试次数过多！	高	拒绝	查看	添加例外
2	2016-05-30 20:57:41	弱口令类型-长度...	-	61.147.121.73	中国江苏	10.1.1.110	-	检测到使用弱密码登录FTP！	中	允许	查看	添加例外
3	2016-05-30 20:07:45	方法过滤	www.baidu.com:443www.baidu...	22.251.63.45	美国	10.1.1.2	-	检测到不合法的HTTP请求方法！	中	拒绝	查看	添加例外
4	2016-05-30 19:37:29	WEBSSH上传	www.ghidri.com.cn/pvvp35535.bt	222.73.144.34	中国上海	10.1.1.1	13080089	攻击语句: <%eval(eval(chr(	高	拒绝	查看	添加例外
5	2016-05-30 19:12:47	信息泄漏攻击	www.ghidri.com.cn/wwwroot.rar	120.52.18.48	中国河北	10.1.1.1	-	Source code disclosure exists! At...	中	拒绝	查看	添加例外
6	2016-05-30 19:05:23	WEB登录弱口令防护	mail.ghidri.com.cn/?q=login...	222.73.144.32	中国上海	10.1.1.2	-	检测到使用弱密码登录WEB！	中	允许	查看	添加例外
7	2016-05-30 19:00:38	WEB登录明文传输...	mail.ghidri.com.cn/?q=login.do	222.73.144.32	中国上海	10.1.1.2	-	检测到使用明文登录，登录的账户...	中	允许	查看	添加例外
8	2016-05-30 19:00:16	WEB登录明文传输...	mail.ghidri.com.cn/?q=login...	222.73.144.32	中国上海	10.1.1.2	-	检测到使用明文登录，登录的账户...	中	允许	查看	添加例外
9	2016-05-30 18:59:59	信息泄漏攻击	61.189.156.5/phpMyAdmin	113.10.160.166	中国香港	10.1.1.10	13070055	攻击语句: GET /phpMyAdmin/H...	高	拒绝	查看	添加例外
10	2016-05-30 17:49:19	信息泄漏攻击	61.189.156.11/phpMyAdmin/php...	113.10.160.166	中国香港	10.1.1.2	13070055	攻击语句: GET /phpMyAdmin/p...	高	拒绝	查看	添加例外

将鼠标移动到 **查看** 处，会显示出具体信息，页面如下：

## 序号5

时间:	2016-05-30 19:12:47
类型:	信息泄漏攻击
协议:	HTTP
方法:	HEAD
URL/目录:	www.ghidri.com.cn/wwwroot.rar
源区域:	outside
源IP:	120.52.18.48
源IP归属地:	中国河北
源端口:	6311
目的区域:	DMZ
目的IP:	10.1.1.1
目的端口:	80
规则ID号:	-
回复状态码:	-
四看法策略名:	web
描述:	Source code disclosure exists! Attack Type:信息泄漏攻击
严重等级:	中
动作:	拒绝

攻击者利用此漏洞收集WEB系统的安全缺陷，并以此为基础不断的刺

如果出现误判的情况，可以点击[添加例外](#)，将对应的 URL 或 IP 添加为白名单，放通 WAF 应用防护的拒绝。到 WEB 应用防护的排除列表可以查看得到。界面如下。

**添加例外**

URL:  i

**排除选项**

**排除例外**  
URL将被添加为白名单，WEB应用防护功能将不再检查访问此URL的所有请求。

**仅排除参数值符合以下特征的请求**  
WEB应用防护的网站攻击检测将跳过这些参数的检查。主要用于正常业务下某些请求参数因携带特征串而被检测为攻击的情况，可以只针对这些参数排除。  
参数特征串定义：

序号	参数名称	参数特征串	编辑

**提交** **取消**

点击左上角的  导出日志 可以将数据导出成 EXCEL 表格方式。



必须在『服务器保护』→『WEB 应用防护』中勾选，检测攻击后操作的日志勾选上了“记录”，才能查询到日志。

### 4.2.3. 漏洞攻击防护

漏洞攻击防护主要用于查询『漏洞攻击防护』模块检测出的各种漏洞攻击行为。界面如下：

漏洞攻击防护

设置查询条件点击"查询"按钮开始查询

起始时间:	2017-08-20	00:00			
结束时间:	2017-08-20	23:59			
攻击者区域:	所有区域				
攻击者IP:	所有				
受攻击者区域:	所有区域				
受攻击者IP:	所有				
漏洞类型:	所有漏洞				
漏洞ID:	所有				
严重等级:	<input checked="" type="checkbox"/> 致命	<input checked="" type="checkbox"/> 高	<input checked="" type="checkbox"/> 中	<input checked="" type="checkbox"/> 低	<input checked="" type="checkbox"/> 信息
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝			

查询结果从新标签页中打开

#### 4.2.3.1. 漏洞攻击防护查询案例

典型应用案例：某客户需要查询出5月30日当天从外网区到内网区，攻击服务器的漏洞详细信息。

第一步：设置好查询条件，页面如下：

设置查询条件点击“查询”按钮开始查询

起始时间：	<input type="text" value="2016-05-30"/>	<input type="button" value="15"/>	00:00
结束时间：	<input type="text" value="2016-05-30"/>	<input type="button" value="15"/>	23:59
攻击者区域：	<input type="text" value="outside"/>		
攻击者IP：	<input type="text" value="所有"/>		
受攻击者区域：	<input type="text" value="inside"/>		
受攻击者IP：	<input type="text" value="所有"/>		
漏洞类型：	<input type="text" value="所有漏洞"/>		
漏洞ID：	<input type="text" value="所有"/>		
严重等级：	<input checked="" type="checkbox"/> 致命 <input checked="" type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input checked="" type="checkbox"/> 低 <input checked="" type="checkbox"/> 信息		
动作：	<input checked="" type="checkbox"/> 允许 <input checked="" type="checkbox"/> 拒绝		
<input type="button" value="查询"/> <input type="button" value="关闭"/>		<input checked="" type="checkbox"/> <b>查询结果从新标签页中打开</b>	

第二步：点击**查询**，设备会过滤出外网区到内网区，含有漏洞攻击防护漏洞

攻击的详细条目。界面如下：

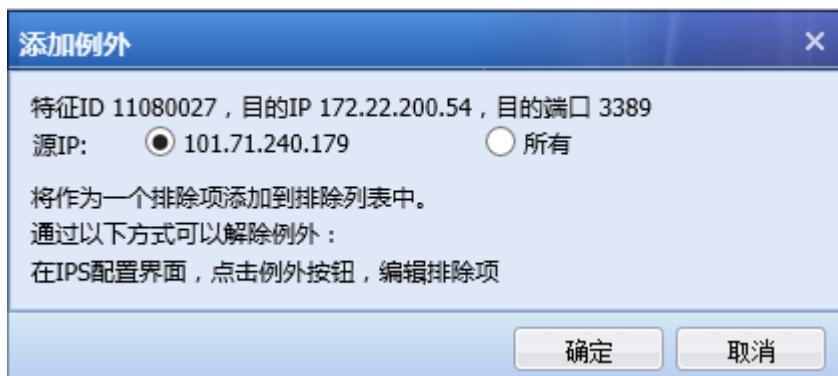
序号	时间	类型	攻击者IP	攻击者归属地	受攻击者IP	漏洞ID	漏洞名称	参考信息	严重等级	动作	查看	添加例外
1	2016-05-30 23:46:14	口令暴力破解攻击	101.71.240.179	中国浙江	172.22.200.54	11080027	RDP服务器暴力破解攻击	-	高	拒绝	查看	添加例外
2	2016-05-30 23:44:46	口令暴力破解攻击	115.28.163.149	中国山东	172.22.200.54	11080027	RDP服务器暴力破解攻击	-	高	拒绝	查看	添加例外
3	2016-05-30 23:41:30	口令暴力破解攻击	222.186.50.108	中国江苏	172.22.200.112	11080015	MS_SQL服务器暴力破解攻击	-	高	拒绝	查看	添加例外
4	2016-05-30 23:39:24	口令暴力破解攻击	117.184.206.38	中国上海	172.22.200.112	11080015	MS_SQL服务器暴力破解攻击	-	高	拒绝	查看	添加例外
5	2016-05-30 23:34:56	口令暴力破解攻击	222.186.129.107	中国江苏	172.22.200.112	11080015	MS_SQL服务器暴力破解攻击	-	高	拒绝	查看	添加例外
6	2016-05-30 23:30:18	口令暴力破解攻击	155.94.224.158	美国	172.22.200.54	11080027	RDP服务器暴力破解攻击	-	高	拒绝	查看	添加例外
7	2016-05-30 23:28:48	口令暴力破解攻击	115.28.182.188	中国山东	172.22.200.112	11080015	MS_SQL服务器暴力破解攻击	-	高	拒绝	查看	添加例外
8	2016-05-30 23:28:24	口令暴力破解攻击	58.221.60.180	中国江苏	172.22.200.112	11080015	MS_SQL服务器暴力破解攻击	-	高	拒绝	查看	添加例外
9	2016-05-30 23:26:48	口令暴力破解攻击	222.186.58.165	中国江苏	172.22.200.112	11080015	MS_SQL服务器暴力破解攻击	-	高	拒绝	查看	添加例外
10	2016-05-30 23:24:02	口令暴力破解攻击	113.195.162.138	中国江西	172.22.200.54	11080027	RDP服务器暴力破解攻击	-	高	拒绝	查看	添加例外

将鼠标移动到**查看**处，会显示出具体信息，页面如下：

**序号1**

<b>时间:</b>	2016-05-30 23:46:14
<b>类型:</b>	口令暴力破解攻击
<b>协议:</b>	TCP
<b>攻击者区域:</b>	outside
<b>攻击者IP:</b>	101.71.240.179
<b>攻击者归属地:</b>	中国浙江
<b>URL/目录:</b>	-
<b>攻击者端口:</b>	54742
<b>受攻击者区域:</b>	inside
<b>受攻击者IP:</b>	172.22.200.54
<b>受攻击者端口:</b>	3389
<b>漏洞ID:</b>	11080027
<b>漏洞名称:</b>	RDP服务器暴力破解攻击
<b>匹配策略名:</b>	ips
<b>描述:</b>	RDP_win8服务遭受到口令暴力破解攻击（56次/分钟）
<b>解决方案:</b>	将扫描IP地址列入黑名单，阻止攻击者进行暴力破解攻击。
<b>参考信息:</b>	-
<b>严重等级:</b>	高
<b>动作:</b>	拒绝

如果出现误判的情况，可以点击[添加例外](#)，将对应的特征 ID，目的 IP，目的端口添加到例外中，放通漏洞攻击防护的拒绝。添加后到漏洞攻击防护策略的例外排除可以查看。界面如下。



点击左上角的 [导出日志](#) 可以将数据导出成 EXCEL 表格方式。



必须在控制面板策略-安全防护策略处新建规则，并且检测攻击后操作的日志勾选上了“记录”，设备才能记录日志。

#### 4.2.4. 僵尸网络

僵尸网络用于查询『内容安全』 → 『僵尸网络』检查出来的日志，页面如下：



设置查询条件点击"查询"按钮开始查询

起始时间: 2016-05-19 00:00

结束时间: 2016-05-19 23:59

源区域: 所有区域

源IP/用户:  所有  IP  用户  组

目的区域: 所有区域

类型: 所有类型

特征ID: 所有

严重等级:  高  中  低  信息

动作:  允许  拒绝

查询  查询结果从新标签页中打开

##### 4.2.4.1. 僵尸网络查询案例

典型应用案例：用户要查询内网哪些 IP 地址或用户产生僵尸网络流量的详细信息。

第一步：设置查询条件，界面如下：

僵尸网络

设置查询条件点击“查询”按钮开始查询

起始时间:	2016-05-19	00:00
结束时间:	2016-05-19	23:59
源区域:	所有区域	
源IP/用户:	<input checked="" type="radio"/> 所有 <input type="radio"/> IP <input type="radio"/> 用户 <input type="radio"/> 组	
目的区域:	所有区域	
类型:	所有类型	
特征ID:	所有	
严重等级:	<input checked="" type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input checked="" type="checkbox"/> 低 <input checked="" type="checkbox"/> 信息	
动作:	<input checked="" type="checkbox"/> 允许 <input checked="" type="checkbox"/> 拒绝	

查询结果从新标签页中打开

第二步：点击**查询**，设备会根据过滤条件查询出符合条件的信息。界面如下

查询条件   导出日志													
查询条件: 时间(2016-05-19 00:00~2016-05-19 23:59)   源区域(所有区域)   源IP/用户(所有)   目的区域(所有区域)   特征ID(所有)   类型(所有类型)   严重等级(高,中,低,信息)   动作(允许,拒绝)													
序号	时间	类型	源IP/用户	目的IP	目的IP归属地	严重等级	动作	描述	数据包	风险详情	详细	白名单	黑名单

点击左上角的  导出日志 可以将数据导出成 EXCEL 表格方式。

#### 4.2.5. 内容安全

【网站访问】用于查询内网用户上网访问网站的详细情况。例如可以查询出内网某个 IP 地址在一天之内访问了哪些具体的 URL。网站访问查询界面如下：

内容安全

网站访问 邮件安全

设置查询条件点击"查询"按钮开始查询

起始时间: 2016-05-19 00:00

结束时间: 2016-05-19 23:59

源区域: 所有区域

源IP/用户:  所有  IP  用户  组

目的区域: 所有区域

目的IP: 所有

网站分类: 所有类型

目标域名:

动作:  允许  拒绝

查询  查询结果从新标签页中打开



#### 4.2.5.1 网站访问查询案例

典型应用场景：某客户需要查询出 5 月 30 日当天源 IP 是 200.200.2.51 访问的所有网站情况。

第一步：设置好查询条件，界面如下：

网站访问 邮件安全

查询条件 导出日志

设置查询条件点击“查询”按钮开始查询

起始时间: 2016-05-01 00:00  
结束时间: 2016-05-30 23:59  
源区域: 所有区域  
源IP/用户:  所有  IP  用户  组  
目的区域: 所有区域  
目的IP: 所有  
网站分类: 所有类型  
目标域名:  
动作:  允许  拒绝

查询 关闭  查询结果从新标签页中打开

第二步：点击**查询**，设备将根据过滤条件查询出相应信息，页面如下：

查询条件: 时间(2016-05-30 00:00~2016-05-30 23:59) | 源区域(所有区域) | 源IP/用户(IP:200.200.2.51) | 目的区域(所有区域) | 目的IP(所有) | 动作(允许,拒绝) | 网站分类(所有类型)

序号	时间	网站类型	目标域名	URL	源IP/用户	动作	详细

点击左上角的  导出日志 可以将数据导出成 EXCEL 表格方式。

【邮件安全】用于查询邮件安全的详细信息，邮件安全查询界面如下：

网站访问 邮件安全

设置查询条件点击“查询”按钮开始查询

起始时间:	2016-05-19	19	00:00	
结束时间:	2016-05-19	19	23:59	
源区域:	所有区域			
源IP/用户:	<input checked="" type="radio"/> 所有	<input type="radio"/> IP	<input type="radio"/> 用户	<input type="radio"/> 组
目的区域:	所有区域			
目的IP:	所有			
类型:	所有类型			
发件人邮箱:				
收件人邮箱:				
动作:	<input checked="" type="checkbox"/> 放行	<input checked="" type="checkbox"/> 阻断		
严重等级:	<input checked="" type="checkbox"/> 高	<input checked="" type="checkbox"/> 中	<input checked="" type="checkbox"/> 低	

查询结果从新标签页中打开

#### 4.2.5.2 邮件安全查询案例

典型应用场景：某客户需要查询出5月30日当天源IP是200.200.2.51的所有类型的邮件安全情况。

第一步：设置好查询条件，界面如下：

网站访问 | 邮件安全

设置查询条件点击“查询”按钮开始查询

起始时间:	2016-05-30	00:00
结束时间:	2016-05-30	23:59
源区域:	所有区域	
源IP/用户:	<input type="radio"/> 所有 <input checked="" type="radio"/> IP <input type="radio"/> 用户 <input type="radio"/> 组	
目的区域:	所有区域	
目的IP:	所有	
类型:	所有类型	
发件人邮箱:		
收件人邮箱:		
动作:	<input checked="" type="checkbox"/> 放行 <input checked="" type="checkbox"/> 阻断	
严重等级:	<input checked="" type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input checked="" type="checkbox"/> 低	

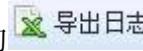
**查询**  查询结果从新标签页中打开

第二步：点击**查询**，设备将根据过滤条件查询出相应信息，页面如下：

查询条件 | 导出日志

查询条件: 时间(2016-05-30 00:00~2016-05-30 23:59) | 源区域(所有区域) | 源IP/用户(IP:200.200.2.51) | 目的区域(所有区域) | 目的IP(所有) | 类型(所有类型) | 动作(放行,阻断) | 严重等级(高,中,低)

序号	时间	源IP/用户	目的IP	类型	收件人	发件人	邮件主题	描述	详细

点击左上角的  导出日志 可以将数据导出成 EXCEL 表格方式。

#### 4.2.6. 应用控制

应用控制用于查询控制台中『内容安全』→『应用控制策略』所产生的所有日志信息。界面如下：

设置查询条件点击“查询”按钮开始查询

起始时间:	2016-05-30	15	00:00	
结束时间:	2016-05-30	15	23:59	
源区域:	所有区域			
源IP/用户:	<input checked="" type="radio"/> 所有	<input type="radio"/> IP	<input type="radio"/> 用户	<input type="radio"/> 组
目的区域:	所有区域			
目的IP:	所有			
服务/应用:	全部			
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝	<input checked="" type="checkbox"/> 联动拒绝	
<input type="button" value="查询"/> <input type="button" value="关闭"/> <input checked="" type="checkbox"/> 查询结果从新标签页中打开				

#### 4.2.6.1. 应用控制查询案例

典型应用场景：某客户需要查询出5月30日当天从内网区到外网区的所有被应用控制策略拒绝的日志情况。

第一步：设置好查询条件，界面如下：

查询条件 | 导出日志 |

设置查询条件点击"查询"按钮开始查询

起始时间:	2016-05-30	00:00	
结束时间:	2016-05-30	23:59	
源区域:	所有区域		
源IP/用户:	<input checked="" type="radio"/> 所有 <input type="radio"/> IP <input type="radio"/> 用户 <input type="radio"/> 组		
目的区域:	所有区域		
目的IP:	所有		
服务/应用:	全部		
动作:	<input type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝	<input type="checkbox"/> 联动拒绝

查询结果从新标签页中打开

第二步：点击**查询**，设备会根据过滤条件查询出符合条件的信息，页面如下：

查询条件: 时间(2016-05-30 00:00~2016-05-30 23:59) | 源区域(Inside) | 源IP/用户(所有) | 目的区域(outside) | 目的IP(所有) | 服务/应用(所有) | 设备名称() | 动作(拒绝,联动拒绝)

序号	时间	服务/应用	协议	源区域	源IP/用户	源端口	目的端口	匹配策略名	详细

#### 4.2.7. SSL VPN 用户日志

记录 AF 的 SSL VPN 功能的相关日志。界面如下：

SSL VPN用户日志

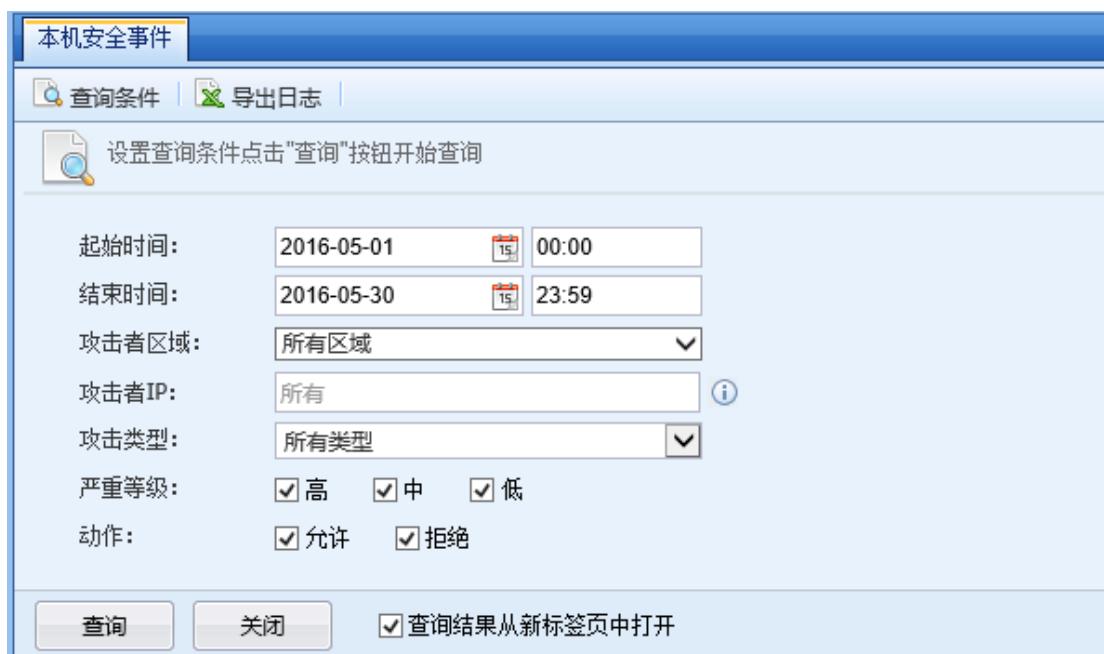
设置查询条件点击"查询"按钮开始查询

起始时间:	2018-07-01	00:00
结束时间:	2018-11-26	23:59
IP/用户:	<input checked="" type="radio"/> 所有 <input type="radio"/> IP <input type="radio"/> 用户	

查询结果从新标签页中打开

## 4.2.8. 本机安全事件

AF 自身有抵御渗透攻击的功能。本机安全事件用于记录和查询 AF 被攻击的日志。界面如下：



本机安全事件

设置查询条件点击“查询”按钮开始查询

起始时间:	2016-05-01	00:00
结束时间:	2016-05-30	23:59
攻击者区域:	所有区域	
攻击者IP:	所有	
攻击类型:	所有类型	
严重等级:	<input checked="" type="checkbox"/> 高 <input checked="" type="checkbox"/> 中 <input checked="" type="checkbox"/> 低	
动作:	<input checked="" type="checkbox"/> 允许 <input checked="" type="checkbox"/> 拒绝	

查询    关闭     查询结果从新标签页中打开

可以查询的攻击类型包括：端口扫描、ICMP 洪水攻击、UDP 洪水攻击、SYN 洪水攻击、DNS 洪水攻击、黑名单中的 IP 报文。

## 4.2.9. 本机访问控制

AF 有对自身的访问控制策略。本机访问控制用于记录和查询 AF 被访问匹配访问控制的相关日志。界面如下：

本机访问控制

查询条件 | 导出日志 |

设置查询条件点击“查询”按钮开始查询

起始时间:	2018-11-26	00:00
结束时间:	2018-11-26	23:59
源区域:	所有区域	
源IP:	所有	
目的IP:	所有	
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝

查询 | 关闭 |  查询结果从新标签页中打开

#### 4.2.9.1. 本机访问控制查询案例

典型应用场景：某客户需要查询出 11 月 26 日当天从源 IP 为 192.168.1.20 的用户，访问 AF 并匹配到本机访问控制策略的日志。

第一步：设定好查询条件，页面如下：

本机访问控制

查询条件 | 导出日志 |

设置查询条件点击“查询”按钮开始查询

起始时间:	2018-11-26	00:00
结束时间:	2018-11-26	23:59
源区域:	所有区域	
源IP:	192.168.1.20	
目的IP:	所有	
动作:	<input checked="" type="checkbox"/> 允许	<input checked="" type="checkbox"/> 拒绝

查询 | 关闭 |  查询结果从新标签页中打开

第二步：点击查询，设备将根据过滤条件查询出符合的信息，页面如下：

本机访问控制									
查询条件：时间:2018-07-01 00:00~2018-11-26 23:59   源区域(所有区域)   目的IP(所有)   动态/允许/拒绝									
序号	时间	服务	协议	源区域	源端口	源端口	目的端口	匹配策略名	详细
1	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56377	443	2	放行
2	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56377	443	2	放行
3	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56377	443	2	放行
4	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56377	443	2	放行
5	2018-11-26 20:00:50	Other	TCP	内网区域	192.168.1.20	56377	443	2	放行
6	2018-11-26 20:00:50	Other	TCP	内网区域	192.168.1.20	56377	443	2	放行
7	2018-11-26 20:00:50	Other	TCP	内网区域	192.168.1.20	56377	443	2	放行
8	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56376	443	2	放行
9	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56376	443	2	放行
10	2018-11-26 20:00:50	SSL	TCP	内网区域	192.168.1.20	56376	443	2	放行
11	2018-11-26 20:00:50	Other	TCP	内网区域	192.168.1.20	56376	443	2	放行
12	2018-11-26 20:00:50	Other	TCP	内网区域	192.168.1.20	56376	443	2	放行
13	2018-11-26 20:00:50	Other	TCP	内网区域	192.168.1.20	56376	443	2	放行
14	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56375	443	2	放行
15	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56375	443	2	放行
16	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56375	443	2	放行
17	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56375	443	2	放行
18	2018-11-26 20:00:49	Other	TCP	内网区域	192.168.1.20	56375	443	2	放行
19	2018-11-26 20:00:49	Other	TCP	内网区域	192.168.1.20	56375	443	2	放行
20	2018-11-26 20:00:49	Other	TCP	内网区域	192.168.1.20	56375	443	2	放行
21	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56374	443	2	放行
22	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56374	443	2	放行
23	2018-11-26 20:00:49	SSL	TCP	内网区域	192.168.1.20	56374	443	2	放行
24	2018-11-26 20:00:49	Other	TCP	内网区域	192.168.1.20	56374	443	2	放行
25	2018-11-26 20:00:49	Other	TCP	内网区域	192.168.1.20	56374	443	2	放行
26	2018-11-26 20:00:48	Other	TCP	内网区域	192.168.1.20	56374	443	2	放行
27	2018-11-26 20:00:48	SSL	TCP	内网区域	192.168.1.20	56373	443	2	放行
28	2018-11-26 20:00:48	SSL	TCP	内网区域	192.168.1.20	56373	443	2	放行
29	2018-11-26 20:00:48	SSL	TCP	内网区域	192.168.1.20	56373	443	2	放行

以上数据可以看出源 IP 为 192.168.1.20 的用户，有访问本机的控制台的相关日志记录。

## 4.2.10. 用户登录/注销

用户登录/注销主要是用于查询 AF 开启认证系统模块后，普通用户通过 AF 的认证模块的登录和注销信息。例如可以查询出某一天中午 12: 00 到 13:00 有哪些用户登录/注销查询，页面如下：

