深信服下一代防火墙 AF

用户手册

产品版本	8.0.85
文档版本	05
发布日期	2023-05-26

深信服科技股份有限公司

版权声明

版权所有 © 深信服科技股份有限公司 2023。 保留一切权利（包括但不限于修订、最终解释权）。

除非深信服科技股份有限公司（以下简称“深信服公司”）另行声明或授权，否则本文件及本文件的相关内容所包含或涉及的文字、图像、图片、照片、音频、视频、图表、色彩、版面设计等的所有知识产权（包括但不限于版权、商标权、专利权、商业秘密等）及相关权利，均归深信服公司或其关联公司所有。未经深信服公司书面许可，任何人不得擅自对本文件及其内容进行使用（包括但不限于复制、转载、摘编、修改、或以其他方式展示、传播等）。

特别提示

您购买的产品、服务或特性等应受深信服科技股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，深信服科技股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新，如有变更，恕不另行通知。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保，深信服科技股份有限公司不对本文档中的遗漏、变更及错误所导致的损失和损害承担任何责任。

联系我们

售前咨询热线：400-806-6868

售后服务热线：400-630-6430 （中国大陆）

您也可以访问深信服科技官方网站：www.sangfor.com.cn获得最新技术和产品信息

7*24小时智能客服，排障咨询好帮手：

https://bbs.sangfor.com.cn/plugin.php?id=common_plug:online&ref=文档

打开微信扫一扫
可在手机端咨询

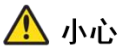
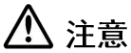
修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

日期	文档版本	修改内容
2022-02-22	01	文档第一次发布
2022-04-22	02	新增虚拟系统和 Sangforvpn 组网场景内容
2022-09-06	03	修改为 69 版本
2022-12-26	04	增加云蜜罐，修改页面变化
2023-05-26	05	增加物联网安全、云安全访问服务、智能运营、TOPN、SLB 服务器池、包回放工具等，修改页面变化

符号说明

在本文中可能出现下列标志，它们所代表的含义如下。

图形	文字	使用原则
	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。
	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。
	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
	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。。
	说明	对操作内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

文字描述	代替符号	举例
窗口名、菜单名等	方括号“[ ]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号“< >”	单击<确定>按钮。

目录

1. 产品概述

1.1. 产品简介

深信服下一代防火墙AF被赋予了风险预知、深度安全防护、检测响应的能力，最终形成了全程保护、全程可视的融合安全体系。

融合不是单纯的功能叠加，而是依照业务开展过程中会遇到的各类风险而提供的对应安全技术手段的融合，能够为业务提供全流程的保护，融合安全包括从事前的资产风险发现、策略有效性检测，到事中所应具备的各类安全防御手段以及事后的持续检测和快速响应机制，并将这一过程中所有的相关信息通过多种方式呈现给用户。

1.2. 产品关键特性

一、 事前预知：资产/脆弱性/策略有效性

深信服下一代防火墙AF能够在事前对内部的服务器进行自动识别开放端口、是否存在的漏洞、弱密码等风险，同时还能判断识别出的资产是否有对应的安全防护策略生效。

二、 事中防御：完整的防御体系+安全联动+威胁情报

深信服下一代防火墙AF在事中防御层面融合了多种安全技术，提供了L2-L7完整的安全防御体系，确保安全防护不存在短板，同时还能通过安全联动功能加强防御体系的时效性和有效性，包括和云端、终端的联动、各个模块间的联动等。此外，深信服下一代防火墙AF还广泛的开展第三方安全机构合作，与国家漏洞信息库、VirusTotal、恶意链接库等多来源威胁情报的输入，帮助用户能够在安全事件爆发之前就提前做好防御的准备。

三、 事后检测&响应：威胁行为的持续检测&快速响应

传统安全建设主要集中在边界安全防御，缺乏对绕过安全防御措施后的检测及响应能力，如果能做好事后的检测及响应措施，可以极大程度降低安全事件产生的影响。深信服下一代防火墙AF融合了事后检测及快速响应技术，即使在黑客入侵之后，也能够帮助用户及时发现入侵后的恶意行为，如检测僵尸主机发起的恶意行为，网页篡改，网站黑链植入及网站Webshell后门检测等，并快速推送告警事件，协助用户进行响应处置。

2. 安装部署

本节主要写作安装前的准备工作，包括准备工具、环境、软硬件材料等。

2.1. 安装前准备

2.1.1. 环境要求

深信服下一代防火墙AF可在以下环境下使用，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，保证使用环境有防尘措施、空气通畅、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。

表1 AF环境说明

参数	规范要求
电压	110V~230V
温度	0～45℃
湿度	5～90%
电源	交流 110V 到 230V 电源，接通电源之前，请保证您的电源有良好的接地措施。

2.1.2. 产品外观

深信服下一代防火墙AF前面板（以AF-2000-FA2150A为例）。

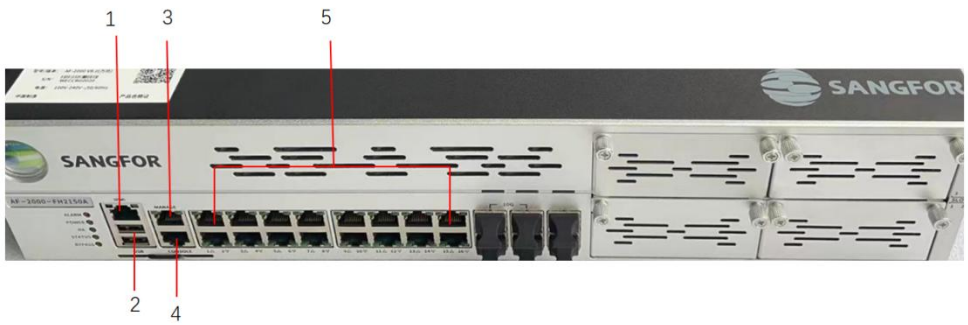


表2 AF-2000-FH2150A网口对照表

设备名称	序号（正面）	说明
AF-2000-FH2150A	1	IPMI 口
	2	USB 口（2 个）
	3	带外管理接口（ETH0）
	4	console 口
	5	ETH1-16

深信服下一代防火墙AF背面板（以AF-2000-FH2150A为例）。

表3 AF-2000-FH2150A背面对照表

设备名称	序号（背面）	说明
AF-2000-FH2150A	1	电源开关
	2	电源口
	3	电源口

注意事项：

1. 告警灯在设备启动期间是红灯长亮的。通常一两分钟后红灯熄灭，说明正常启动。如红灯长时间不灭，请关闭设备等待5分钟后重新开机。
2. 如果还是长亮，请联系深信服科技客服确认是否设备损坏。正常启动后，有时红灯会闪烁，属于正常现象，红灯闪烁表示设备正在写系统日志。
3. console仅供开发和测试调试使用。最终用户需从网口通过控制台接入。

2.1.3. 配置与管理

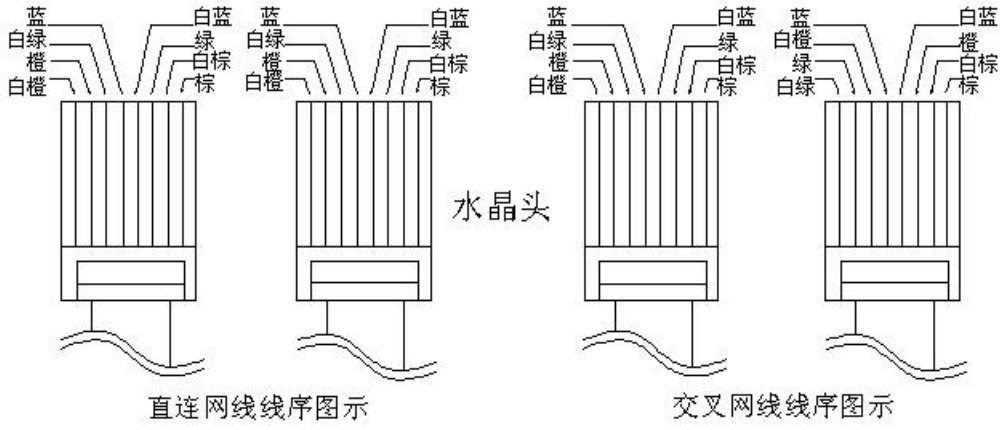
在配置设备之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用（如Internet Explorer、谷歌、火狐等主流的浏览器），然后把电脑与深信服下一代防火墙AF连接在同一个局域网内，通过网络对设备进行配置。