**用户登录/注销**

设置查询条件点击"查询"按钮开始查询

起始时间:	2016-05-01	00:00		
结束时间:	2016-05-30	23:59		
源IP/用户名:	<input checked="" type="radio"/> 所有	<input type="radio"/> IP	<input type="radio"/> 用户	<input type="radio"/> 组

**查询**  查询结果从新标签页中打开

### 4.2.10.1. 用户登录查询案例

典型应用场景：某客户需要查询出 5 月 30 日当天从源 IP 为 200.200.2.113

这个IP是否通过AF的认证系统模块。

第一步：设定好查询条件，页面如下：

用户登录/注销

查询条件 | 导出日志

起始时间：2011-05-30 00:00

结束时间：2011-05-30 23:59

源IP/用户名：  所有  IP  用户  组  
200.200.2.113

查询 | 关闭  查询结果从新标签页中打开

第二步：点击**查询**，设备将根据过滤条件查询出符合的信息，页面如下：

用户登录/注销

查询条件：时间(2011-05-30 00:00~2011-05-30 23:59) | 源IP/用户名(IP:200.200.2.113)

序号	用户名	组名	登录IP	登录时间	注销时间	在线时长	详细
1	200.200... /	/	200.200.2.113	2011-05-30 08:33:33	2011-05-30 19:25:42	10小时52分9秒	<b>查看</b>

序号 1

用户名： 200.200.2.113  
组名： /  
登录IP： 200.200.2.113  
登录时间： 2011-05-30 08:33:33  
注销时间： 2011-05-30 19:25:42  
在线时长： 10小时52分9秒

从以上信息可以看出，5月30日当天200.200.2.113这个IP地址通过AF的认证。并且在线10小时52分9秒。

#### 4.2.11. 系统操作

系统操作用于查询用户登录控制面板的登录注销日志以及所做过的所有操作日志，例如可以查询出admin这个账号在某天登录控制台做过哪些操作。系统操作查询页面如下：

系统操作

设置查询条件点击“查询”按钮开始查询

起始时间：	2013-09-01	<input type="button" value="日历"/>	00:00
结束时间：	2013-11-06	<input type="button" value="日历"/>	23:59
管理员：	所有用户		
描述：			

查询结果从新标签页中打开

从 AF5.1 版本开始支持查询管理员对 VPN 模块的操作日志，如下图所示：

系统操作

查询条件 | 导出日志 | 帐删除日志

查询条件：时间(2014-04-18 00:00~2014-04-18 23:59) | 用户(所有用户) | 描述()

序号	用户名	主机IP	操作对象	操作	日期时间	详细
1	admin	172.16.100.254	用户登录数据中心	登录	2014-04-18 11:32:50	<a href="#">查看</a>
2	admin	172.16.100.254	VPN->用户名	序号2		<a href="#">查看</a>
3	admin	172.16.100.254	VPN	用户名：	admin	<a href="#">查看</a>
4	admin	172.16.100.254	VPN->基本设	主机IP：	172.16.100.254	<a href="#">查看</a>
5	admin	172.16.100.254	用户登录数据	操作对象：	VPN->用户管理	<a href="#">查看</a>
6	admin	172.16.100.254	用户登录	操作：	新增	<a href="#">查看</a>
7	admin	172.16.100.254	用户登录	日期时间：	2014-04-18 11:32:43	<a href="#">查看</a>
8	admin	172.16.100.254	用户登录	描述：	添加Sangfor VPN用户：test	<a href="#">查看</a>

#### 4.2.11.1. 系统操作查询案例

典型应用场景：某客户需要查询出 11 月 6 日当天 admin 这个账号登录控制台之后做过哪些操作。

第一步：设置好查询条件，界面如下：

系统操作

设置查询条件点击"查询"按钮开始查询

起始时间： 2013-11-06 00:00

结束时间： 2013-11-06 23:59

管理员： admin

描述：

查询结果从新标签页中打开

第二步：点击**查询**，设备根据过滤条件查询出相关信息，页面如下：

系统操作

查询条件 | 导出日志 | 删除日志

查询条件：时间(2013-11-06 00:00~2013-11-06 23:59) | 用户(admin) | 描述()

序号	用户名	主机IP	操作对象	操作	日期时间	详细
1	admin	192.200.200.135	策略路由	新增策略路由	2013-11-06 17:08:16	<input type="button" value="查看"/>
2	admin	192.200.200.135	策略路由	新增策略路由	2013-11-06 16:55:17	<input type="button" value="查看"/>
3	admin	192.200.200.135	策略路由	新增策略路由	2013-11-06 16:54:23	<input type="button" value="查看"/>
4	admin	192.200.200.135	静态路由			<input type="button" value="查看"/>
5	admin	192.200.200.135	管理员帐号			<input type="button" value="查看"/>
6	admin	192.200.200.135	静态路由			<input type="button" value="查看"/>
7	admin	192.200.200.135	用户注销			<input type="button" value="查看"/>
8	admin	192.200.200.135	用户登录			<input type="button" value="查看"/>
9	admin	192.200.200.118	用户登录数据			<input type="button" value="查看"/>
10	admin	192.200.200.118	用户登录			<input type="button" value="查看"/>
11	admin	192.200.200.135	用户登录			<input type="button" value="查看"/>
12	admin	192.200.200.180	用户登录			<input type="button" value="查看"/>
13	admin	192.200.200.180	用户注销			<input type="button" value="查看"/>
14	admin	192.200.200.121	用户登录			<input type="button" value="查看"/>

## 4.3. 报表

报表功能模块用于设置自定义报表和订阅报表。主要分为两个模块：[自定义报表]、[报表订阅]。

### 4.3.1. 报表订阅

报表订阅用于生成周期性报表，并且可以定期将生成报表发送到指定的邮箱。可生成的报表分为两类，分别是：综合安全风险报表和汇总报表。

**综合安全风险报表：**用于分析指定的业务系统和终端用户，对指定对象进行安全风险分析汇总，综合安全风险报表新。

**汇总报表：**包括业务系统安全状况、终端用户安全状况、流量排名、应用行为排名、访问网站排名等。用户可根据需要指定统计的内容，从而生成自己需要的报表。

其中综合安全风险报表高级选项新增用户/业务排行、安全漏洞分析、拦截率统计、自定义评分等级、报表名称、报表摘要以及报表 logo 选项。如下图所示：

**新增综合安全风险报表**

**统计条件**

业务系统IP:  全部  指定业务系统IP

用户终端IP:  全部  指定用户终端IP

**报表内容**

安全风险概况 (从整体展示安全状况，快速了解业务和网络的安全风险。适用于管理者)

业务安全分析 (分析具体的业务系统的安全风险详情，帮助用户确认安全问题并提供解决方案。适用于具备探究精神的管理者)

用户安全分析 (分析具体的客户端的安全风险详情，帮助用户确认安全问题并提供解决方案。适用于具备探究精神的普通用户)

安全评分细则和危害说明 (细化安全风险规则和危害解释，更全面了解安全风险和安全评级状况。适用于具备探究精神的普通用户)

**生成选项**

生成周期:  每天  每周  每月

生成完后:  仅保存在已生成报表中（可点击“报表订阅”中相应报表的“已生成”来查看）  
 保存到已生成报表中，并发送到指定邮箱

(多个邮箱请用“;”隔开，最多支持5个邮箱)

**配置高级选项**

**确定** **取消**

### 高级选项

用户/业务排行: 前 10

安全漏洞分析:  开启

拦截率统计:  开启

自定义评分等级:  默认  自定义

报表名称:  默认  自定义

报表摘要:  默认  自定义

报表logo:  默认  自定义

**SANGFOR**

自定义logo尺寸高度不超过80px，超过高度会被等比压缩，格式支持.png。

收起高级选项↑



支持自定义报表的 logo

汇总报表设置条件如下：

## 新增汇总报表

报表名称：

## 统计条件

统计IP范围： 全部  IP  组显示图表： 统计图  趋势图  统计&趋势统计数量： 

## 报表内容

快速设置： 

## 安全统计

安全类型： 安全汇总  服务器  主机严重等级： 致命  高  中  低  信息

## 流量统计

排行依据： 总流量  上行流量  下行流量统计方式： 应用名称  应用类型  组  IP/用户统计应用：

## 应用统计

统计方式： 应用名称  应用类型  IP/用户统计应用：

## 访问网站

排行依据： 总流量  访问次数  拦截数统计方式： 网站类型  网站域名  IP/用户

## 订阅选项

订阅周期： 每天  每周  每月订阅方式： 不发送，只保存在已生成报表中 发送到邮箱  多个邮箱请用“;”隔开，最多支持5个

1、重构以前的 PDF 报表，结合安全状况>入侵风险、僵尸主机算法，展示出“已被黑”服务器和“已被感染”主机，并对该服务器、主机进行详细的举证说明。

2、攻击趋势可以从总体上看到最近几个月网络安全状况。

3、业务安全针对内网服务器进行安全综合分析，找到被感染的服务

器。

4、用户安全针对内网主机，分析防火墙日志，找到内网被感染病毒的主机

5、针对业务、用户安全汇总情况，并对服务器、主机进行举证说明，同时提供对应的修复建议。

#### 4.3.1.1. 订阅报表设置案例

典型应用场景：某客户需要订阅一张汇总报表，报表只需要统计所有内网用户的总流量和上下行流量排名。每周统计一次，并且从 sangfor@sangfor.com 这个邮箱发送到管理员邮箱 test@sangfor.com 。

第一步：在设置报表订阅之前，首先需要在系统设置中设置好邮件服务器。填写 sangfor@sangfor.com 这个邮箱对应 SMTP 服务器的 IP 地址信息，账号密码，发件人填写 sangfor@sangfor.com，界面如下：



第二步：进入报表订阅设置页面，点击新增**汇总报表**，在报表设置页面勾选<流量统计>，并勾选排行依据中的“总流量”、“上行流量”、“下行流量”，界面如下：

新增汇总报表

报表名称: 网络安全汇总报表\_20150519

**统计条件**

统计IP范围:  全部  IP  组

显示图表:  统计图  趋势图  统计&趋势

统计数量: 10

**报表内容**

快速设置: [简单报表](#) [完整报表](#)

-  安全统计

    安全类型:  安全汇总  服务器  主机

    严重等级:  致命  高  中  低  信息

-  流量统计

    排行依据:  总流量  上行流量  下行流量

    统计方式:  应用名称  应用类型  组  IP/用户

    统计应用:

-  应用统计

    统计方式:  应用名称  应用类型  IP/用户

    统计应用:

-  访问网站

    排行依据:  总流量  访问次数  拦截数

    统计方式:  网站类型  网站域名  IP/用户

**订阅选项**

订阅周期:  每天  每周  每月

订阅方式:  不发送, 只保存在已生成报表中

发送到邮箱  多个邮箱请用";" 隔开, 最多支持5个

第三步：点击**确定**保存。界面如下：

报表订阅							
操作		新增	删除	启用	禁用		
状态	操作	报表名称	已生成	最近生成	订阅邮箱	订阅周期	创建者
<input type="checkbox"/>	<input type="checkbox"/>	网络安全汇总报表_20150519	0	-	test@sangfor.com	每周	admin

## 4.3.2. 自定义报表

自定义报表用于用户自行定义自己所需信息的报表。自定义报表包括：综合安全风险报表、汇总报表以及健康检查报表三类。

### 4.3.2.1. 生成自定义报表案例

典型应用场景：某客户需要自定义一张报表，报表只需要统计 5 月 14 日到 5 月 20 日内网用户访问所有网站的次数排名，其余信息都不需要。将报表生成到设备里面。以便可以在已生成报表中查询。

第一步：进入自定义报表页面，勾选<汇总报表>，点击下一步：



第二步：在报表设置页面设置统计的时间范围，报表内容处勾选<访问网站>，并且勾选排行依据和统计方式。界面如下：

报表名称：

**统计条件**

时间范围：  至

统计IP范围：  全部  IP  组

显示图表：  统计图  趋势图  统计&趋势

统计数量：

**报表内容**

快速设置： [简单报表](#) [完整报表](#)

安全统计

安全类型：  安全汇总  服务器  主机

严重等级：  致命  高  中  低  信息

流量统计

排行依据：  总流量  上行流量  下行流量

统计方式：  应用名称  应用类型  组  IP/用户

统计应用：

应用统计

统计方式：  应用名称  应用类型  IP/用户

统计应用：

访问网站

排行依据：  总流量  访问次数  拦截数

统计方式：  网站类型  网站域名  IP/用户

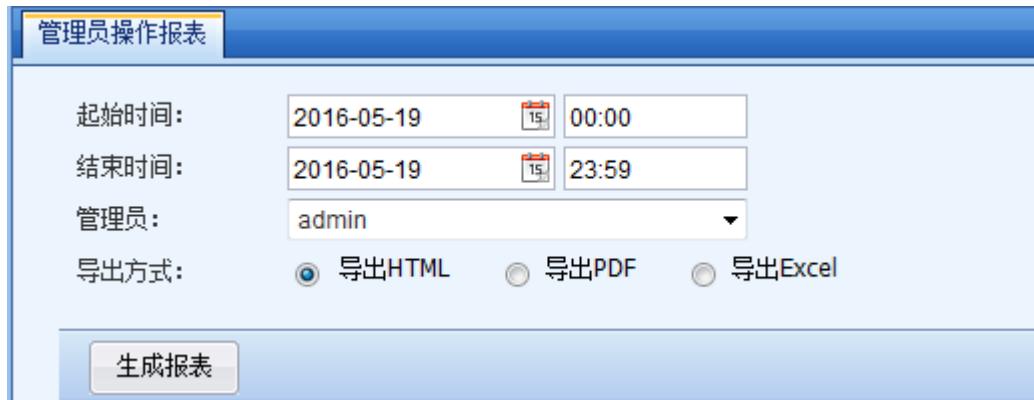
第三步：点击**立即生成 PDF**，设备会生成相应的报表。



自定义报表只能生成一次性报表，不能循环生成。

### 4.3.3. 管理员操作报表

用于导出管理员在控制台上对系统的操作日志报表，可以查看指定管理员的系统操作。界面如下：



The screenshot shows the 'Administrator Operation Report' interface. It includes fields for 'Start Time' (2016-05-19, 00:00), 'End Time' (2016-05-19, 23:59), 'Administrator' (admin), and 'Export Method' (HTML). A 'Generate Report' button is at the bottom.

### 4.4. 系统

系统主要用于设置与数据中心相关的一些设置，例如可以在系统中设置报表的生成时间具体到分钟，可以在系统中设置日志导出的条目数，设置超时时间，删除日志等操作。界面如下：



The screenshot shows the 'System Settings' interface under the 'System' category in the navigation menu. It includes sections for 'Email Server Settings' (SMTP server, verify server), 'Report Generation Settings' (report generation time from 00:00 to 06:00, automatic deletion of 7 days old reports, maximum 1000 reports), 'Log Settings' (log export limit 1000, support log limit 10,000,000), and 'Other Settings' (timeout 10 minutes, flow unit bps/bps). A 'Confirm' button is at the bottom.

## 4.4.1. 系统设置

点击**系统设置**，页面如下：

The screenshot shows the 'System Settings' page with the following sections:

- 邮件服务器设置 (Email Server Configuration):**
  - SMTP服务器 (SMTP Server): smtp.qq.com
  - 服务器需要验证 (Server needs verification)
  - 用户名 (Username): 593286995@qq.com
  - 密码 (Password): ..... (redacted)
  - 发件人 (From): 593286995@qq.com
- 报表生成设置 (Report Generation Settings):**
  - 报表生成时间 (Report generation time): 00:00 到 06:00
  - 自动删除报表 (Automatic report deletion):
    - 自动删除 (Delete automatically) 7 天前的报表 (Reports from 7 days ago)
    - 最多保存 (Save up to) 1000 份报表 (1000 reports)
- 日志设置 (Log Settings):**
  - 日志导出 (Log export): 日志列表最多只能导出最近 1000 条日志 (The log list can only export the most recent 1000 logs)
  - 支持日志量 (Supported log volume): 10000000 条 (10,000,000 logs)
- 其他设置 (Other Settings):**
  - 超时设置 (Timeout settings): 1000 分钟 (1000 minutes)

[邮件服务器设置]: 此处的设置主要是用于 4.3.1 中报表订阅的时候设置发送邮件服务器。

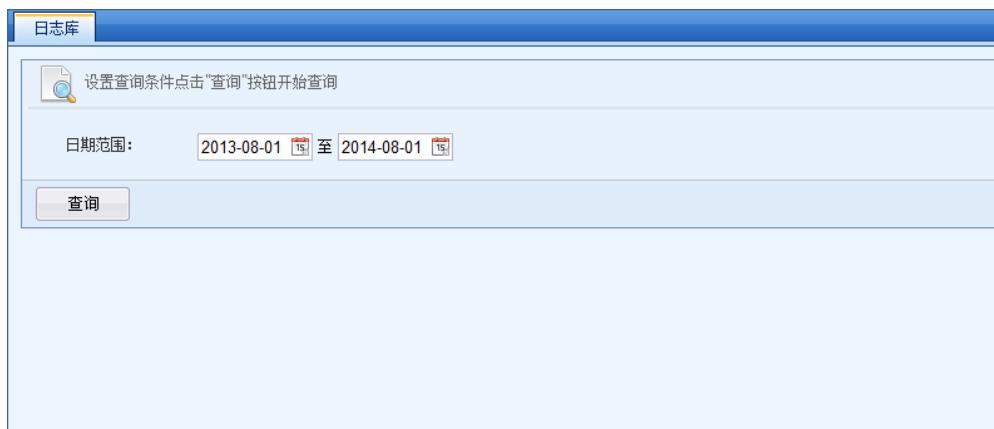
[报表生成设置]: 设备会在指定的时间内生成 4.3 中设置好的报表。并且可以指定报表的生成时间。

[日志设置]: 用于设置日志查询中导出日志的最大条目数以及支持显示的最大日志量，此处默认没有设置成最大主要是考虑设备的性能损耗。

[其他设置]: 用于设置数据中心页面的超时时间和流速单位。

## 4.4.2. 日志库

用于查询指定时间内的日志文件大小，并且做删除等操作。界面如下：



设置好查询日志范围，点击**查询**，设备会查询出指定日期范围内的日志，页面如下：



日期	日志大小
20140718	69 KB
20140719	69 KB
20140720	69 KB
20140721	69 KB
20140722	69 KB
20140723	69 KB
20140724	69 KB
20140725	69 KB
20140726	69 KB
20140727	69 KB
20140728	69 KB
20140729	69 KB
20140730	69 KB
20140731	69 KB

勾选某一天的日志，点击**删除**，可以删除选中的日志。



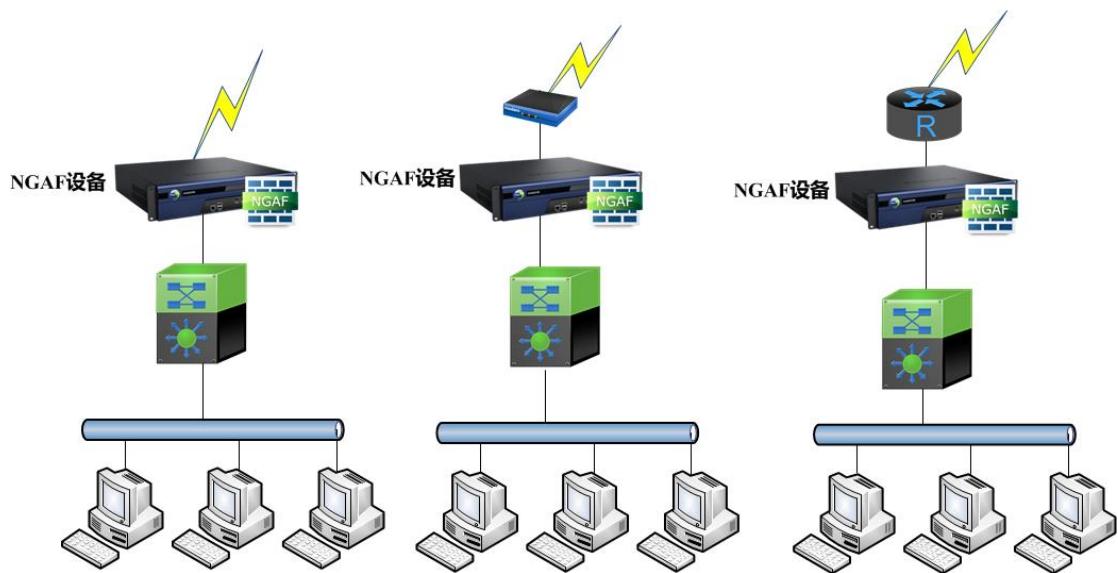
设备只能删除以天为单位的日志，不能删除某一条日志。

# 第5章 案例集

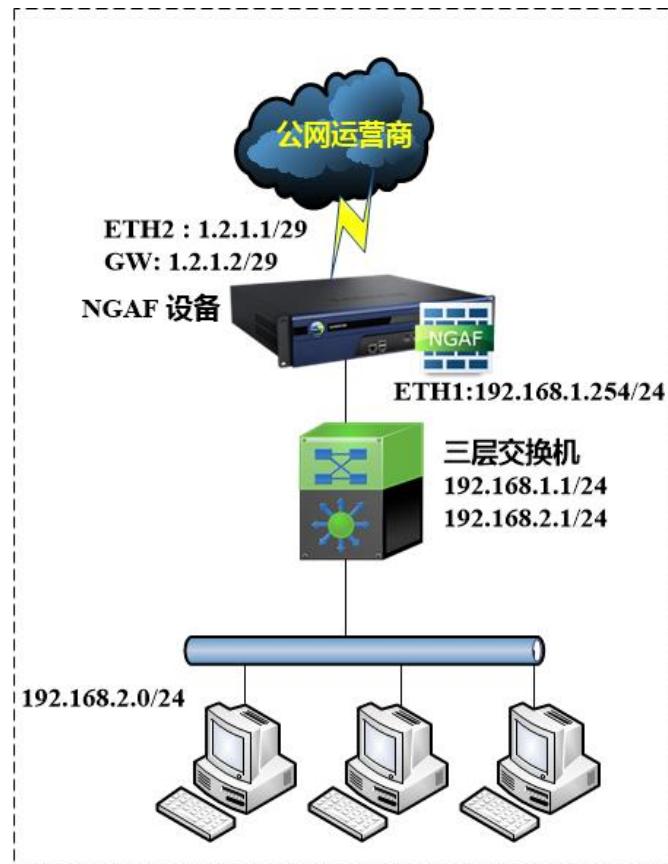
## 5.1. 设备部署配置案例

### 5.1.1. 路由接口配置案例

路由接口的典型应用环境是将 SANGFOR AF 设备以路由模式部署在公网出口，代理内网上网，像一个路由器一样部署在网络中，如下图所示：



配置案例：某用户网络是跨三层的环境，购买 AF 设备打算部署在公网出口，代理内网用户上网，公网线路是光纤接入固定分配 IP 的。



第一步：通过管理口(ETH0)的默认 IP 登录设备。管理口的默认 IP 是 10.251.251.251/24，在计算机上配置一个相同网段的 IP 地址，通过 <https://10.251.251.251> 登录设备。

第二步：配置外网接口，通过『网络』→『接口/区域』，点击需要设置成外网接口的接口，如 eth2，出现以下页面：



接口[类型]选择路由。

[基本属性]可以设置是否为 WAN 口和允许 PING。如果是 WAN 口，是否与 IPSEC VPN 出口线路匹配。连接上行链路的接口需要勾选 WAN 口。

[区域]选择接口 eth2 所属的区域。区域需要提前设置，本例将 ETH2 划入 WAN 区域，对于区域的设置请参考章节 3.3.1.5 区域设置。

[连接类型]包括静态 IP、DHCP、ADSL 拨号三种，根据该线路的特征进行配置，如果选择静态 IP，需要填写好 IP 地址/掩码以及下一跳网关；如果该接口是 DHCP 自动获得地址，则设置 DHCP；如果线路是 ADSL 拨号，则配置好拨号所需的用户名、密码和其他拨号参数。

静态 IP 地址可以填写成“IP/掩码”和“IP/掩码-HA”两种形式，后一种形式表示同步网口配置时，不同步 IP 地址，“IP/掩码-HA”的形式适用于 AF 设备双机部

署的环境。

本案例中外网接口连接的是静态IP的光纤线路，所以选择静态IP，并且配置ISP提供给该光纤线路的公网IP地址和下一跳网关。

[线路带宽]设置公网链路的上下行带宽。点击▼可以修改带宽单位，包括KB/s, MB/s, GB/s。

[链路故障检测]用于检测链路的好坏。如果需要进行链路故障检测，则可以点击设置按钮，设置检测方法，如下：



勾选[启用]，开启链路故障检测。

链路检测方法包括ARP、DNS解析和PING，如果选择DNS解析则需要配置DNS服务器和解析域名，若开启PING检测，则填写PING检测IP。同一个接口的链路检测方法。本例中开启PING检测，通过PING目标IP为1.2.1.2的地址来检测链路的好坏。

[高级配置]用来设置网口的工作模式，MTU，MAC地址，如果需要修改，点击**设置**，页面如下：



1. 接口的下一跳网关仅用于接口的链路检测和策略路由功能，设置了下一跳网关，不会在设备上产生 0.0.0.0/0 的缺省路由，需要手动设置默认路由。
2. 接口的线路带宽设置与流量管理的带宽设置没有关联，接口处的线路带宽设置用于策略路由的调度。策略路由功能见章节 3.3.2.2.

第三步：配置内网接口。选择空闲网口、点击接口名称进入配置页面，配置内网接口接口类型为路由接口，WAN 口类型为否、配置 IP 地址等，如下图所示：



第四步，配置路由，需要配置一条到 0.0.0.0/0.0.0.0 的默认路由指向前置网关 1.2.1.2，同时因为本例内网接口接的跨三层的多个网段，需要添加到各网段的静态路由到三层交换机，静态路由配置请参见章节 3.3.2.1

第五步，配置代理内网上网，请参见章节 3.3.6.1 源地址转换。

第六步，基本配置完毕后，将设备接入网络中，eth2 口连接光纤，eth1 口接内网三层交换机。



1. 设备工作在路由模式时，局域网内计算机的网关都是指向设备内网接口 IP 或指向三层交换机，三层交换机的网关再指向设备。上网数据由设备做 NAT 或路由转发出去。

2. 当设备有多个路由接口时，多个路由接口可以设置同网段的 IP 地址，通过静态路由决定数据从哪个网口转发。

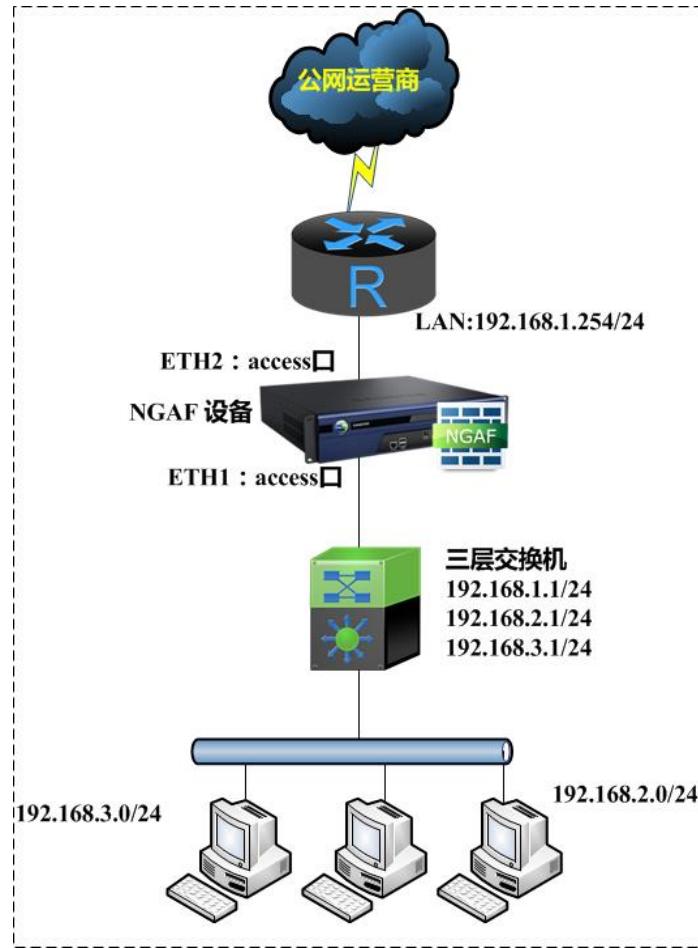
3. 设备支持配置多个 WAN 口属性的路由接口连接多条外网线路，但是需要开通多条线路的授权。

### 5.1.2. 透明接口配置案例

当数据进出 AF 设备的网口处于透明接口模式时，设备相当于透明模式部署，视为一根带过滤功能的网线。一般在不方便更改原有网络拓扑结构的情况下启用，把设备接在原有网关及内网用户之间，不要更改原有网关及内网用户的配置，对 AF 设备进行一些基本配置即可使用，透明模式的主要特点是对用户做到完全透明。透明接口分为 ACCESS 接口和 TRUNK 接口。

#### 5.1.2.1. ACCESS 接口配置案例

配置案例：用户的网络拓扑如下所示，AF 设备做透明模式，内网接三层交换机，内网网段有 192.168.2.0/255.255.255.0、192.168.3.0/255.255.255.0 两个网段。



第一步：通过管理口(ETH0)的默认 IP 登录设备。管理口的默认 IP 是 10.251.251.251/24，在计算机上配置一个同网段的 IP 地址，通过 <https://10.251.251.251> 登录设备。

第二步：配置外网接口，通过『网络』→『接口/区域』→『物理接口』，点击需要设置成外网接口的接口，如 eth2，出现以下页面：



接口[类型]选择透明。

[区域]选择接口 eth2 所属的区域。区域需要提前设置，本例选择 WAN，对于区域的设置请参考章节 3.3.1.5 区域设置。

[基本属性]可以设置是否为 WAN 口。是否为 WAN 口，如果是 WAN 口，是否与 IPSEC VPN 出口线路匹配。连接上行链路的接口需要勾选 WAN 口。

[连接类型]可以选择为 access 或者 trunk。本案例中网口类型选择 access 口。一般情况下 access 接口属于 VLAN1，可以不修改，也可以把设置成其他 VLAN，但设备的两个接口必须在相同 VLAN。

[高级配置]用来设置网口的工作模式，MTU，MAC 地址，如果需要修改，点击**设置**，页面如下：



第三步：配置内网接口。选择空闲网口、点击接口名称进入配置页面，配置内网接口接口类型为透明接口，WAN 口类型为否，连接类型选择 access 等，如下图所示：

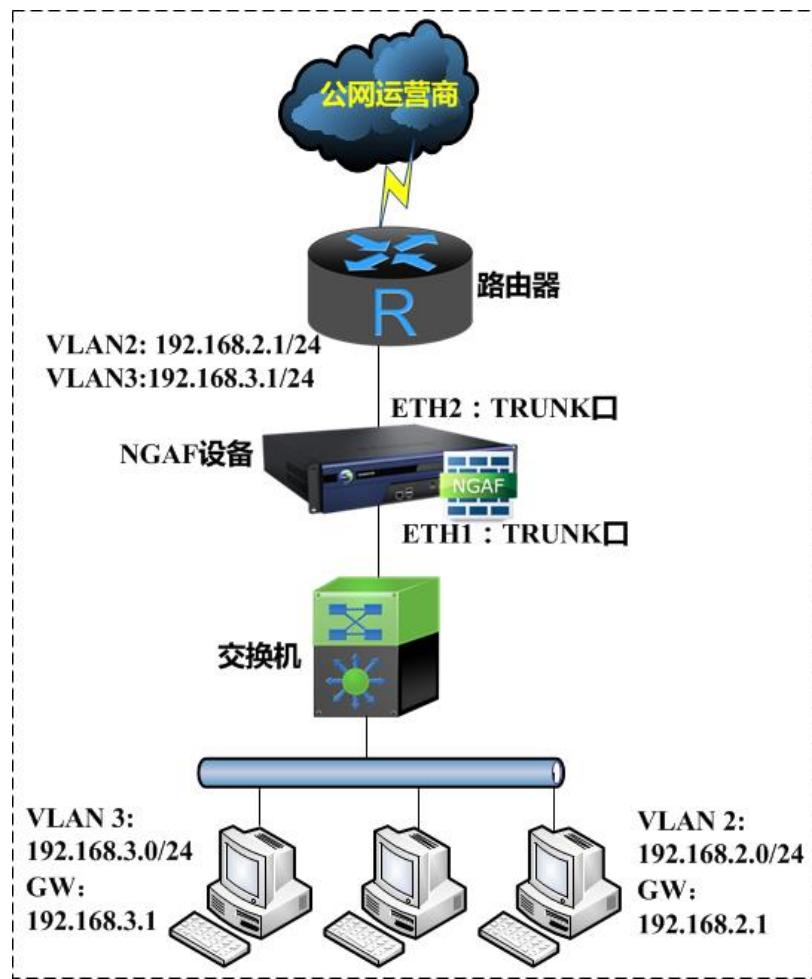


第四步，设置 VLAN 接口，为 VLAN 接口设置 IP 地址，则可以通过 VLAN 接口的 IP 地址登陆设备控制面板做管理，VLAN 接口的配置详见章节 3.3.1.3 。也可以通过专门的管理口登录设备进行管理。

第五步，基本配置完毕后，将设备接入网络中，eth2 口连接前置路由器，eth1 口接内网三层交换机。

### 5.1.2.2. TRUNK 接口配置案例

配置案例：用户网络拓扑如下所示，设备透明模式部署，内网交换机划分了 VLAN 但没有启用路由功能，前置路由器做各个 VLAN 的网关。内网网段有 192.168.2.0/255.255.255.0、192.168.3.0/255.255.255.0 两个网段，分别属于 VLAN2 和 VLAN3，交换机和路由器之间跑 trunk 协议。



第一步：通过管理口（ETH0）的默认 IP 登录设备。管理口的默认 IP 是 10.251.251.251/24，在计算机上配置一个同网段的 IP 地址，通过 <https://10.251.251.251> 登录设备。

第二步：配置外网接口，通过『网络』→『接口/区域』，点击需要设置成外网接口的接口，如 eth2，出现以下页面：



接口[类型]选择透明。

[区域]选择接口 eth2 所属的区域。区域需要提前设置，本例选择 WAN，对于区域的设置请参考章节 3.3.1.5 区域设置。

[基本属性]可以设置是否为 WAN 口。连接上行链路的接口需要勾选 WAN 口。是否为 WAN 口，如果是 WAN 口，是否与 IPSEC VPN 出口线路匹配。

[连接类型]可以选择为 access 或者 trunk。本案例中网口类型选择 trunk 口。一般情况下 native1 和 VLAN 范围 1-1000 不需要修改，也可以把 VLAN 范围设置成需要通过设备穿透的 VLAN 号，在本案例中，也可以设置成 VLAN 2-3。

[高级配置]用来设置网口的工作模式，MTU，MAC 地址，如果需要修改，

点击设置，页面如下：



第三步：配置内网接口。选择空闲网口、点击接口名称进入配置页面，配置内网接口接口类型为透明接口，WAN 口类型为否，连接类型选择 trunk 等，如下图所示：



第四步，设置 VLAN 接口，本案例中，需要添加 VLAN2 和 VLAN3 接口，  
页面如下：

**新建VLAN接口**

接口名称: Veth. 2

描述:

所属区域: 内网区域

基本属性:  允许PING  
 与IPSec VPN出口线路匹配: 线路1

连接类型:  静态IP  DHCP

静态IP地址:  可以直接在此处输入、编辑、删除

下一跳网关:

链路故障检测

高级配置

**新建VLAN接口**

接口名称: Veth. 3

描述:

所属区域: 内网区域

基本属性:  允许PING  
 与IPSec VPN出口线路匹配: 线路1

连接类型:  静态IP  DHCP

静态IP地址:  可以直接在此处输入、编辑、删除

下一跳网关:

链路故障检测

高级配置

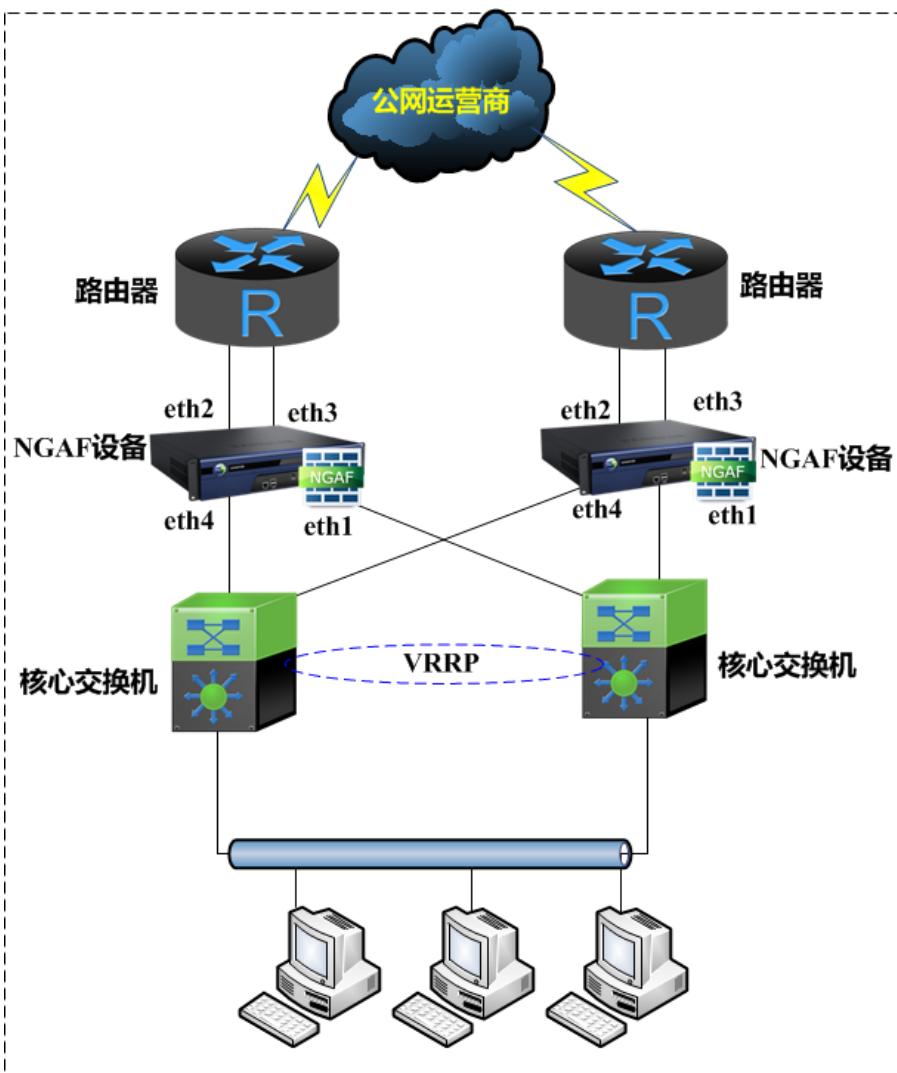
第五步，基本配置完毕后，将设备接入网络中，eth2 口连接前置路由器，eth1 口接内网三层交换机。



以上网络环境中也可以使用虚拟网线接口进行部署，也推荐使用虚拟网线部署，详细配置参考下节案例。

### 5.1.3. 虚拟网线接口配置案例

配置案例：某用户网络环境如下图所示，用户内网有两台三层交换机和两台路由器做负载均衡。现在在网站中透明部署 AF 设备，不希望更改原来的上网方式。



在此网络环境中透明部署 AF 设备，要求 eth4 和 eth2 这对网口与 eth1 和 eth3

这对网口二层隔离，即进入 eth4 口的数据必须从 eth2 口转发，进入 eth1 口的数据必须从 eth3 口转发，我们可以通过虚拟网线接口来配置实现。

第一步：通过管理口（ETH0）的默认 IP 登录设备。管理口的默认 IP 是 10.251.251.251/24，在计算机上配置一个同网段的 IP 地址，通过 <https://10.251.251.251> 登录设备。

第二步：配置外网接口，通过『网络』→『接口/区域』，点击需要设置成外网接口的接口，如 eth2，出现以下页面：



接口[类型]选择虚拟网线。

[区域]选择接口 eth2 所属的区域。区域需要提前设置，本例选择 WAN，对于区域的设置请参考章节 3.3.1.5 区域设置。

[接口二]选择形成一对虚拟网线的另外一个接口，本例中 eth2、eth4 是一对

虚拟网线接口，则接口二选择 eth4。

[基本属性]可以设置是否为 WAN 口。连接上行链路的接口需要勾选 WAN 口。

[高级配置]用来设置网口的工作模式，MTU，MAC 地址，如果需要修改，点击**设置**，页面如下：



配置完成后点击**确定**保存配置，按照同样的方法设置外网接口 eth3。

第三步：配置内网接口。选择空闲网口、点击接口名称进入配置页面，配置内网接口接口类型为虚拟网线，WAN 口类型为否，如下图所示：

编辑物理接口

启用

名称： eth4  
描述：  
类型： 虚拟网线  
所属区域： lan  
接口一： eth4  
接口二： eth2  
基本属性：  
 WAN口  
 与IPSec VPN出口线路匹配： 线路1

高级配置  
配置工作模式, MTU, MAC

配置完成后点击**确定**保存配置，按照同样的方法设置内网接口 eth4。

第四步：设置虚拟网线。『网络』→『接口/区域』→『虚拟网线』，新增虚拟网线，配置详见章节 3.3.1.5。

第五步：本案例中要实现内网交换机和路由器的主备切换，还需要在『网络』→『接口/区域』→『接口联动』，开启接口联动，配置详见章节 3.3.1.6.

第六步，基本配置完毕后，将设备接入网络中，eth2 和 eth3 口连接前置路由器，eth4 和 eth1 口分别接内网的两个三层交换机。



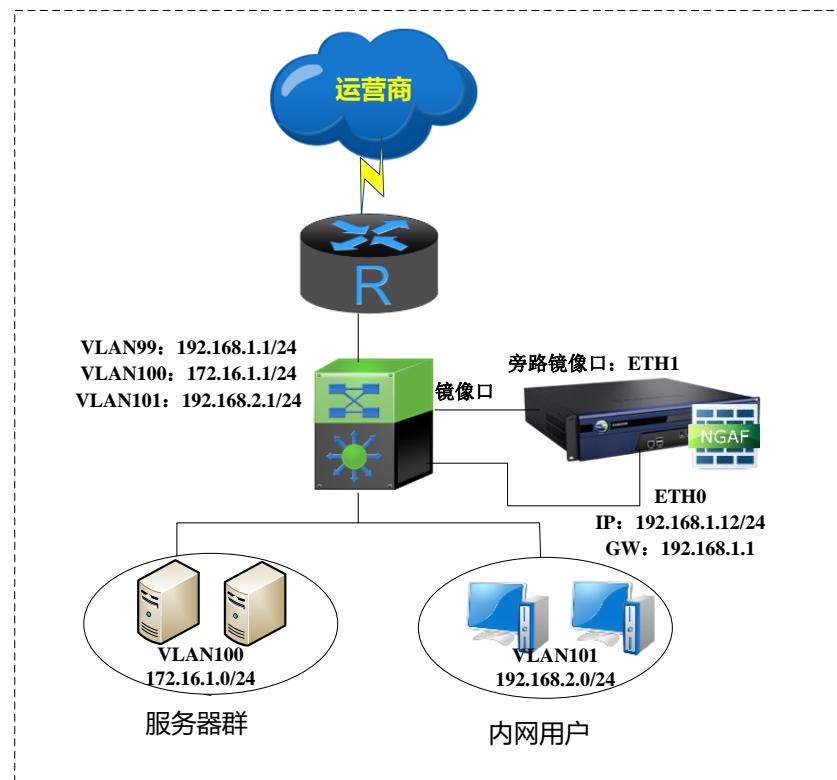
管理口不支持设置成虚拟网线接口，如果要设置 2 对或者 2 对以上虚

拟网线，要求设备不少于 5 个接口，除了配置成虚拟网线接口，还必须预留一个专门的管理口。

### 5.1.4. 旁路镜像接口配置案例

**旁路模式：**实现防护功能的同时，可以完全不需改变用户的网络环境，并且可以避免设备对用户网络造成中断的风险。用于把设备接在交换机的镜像口或者接在 HUB 上，保证外网用户访问服务器的数据经过此交换机或者 HUB，并且设置镜像口的时候需要同时镜像上下行的数据，从而实现对服务器的保护。

配置案例：用户的网络拓扑如下所示，AF 设备旁路部署，内网接三层交换机，用户网段为 192.168.2.0/24，服务器网段为 172.16.1.0/24，客户希望 AF 能够对服务器进行漏洞攻击防护、WEB 应用防护以及防止敏感信息的泄露。



第一步：通过管理口(ETH0)的默认 IP 登录设备。管理口的默认 IP 是 10.251.251.251/24，在计算机上配置一个同网段的 IP 地址，通过

https://10.251.251.251 登录设备。

第二步：配置管理口，旁路部署时，设备通过管理口来阻断连接。通过『网络』→『接口/区域』→『物理接口』，点击 eth0，配置页面如图：



第三步：配置旁路镜像口，通过『网络』→『接口/区域』→『物理接口』，点击 eth1，配置页面如图：



接口[类型]选择旁路镜像。

[区域]选择接口 eth1 所属的区域。区域需要提前设置，本例选择旁路区域，对于区域的设置请参考章节 3.3.1.5 区域设置。

[启用旁路流量统计]用于开启旁路镜像口的流量统计，在[网络对象]中选择需要统计流量的内网 IP。

[高级配置]用来设置网口的工作模式，MTU，MAC 地址，如果需要修改，点击设置，接口如下：



第四步：配置路由，需要配置一条到 0.0.0.0/0.0.0.0 的默认路由指向前置网关 192.168.1.1。进入『网络』→『路由』→『静态路由』，配置页面如下：

新增单个静态路由

目的地址：	0.0.0.0
子网掩码：	0.0.0.0
下一跳IP地址：	192.168.1.1
接口：	自动选择接口
度量值：	0

保存 取消

第五步：配置防护规则。以配置业务保护策略为例，讲解旁路模式下，如何设置业务保护策略。通过『策略』→『安全策略』→『安全防护策略』，新增业务保护策略，配置页面如图：

新增业务保护策略

常规 评估 防御 检测响应

策略名称：	保护业务
描述：	保护业务
状态：	<input checked="" type="checkbox"/> 启用
要保护的对象	
区域：	旁路镜像
网络对象/用户：	<input checked="" type="radio"/> 网络对象 web服务器
需抵御的对象	
区域：	旁路镜像
网络对象：	全部

下一步 取消

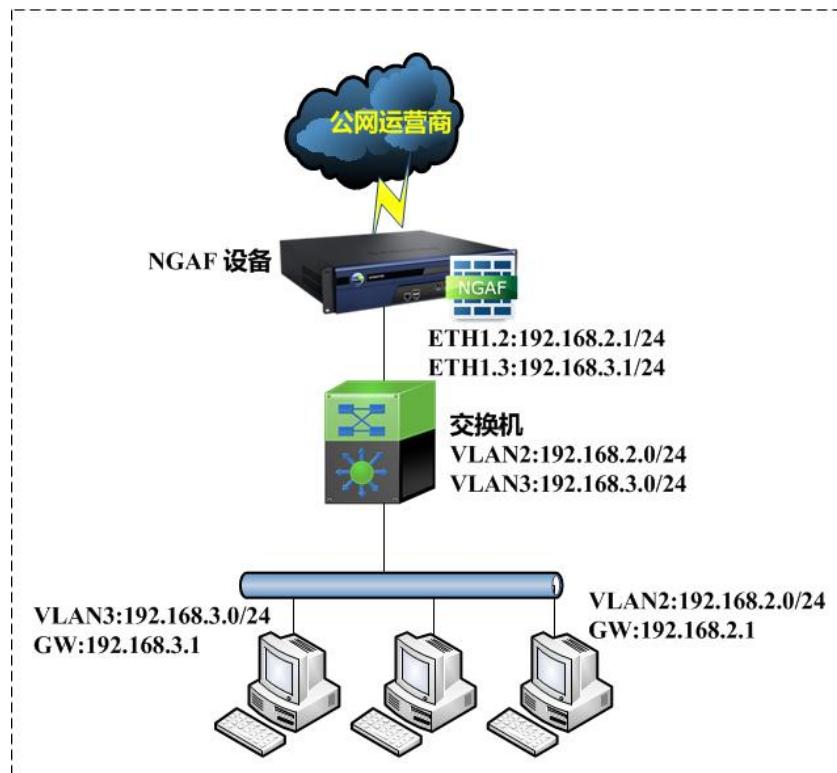
旁路模式下，要保护的对象中区域和需抵御的对象都要选择旁路接口所在的区域，要保护的对象的网络对象选择服务器网段所在的业务组即可。

第六步：基本配置完毕后，将设备接入网络中，eth1 口连接三层交换机的镜

像口，eth0 口接内网三层交换机的 VLAN99 范围内的接口即可。

### 5.1.5. 子接口配置案例

配置案例：某用户网络环境如下图所示，用户内网的交换机划分了2个VLAN，内网用户分别划分在VLAN2 和 VLAN3，部署AF 设备，通过AF 做 VLAN 间路由和内网 VLAN 的网关。



第一步，配置内网接口，通过『网络』→『接口/区域』→『物理接口』，点击需要设置成内网接口的接口，如 eth2。内网接口必须设置成路由接口，WAN 口属性为否，IP 地址和网关可任意配置，如下图所示：



第二步，添加 VLAN 子接口。通过『网络』→『接口/区域』→『子接口』，  
点击**新增**，如下图所示：



[物理接口]选择在哪个物理接口下添加子接口，只能在路由口下添加子接口。

[VLAN ID]设置此子接口的 VLAN ID。

[连接类型]可以选择静态 IP 或者 DHCP，如静态 IP，则填写对应 VLAN 的网关地址。

[链路故障检测]与[高级配置]与路由接口设置方法相同，此处不再赘述。

点击**提交**，保存配置，并按照相同的方法新增 VLAN3 的子接口。



同一个物理网口下可以添加多个子接口，物理网口的 IP 地址可以任意设置，但必须与子接口的 IP 地址在不同网段。

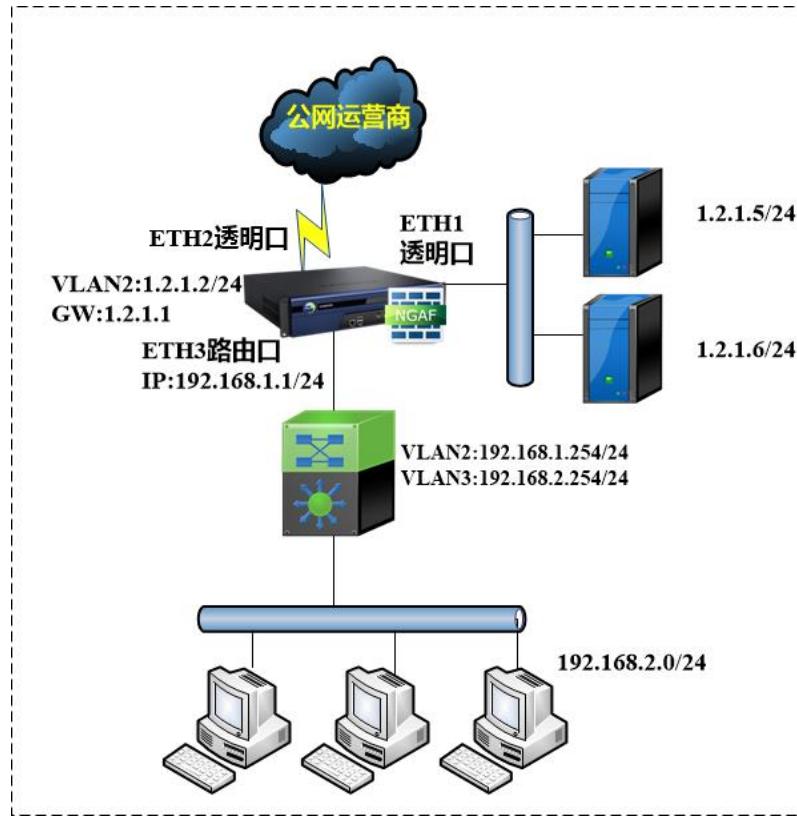
### 5.1.6. 混合部署配置案例

配置案例：某用户内网有大量服务器群需要提供用户通过公网访问，并且每个服

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

服务器均分配公网地址。在公网出口部署 AF 设备，实现用户能够直接通过公网地址访问服务器群，不希望通过端口映像的方式发布服务器，且能实现 AF 设备代理内网的内网上公网。用户网络拓扑如下所示：



此案例中用户需要通过服务器的公网 IP 访问到服务器，则可以把 AF 设备连接公网的 eth2 口和连接局域网内服务器群的 eth1 口设置成透明 access 接口，且属于同一个 VLAN。设置 VLAN 接口，且给 VLAN 接口配置公网地址。连接内网的 eth3 口设置成路由口，内网用户上公网时转换源 IP 地址成 VLAN 接口的公网地址，则可实现用户的需求。

第一步，设置外网接口 eth2。通过『网络』→『接口/区域』→『物理接口』，点击 **eth2**，进行如下设置：



第二步，设置内网接口 eth1。通过『网络』→『接口/区域』→『物理接口』，  
点击 eth1，进行如下设置：



第三步，设置内网接口 eth3。通过『网络』→『接口/区域』→『物理接口』，点击 eth3，进行如下设置页面：

编辑物理接口

启用

名称: eth3  
描述: 网络适配器6  
类型: 路由  
所属区域: 内网区域  
基本属性:  
 允许PING  
 WAN口  
 与IPSec VPN出口线路匹配: 线路1