2.1.4. 单设备接线方式

- 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 ETH0 口与管理终端连接，对 AF 设备进行配置。
- 请用标准的 RJ-45 以太网线将 ETH2 口与 Internet 接入设备相连接，如路由器、光纤收发器或 ADSL Modem 等。

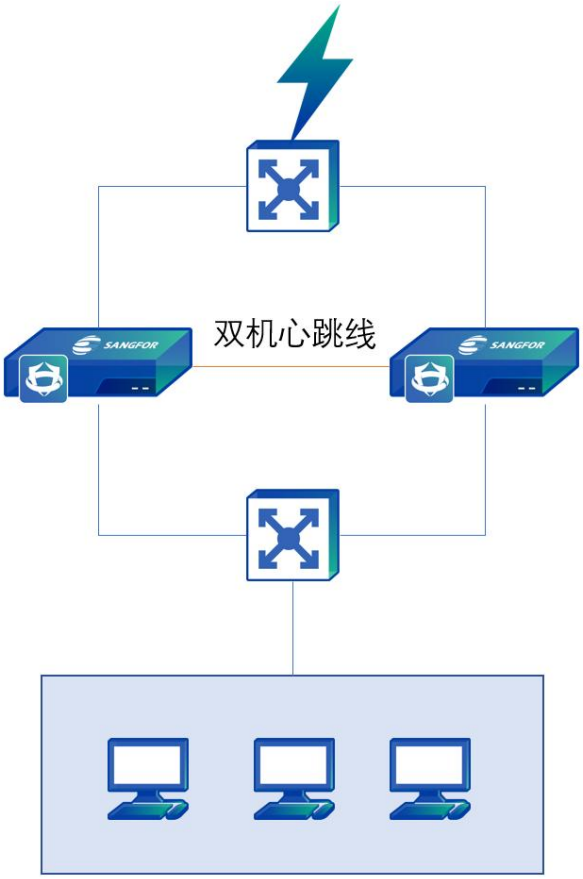
注意事项

1. 多线路的AF设备可以支持多条Internet线路，此时将ETH2口与第二条Internet接入设备相连，ETH3口与第三条Internet线路相连，依此类推。
2. 使用标准RJ-45以太网线将DMZ口与DMZ区的网络连接，一般而言，DMZ区放置对外提供服务的Web服务器、EMAIL服务器等。AF设备可以为这些服务器提供安全保护。
3. 设备正常工作时POWER灯常亮，WAN口和LAN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。
4. WAN口直接连接MODEM应使用直连线、连接路由器应使用交叉线；LAN口连接交换机应使用直连线、直接连接电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线顺序不同，如下图。



2.1.5. 双机备份接线方式

若采用AF双机热备的工作方式，按以下接线方式进行外网线路和内网线路的接线。



使用标准RJ-45以太网线将两台AF设备的ETH2（或其他可用接口）口（若使用多线路技术，接线方式类似，保证两台设备的外网接口接到同一个外网线路即可）接到同一交换机上，再使用标准的RJ-45以太网线与Internet接入设备相连接，如路由器、光纤收发器或ADSL Modem等。

- 选一个空闲网口作为 HA 口，将两台 AF 设备的 HA 口用网线连接起来。
- 使用标准 RJ-45 以太网线将两台 AF 设备的 ETH1（或其他可用接口）口接到同一交换机上，再使用标准的 RJ-45 以太网线与局域网交换机相连，连接到内部局域网。
- 接线完毕后，分别打开两台设备的电源，即可进行系统配置。双机系统配置时和单机系统配置一样，仅对一台主设备进行配置，另外一台从设备将自动进行同步，无需另行配置。

2.1.6. Web 控制台登录介绍

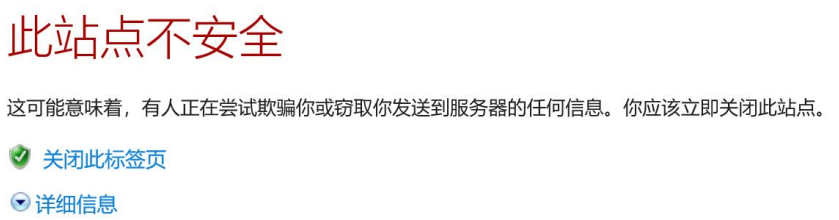
下一代防火墙AF支持安全的HTTPS登录，是使用HTTPS协议的标准端口登录，为了防止配置过程中被截获而产生安全隐患。

下一代防火墙AF设备，eht0网口作为带外管理口默认的出厂IP为： eth0：10.251.251.251/24。

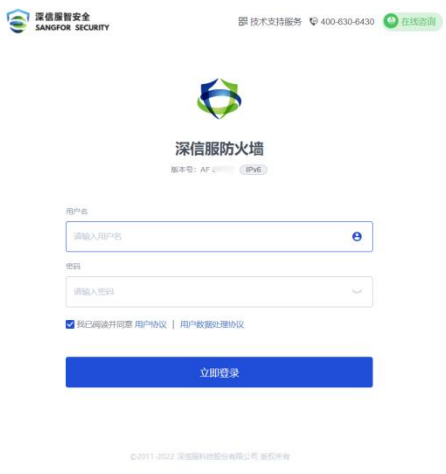
如果电脑连接的是设备的eth0口， 需要先在电脑上配置一个10.251.251.0/24网段的地址，打开浏览器输入https://10.251.251.251 登录设备网关控制台。

操作步骤

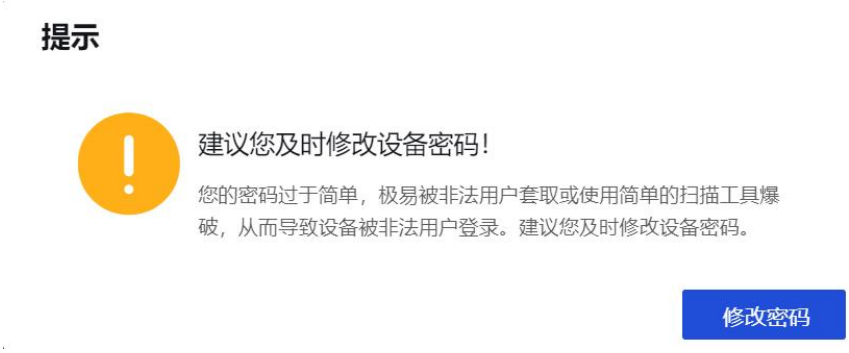
步骤1.首先为本机器配置一个10.251.251.X网段的IP（如配置10.251.251.100），然后在IE浏览器中输入网址：https://10.251.251.251。出现一个如下图的安全提示，点击<详细信息>再点击<转到此网页>会跳转到控制台登录页面。



步骤2.在登录框输入用户名和密码，默认情况下用户名和密码均为：admin。阅读《用户协议&隐私政策》（若对次协议有疑问，请联系“深信服”沟通），勾选我已阅读并同意，点击<登录>按钮即可登录AF设备进行配置。