IPv4

静态IP  DHCP  ADSL拨号

静态IP地址: 192.168.1.1/24  
下一跳网关: 192.168.1.254

线路带宽  
上行: 80 Mbps  
下行: 80 Mbps

链路故障检测  
配置检测方式、检测参数

高级配置  
配置工作模式, MTU, MAC

第四步，设置 VLAN 接口。通过『网络』→『接口/区域』→『VLAN 接口』，  
点击**新增**，进行如下设置页面：

**新建VLAN接口**

接口名称：	Veth.2	(i)
描述：		
所属区域：	WAN	(v)
基本属性：	<input checked="" type="checkbox"/> 允许PING	
连接类型：	<input checked="" type="radio"/> 静态IP	<input type="radio"/> DHCP
静态IP地址：	1.2.1.2/24	(i)
下一跳网关：		

**链路故障检测**

配置多个外网线路的情况下，某个线路故障时，流量会自动切换到其它线路上

**高级配置**

配置MTU值

**提交 取消**

第五步：『网络』→『路由设置』→『静态路由』→『IPv4』配置设备上网的默认路由与数据回包路由，页面如下：

**新增单个静态路由**

目的地址：	0.0.0.0	(i)
子网掩码：	0.0.0.0	
下一跳IP地址：	1.2.1.1	
接口：	veth.2	(v)
度量值：	0	

**保存 取消**

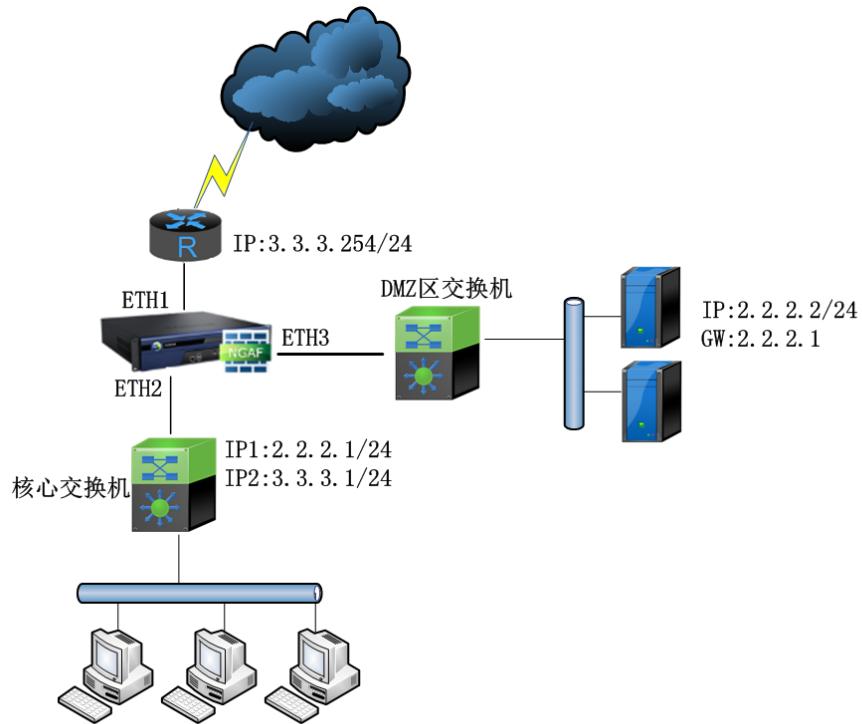


配置完成。AF 设备代理内网上网，还需要设置源地址转换，详细配置请参见[防火墙章节 3.3.6.1](#)

### 5.1.7. 二次穿透部署案例

案例背景：AF 安全模块基于会话连接来检测，一次会话只作一次安全逻辑检测，当一次会话数据多次穿透 AF 时，无法作安全功能检测。AF6.8 版本支持，自动识别并处理数据包两次穿透防火墙的情况。

案例应用：[内网服务器与核心交换路由间，部署有AF 防火墙；核心交换设备与外网流量也经过AF 防火墙。外网访问内网服务器时，流量穿透AF 防火墙到达核心交换，核心交换转发流量再次穿透AF 防火墙，到达内网服务器\(AF 设备的三个口都是二层口\)。](#)



二次穿透环境 AF 设备支持如下功能：保证正常外网访问内网互访能通；并支持以下安全功能的开启和检测：DOS/DDOS 防护、应用控制、内容安全策略、僵尸网络检测、漏洞攻击防护、WEB 应用防护、网站防篡改、实时漏洞分析、威胁情报预警与处置、内容安全、流量审计。



二次穿透环境 AF 设备的场景不支持流量管理

## 5.2. 策略路由配置案例

### 5.2.1. 策略路由配置案例 1

配置案例：某用户需要访问一个网上银行，地址是 127.8.66.42，访问协议是 HTTPS，网上银行会校验连入的 IP 地址，如果同一连接中的源 IP 发生了改变，网上银行会断开链接，导致无法访问。设置一条策略路由，指定访问到这个目标地址的数据固定走 eth3 接口连接的线路出去。

在【导航菜单】页面中的『网络』→『路由』→『策略路由』，点击**新增**，  
新增源地址策略路由，页面如下：

**新建源地址策略路由**

启用

名称：  
描述：  
生效时间：  
插入到：

**源**

区域：

网络对象：

**目的**

网络对象

ISP地址

国家/地区

**协议和端口**

设置协议和端口条件

**应用**

设置应用

**链路故障检测**

当IPSecVPN中开启了与专线互备路由时，链路故障后，可自动切换到VPN线路上。

**接口与下一跳**

接口

下一跳

[名称]和[描述]：设置策略路由的名称和描述信息。

【生效时间】：设置策略路由的生效时间，可以点击下拉框来选择和设置时间计划，如下图所示：

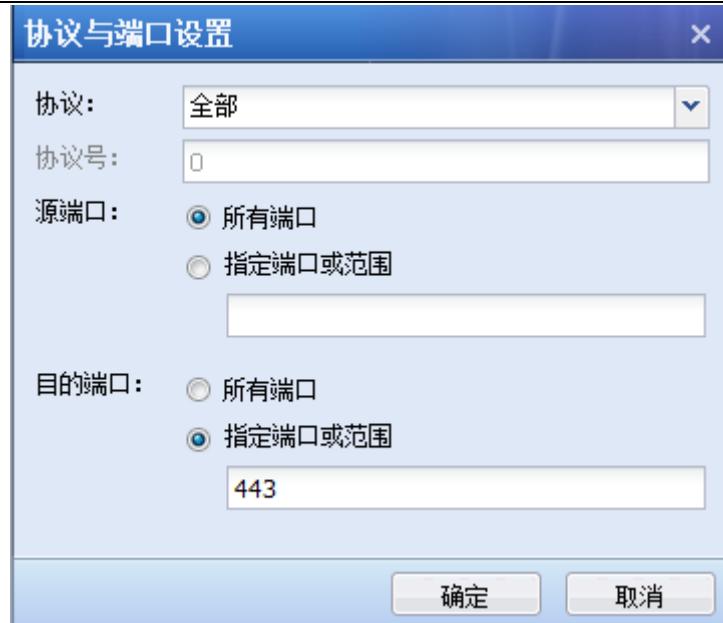


『源』：选择源区域和网络对象，必须选择源区域。

『目的』：选择目的网络对象、ISP地址或者国家/地区。本案例中，需要对目的IP为127.8.66.42的HTTPS应用匹配策略路由，点击下拉框来选择和设置目的网络对象，如下图所示：



『协议和端口』：选择协议和端口条件，点击【设置】，如下图所示：



『接口与下一跳』：选择符合条件的数据报从哪个接口或者下一跳进行转发。

点击提交，保存配置，在如下页面查看新增成功的策略路由：

A screenshot of a network configuration interface showing a table of policy routes. The table has columns for序号 (Index), 名称 (Name), 源区域 (Source Area), 目的网络对象 (Destination Network Object), 协议 (Protocol), 应用 (Application), 接... (Interface), 接口选择策略 (Interface Selection Strategy), 链路状态 (Link Status), 生效时间 (Effective Time), 状态 (Status), and 操作 (Operation). One entry is visible: index 1, name '网银', source area '3层区域LAN', destination '网上银行', protocol '全部', application '全部/全部', interface 'eth3-', selection strategy '未检测' (Not detected), effective time '全天' (All day), status '正常' (Normal), and operation icons.

### 5.2.2. 策略路由配置案例 2

配置案例：某用户有 2 条外网线路，分别是 2M 和 10M 的电信线路，用户希望实现内网用户访问公网的时候自动选择流量最小的线路。

在【导航菜单】页面中的『网络』→『路由』→『策略路由』，点击新增，新增多线路负载路由，页面如下：

### 新建多线路负载路由

启用

名称：

描述：

生效时间：

插入到：

**源**

区域：

网络对象：

**目的**

网络对象

ISP地址

国家/地区

**协议和端口**

设置协议和端口条件

**应用**

设置应用

**接口**

<input type="button" value="添加"/>	<input type="button" value="移除"/>	线路接口	链路状态	上移/下移	删除
<input type="checkbox"/>	<input type="checkbox"/>	eth2	未检测	<input type="button" value="↑"/> <input type="button" value="↓"/>	<input type="button" value="X"/>
<input type="checkbox"/>	<input type="checkbox"/>	eth3	未检测	<input type="button" value="↑"/> <input type="button" value="↓"/>	<input type="button" value="X"/>

[名称]和[描述]：设置策略路由的名称和描述信息。

[生效时间]：设置策略路由的生效时间，可以点击  来选择和设置时间计划，  
如下图所示：



『源』：选择源区域和网络对象，必须选择源区域。

『目的』：选择目的网络对象、ISP 地址或者国家/地区。ISP 地址需要预先设置 ISP 地址库，具体设置方法参见章节 3.4.6。均本案例中，需要对所有公网访问的应用匹配策略路由，选择全部 IP。

『协议和端口』：选择协议和端口条件。 本案例中，需要对所有内网用户访问公网的应用做策略路由，可以不做配置，代表全部。

『接口』：选择做多线路负载的线路。本案例中，需要对两条外网线路做负载，点击添加，选择连接两条外网线路的接口，如下图：



『接口选择策略』：选择外网线路的调度算法。设备支持四种调度算法：轮询，带宽比例，加权最小流量，优先使用前面的线路。

轮询：平均分配连接到多条外网线路。

带宽比例：按照外网线路带宽的比例来分配连接

加权最小流量：通过比较当前线路流量与线路带宽的比值，选择最小的线路

优先分配连接。

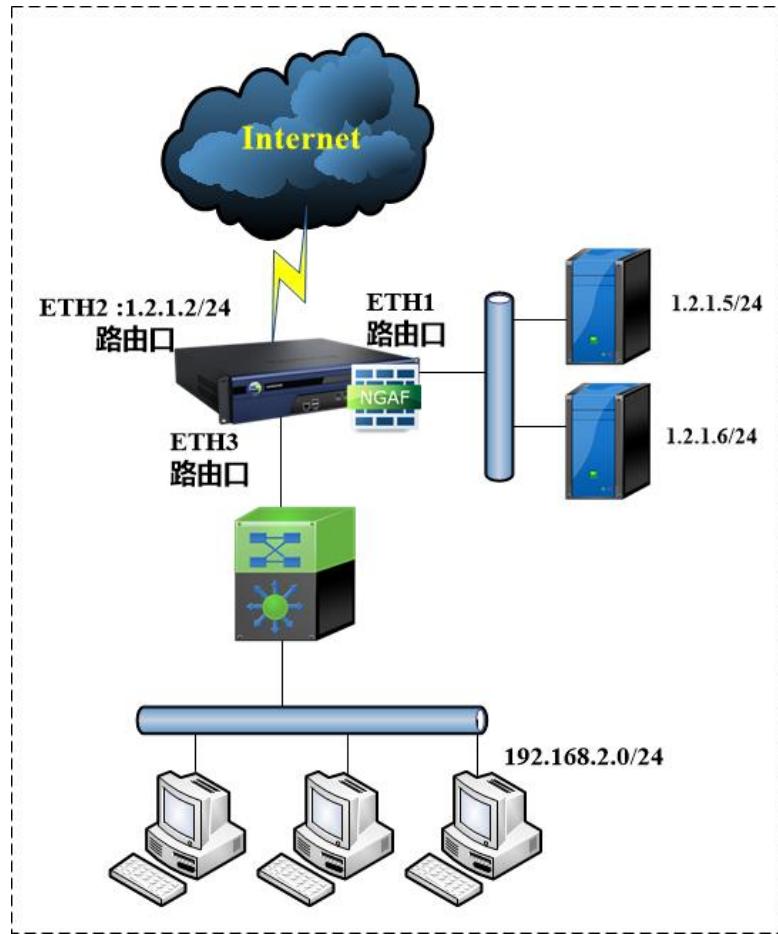
优先使用前面的线路：用于线路需要做主备的场景，则所有连接均分配到第一条线路，如果第一条线路故障，才把连接切换到第二条选择的可用线路。



1. 如果要实现多条外网线路的负载，必须开启链路检测，具体设置方法请查看章节 3.3.1.1.
2. 多线路负载只能选择 WAN 口属性的接口。
3. 每一条外网线路必须有一条策略路由与之对应，可以是基于源 IP 的策略路由或者多线路负载策略路由。

### 5.3. ARP 代理配置案例

配置案例：某用户的网络环境如下图所示，服务器群部署在内网，均分配公网 IP 地址，AF 设备需要代理内网的私有 IP 上公网，同时实现用户通过公网 IP 访问内网服务器的场景。客户不允许使用混合部署的情况下，需要使用 ARP 代理来实现。



第一步，通过『高级网络配置』→『ARP』→『ARP 代理』，开启 ARP 代理，如下图所示：



勾选[开启 ARP 代理]，出现如下提示页面：



点击**是**，开启和保存配置。

第二步，新增 ARP 代理。点击**新增**，如下图所示：



[起始地址]和[结束地址]：填写服务器的 IP 范围。

[网络接口]：服务器连接的设备接口。本案例中，服务器连接在 eth1 口下，故选择 eth1 接口。

点击**提交**，保存和生效配置。用户即可实现通过公网 IP 访问内网服务器，无需在 AF 设备上添加端口映像规则。



1.该案例用户的需求可以通过 AF 设备的混合模式部署或者通过路由模式部署+ARP 代理两种方式来实现。使用 ARP 代理功能时，AF 设备的外网口必须配置公网 IP 地址，连接内网服务器的接口必须是路由口，任意配置一个与其他网段不冲突的 IP 地址。

## 5.4. DHCP 配置案例

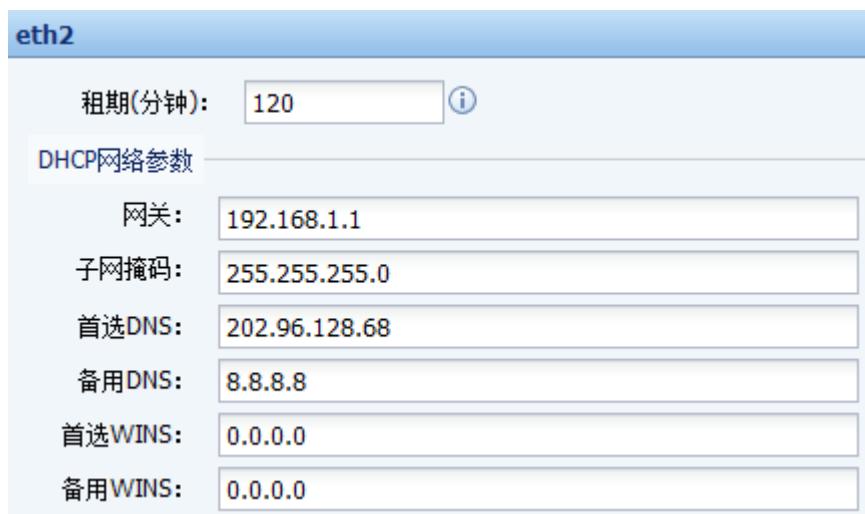
### 5.4.1. 服务器配置案例

配置案例：某用户 AF 设备的内网口 eth2 下接内网网段，用户要求通过 AF 自动分配 192.168.1.100-192.168.1.199 这段 IP 地址给会议室的用户上网，其中经

理的计算机固定分配 192.168.1.100 的 IP 地址。

第一步，开启 DHCP 服务。

第二步，在【DHCP 服务接口列表】中选择 eth2 口进行 DHCP 配置。配置租期和 DHCP 网络参数：

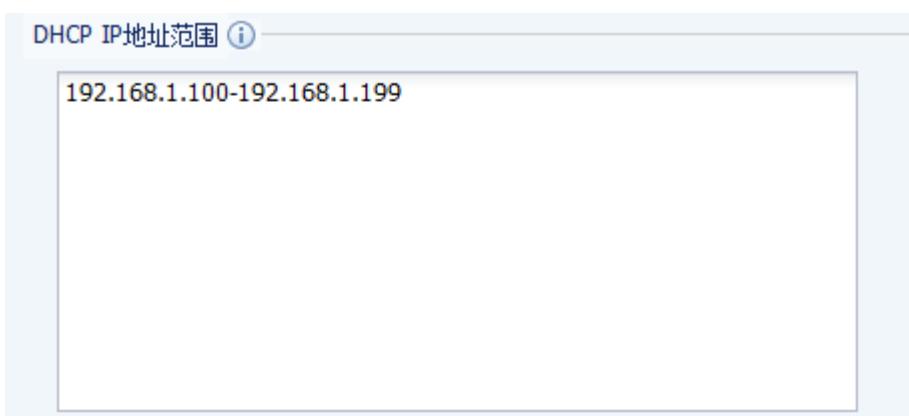


DHCP 网络参数	
网关:	192.168.1.1
子网掩码:	255.255.255.0
首选DNS:	202.96.128.68
备用DNS:	8.8.8.8
首选WINS:	0.0.0.0
备用WINS:	0.0.0.0

[租期（分钟）]：设置 IP 地址分配的租期，即使用时间。

『DHCP 网络参数』中设置 DHCP 自动分配的网关地址、DNS 地址和 WINS 地址。

第三步：设置『DHCP IP 地址范围』，即设置可以自动分配的 IP 地址。



DHCP IP 地址范围	
192.168.1.100-192.168.1.199	

第四步：设置保留 IP，点击**保留 IP 设置**，设置保留 IP，即根据计算机的

MAC 地址，固定分配一个 IP 给相应的计算机。



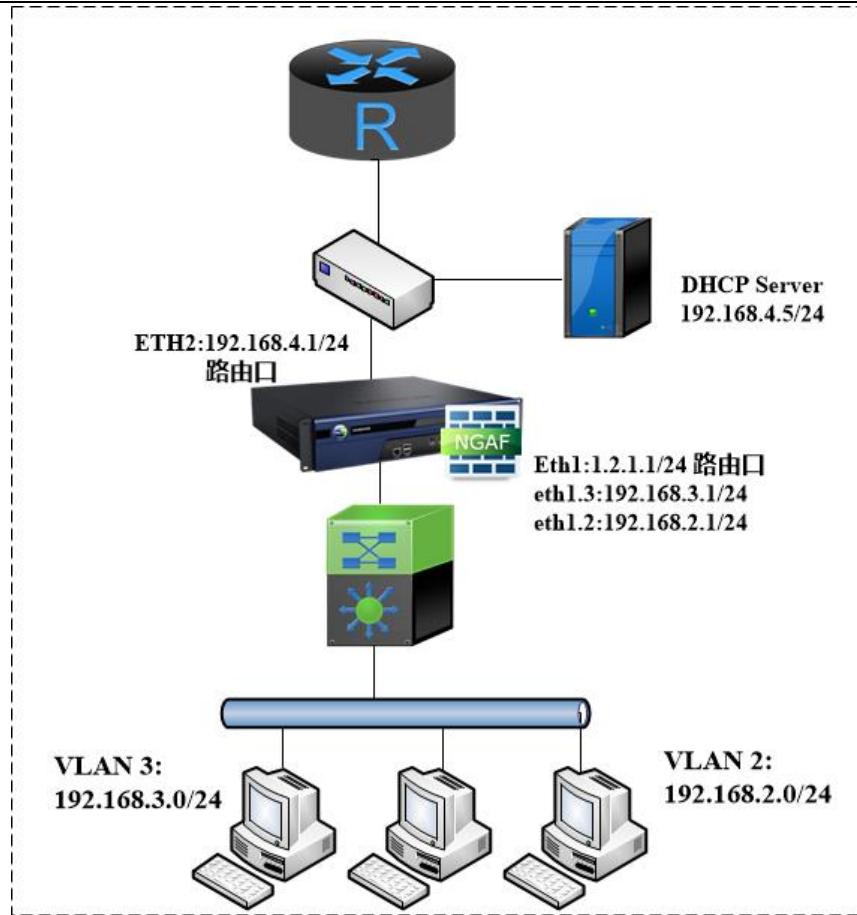
点击 **添加**，在弹出框中填入名称、固定分配的 IP 地址以及 MAC、机器名等。



查看 DHCP 的运行状态以及 DHCP 的分配状态，请在【导航菜单】中进入【运行状态】→【DHCP 运行状态】页面进行查看。

#### 5.4.2. DHCP 中继配置案例

配置案例：某用户网络环境如下所示，内网交换机划分多个 VLAN，统一通过 DHCP 服务器分发 IP 地址，要求 AF 设备充当内网 VLAN 的网关和 DHCP 中继。



第一步，AF设备上的接口配置。本案例中，eth1口设置成路由口，并在eth1口上设置VLAN2和VLAN3的子接口；eth2口设置成路由口。接口配置详见章节3.3.1.，此处不再赘述。

第二步，启用DHCP中继功能。 启用DHCP中继

第三步，设置对[以下接口启用中继]和DHCP服务器地址。[以下接口启用中继]必须同时选择设备与DHCP服务器通信的接口和DHCP客户端通信的接口，接口如下：

启用DHCP中继 [\(i\)](#)

对以下接口启用中继

可选：	已选：
eth0	
eth1	
	增加 >
	< 移除

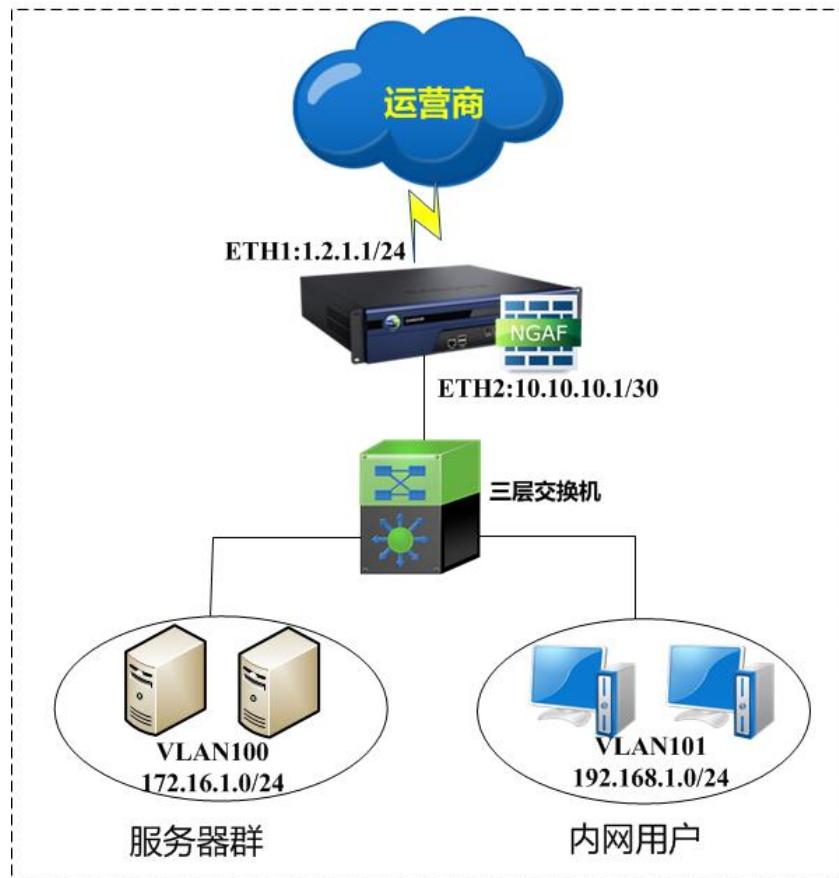
DHCP服务器地址： 192.168.4.5



**DHCP 中继支持所有的路由口，子接口和 VLAN 网口，不支持 ADSL 拨号类型的路由口。如果启用 DHCP 中继的网口未接线，则影响 DHCP 中继的结果。**

## 5.5. Dos/DDos 防护配置案例

某客户拓扑如下，内网有服务器网段 172.16.1.0/24，内网用户为 192.168.1.0/24 网段。之前有出现过服务器受到洪水攻击，导致应用中断的情况。客户希望通过 DOS/DDOS 防护设置来保护内网服务器以及内网用户；内网用户中毒发送过高的会话和数据也需要将其中断，以保证网络的稳定性；针对 AF 设备本身的攻击要能够防御，当出现攻击时不允许来自国外的 IP 地址访问内网服务器，只允许内网用户网段对外进行访问。



第一步：在设置 DOS 攻击防护之前，首先必须定义好区域，首先要到『网络』→『接口/区域』定义好接口所属的【区域】。『对象』→『IP 组』定义好内网服务器所属的【IP 组】。此案例中将需要将 ETH2 定义为[内网区域]。ETH1 定义为[外网区域]。172.16.1.10/24 定义为[服务器组]，内网用户网段 192.168.1.0/24 定义为[内网网段]。

第二步：『策略』→『安全策略』→『DOS/DDOS 防护』，新增外网对内攻击防护策略，进入设置页面。设置源区域为[外网区]，勾选 ARP 洪水攻击防护，设置扫描防护。页面如下：

### 新增外网对内攻击防护策略

启用

名称: 外网防护

描述:

源

外网区域: 外网区域

ARP洪水攻击防护

每源区域阈值(packet/s): 5000

扫描防护

扫描攻击类型: 已选防护: IP地址扫描防护,端口扫描防护

DoS/DDoS攻击防护

内网IP组: 服务器组

DoS/DDoS攻击类型: 已选防护: SYN洪水攻击防护, UDP洪水攻击防护, ...