步骤3.当用户密码过于简单，则会被检测为弱密码，控制台会处理：登录后检查为弱密码，则会弹出以下提示。



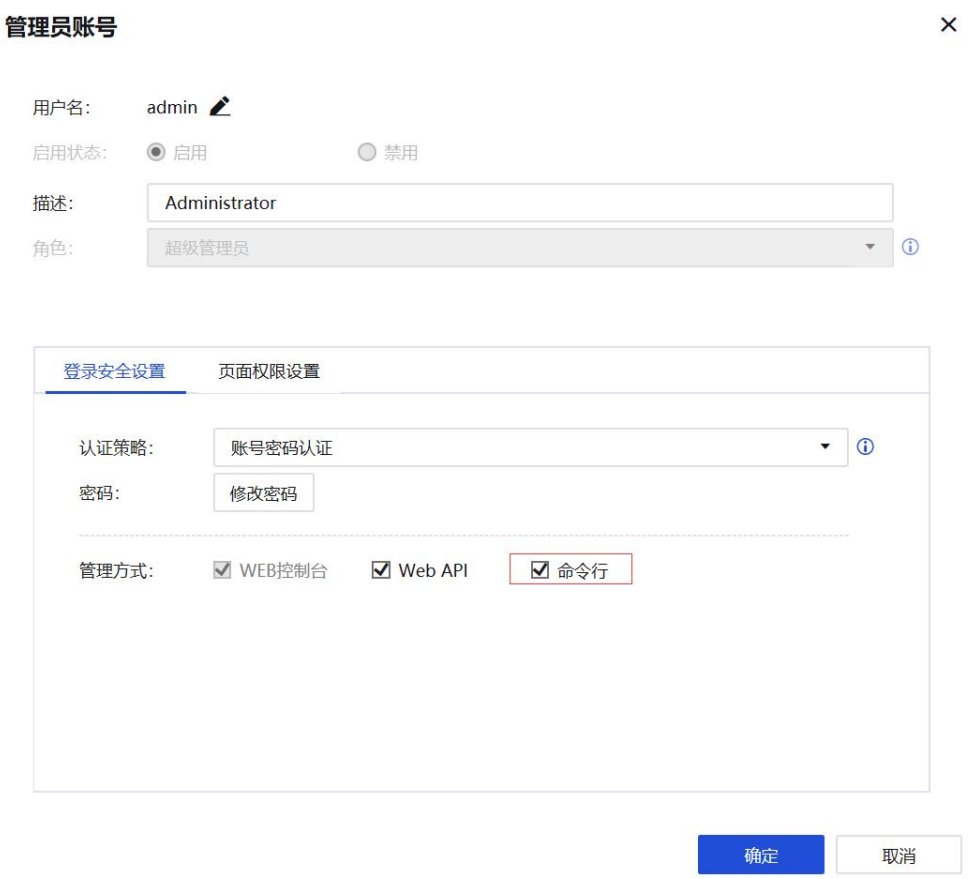
步骤4.点击[修改密码]后进入修改密码页面，进行密码的修改。

2.1.7. 命令行登录介绍

下一代防火墙AF同时也支持安全的SSH登录，登录成功后可以通过命令行模式来进行设备管理。

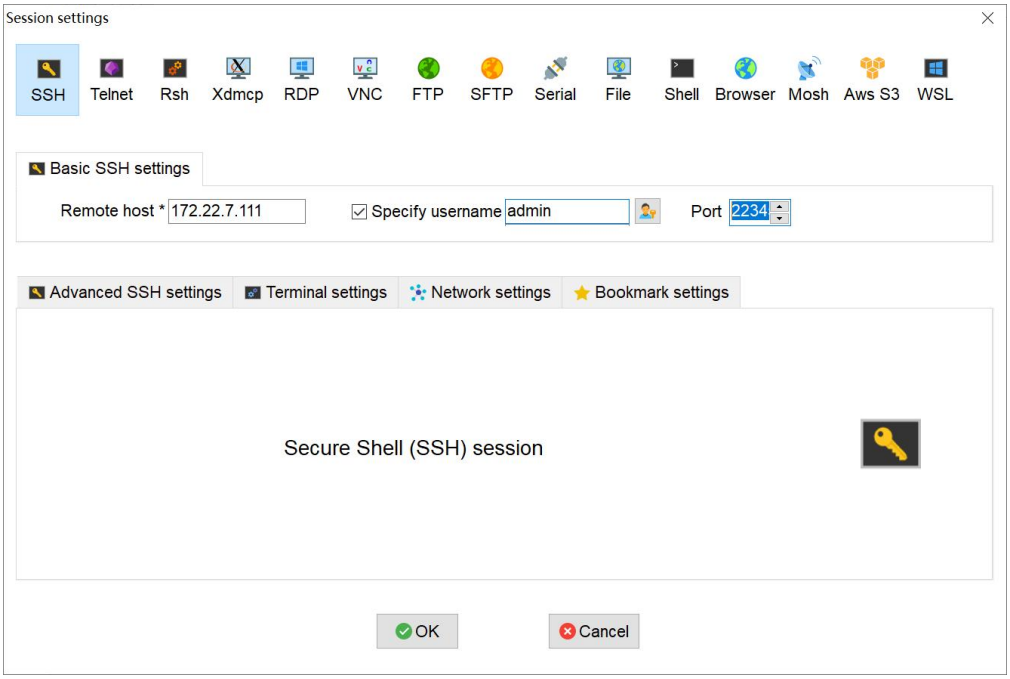
操作步骤

步骤1.通过Web控制台进入[系统/管理员账号]选择需要进行命令行管理的账号，勾选上<命令行>权限。

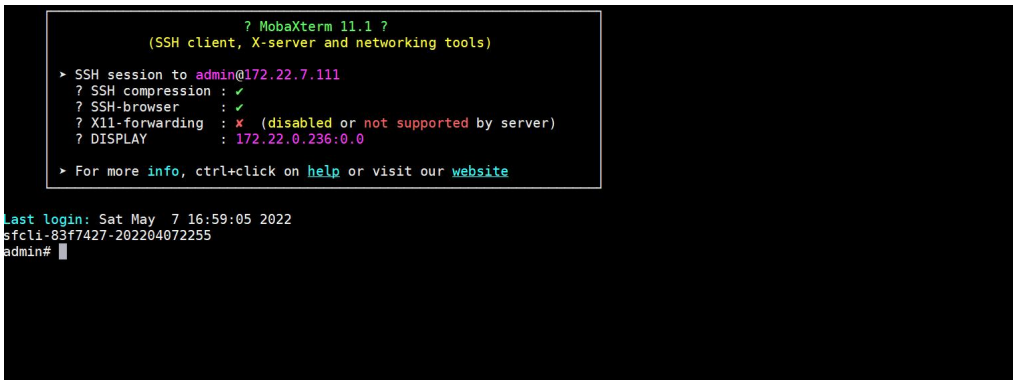


步骤2.在[网络/接口]里选择需要命令行管理接入的网络接口开启<SSH>功能。

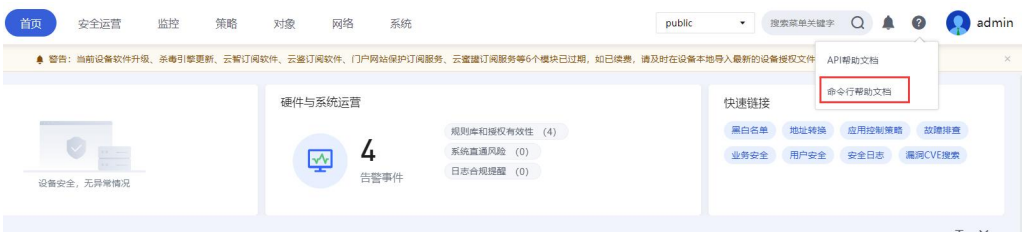
步骤3.使用SSH管理工具连接22345端口，输入对应管理员账号密码进行登录。



步骤4.登录成功后进入命令行模式，如下图所示。



命令行管理模式具体支持的命令参数本手册不做介绍，可以参考控制台的命令行帮助文档，如图所示。



2.2. 部署模式

部署模式是用于设置设备的工作模式，可把设备设定为路由模式、透明模式、虚拟网线模式、旁路模式和混合模式。选择一个合适的部署模式，顺利将设备架到网络中并

且使其能正常使用的基础。

表4 部署模式说明表

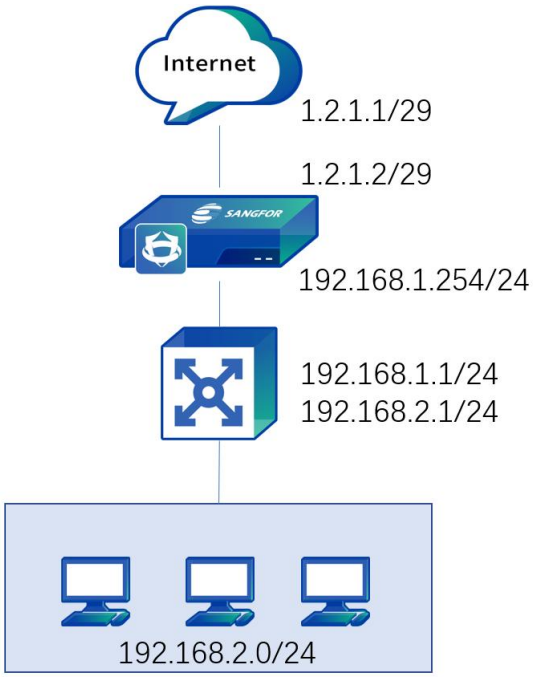
部署模式	场景说明
路由模式	设备可以作为一个路由设备使用，对网络改动最大，但可以实现设备的所有的功能。
透明模式	可以把设备视为一条带过滤功能的网线使用，一般在不方便更改原有网络拓扑结构的情况下启用，平滑架到网络中，可以实现设备的大部分功能。
虚拟网线模式	是透明部署中另外一种特殊情况，无需检查 MAC 表，直接从虚拟网线配对的接口转发，且虚拟网线转发效率高于透明模式。
旁路模式	设备连接在内网交换机的镜像口或 HUB 上，镜像内网用户的数据，通过镜像的数据实现对流量进行检测。可以完全不需改变用户的网络环境，并且可以避免设备对用户网络造成中断的风险，但这种模式下设备只对流量进行检测，无法对恶意流量进行阻断。
混合模式	主要指设备的各个网口，既有 2 层口，又有 3 层口的情况，特别是当 DMZ 区域服务器集群需要配置公网 IP 地址的时候。

2.2.1. 路由模式

路由部署的典型应用环境是将AF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。外网口接ADSL拨号或者公网线路，内网口接内网交换机。

路由模式配置案例

某企业网络是跨三层的环境，打算把AF设备部署在公网出口，代理内网用户上网，公网线路是光纤接入固定分配IP的，如下图所示。



步骤1.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。

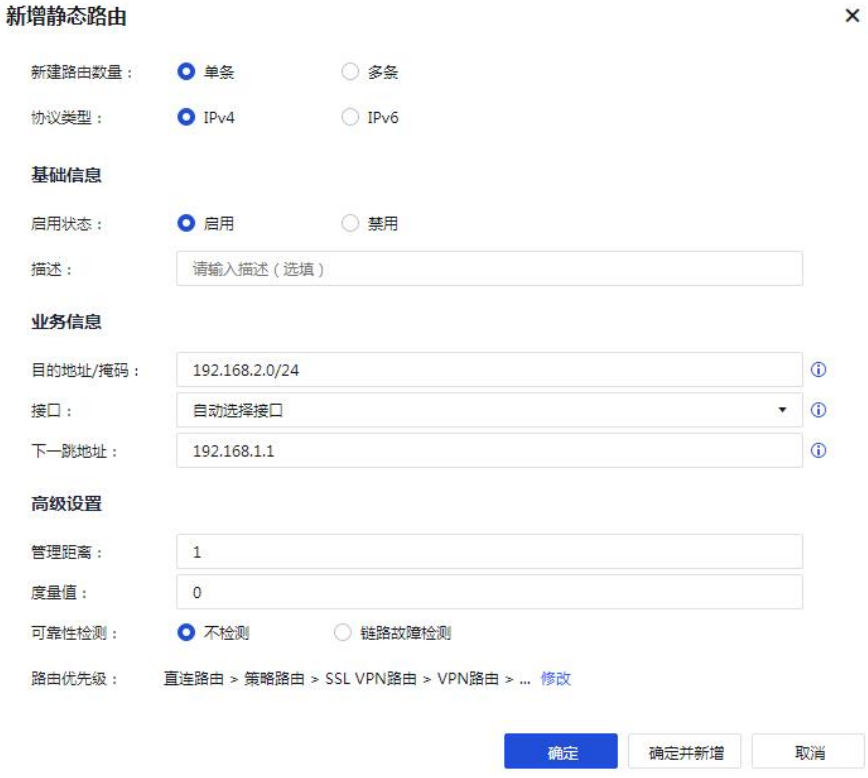
步骤2.配置外网接口，通过[网络/接口/区域]，点击需要设置成外网接口的接口，选择eth2作为外网接口，选择路由类型，区域选择自定义的外网区，勾选WAN口属性，配置IP 1.2.1.2/29，下一跳地址 1.2.1.1等。如下图所示。

⚠ 注意：

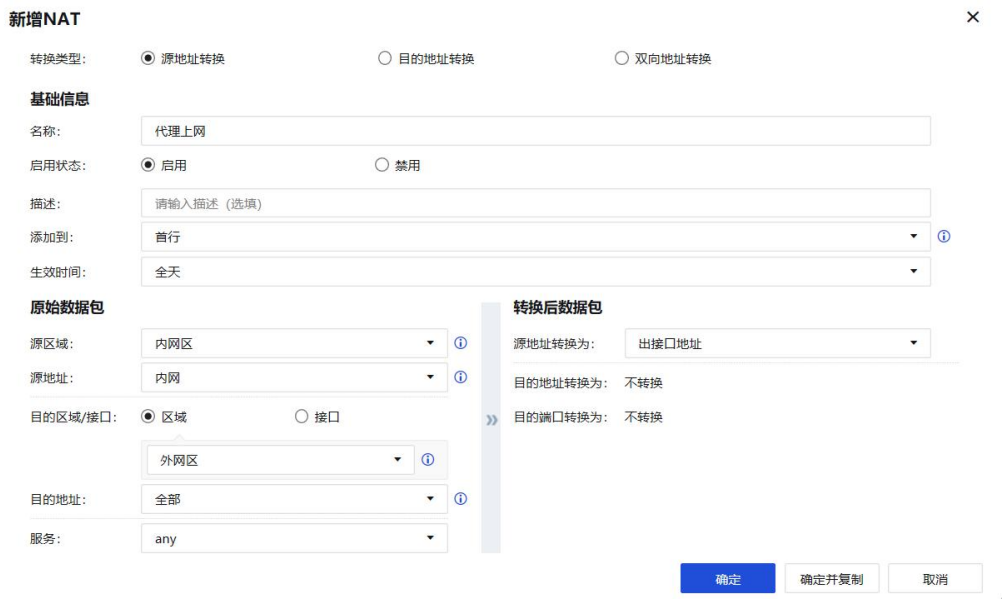
1. 非带外管理接口的下一跳网关仅用于接口的链路检测和策略路由功能，设置了下一跳网关，不会在设备上产生 0.0.0.0/0 的缺省路由，需要手动设置默认路由。
2. 接口的线路带宽设置与流量管理的带宽设置没有关联，接口处的线路带宽设置用于策略路由的调度，不可设置为 0。

步骤3.配置内网接口。选择空闲网口、点击接口名称进入配置页面，选择eth3作为内网接口，选择路由类型，区域选择自定义的内网区，配置IP 192.168.1.254/24，如下图所示。

步骤4.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，还需要配置另一条添加各网段的静态路由到三层交换机，进入[网络/路由/静态路由]进行配置，点击<新增>静态路由，配置默认路由目的地址/掩码为 0.0.0.0/0，下一跳地址 1.2.1.1，回包路由（内网网段路由）目的地址/掩码为192.168.2.0/24，下一跳地址192.168.1.1。如下图所示。