检测攻击后操作

记录日志  阻断

『内网 IP 组』选择目的服务器为[服务器组]或者全部。

『DOS/DDOS 攻击类型』可以分别设置 SYN Flood、UDP Flood、DNS Flood、ICMP Flood 的阈值，如下图所示：



### SYN Flood 防护

[每目的 IP 激活阈值(packet/s)]: 统计到达每个目的 IP 的 SYN 包的 PPS (packets per second)，如果超过设定值则触发 NGFW SYN 代理机制，以减少服务器压力，建议比丢包阀值低，最好为其一半。取值范围为 1-100000000。

[每目的 IP 丢包阈值(packet/s)]: 统计到达每个目的 IP 的 SYN 包 PPS(packets per second)，如果超过设定值则触发防护机制。取值范围为 1-100000000。

[源 IP 封锁阈值(packet/s)]: 统计到达每个源 IP 的 SYN 包 PPS (packets per second)，如果超过设定值则触发防护机制。取值范围为 1-100000000。

[封锁时间(s)]: 针对每个源 IP 达到超过设定值后，自动进行封锁时间。取值范围为 0~1800s，在攻击者列表可以查看攻击 IP、封锁时间。

### UDP Flood 防护:

[每目的 IP 丢包阈值(packet/s)]: 统计到达每个目的 IP 的 UDP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[源 IP 封锁阈值(packet/s)]: 统计到达每个源 IP 的 UDP 包 PPS，如果超过设

定值则触发防护机制。取值范围为 0~100000000。

[封锁时间(s)]: 针对每个目的 IP、源 IP 达到超过设定值后，自动进行封锁时间。取值范围为 0~1800s，在攻击者列表可以查看攻击 IP、封锁时间。

### DNS Flood 防护

[每目的 IP 丢包阈值(packet/s)]: 统计到达每个目的 IP 的 DNS 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[源 IP 封锁阈值(packet/s)]: 统计到达每个源 IP 的 DNS 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[封锁时间(s)]: 针对每个目的 IP、源 IP 达到超过设定值后，自动进行封锁时间。取值范围 0~1800s，在攻击者列表可以查看攻击 IP、封锁时间。

### ICMP Flood 防护:

[每目的 IP 丢包阈值(packet/s)]: 统计到达每个目的 IP 的 ICMP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[源 IP 封锁阈值(packet/s)]: 统计到达每个源 IP 的 ICMP 包 PPS，如果超过设定值则触发防护机制。取值范围为 0~100000000。

[封锁时间(s)]: 针对每个目的 IP、源 IP 达到超过设定值后，自动进行封锁时间。取值范围 0~1800s。在攻击者列表可以查看攻击 IP、封锁时间。

『检测攻击后操作』：可以勾选操作[记录日志]和[阻断]。

点击 **高级防御选项**，可基于数据包攻击类型，IP 协议报文选项，TCP 协议报文选项来开启防护，默认不勾选。如下图所示：



点击提交保存配置即可。页面如下：

DoS/DDoS 防护						
新增		删除		启用		禁用
序号	名称	防护方向	描述	策略类型	攻击源区域	状态
1	外网防护	外网->内网		ARP洪泛攻击防护开启 扫描防护开启 DOS/DDOS攻击防护开启	外网区域	✓

第三步：『策略』→『安全策略』→『DOS/DDOS 防护』，新增内网对外攻击防护策略。选择源区域为[内网区]，选择仅允许内网服务器段和内网用户从源区域穿透设备。页面如下：

**新增内网对外攻击防护策略**

启用

注意：如果您的内网到防火墙本机之间是SNAT的部署环境，请勿启用此防护策略！

名称：

描述：

**源**

内网区域：

内网IP组：

**扫描防护**

扫描攻击类型：**已选防护：IP地址扫描防护,端口扫描防护**

**DoS/DDoS攻击防护**

DoS/DDoS攻击类型：**已选防护：SYN洪水攻击防护,UDP洪水攻击防护,...**

**检测攻击后操作**

记录日志     阻断

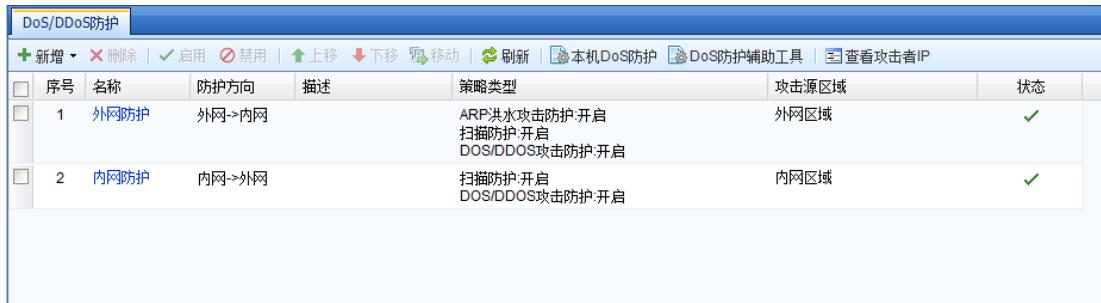
**高级防御选项**

**提交** **取消**

扫描防护、DOS/DDOS 攻击防护、检测攻击后操作与外网攻击防护策略设置相同，点击**高级防御选项**，可开启基于数据包攻击类型的防御，如下图所示：



点击**提交**后，保存和生效配置，如下图所示：



序号	名称	防护方向	描述	策略类型	攻击源区域	状态
1	外网防护	外网->内网	ARP洪水攻击防护开启 扫描防护开启 DOS/DDOS攻击防护开启		外网区域	
2	内网防护	内网->外网	扫描防护开启 DOS/DDOS攻击防护开启		内网区域	

第四步：『策略』→『安全策略』→『DOS/DDOS 防护』→『本机 DOS 防护』，开启本机 DOS 防护，如下图所示：



启用

**扫描防护**

扫描攻击类型：**已选防护：端口扫描防护**

**DoS/DDoS 攻击防护**

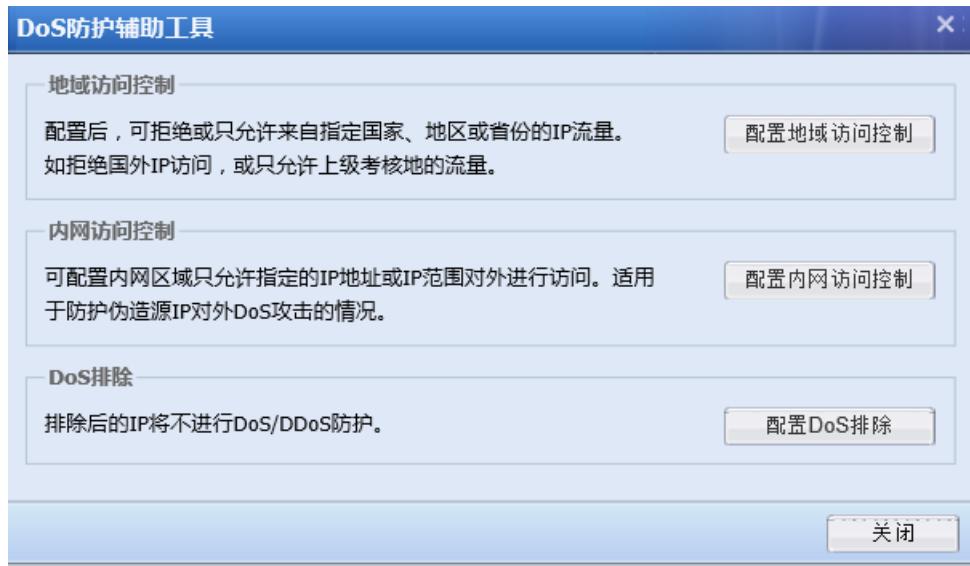
DoS/DDoS 攻击类型：**已选防护：SYN洪水攻击防护, UDP洪水攻击防护, ...**

**检测攻击后操作**

记录日志       阻断

**提交** **取消**

第五步：『策略』→『安全策略』→『DOS/DDOS 防护』→『DOS 防护辅助工具』，设置地域访问控制、内网访问控制和 DoS 排除，如下图所示：



点击**配置地域访问控制**，新增不允许国外IP访问的策略，外网区域选择[外网区域]，目的网络对象选择[服务器组]，控制方式设置[只允许以下国家/地区访问]，国家/区域选择[中国大陆]，如下图所示：



点击**提交**，保存和生效配置。

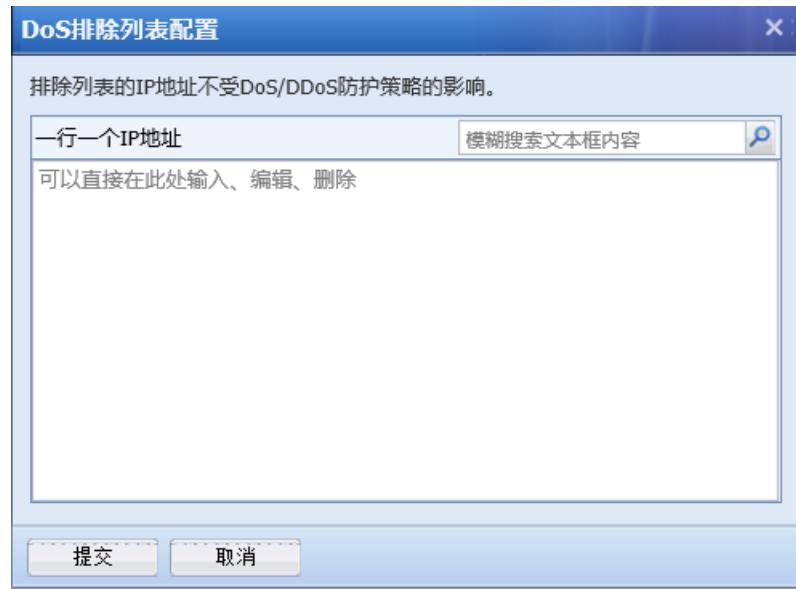
DoS/DDoS防护 > 地域访问控制								
操作		名称	描述	外网区域	目的IP组	国家控制方式	国家	状态
<input type="checkbox"/>	1	不允许国外IP访问		外网区域	服务器组	只允许以下国家/…	中国大陆	 

点击**配置内网访问控制**，内网区域选择[内网区域]，内网IP组选择[服务器组]和[内网网段]，如下图所示：



点击**提交**，保存和生效配置。

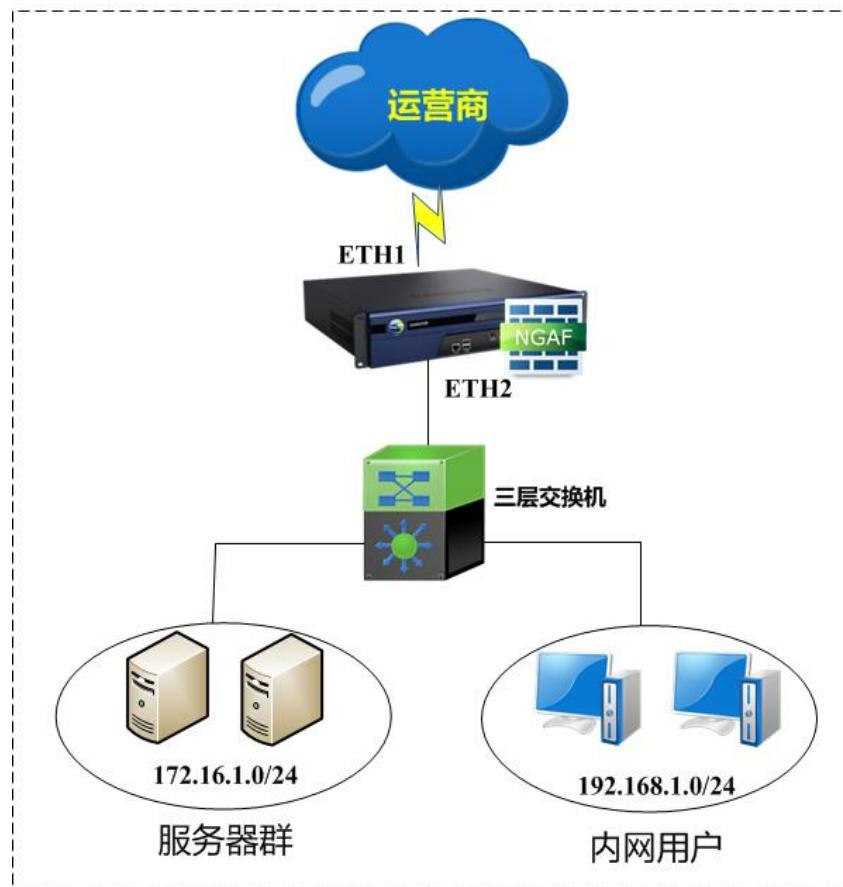
点击**DoS排除**，添加排除IP地址。



点击**提交**，保存和生效配置。

## 5.6. 应用控制策略配置案例

某用户拓扑如下，由于内网用户在上班时间看在线视频、玩游戏等导致工作效率很低。用户希望能够禁止内网用户上班时间玩游戏，看在线视频。但是下班时间可以正常使用。用户的上班时间是上午 8:00-12:00，下午 2:00-6:00。



第一步：在设置应用控制策略之前，必须定义好对象。首先要在『网络』→『接口/区域』定义好接口所属的【区域】。『对象』→『IP组』定义好内网服务器所属的【IP组】。『对象』→『时间计划』定义好用户的上班时间。详细配置请参考3.4.7章节。此案例中将需要将ETH2定义为[内网区]。ETH1定义为[外网区]。192.168.1.0/24定义为[内网用户]。循环时间计划组为[上班时间]。如图：

序号	名称	IP范围	描述	删除
1	内网用户	192.168.1.0/24		X

时间计划				
单次时间计划				
<input type="button" value="新增"/>	<input type="button" value="删除"/>			
<input type="button" value="刷新"/>				
序号	名称	生效时间	时间组描述	删除
1	全天	周一至周日:上午 0:00 - 下午 11:59分(包含最...)	全天	X
2	上班时间	周一至周五:上午 8:00 - 上午 12:00 ...		X

接口/区域					
物理接口		子接口	VLAN接口	聚合接口	区域
<a href="#">+ 新增</a>	<a href="#">- 删除</a>	<a href="#">刷新</a>			
	区域名称	转发类型	接口列表	管理选项	管理地址
<input type="checkbox"/>	内网区	三层区域	eth2	WebUI, ssh, snmp	全部
<input type="checkbox"/>	外网区	三层区域	eth1	WebUI, ssh, snmp	全部

第二步：『策略』→『访问控制』→『应用控制策略』，点击新增，填写好规则名称。

选择源区域为[内网区]，源IP组为[内网用户]，源端口设置为[全部]。

选择目的区域为[外网区]，由于内网用户看在线视频，玩游戏的目标IP不确定，所以目标IP选择全部。

由于在线视频，游戏等数据无法通过端口进行封堵，所以此处在应用中选择网络流媒体、P2P流媒体和游戏规则库。选择生效时间为前面定义的[上班时间]，动作拒绝。页面如下：

新增应用控制策略

启用

基础信息

名称: 禁止上班时间玩游戏, 看视频  
描述: 可以为空, 最多为256个字符  
分组和优先级: 默认分组 | 1 | 之前

访问者条件

区域: 内网区  
地址: 网络对象 | 内网IP组  
端口: 非必填, 默认为全部端口

被访问者条件

区域: 外网区域  
网络对象: 全部  
服务/应用: 应用 | 网络流媒体/全部, 游戏/全部, P2P流

生效条件设置

动作选项:  允许  拒绝  
生效时间: 上班时间  
高级选项: 设置

保存并继续新增 确定 取消

第三步：点击提交保存新建的规则即可，页面如下：

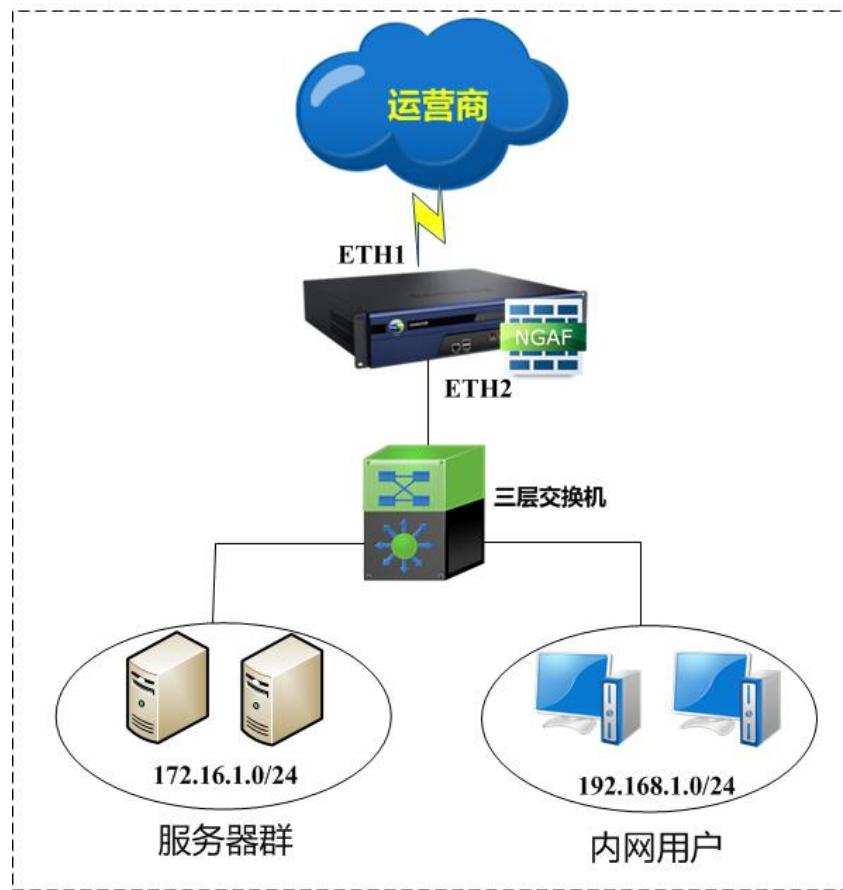
应用控制策略														
优先级	名称	分组	源区域	源网络对象/用户	目的区域	目的网络对象	服务/应用	生效时间	更新时间	动作	匹配	状态	操作	
1	禁止内网用户上...	默认分组	内网区	内网用户 192.168.1.0/24	外网区	全部	网络流媒体/全部 游戏/全部 P2P流媒体/全部	上阳时间	07-07 14:20:57	拒绝	0	✓		
2	all	默认分组	mana lan ...	全部	mana lan ...	全部	预定义服务/any	全天	04-14 16:53:49	允许	9999+	✓		
3	默认策略	-	全部	全部	全部	全部	全部/全部	全天	-	拒绝	0	✓		



1. 设备默认有一条全部拒绝的策略是不能删除的。因为防火墙默认是不允许所有数据进行通信。需要手动新建规则放通。
2. IP 组需预先设置，或者直接选取组织结构中特定的用户组。

## 5.7. 内容安全策略配置案例

某用户拓扑如下，用户希望实现不允许内网用户访问非法、色情，以及反动类的网站。设置内网用户上班时间不允许上传下载音乐和电影格式的文件。用户的上班时间是上午 8:00-12:00，下午 2:00-6:00。



第一步：在设置策略之前，需要在『网络』→『接口/区域』定义好接口所属的【区域】。『对象』→『网络对象』定义好内网用户所属的【IP组】。详细配置请参考 3.4.1 章节。此案例中将需要将 ETH2 定义为[内网区]。ETH1 定义为[外网区]。192.168.1.0/24 定义为[内网用户]。如图：

网络对象		服务器识别		
+ 新增		× 删除	刷新	导入
序号	名称	类型	IP范围	描述
1	内网用户	IP组	192.168.1.0/24	<span style="color: red;">删除</span>

接口/区域					
物理接口		子接口	VLAN接口	聚合接口	区域
+ 新增		× 删除	刷新	接口联动	
<input type="checkbox"/>	区域名称	转发类型	接口列表	管理选项	管理地址
<input type="checkbox"/>	内网区	三层区域	eth2	WebUI, ssh, snmp	全部
<input type="checkbox"/>	外网区	三层区域	eth1	WebUI, ssh, snmp	全部

时间计划				
单次时间计划		循环时间计划		
<input type="button" value="新增"/>	<input type="button" value="删除"/>	<input type="button" value="刷新"/>		
<input type="checkbox"/>	序号	名称	生效时间	时间组描述
-	1	全天	周一至周日:上午 0:00 - 下午 11:59分(包含最...)	全天
<input type="checkbox"/>	2	上班时间	周一至周五:上午 8:00 - 上午 12:00 ...	

第二步：进入『对象』→『安全策略模板』→『内容安全』的 URL 过滤规则页面，填写好模板名称。选择需要过滤的网站类型（设备内置）并勾选文件安全选项。生效时间选择上班时间。页面如下：



第三步：点击 **高级选项**，由于某些非法网站可能是 HTTPS 类型的，所以同时勾选 HTTP (get)、HTTP (post) 和 HTTPS。文件类型组选择电影和音乐格式（设备内置），由于用户上传和下载都要过滤，所以方向选择[过滤上传和下载]。界面配置如下：



点击**提交**保存规则即可。

第四步：进入『策略』→『安全策略』→『安全防护策略』，新增用户保护策略。由于内网用户属于[内网区]，所以此处选择源区域为[内网区]，源网络对象选择[内网用户]，目的区域[外网区]，目的网络对象为[全部]。页面如下：

新增用户防护策略

常规 → 防御 → 检测响应

策略名称: 内容安全策略  
描述: 可以为空，最多为95个字符  
状态:  启用

源

区域: 内网区  
网络对象/用户:  网络对象  
内网IP组  
 用户/组  
请选择

目的

区域: 外网区域  
网络对象: 全部

下一步 取消

第五步：在防御页面勾选内容安全，且选择创建的内容安全策略模板。动作勾选拒绝，并根据需要，选择是否勾选[日志]记录。页面如下：

新增用户防护策略

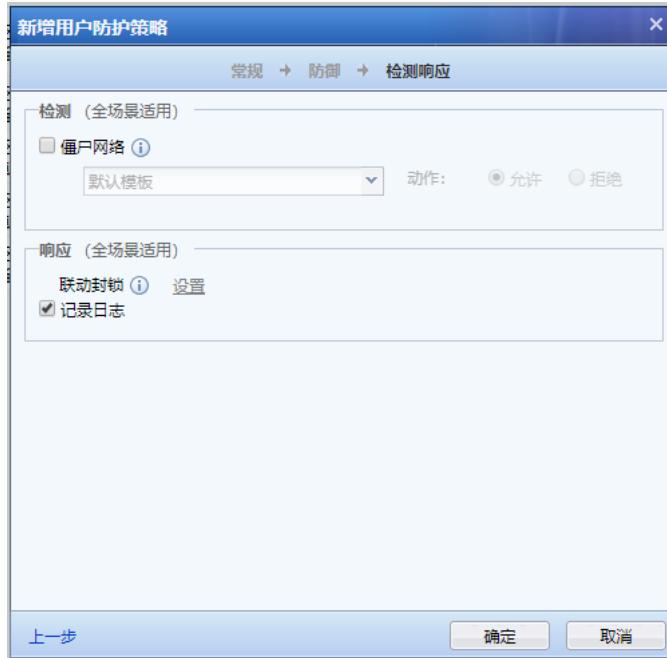
常规 → 防御 → 检测响应

基础防御 (全场最适用)

漏洞攻击防护 ①  
默认模板\_上网管控场景 动作:  允许  拒绝

内容安全( SAVE安全智能文件检测 ) ①  
内容安全策略 动作:  允许  拒绝

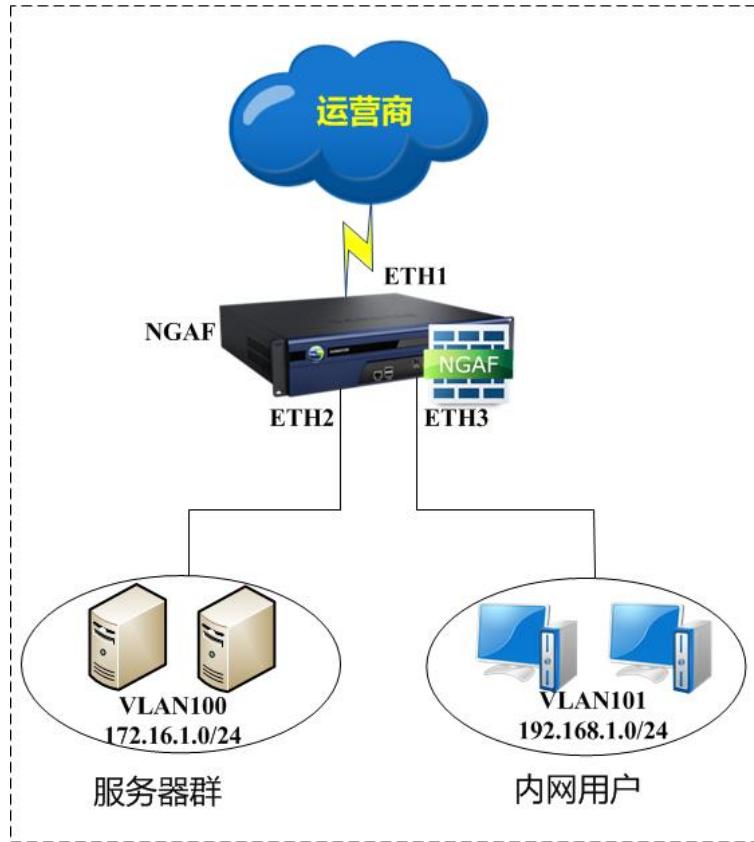
上一步 下一步 取消



点击**确认**保存策略即可。

## 5.8. 漏洞攻击防护典型配置案例

某客户拓扑如下，防火墙路由模式部署。内网服务器区与用户区通过分别位于防火墙两个不同的接口。客户希望利用漏洞攻击防护功能即保护服务器，又保护客户端。



第一步：首先要在『网络』->『接口/区域』，将防火墙三个接口划分到不同区域。本案例中，将ETH1定义成外网区，ETH2定义成DMZ区，ETH3口定义成内网区。『对象』->『网络对象』将172.16.1.0/24定义成服务器组，192.16.1.0/24定义成内网用户，界面如下：

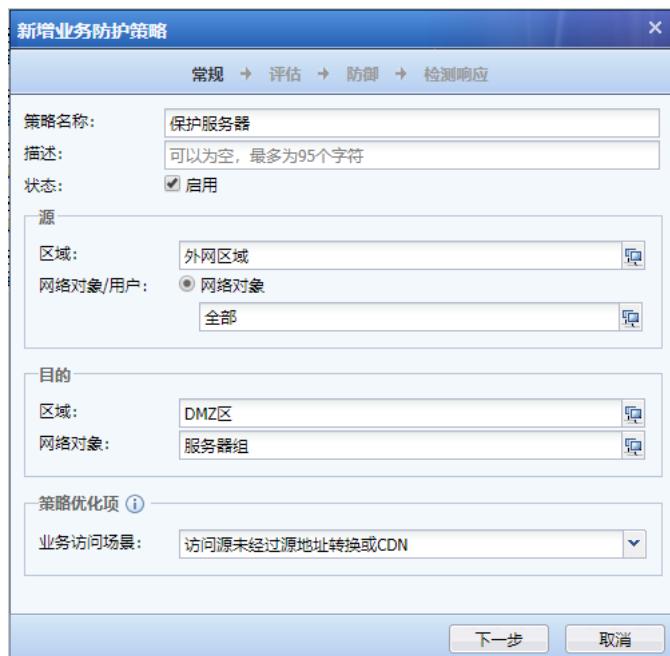
接口/区域						
物理接口		子接口		VLAN接口	聚合接口	
				区域	接口联动	
<span style="color: green;">+ 新增</span> <span style="color: red;">- 删除</span> <span style="color: blue;">↻ 刷新</span>						
<input type="checkbox"/>	区域名称	转发类型	接口列表		管理选项	管理地址
<input type="checkbox"/>	外网区	三层区域	eth1		WebUI, ssh, snmp	全部
<input type="checkbox"/>	内网区	三层区域	eth3		WebUI, ssh, snmp	全部
<input type="checkbox"/>	DMZ区	三层区域	eth2		WebUI, ssh, snmp	全部