步骤5.配置代理内网，进入[策略/地址转换/IPv4地址转换]，点击<新增>，配置源地址转换，源区域选择自定义的内网区，源地址选择自定义的内网，目的区域选择自定义的外网区，目的地址为全部，服务为any，源地址转换为出接口地址。如下图所示。



步骤6.配置应用控制策略，放通内网用户上网权限，进入[策略/访问控制/应用控制策略]，点击<新增>，放通内到外的数据访问权限，源区域选择自定义的内网区，源地址选择自定义的内网，目的区域选择自定义的外网区，目的地址为全部，服务为any，应用为全部。如下图所示。

步骤7.基本配置完毕后，将设备接入网络中，eth2口连接光纤，eth3口接内网三层交换机。

⚠ 注意：

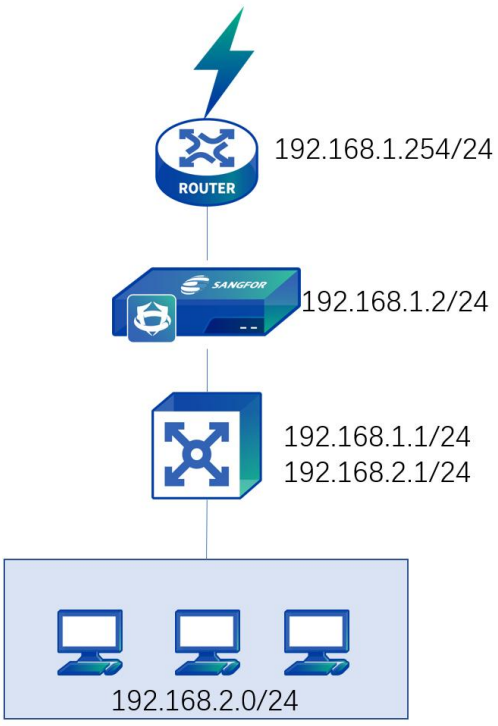
1. 设备工作在路由模式时，局域网内计算机的网关都是指向设备内网接口 IP 或指向三层交换机，三层交换机的网关再指向设备。上网数据由设备做 NAT 或路由转发出去。
2. 当设备有多个路由接口时，多个路由接口可以设置同网段的 IP 地址，通过静态路由决定数据从哪个网口转发。
3. 设备支持配置多个 WAN 口属性的路由接口连接多条外网线路，但是需要开通多条线路的授权。

2.2.2. 透明模式

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。

Access口透明模式部署案例

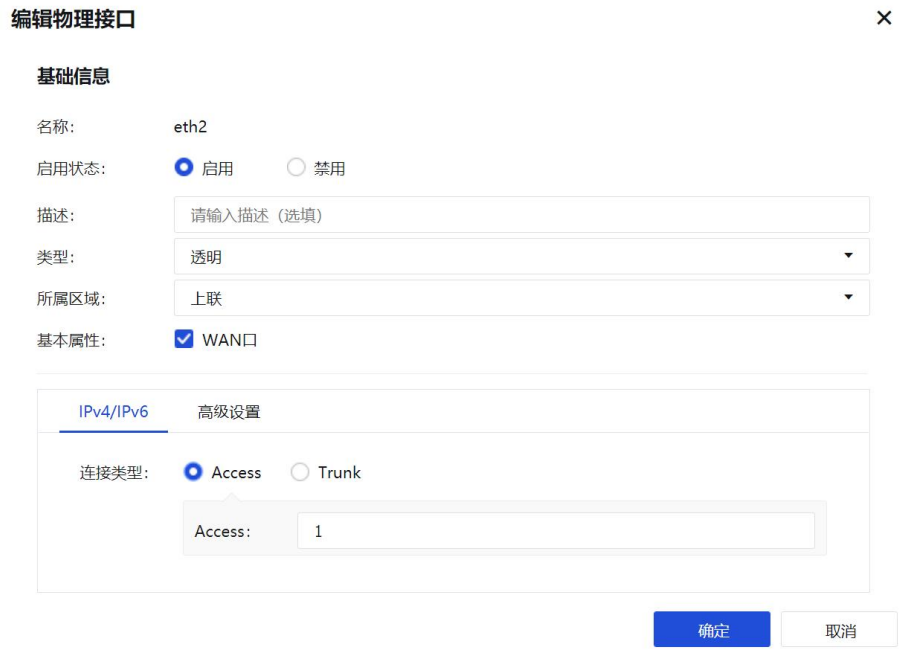
某企业网络是跨三层的环境，有路由器部署在公网出口，不能改动原有环境，需要将AF设备透明部署进网络中，如下图所示。



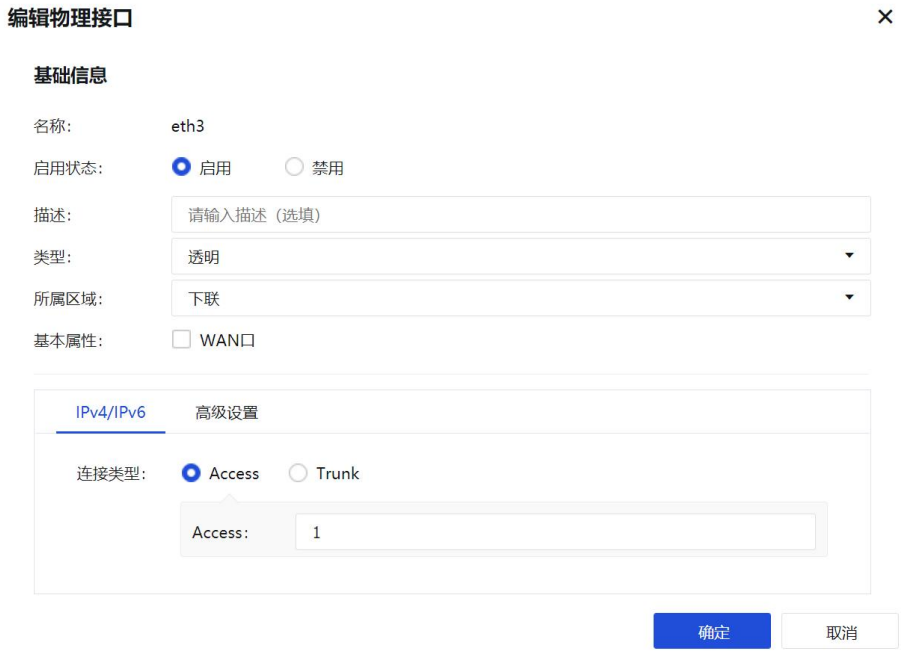
步骤1.通过管理口(ETH0)的默认IP登录设备。管理口的默认IP是10.251.251.251/24，在计算机上配置一个相同网段的IP地址，通过

https://10.251.251.251登录设备。

步骤2.在[网络/接口/物理接口]中，点击需要设置成外网接口的接口，选择eth2作为上联外网接口，选择透明类型，区域选择自定义的上联区，勾选WAN口属性，连接类型为Access 1，如下图所示。



步骤3.在[网络/接口/物理接口]中，点击需要设置成内网接口的接口，选择eth3作为下联内网接口，选择透明类型，区域选择自定义的下联区，连接类型为Access 1，如下图所示。



步骤4.配置管理接口，在[网络/接口/VLAN接口]中，配置VLAN接口的逻辑接口作为管理接口，VLAN ID为1，并分配管理地址192.168.1.2/24。如下图所示。

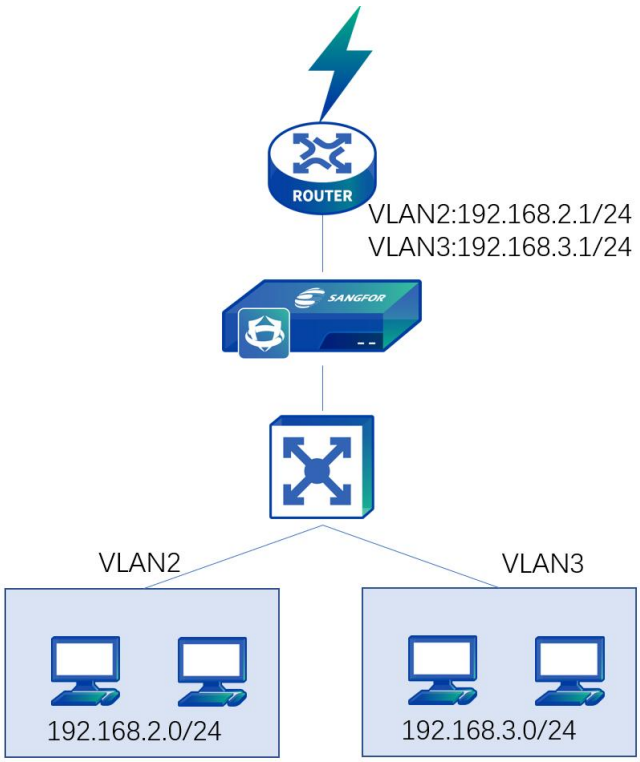
步骤5.配置路由，需要配置一条到0.0.0.0/0.0.0.0的默认路由指向前置网关192.168.1.254；同时因为本例内网接口接的跨三层的多个网段，还需要配置另一条添加各网段的静态路由到三层交换机，进入[网络/路由/静态路由]进行配置，点击<新增>静态路由，配置默认路由目的地址/掩码为 0.0.0.0/0，下一跳地址192.168.1.254，回包路由目的地址/掩码为192.168.2.0/24，下一跳地址192.168.1.1。如下图所示。

步骤6.配置应用控制策略。放通内网用户上网权限：在[策略/访问控制/应用控制策略]中，新增应用控制策略，放通内到外的数据访问权限，源区域选择自定义的下联区，源地址选择自定义的内网，目的区域选择自定义的上联区，目的地址为全部，服务为any，应用为全部。

步骤7.基本配置完毕后，将设备接入网络中，eth2口连接前置路由器，eth3口接内网三层交换机。

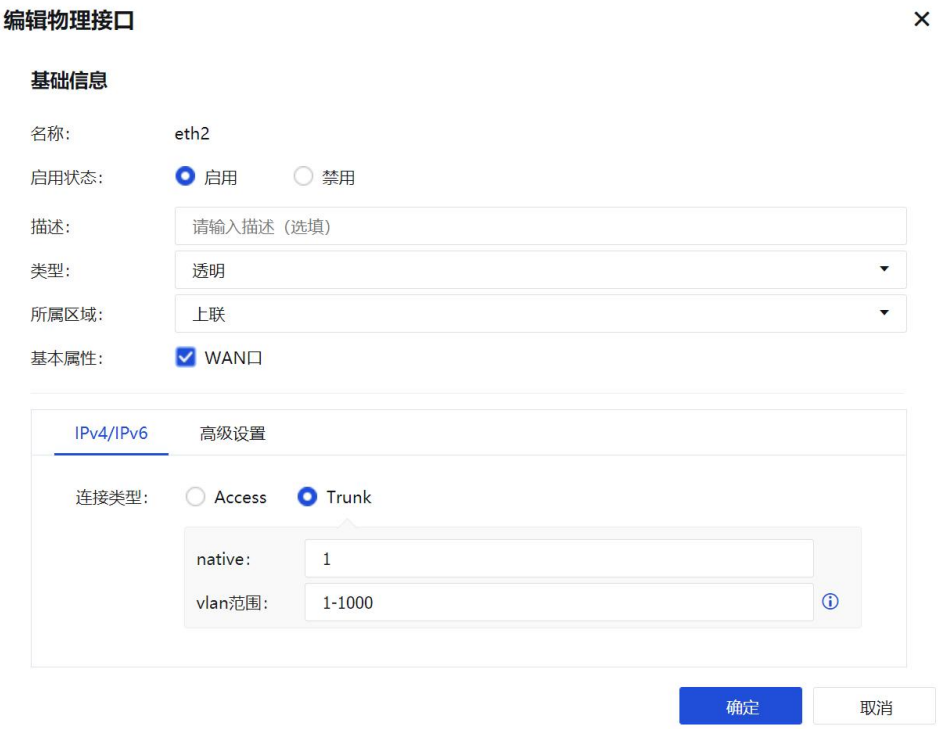
Trunk口透明模式部署案例

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，前置路由器作各个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。

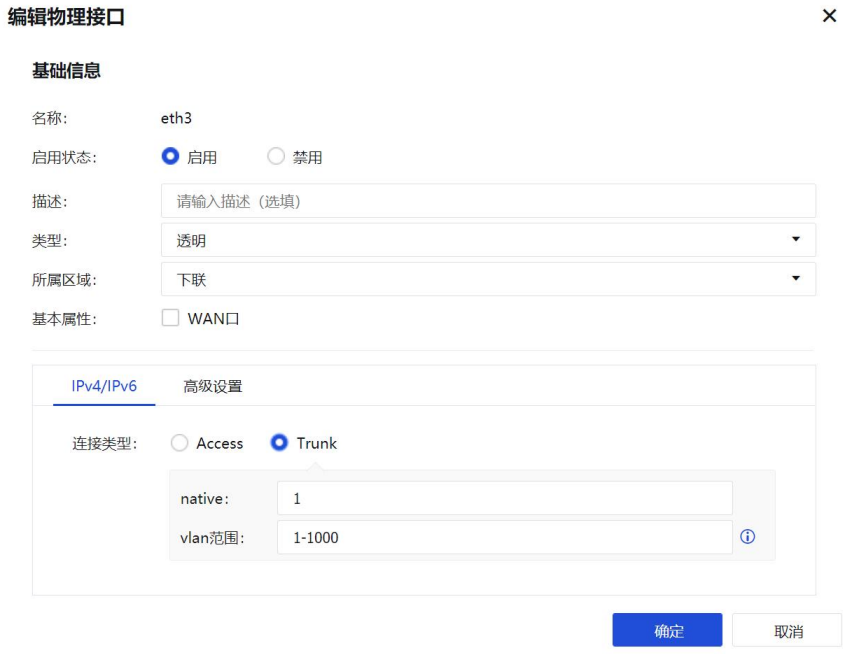


步骤1. 通过管理口(ETH0)的默认IP登录设备。管理口的默认IP是10.251.251.251/24，在计算机上配置一个相同网段的IP地址，通过https://10.251.251.251登录设备。

步骤2. 在[网络/接口/物理接口]中，点击需要设置成外网接口的接口，选择eth2作为上联外网接口，选择透明类型，区域选择自定义的上联区，勾选WAN口属性，连接类型为Trunk，如下图所示。



步骤3. 在[网络/接口/物理接口]中，点击需要设置成内网接口的接口，选择eth3作为下联内网接口，选择透明类型，区域选择自定义的下联区，连接类型为Trunk，如下图所示。



步骤4. 配置管理接口，在[网络/接口/VLAN接口]中，配置VLAN接口的逻辑接口作为管理接口，VLAN ID为2，并分配管理地址192.168.2.2/24。如下图所示。

步骤5. 配置路由，需要配置一条到0.0.0.0/0.0.0.0的默认路由指向和管理IP同网段的前置网关192.168.2.1，进入[网络/路由/静态路由]进行配置，点击<新增>静态路由，配置默认路由目的地址/掩码为 0.0.0.0/0，下一跳地址 192.168.2.1，如下图所示。

步骤6. 配置应用控制策略，放通内网用户上网权限：在[策略/访问控制/应用控制策略]中，新增应用控制策略，放通内到外的数据访问权限，源区域选择自定义的下联区，源地址选择自定义的内网，目的区域选择自定义的上联区，目的地址为全部，服务为any，应用为全部。