网络对象					
服务器识别		IP范围		描述	
<span style="color: green;">+ 新增</span>	<span style="color: red;">- 删除</span>	<span style="color: blue;">↻ 刷新</span>	<span style="color: green;">导入</span>	<span style="color: blue;">导出</span>	<span style="color: gray;">重要级别：所有</span> <span style="color: gray;">类型：所有类型</span> <span style="color: gray;">搜索</span>
<span style="color: green;">+ 新增</span> <span style="color: red;">- 删除</span> <span style="color: blue;">刷新</span>		<span style="color: green;">+ 新增</span> <span style="color: red;">- 删除</span>		<span style="color: green;">+ 新增</span> <span style="color: red;">- 删除</span>	
序号	名称	类型	IP范围	描述	删除
1	内网用户	IP组	192.168.1.0/24		<span style="color: red;">×</span>
2	服务器组	IP组	172.16.1.0/24		<span style="color: red;">×</span>

第二步：设置服务器保护的策略模板。进入『对象』→『安全策略模板』→『漏洞攻击防护』，此例因为无特殊需求，所以使用默认的【默认模板\_业务保

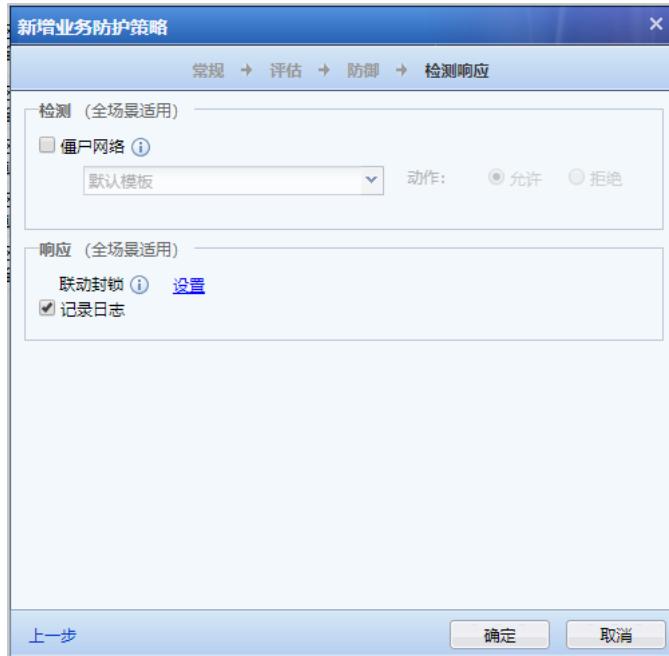
护场景】模块即可，无需编辑。

第三步：设置服务器保护的策略。进入『策略』→『安全策略』→『安全防护策略』，点击**新增**，设置好策略名称。源区域选择外网区，网络对象为全部，目的区域选择DMZ区，网络对象选择服务器组。界面如下：



第四步：在防御页面勾选漏洞攻击防护，且选择创建的漏洞攻击防护服务器模板。动作勾选拒绝，并根据需要，选择是否勾选[日志]记录。页面如下：





点击**确定**，保存即可。

第五步：设置客户端保护的策略模板。进入『对象』→『安全策略模板』→『漏洞攻击防护』，此例因为无特殊需求，所以使用默认的【默认模板\_上网管控场景】模块即可，无需编辑。

第六步：设置客户端保护的策略。进入『策略』→『安全策略』→『安全防护策略』，点击**新增**，设置好策略名称。源区域选择内网区，网络对象为内网用户，目的区域选择外网区，网络对象选择全部。界面如下：

新增用户防护策略

常规 → 防御 → 检测响应

策略名称: 保护客户端

描述: 可以为空，最多为95个字符

状态:  启用

源

区域: 内网区域

网络对象/用户:  网络对象  
内网IP组  
 用户/组  
请选择

目的

区域: 外网区域

网络对象: 全部

下一步 取消

第七步：在防御页面勾选漏洞攻击防护，且选择创建的漏洞攻击防护保护客户端模板。动作勾选拒绝，并根据需要，选择是否勾选[日志]记录。页面如下：

新增用户防护策略

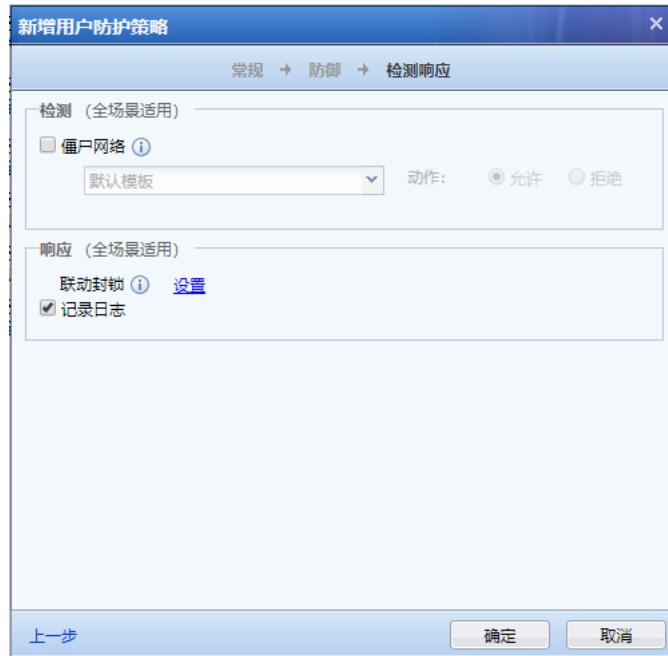
常规 → 防御 → 检测响应

基础防御 (全场最适用)

漏洞攻击防护 ①  
默认模板\_上网管控场景 动作:  拒绝  允许

内容安全( SAVE安全智能文件检测 ) ①  
默认模板 动作:  拒绝  允许

上一步 下一步 取消



点击**确定**，保存即可。

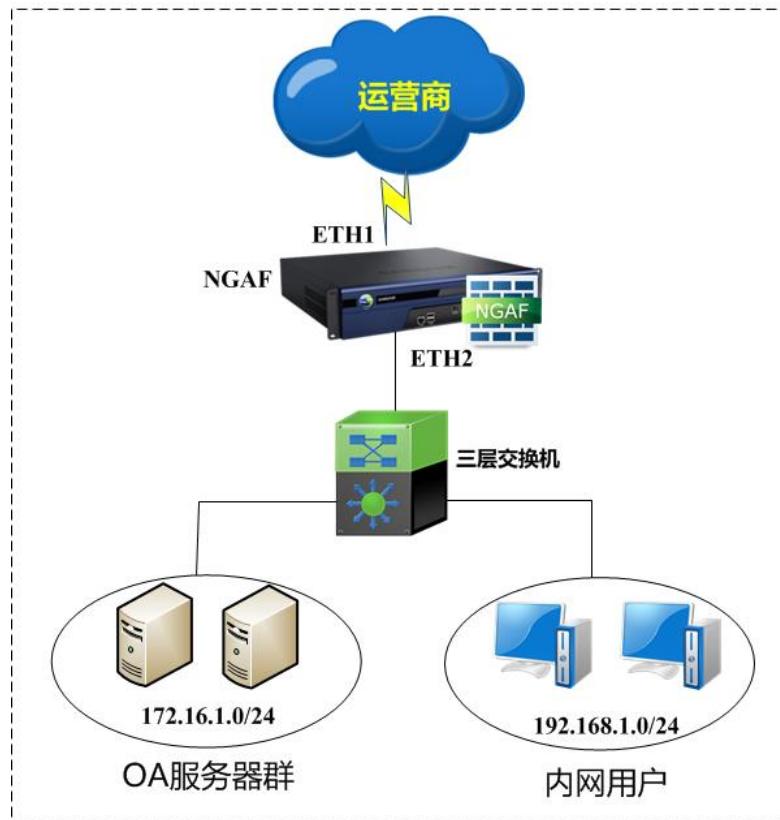


1.由于攻击服务器和客户端使用的攻击手段不同，所以设置保护客户端与保护服务器的客户端漏洞和服务器漏洞规则也是不同的。

## 5.9. WEB 应用防护配置案例

### 5.9.1. WEB 应用防护配置案例一 WAF

某客户拓扑如下，SANGFOR 防火墙路由模式部署在网络出口，客户希望针对内网的 WEB 服务器群进行保护。包括针对 WEB 服务器的 server 字段隐藏，OS 命令注入防护，SQL 命令注入防护，XSS 命令注入防护，CSRF 命令注入防护，[http://www.\\*\\*\\*.com/view/\\*](http://www.***.com/view/*) 此类含有 view 的 URL 全部允许，不需要进行防护，除此之外的其余 URL 都需要进行防护。客户内网服务器提供服务的端口包括 WEB 80 和 FTP 21 。



第一步：在设置策略之前，需要在『网络』→『接口/区域』定义好接口所属的【区域】。『对象』→『IP组』定义好服务器所属的【IP组】。此案例中将需要将 ETH2 定义为[内网区]。ETH1 定义为[外网区]。172.16.1.0/24 定义为[服务器组]。如图：

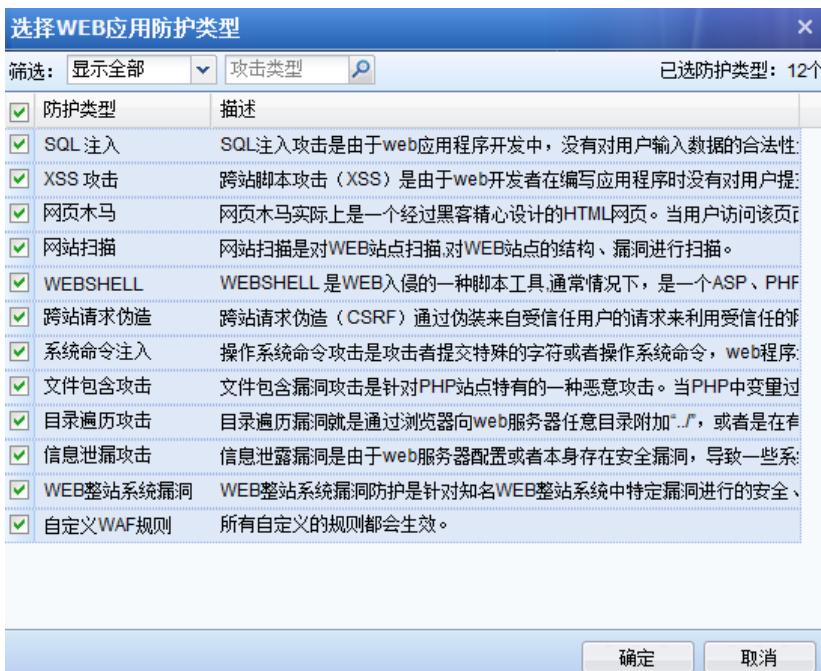
网络对象					重要级别:	类型:	搜索
序号	名称	类型	IP范围	描述	删除		
1	内网用户	IP组	192.168.1.0/24				
2	服务器组	IP组	172.16.1.0/24				

接口/区域					
物理接口		子接口	VLAN接口	聚合接口	区域
				刷新	
区域名称	转发类型	接口列表	管理选项	管理地址	
内网区	三层区域	eth2	WebUI, ssh, snmp	全部	
外网区	三层区域	eth1	WebUI, ssh, snmp	全部	

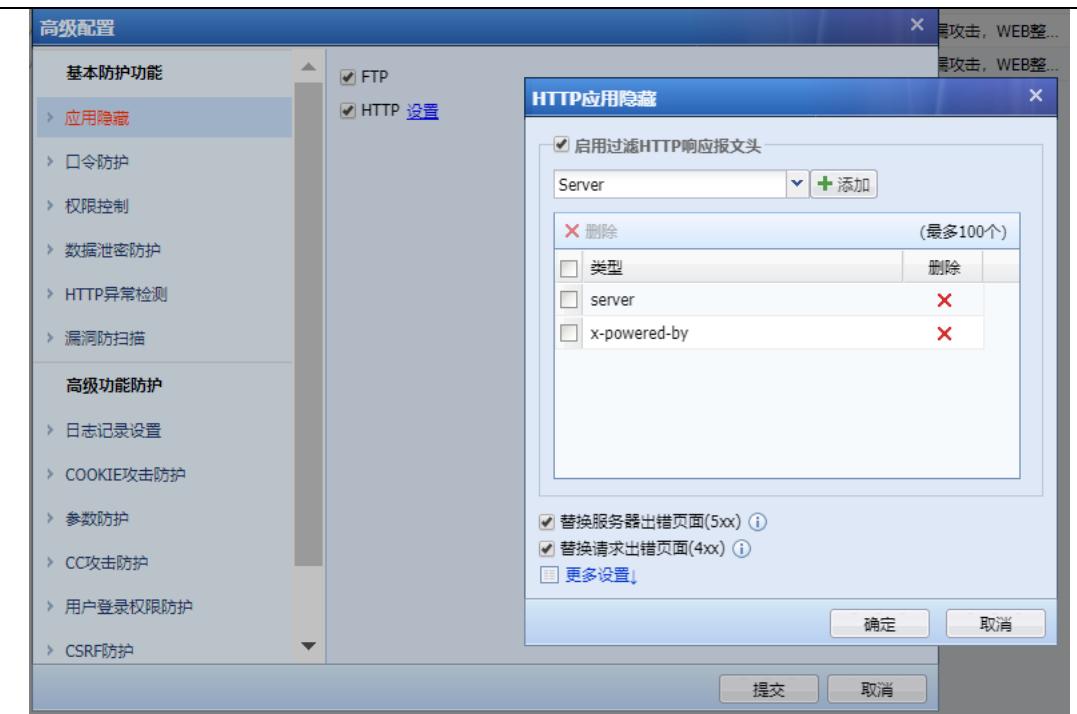
第二步：设置保护服务器模板。进入进入『策略』→『安全防护策略』→『Web应用防护』，点击新增，设置好模板名称。设置端口信息如下如图所示：



第三步：设置服务器的防护类型，勾选所有的防护类型，页面如下：



第四步：设置应用隐藏，该用户要求针对FTP服务器隐藏版本信息，针对HTTP服务器隐藏server字段，则设置如下图，点击**确定**保存即可：

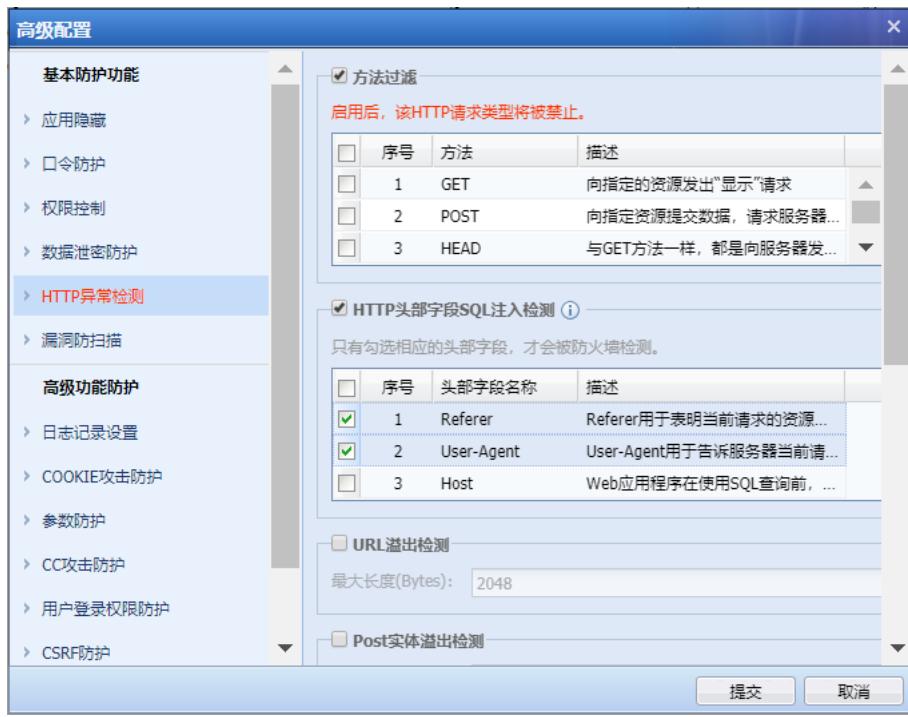
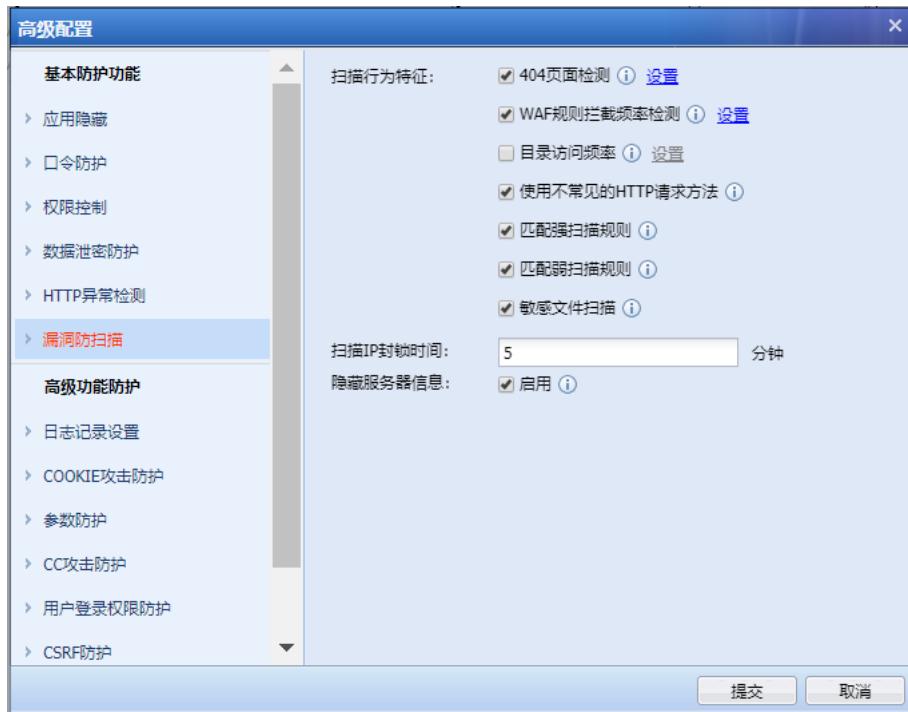


第五步：选择“权限控制”，勾选 URL 防护，点击**设置**，将 view 设置为允许，不进行检测。页面如下：



第六步：设置 HTTP 异常检测和漏洞扫描防护，如下图所示，点击**确定**保存

即可：



第七步：设置服务器保护的策略。进入『策略』→『安全策略』→『安全防护策略』，点击新增，设置好策略名称。源区域选择外网区，网络对象为全部，目的区域选择内网区，网络对象选择服务器组。界面如下：

新增业务防护策略

常规 → 评估 → 防御 → 检测响应

策略名称: 保护服务器  
描述: 可以为空, 最多为95个字符  
状态:  启用

源  
区域: 外网区域  
网络对象/用户:  网络对象  
全部

目的  
区域: 内网区  
网络对象: 服务器组

策略优化项 (i)  
业务访问场景: 访问源未经过源地址转换或CDN

下一步 取消

第八步：在防御页面勾选 Web 应用防护，且选择创建的 Web 应用防护保护服务器模板。动作勾选拒绝，并根据需要，选择是否勾选[日志]记录。页面如下：

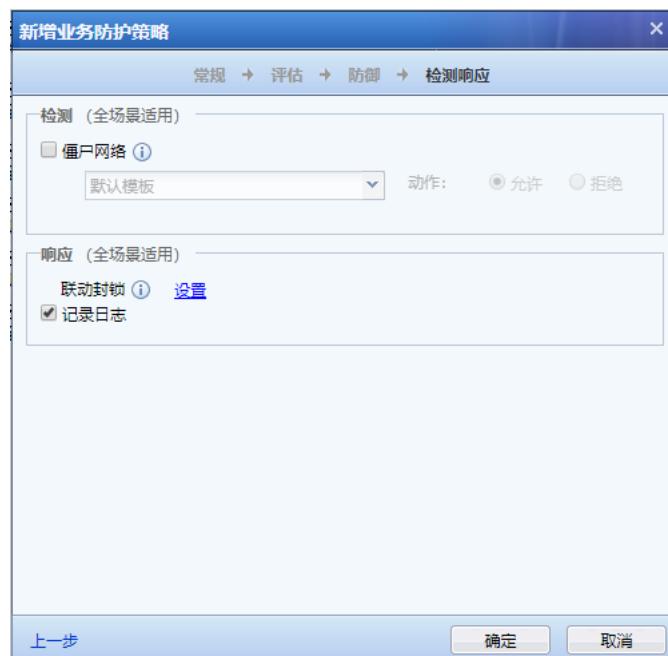
新增业务防护策略

常规 → 评估 → 防御 → 检测响应

增强功能 (业务保护场景适用)  
 实时漏洞分析 (i)

- 黑链
- Webshell
- 漏洞风险
- 配置风险
- 弱口令账号

上一步 下一步 取消



点击**确定**，保存即可。

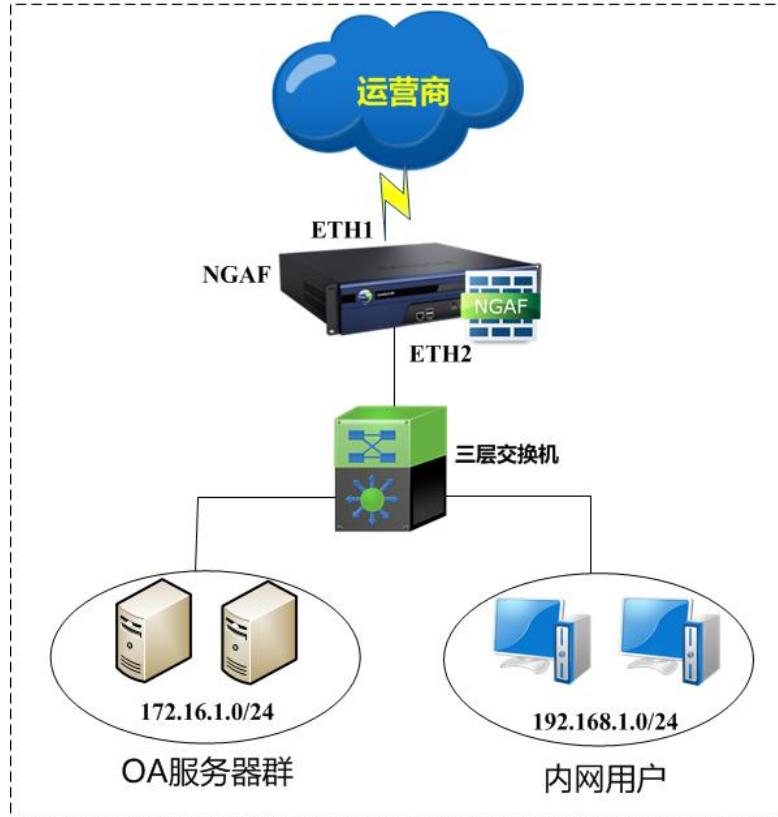
### 5.9.2. WEB 应用防护配置案例二 数据防泄密

某企业客户路由模式部署 SANGFOR AF 于网络出口处，内网部署了 WEB 服务器群，服务器上存有企业客户的数据供用户查询个人信息，但客户希望针对 WEB 服务器群上的数据进行保护，防止用户查询到非本人的信息。客户认为查

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

查询数据里不可能同时出现银行卡号、手机号、身份证号信息，如果同时出现这些信息则属于异常；第二，客户不允许放行从服务器上下载.xls文件。



第一步：在设置策略之前，需要在『网络』→『接口/区域』定义好接口所属的【区域】。『对象』→『IP组』定义好服务器所属的【IP组】。此案例中将需要将ETH2定义为[内网区]。ETH1定义为[外网区]。172.16.1.0/24定义为[服务器组]。如图：

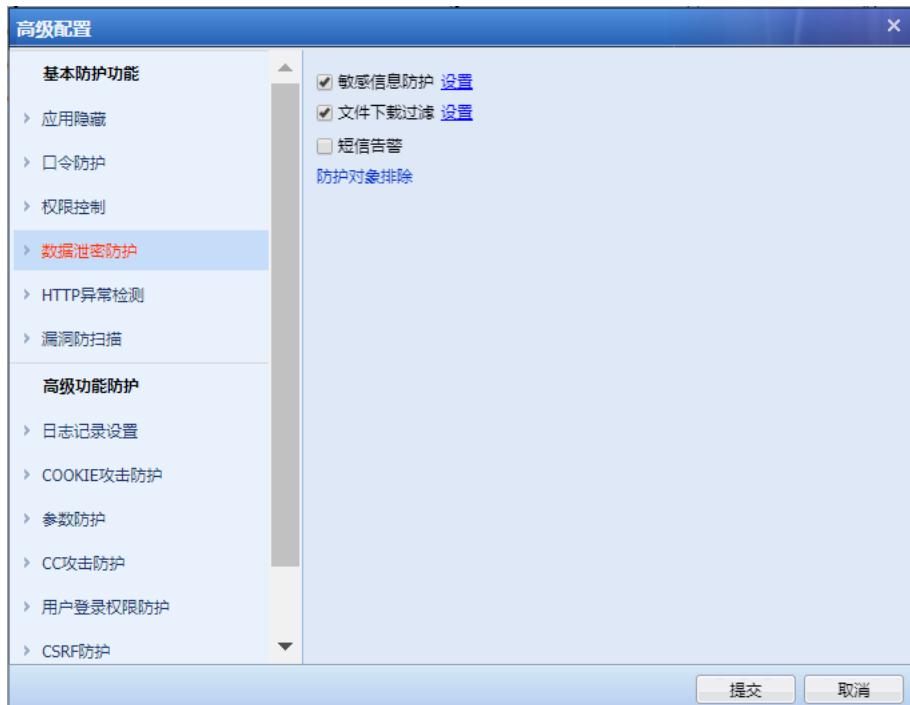
网格对象				服务器识别	重要级别	类型	搜索
序号	名称	类型	IP范围	描述	删除		
1	内网用户	IP组	192.168.1.0/24				
2	服务器组	IP组	172.16.1.0/24				