步骤7. 基本配置完毕后，将设备接入网络中，eth2口连接前置路由，eth3口接内网二层交换机。

2.2.3. 虚拟网线模式

虚拟网线部署与透明部署类似，是透明部署中另外一种特殊情况，和透明部署区别是：

接口也是二层接口，但是被定义成虚拟网线接口；

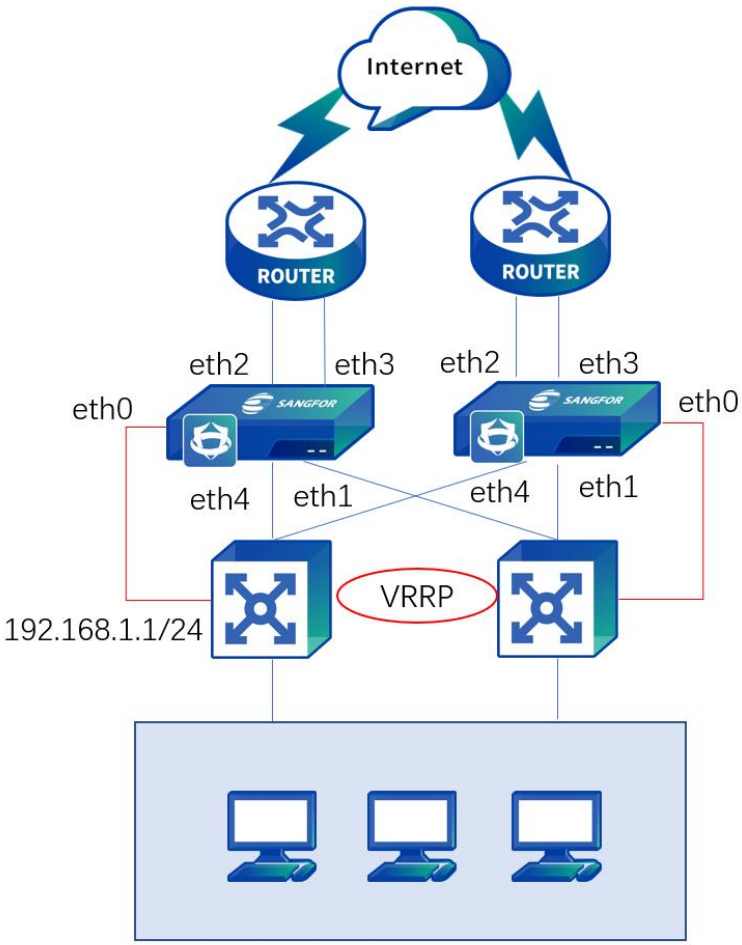
虚拟网络接口必须成对存在，转发数据时，无需检查 MAC 表，直接从虚拟网线配对的接口转发；

虚拟网线接口的转发性能高于透明接口，一般的网桥环境下，推荐使用虚拟网线接口部署；

虚拟网线部署必须通过其他路由口进行外接管理。

虚拟网线模式部署案例

某企业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。



两台AF设备配置方法一样，以其中一台为例讲解配置步骤。

步骤1.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。

步骤2.在[网络/接口/物理接口]中，点击需要设置成外网接口的接口,选择eth2作为上联外网接口，选择虚拟网线类型，区域选择自定义的上联区，如下图所示。

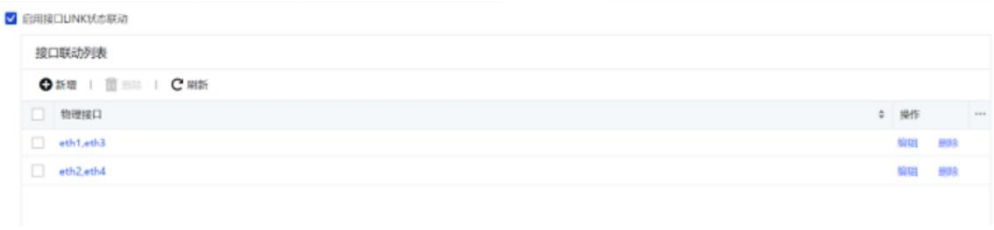
步骤3.在[网络/接口/物理接口]中，点击需要设置成内网接口的接口，选择eth4作为下联内网接口，选择虚拟网线类型，区域选择自定义的下联区，接口选择步骤1定义的eth2，如下图所示。

步骤4.按照步骤2和步骤3的方法配置eth1口和eth3口。

步骤5.配置管理口，在[网络/接口/物理接口]中,选择带外管理口eth0作为管理口，eth0默认IP 10.251.251.251/24 不需要修改，新增一个和内网交换机同网段的

IP192.168.1.2/24作为管理IP，方便内网管理员管理设备，默认网关设置为192.168.1.1，作为管理口本身默认路由。

步骤6.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，在[网络/接口/接口联动]中，勾选[启用接口LINK状态联动]，并选择eth1和eth3，eth2和eth4进行接口联动，如下图所示。



步骤7.配置应用控制策略，放通内网用户上网权限：在[策略/访问控制/应用控制策略]中，新增应用控制策略，放通内到外的数据访问权限，源区域选择自定义的下联区，源地址选择自定义的内网，目的区域选择自定义的上联区，目的地址为全部，服务为any，应用为全部。

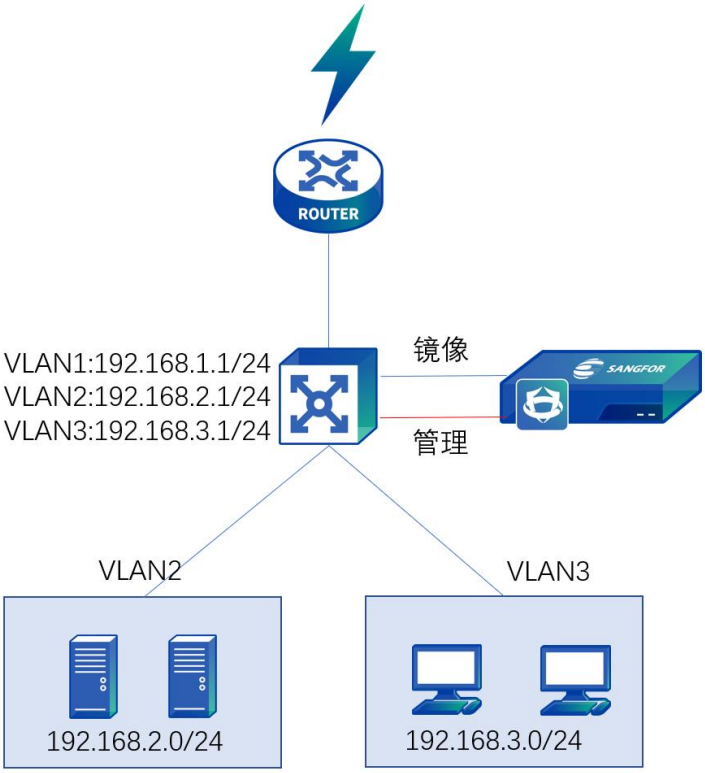
步骤8.基本配置完毕后，将设备接入网络中，eth2和eth3口连接前置路由器，eth4和eth1口分别接内网的两个三层交换机。