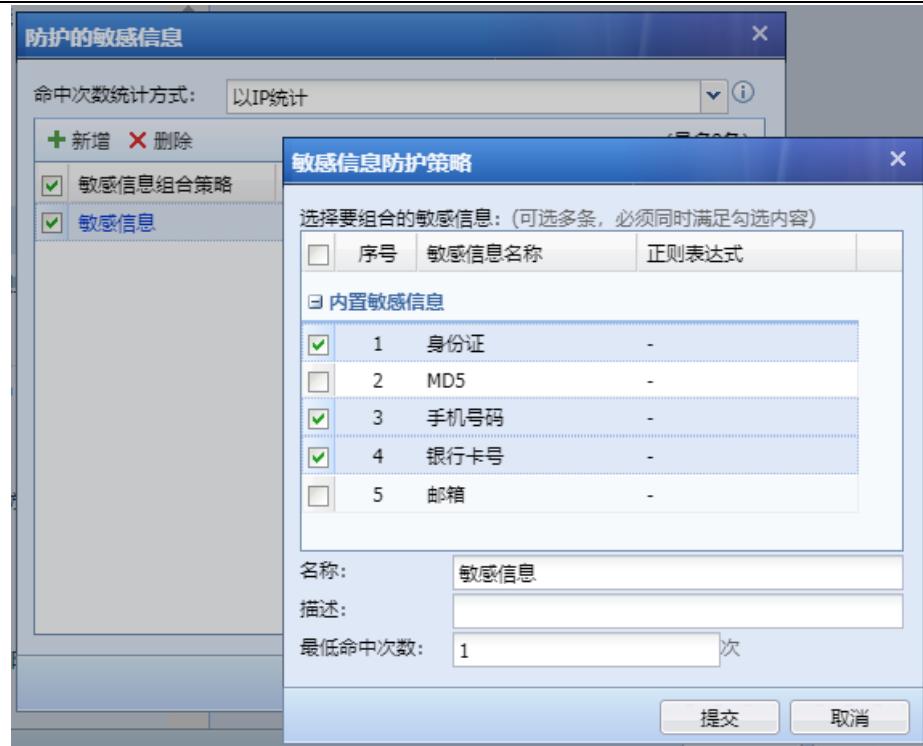
接口/区域							
物理接口		子接口		VLAN接口	聚合接口	区域	接口联动
+ 新增	× 删除	刷新					
<input type="checkbox"/>	区域名称	转发类型		接口列表		管理选项	管理地址
<input type="checkbox"/>	内网区	三层区域		eth2		WebUI, ssh, snmp	全部
<input type="checkbox"/>	外网区	三层区域		eth1		WebUI, ssh, snmp	全部

第二步：设置数据防泄密模板。进入进入『策略』→『安全防护策略』→『Web应用防护』，点击新增，设置好模板名称。设置端口信息如下如图所示：



第三步：设置敏感信息防护，当查询数据里同时出现银行卡号、手机号、身份证号信息时就算一次命中，只要命中一次就算数据泄密，页面如下：





第四步：设置文件下载过滤，不允许从服务器上下载.doc 和.xls 结尾的文档，  
页面如下：



第五步：设置数据防泄密的策略。进入『策略』→『安全策略』→『安全防护策略』，点击新增，设置好策略名称。源区域选择外网区，网络对象为全部，目的区域选择内网区，网络对象选择服务器组。界面如下：



第六步：在防御页面勾选 Web 应用防护，且选择创建的 Web 应用防护防泄密模板。动作勾选拒绝，并根据需要，选择是否勾选[日志]记录。页面如下：





点击**确定**，保存即可。

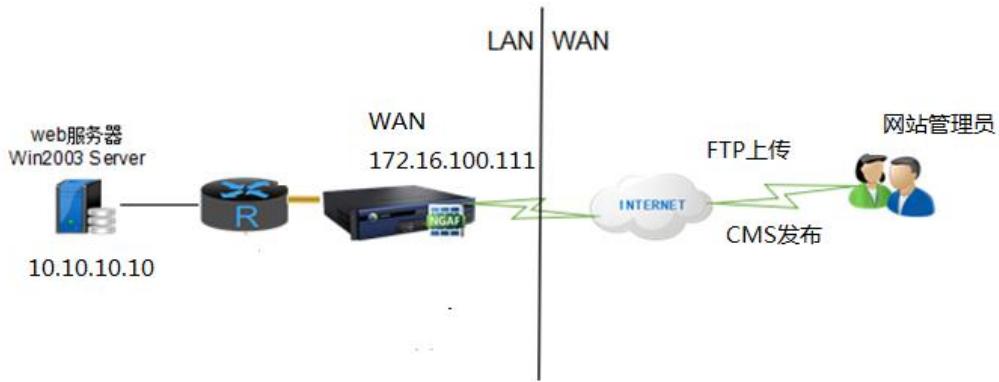
## 5.10. 网站篡改防护 2.0 应用案例

某用户拓扑如下，AF 路由模式 部署。内网有一个网站服务器，用户需求如下：

1. 客户 web 服务器为 Win2003 64 位 IIS 服务器，网站采用 CMS 发布网站内容，ftp 更新代码；
2. 网站管理员邮箱地址 75244@sangfor.com。
3. AF 设备 WAN IP 地址 172.16.100.111，服务器 IP 地址:10.10.10.10。

网站后台 CMS 登录方式：<http://172.16.100.111:8080/admin/>

网站后台 FTP 登录方式：<http://172.16.100.111:8080/ftp.html>



第一步：基础网络配置。参考 3.3 与 3.3.1.5 章节配置好接口 IP 地址，区域等信息将设备部署上架。参考 3.3.6.2 章节分别给服务器做端口映射。

第二步：『系统』→『系统配置』→『通用配置』→『邮件服务器』，邮件服务器配置了 smtp 邮件服务器、发件人邮箱。

第三步：『用户认证』→『服务器访问认证』，点击设置管理员邮箱，新建网站管理员邮箱，页面如下：



新增网站管理员邮箱

姓名:	zyw1
邮箱地址:	75244@sangfor.com

提交 取消

第四步：『用户认证』→『服务器访问认证』，点击新增，新建服务器访问认证策略，页面如下：

新增服务器访问认证

策略名称:	
服务器IP地址:	
网站防护方式	
<input type="checkbox"/> 网站后台登录防护 ( CMS )	HTTP端口: 80 网站管理URL: 可以直接在此处输入、编辑、删除
<input type="checkbox"/> FTP登录防护 FTP端口: 21 配置认证URL: http://www.yoursite.com/ftp.html 管理员登录FTP时，需先在该URL上进行验证码认证，建议格式为：您的网站域名+/ftp.html，如： http://www.baidu.com/ftp.html	
管理员认证方式	
<input checked="" type="checkbox"/> IP认证 (以下IP地址维护网站无需邮件认证) 请选择 <input type="button" value=""/>	
<input checked="" type="checkbox"/> 邮件认证 管理员邮箱地址: <a href="#">配置邮箱列表...</a> <input type="button" value="..."/> 认证通过有效时间: 5 分钟	

提交 取消



The screenshot shows a configuration page for 'FTP登录防护' (FTP Login Protection). On the left, there are fields for 'FTP端口' (Port) set to 21, '配置认证URL' (Authentication URL) set to <http://172.16.1.100>, and '管理员登录用户名' (Administrator Login Username) set to <http://www.sangfor.com>. Under '管理员认证方式' (Administrator Authentication Method), 'IP认证' (IP Authentication) is checked, and '邮件认证' (Email Authentication) is also checked. The '管理员邮箱地址' (Administrator Email Address) field contains '1个' (1) with a circled '1'. The '认证通过有效时间' (Authentication Validity Time) is set to 60 minutes. On the right, a list of users is displayed with columns for '姓名' (Name), '邮箱' (Email), and '状态' (Status). A user named 'zyw' is selected, highlighted with a red oval.

第五步：在服务器上安装 AF 设备的网站篡改防护客户端以及客户端设置，在编辑安全防护策略的防御页面，点击 **Windows 防篡改客户端**：



点击后出现如下页面：



The screenshot shows the download page for the '深信服文件保护系统软件' (Sangfor File Protection System Software). It includes a yellow folder icon, the software name, version 6.2, a brief description about preventing website modification, the applicable platforms (Windows 2003, 2008, 2012), and a download link labeled '点击下载' (Click to Download).

点击**点击下载**，下载网站篡改防护客户端软件。

下载完成后并防护服务器上安装此软件。

程序 logo:



运行客户端，首先需要输入登陆密码，初始密码为：admin

界面如下：



首次登录成功后如果需要修改密码，新密码必须包含数字、字母以及特殊符号，也可以不修改。界面如下：



NGAF安全防护

网页防篡改    关键事件日志

开启客户端：

修改密码

关联防火墙设备

设备IP地址: **172.16.100.111**

防篡改策略: test

网站目录：

+ 添加 - 删除 ✓ 启用 - 禁用 (注释：保护目录最多支持10个)

网站目录	状态
C:\Users\Administrator\Desktop\SiteFactory.Standard_5.1.0.0_20131225\WebSite	启用

允许修改的应用程序：

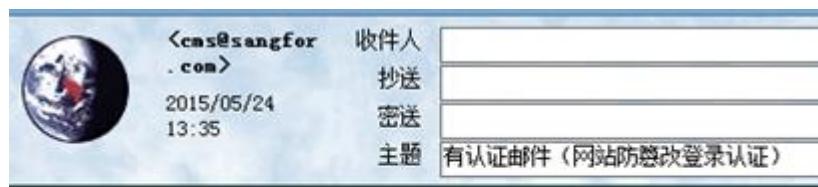
+ 添加 - 删除 ✓ 启用 - 禁用 (注释：信任应用程序最多支持16个)

描述	应用程序	状态
IIS	c:\windows\system32\inetsrv\w3wp.exe	启用
IIS服务器	c:\windows\syswow64\inetsrv\w3wp.exe	启用
windows资源管理器	c:\windows\explorer.exe	禁用

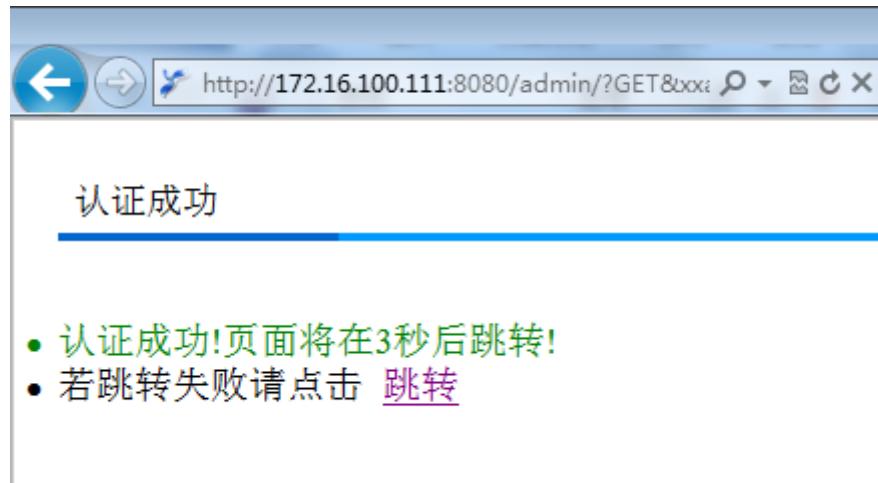
第六步：网站管理员 CMS 登录网站后台发布网站内容，  
<http://172.16.100.111:8080/admin/>

界面如下：





您的认证验证码为：11777  
请在10分钟内登录，过期需重新获取验证码。

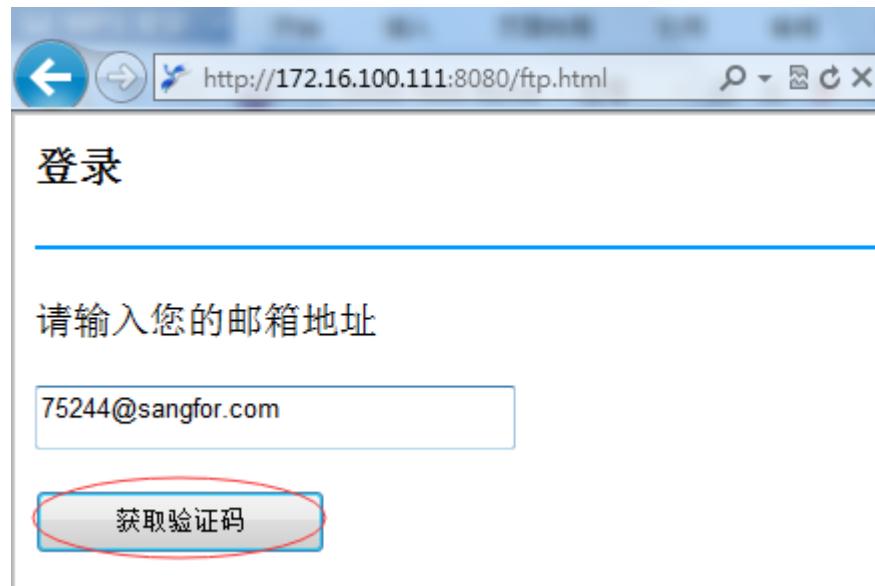


网站管理员通过 AF 认证，可以登录网站后台发布网站内容。

第七步：网站管理员 FTP 登录网站后台更新代码，  
<http://172.16.100.111:8080/ftp.html>

界面如下：





登录

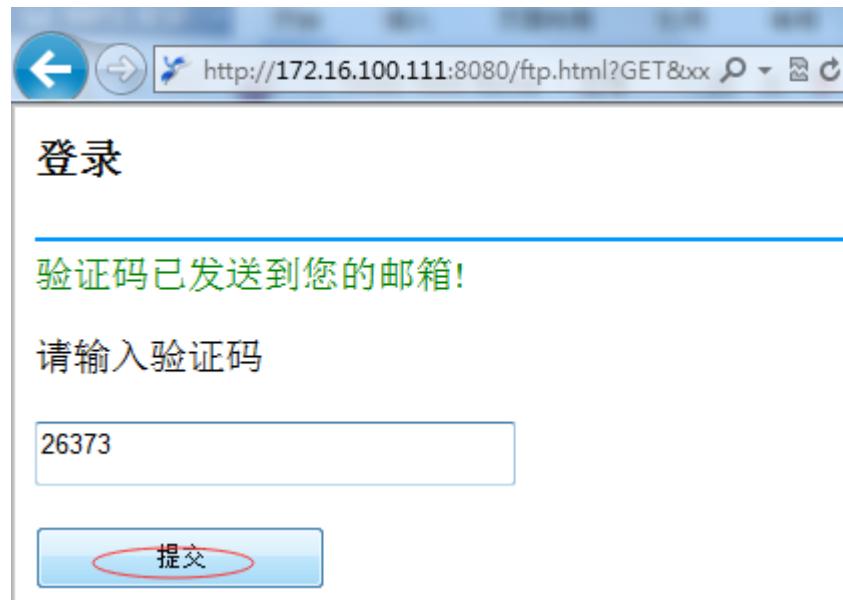
请输入您的邮箱地址

75244@sangfor.com

获取验证码



您的认证验证码为：26373  
请在10分钟内登录，过期需重新获取验证码。



登录

验证码已发送到您的邮箱!

请输入验证码

26373

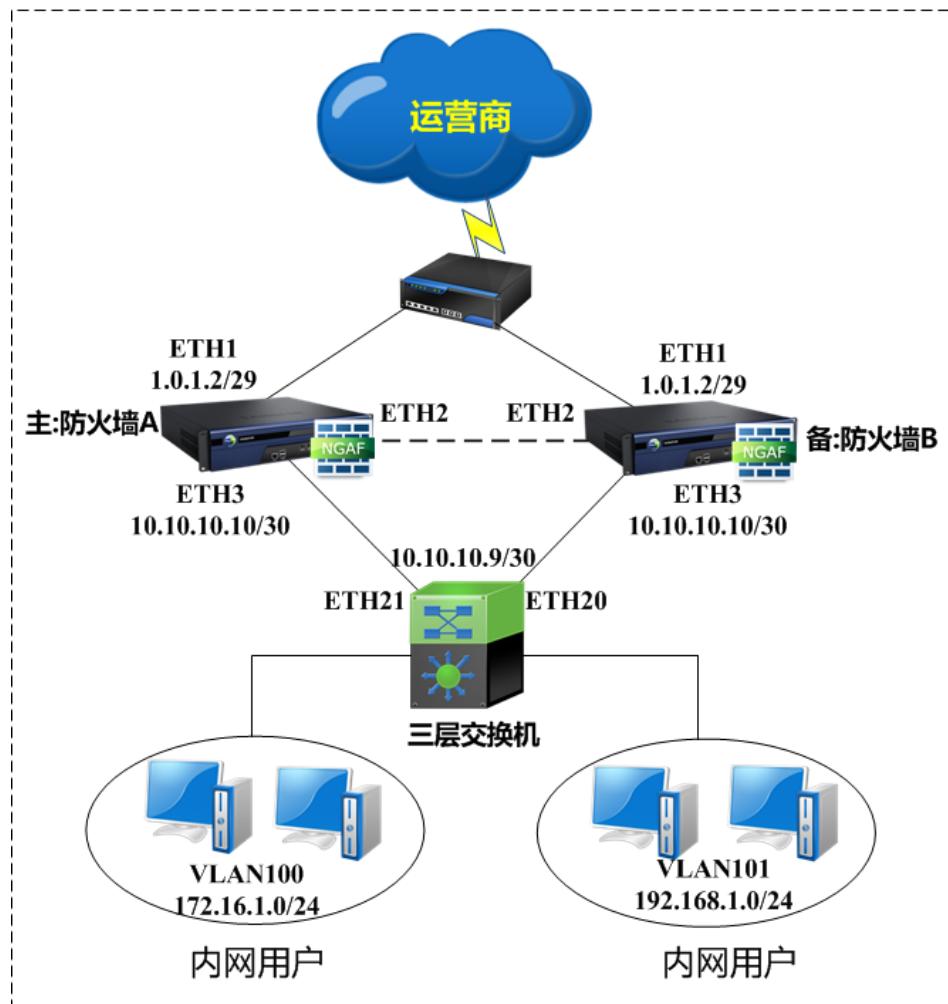
提交



网站管理员通过 AF 认证，可以登录网站后台更新网站代码。

## 5.11. 双机热备案例

某用户网络拓扑如下图所示，用户有两台 SANGFOR AF 防火墙部署在用户网络出口处做 SNAT，代理内网用户上网。防火墙 A 为主防火墙，防火墙 B 为备防火墙。用户希望实现当主防火墙出现问题时，备防火墙接替工作；防火墙 A 故障修复，则防火墙 A 自动切换成主防火墙，以实现防火墙的高度冗余。



第一步：首先配置防火墙 A。进入配置接口，配置接口为路由模式，并且配置好接口 IP 地址等信息。请参考网络配置章节 3.3.1。此处不再赘述。此案例中需要将 ETH1 口定义成[外网区]，ETH3 口定义成[内网区]。将 ETH2 口定义成 HA 口。界面如下：



接口/区域													
物理接口		子接口		VLAN接口		聚合接口		区域		地址		拨号...	
启用	禁用	刷新											
<input type="checkbox"/>	接口...	描述	WAN	接口...	连接...	区域	地址	拨号...	MTU	工作...	PING	网口...	链路...
<input type="checkbox"/>	eth0	管理口	否	路由...	静态IP	10.251.251.2...	---	1500	自动...	允许		未检测	<input checked="" type="checkbox"/>
<input type="checkbox"/>	eth1	WAN	是	路由...	静态IP	外网区	1.0.1.2/29	---	1500	自动...	拒绝		未检测
<input type="checkbox"/>	eth2	双机口	否	路由...	静态IP	DMZ区	10.10.9.9/30-HA	---	1500	自动...	拒绝		未检测
<input type="checkbox"/>	eth3	LAN	是	路由...	静态IP	内网区	10.10.10.10/24	---	1500	自动...	拒绝		未检测

第二步：防火墙 A：配置源地址转换规则。代理内网用户上网。此处请参考 3.3.6.1 章节。

第三步：防火墙 A：进入『高可用性』 - 『基本信息』配置接口，选择本端 ETH2 接口为双机通信口。填写对端地址 10.10.9.10。界面如下：

基本信息 双机热备 配置同步

本机地址 : 10.10.9.9/30-HA(eth2)

对端地址 : 10.10.9.10

第四步：防火墙 A：进入双机热备配置接口，点击新增，本案例中定义虚拟组为 100，防火墙 A 优先级为 100，勾选抢占。本案例中用到 ETH3 与 ETH1 口作为双机检测网口。配置页面如下：

**新增虚拟路由组**

虚拟组 :	100 (1-255)									
优先级 :	100 (1-255)									
抢占 :	<input checked="" type="radio"/> 是 <input type="radio"/> 否									
心跳时间 :	1 (1-60)s									
网口监视 :	<input type="button" value="新增"/> <input type="button" value="删除"/>									
<table border="1"><thead><tr><th>组序号</th><th>网口</th><th>编辑</th></tr></thead><tbody><tr><td>1</td><td>eth1</td><td><input type="button" value="编辑"/></td></tr><tr><td>2</td><td>eth3</td><td><input type="button" value="编辑"/></td></tr></tbody></table>		组序号	网口	编辑	1	eth1	<input type="button" value="编辑"/>	2	eth3	<input type="button" value="编辑"/>
组序号	网口	编辑								
1	eth1	<input type="button" value="编辑"/>								
2	eth3	<input type="button" value="编辑"/>								
接口链路监控 : <input type="button" value="新增"/> <input type="button" value="删除"/>										
<table border="1"><thead><tr><th>组序号</th><th>网口</th><th>编辑</th></tr></thead><tbody><tr><td colspan="3">没有可以显示的数据</td></tr></tbody></table>		组序号	网口	编辑	没有可以显示的数据					
组序号	网口	编辑								
没有可以显示的数据										

第五步：防火墙 A：进入配置同步接口，选择三种配置进行同步，点击保存，  
页面如下：

基本信息 | 双机热备 | 配置同步

启用同步 [\(i\)](#)

自动同步 [\(i\)](#)

同步对象：

待选	已选
	用户认证 配置同步 <b>会话表</b>

增加 

 移除

配置同步角色： 主控 [设置 \(i\)](#)

手动同步 [\(i\)](#)

[手动同步配置](#)

[查看同步报告](#)

[保存](#)

第六步：配置防火墙 B，此处只需要配置防火墙 B 的 ETH2 口以及双机热备信息，其余的配置可以从防火墙 A 同步过来，不需要配置。进入防火墙 B 的配置接口，配置 ETH2 接口 IP 信息，页面如下：



第七步：防火墙 B：进入高可用性配置接口，基本信息，选择本端接口 ETH2。

对端通信 IP 地址 10.10.9.9，点击**保存**，页面如下：

<b>基本信息</b>	<b>双机热备</b>	<b>配置同步</b>
本机地址：	10.10.9.10/30-HA(eth2)	
对端地址：	10.10.9.9	<b>测试</b>
<b>保存</b>		

第八步：防火墙 B：进入双机热备配置接口，设置与对端设备一样的虚拟组 100，优先级设置要比对端设备低，此处设置为 90，备机不抢占，心跳时间设置与对端设备一致，否则无法同步数据。选择网口列表。页面如下：

**新增虚拟路由组**

虚拟组：	100 (1-255)
优先级：	90 (1-255)
抢占：	<input type="radio"/> 是 <input checked="" type="radio"/> 否
心跳时间：	1 (1-60)s
网口监视：	<a href="#">i</a>

**新增** **删除**

	组序号	网口	编辑
	1	eth1	
	2	eth3	

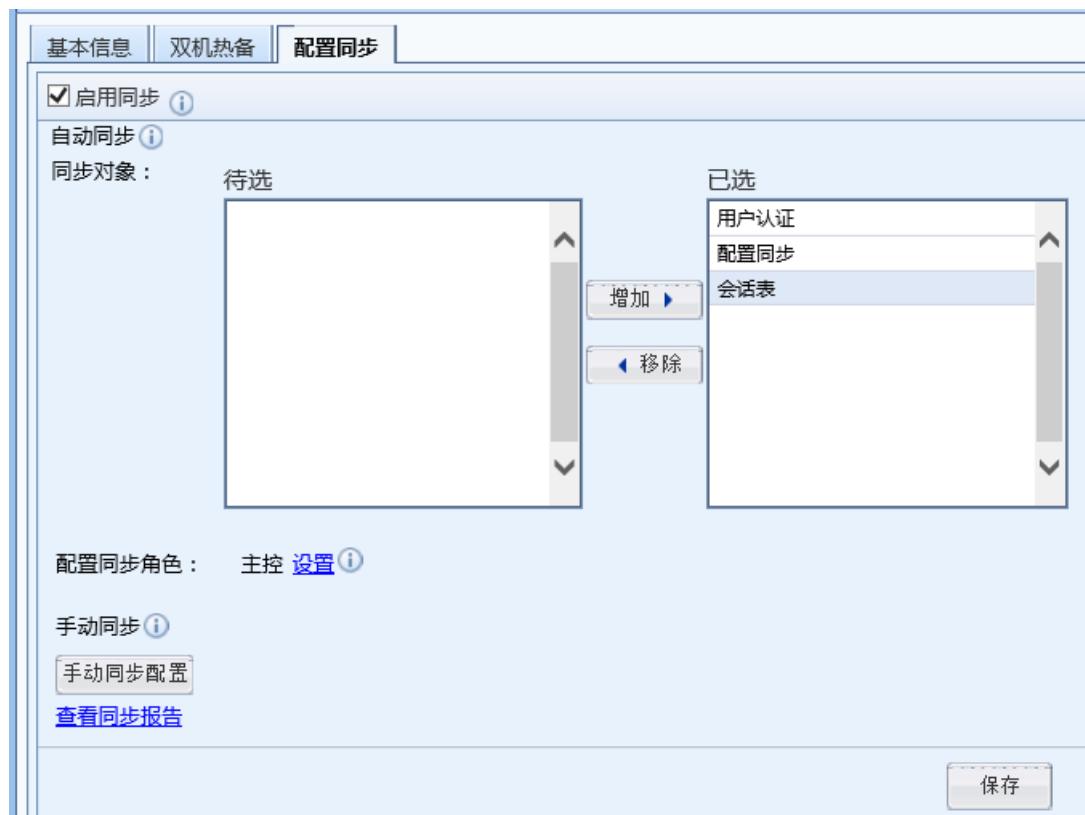
**接口链路监控：** [i](#)

**新增** **删除**

	组序号	网口	编辑
没有可以显示的数据			

**提交** **取消**

第九步：防火墙 B：配置同步针对防火墙 B，备机是一般是备控角色，配置由主控同步过来，且角色为备控的设备，无法修改配置。页面如下：



第十步：将防火墙 A 和防火墙 B 都断电，并且接好在线架。防火墙 A 先开机，待防火墙 A 开机后，再开启防火墙 B。防火墙 A 会向防火墙 B 同步配置信息。注意开机顺序不能反。

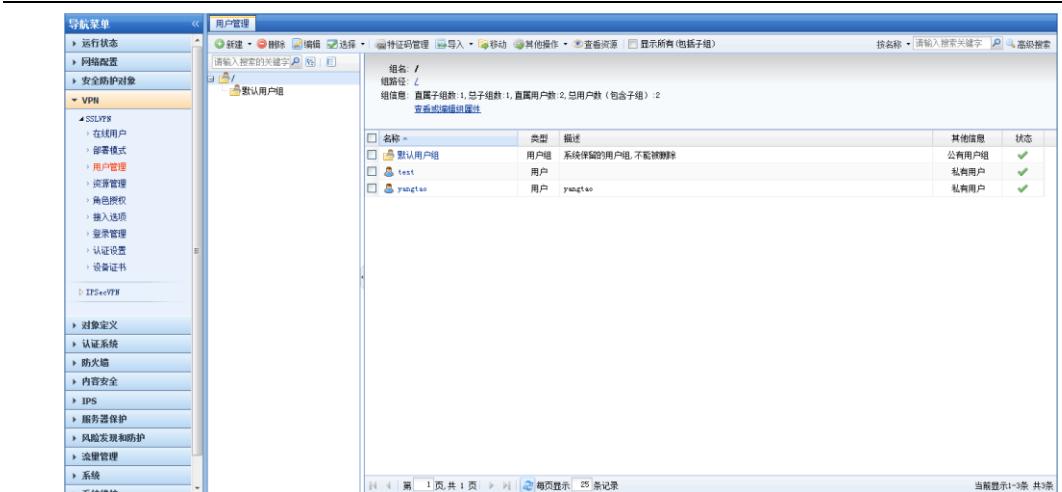
## 5.12. SSL VPN 配置案例

### 5.12.1. 新建用户配置案例

案例目标 1：建立一个采用用户名密码认证的 SSL VPN 用户，用户名为 ww，密码为 123，并启用硬件特征码认证。

配置步骤如下：

第一步：进入『VPN』→『SSL VPN』→『用户管理』页面，点击新建按钮，新增用户，界面如下图所示：



The screenshot shows the Sangfor User Management interface. On the left is a navigation menu with sections like SSLVPN, User Management, and Role Management. The main area displays a table of users and groups. One user, 'yangtao', is selected. The table includes columns for Name, Type, Description, Other Information, and Status. The status column shows green checkmarks for all users.

名称	类型	描述	其他信息	状态
默认用户组	用户组	系统保留的用户组,不能被删除	公有用户组	✓
test	用户		私有用户	✓
yangtao	用户	yangtao	私有用户	✓

第二步：在用户信息编辑页面，设置用户的账号和密码。本例中用户名为ww，密码为123，并勾选[辅助认证]→[硬件特征码]，如下图所示：



This screenshot shows the 'Edit User' form. It has three tabs: 'Basic Properties', 'Authentication Options', and 'Associated Roles'. In the 'Basic Properties' tab, fields include Name (ww), Description, Password, Confirm Password, Phone Number, and Group (选择). Under 'Authentication Options', the account type is set to 'Private User'. The 'Auxiliary Authentication' section is expanded, showing 'Hardware Feature Code' checked. In the 'Associated Roles' tab, the role 'Test' is selected. At the bottom are 'Save and Continue' and 'Save' buttons.

设置好之后，点击**保存**按钮，就可以用这个账号登录 SSLVPN 了。

### 5.12.2. TCP 应用配置案例

**案例背景：**某客户有以下几个服务需加入资源中以便让公司成员通过SSL访问。客户希望登录SSL后，可以直接登录OA系统正常办公。打开财务结算软件后，可以连接服务器并正常使用。

- 1、<http://192.168.1.10> OA 系统，公司办公的主要平台。
- 2、财务结算系统 192.168.1.15 端口 4003 一个财务软件，用于公司的报销、薪资发放等应用。

解决方案：这两个应用均可以使用 TCP 应用实现。

配置步骤如下：

第一步：进入『VPN』→『SSLVPN』→『资源管理』页面，新建一个 TCP 应用，添加 OA 系统。点击**新建**按钮，选择『TCP 应用』，进行如下图设置：



第二步：进入『VPN』→『SSLVPN』→『资源管理』页面，新建一个 TCP 应用，添加财务系统。点击**新建**按钮，选择『TCP 应用』，进行如下图设置：

基本属性

名称:	财务系统 *
描述:	财务系统
类型:	Other
地址:	192.168.1.15/4003:4003

应用程序路径: C:\Program Files\Sangfor\SSL\Client [浏览...]  
程序路径可以使用绝对路径也可以使用环境变量,例如%windir%

所属组: 默认资源组 >>

图标: 

启用该资源  
 允许用户可见

保存并继续添加 保存 取消

其中，类型选择 Other，同时端口范围填 4003。

第三步：进入『VPN』→『SSLVPN』→『角色授权』页面，新建角色，将用户 sangfor 与这两个资源关联起来。有关用户、角色的配置此处不再赘述。

第四步：配置完成后，使用 sangfor 账号登录 SSL，效果如下图所示：



OA 系统直接点击即可访问；财务系统在配置财务系统资源时添加了“应用程序路径”，可以直接点击即可访问，若在配置财务系统资源时未添加“应用程序



深信服，让IT更简单，更安全，更有价值

路径”，需手动启动应用程序。

## 附录 SANGFOR 设备升级系统的使用

SANGFOR 设备升级系统可用于对设备进行内核版本升级和备份恢复设备配置。在设备出现致命错误时，也可通过 SANGFOR 设备升级系统把设备恢复到出厂状态。同时，SANGFOR 设备升级系统还可以启动技术支持工具来检查系统网口工作状态，路由等配置信息以及更改网口工作模式等。

SANGFOR 设备升级系统为绿色版软件，解压后即可使用，解压文件里包含一个文件夹和一个主程序，页面如下：



STARTUP  
文件夹



SANGFOR Firmware Updater  
Sangfor Firmware Updater  
SANGFOR

双击打开主程序的主页面，页面如下：



『设备 IP 地址』：连接的 SANGFOR 设备的 IP 地址，格式为 IP: 端口，也可以直接输入 IP 地址进行访问，则默认连接的是该 IP 地址的 51111 端口。

『管理员密码』：AF设备的默认密码为 dlanrecover 或者是与AF设备的控制面板密码保持一致，与所连接的AF设备的版本有关。

『查找设备』：通过点击**查找设备**来搜索局域网内部的SANGFOR设备。



输入SANGFOR设备的IP地址以及管理员密码后，点击**连接**即可连接到设备进行系统升级、恢复默认配置等操作，页面如下：



『当前设备信息』：用于显示连接的 SANGFOR 设备的版本信息以及连接的 IP 地址。

『设备升级』：对当前连接的 SANGFOR 设备进行升级操作，包括在线升级和从本地加载升级包进行升级。

#### 在线升级：

选择在线升级，点击 **选择版本**，SANGFOR 设备升级系统会自动判定设备当前版本支持升级到哪个版本，并自动列出可以支持升级的版本信息，选择期望升级到的版本，点击 **确定** 后，系统会自动从服务器上下载升级包进行升级操作。



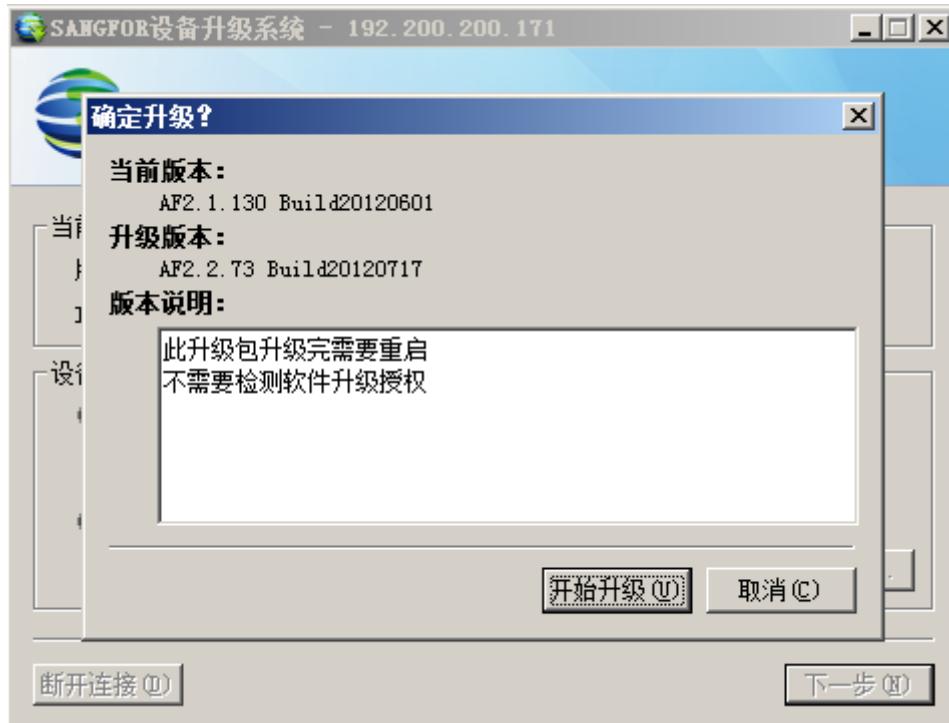
1. 使用 SANGFOR 设备升级系统进行在线升级时，要求所连接的 SANGFOR 设备能够正常上网，否则将不能进行在线升级。

2. SANGFOR 设备的某些版本不支持在线升级功能，具体请联系深信服科技客户服务中心确认。

## 从本地载入升级包：

选择从本地加载升级包，点击**浏览**，选择下载到本地的相应升级包，然后点击**下一步**，显示当前升级包的基本信息，确认无误后，点击**开始升级**进行升级操作，页面如下：





升级完成后，设备升级状态里会显示“升级成功”，页面如下：



1. 升级具有一定的风险，如升级不当会导致设备损坏。请勿自行升级。如

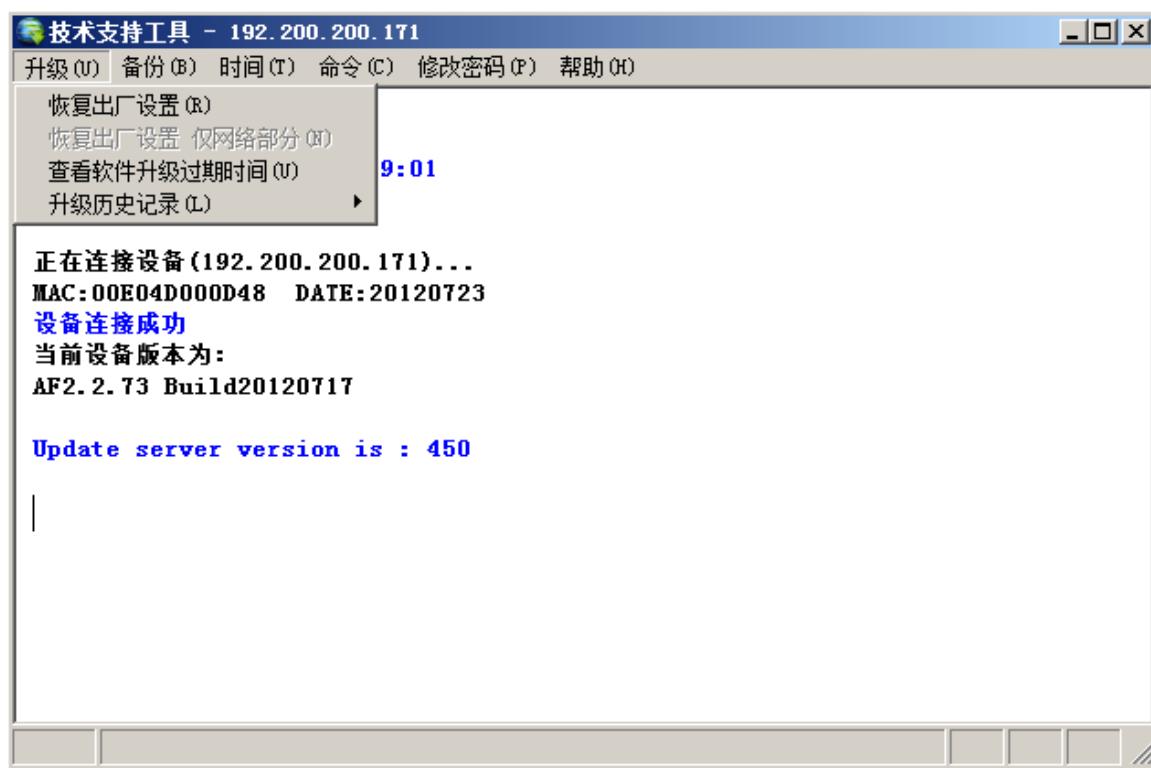
需升级请联系深信服科技客户服务部。

### 启动技术支持工具：

SANGFOR 设备升级系统连接到 SANGFOR 设备后，可以按 F10 或 Ctrl+Shift+F10 启动技术支持工具。技术支持工具有『升级』、『备份』、『时间』、『命令』、『修改密码』和『说明』几个菜单，下面分别介绍它们的功能。



『升级』：包括恢复出厂设置，恢复出厂设置仅网络部分，查看软件升级过期时间和升级历史记录。如下图：



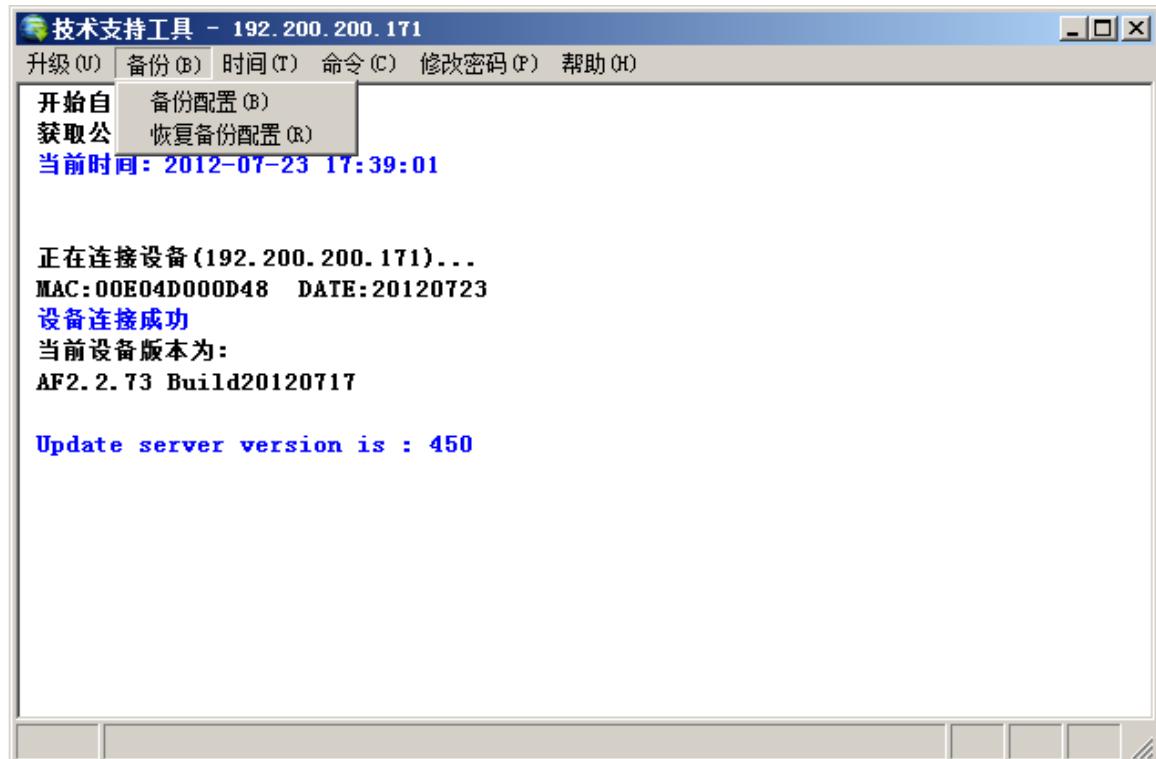
[恢复出厂设置]: 用于将 SANGFOR 硬件设备恢复到默认配置，需要通过加载升级包将设备恢复出厂设置。

[恢复出厂设置仅网络部分]: 只能在没有连接到设备时才能使用。会将设备的网络配置恢复到默认出厂配置，此操作是通过广播包发送命令进行操作的，会对局域网内的所有 SANGFOR 硬件网关生效，有一定危险性，请勿擅自点击操作。

[查看软件升级过期时间]: 检测当前网关是否处于升级服务有效期内。若不在升级服务有效期内，则不能升级，需要购买相应授权才能升级。

[升级历史记录]: 用于查看当前设备的以往升级历史，或者查看或清除本地的历史升级记录。

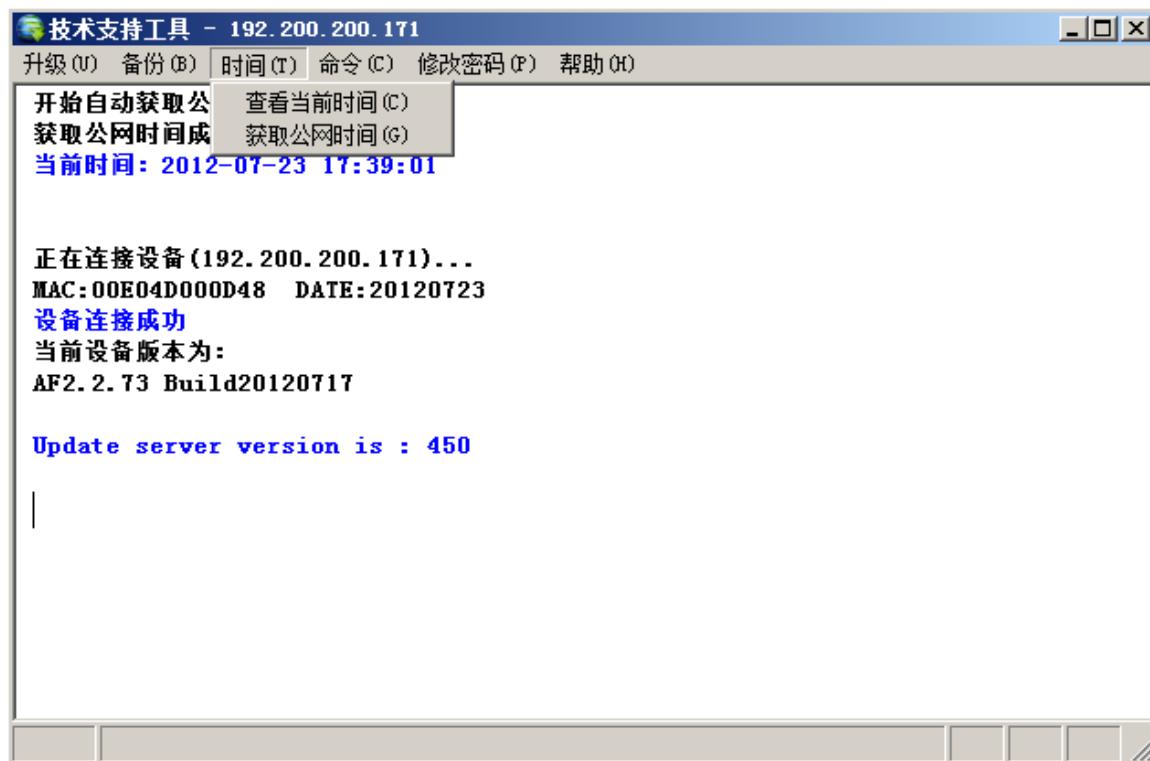
『备份』：包括备份配置、恢复备份配置选项，如下图：



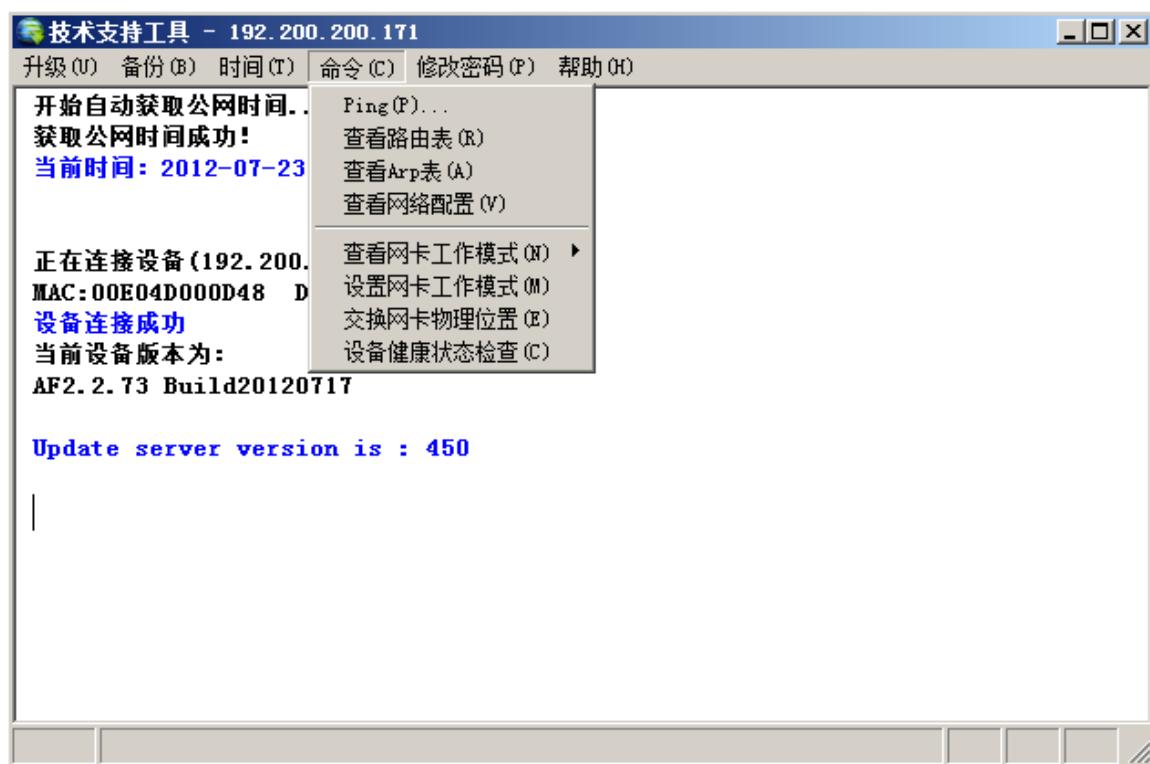
[备份配置]: 将设备现有的配置信息进行备份。

[恢复备份配置]: 将以前备份过的配置信息恢复到设备中。

『时间』用来查看当前时间和同步公网时间，来效验设备升级授权是否过期。



『命令』：包括 Ping、查看路由表、查看 Arp 表、查看网络配置、查看网卡工作模式、设置网卡工作模式、交换网卡物理位置以及设备健康状态检查选项。如下图：



[Ping]: 登录设备后，从设备往外网 ping，以验证设备是否和外网连通。

[查看路由表]: 查看设备本机的路由表。

[查看 Arp 表]: 查看设备本机的 ARP 表。

[查看网络配置]: 查看设备本机的网络配置，包括接口 IP 配置等。

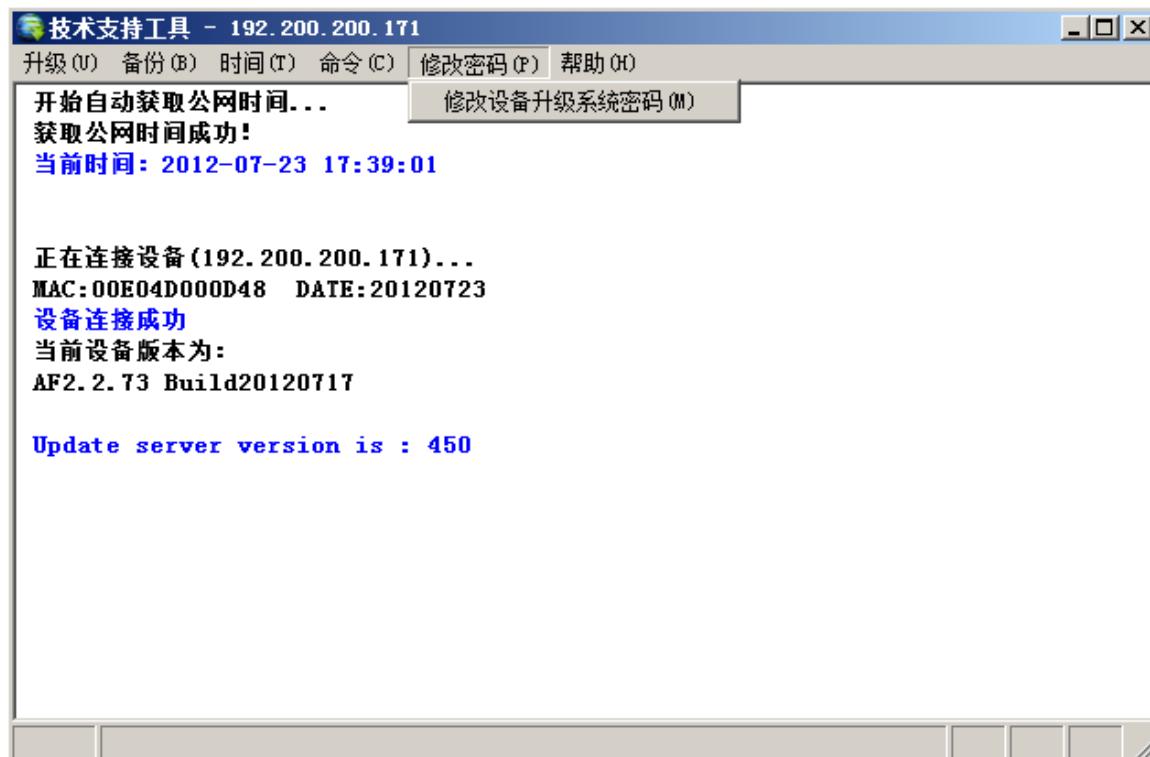
[查看网卡工作模式]: 查看设备各网卡的工作模式。

[设置网卡工作模式]: 设置指定网卡的工作模式。

[交换网卡物理位置]: 用于交换网卡的物理位置。

[设备健康状态检查]: 通过在线检测或者是上传脚本来检测设备的硬件状态。

『修改密码』：用于修改 SANGFOR 设备升级系统密码。



『说明』包括公网首页的链接，技术支持论坛的链接和查看当前 Updater 的版本信息。





## 1、跨版本升级时，按要求升级前置包