2. 2. 4. 旁路模式

旁路模式实现防护功能的同时，可以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。

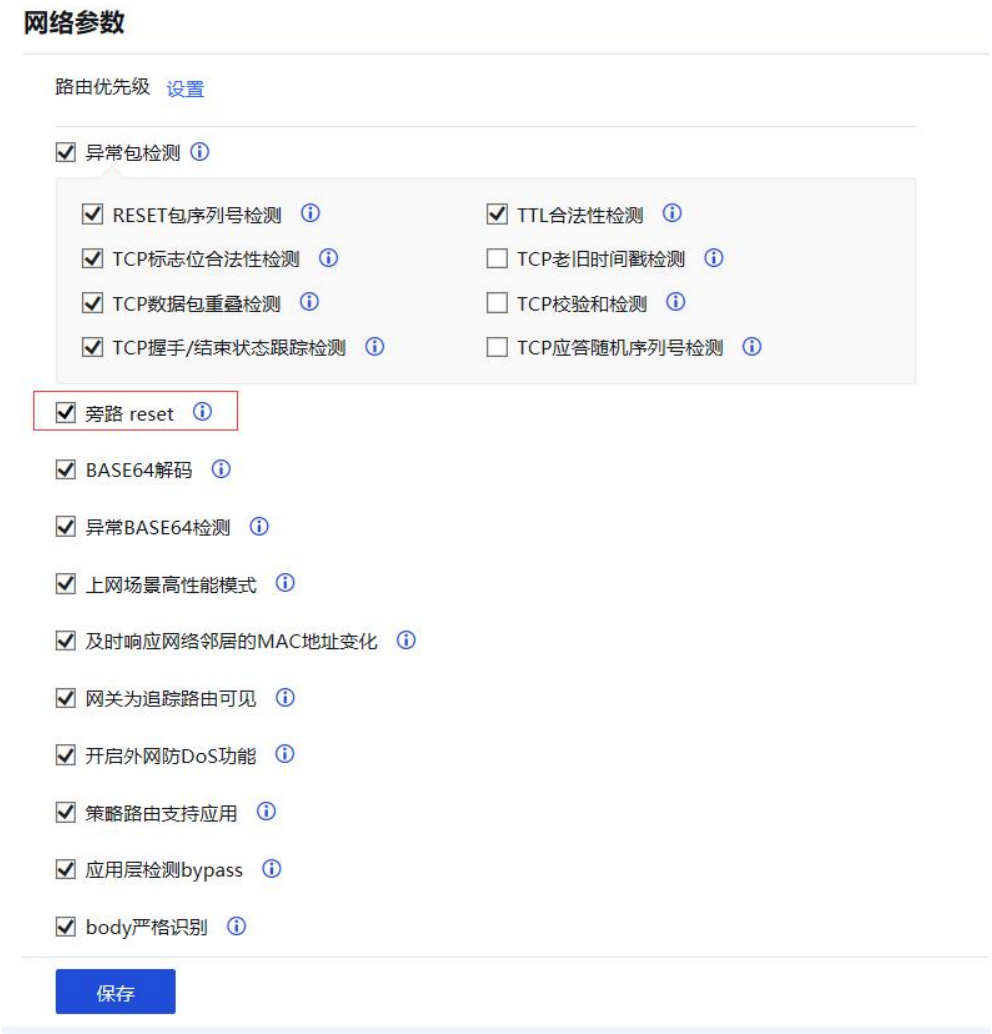
旁路模式部署案例

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192.168.3.0/24，服务器网段为192.168.2.0/24，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。



步骤1.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。

步骤2.在[系统/通用配置/网络参数]中勾选[旁路reset]功能，旁路模式下通过管理口发送TCP RESET报文进行控制。



步骤3.配置管理口，旁路部署时，设备通过管理口来阻断连接。在[网络/接口/物理接口]中,选择带外管理口eth0作为管理口，eth0默认IP 10.251.251.251/24 不需要修改，新增一个和内网交换机同网段的IP192.168.1.2/24作为管理IP，方便内网管理员管理设备，默认网关设置为192.168.1.1，作为管理口本身默认路由，如下图所示。

步骤4.配置旁路镜像口，在[网络/接口/区域/物理接口]，选择eth1作为旁路镜像口，点击eth1，选择旁路镜像类型，区域选择自定义的内网，[旁路流量统计]勾选启用，[网络对象]选择自定的服务器网段，如下图所示。

步骤5.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。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，如下图所示。

步骤6.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VLAN1范围内的接口即可。

⚠ 注意：

旁路部署支持的功能仅有：APT（僵尸网络）、PVS（实时漏洞分析）、WAF（web 应用防护）和漏洞攻击防护，在不需要阻断时不用勾选[旁路 reset]功能。

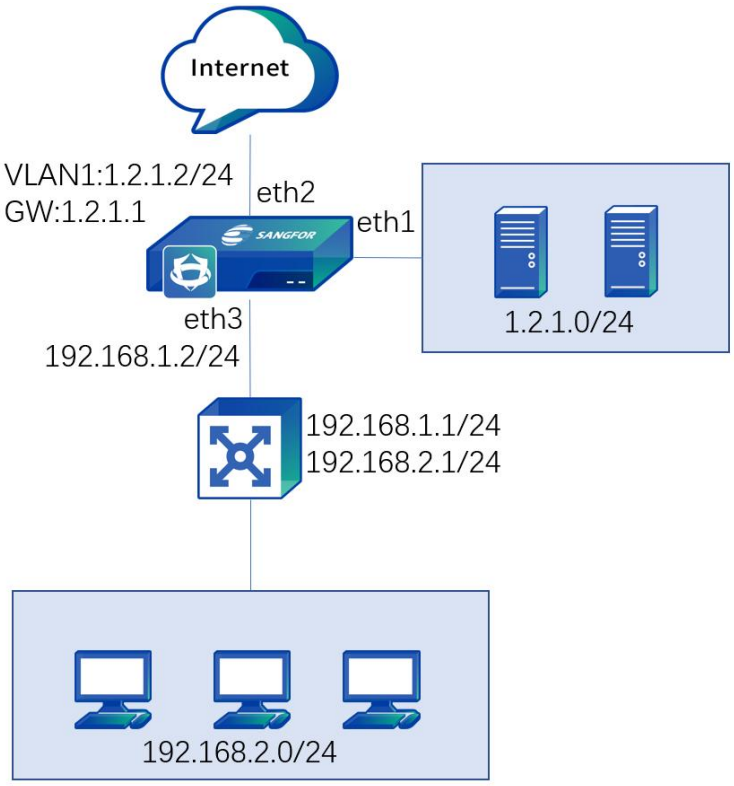
2.2.5. 混合模式

混合部署是指AF设备同时存在路由接口，透明接口或者虚拟网线接口的情况。根据不同的客户需求，可以采用不同的部署方式来实现。

混合模式部署案例

某企业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

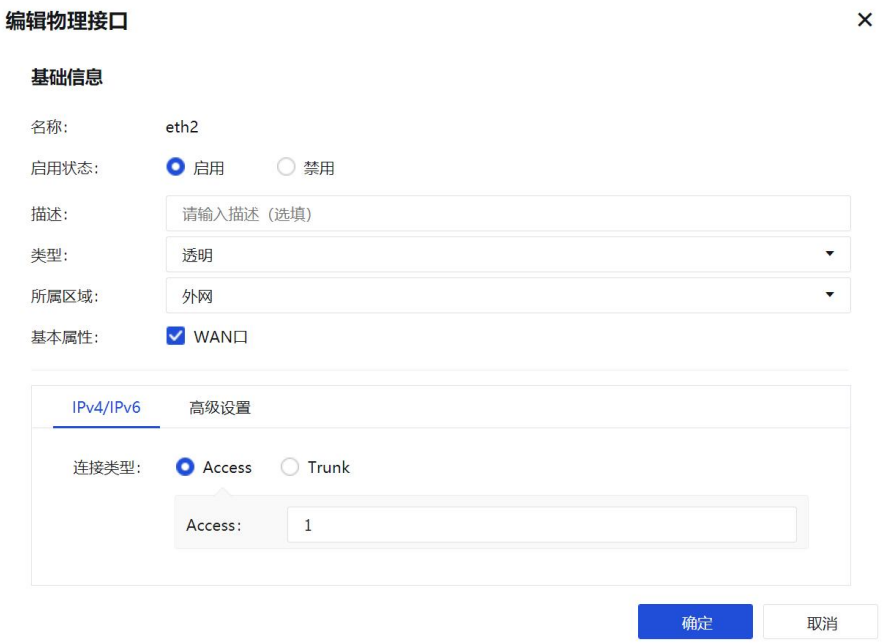
望通过端口映像的方式发布服务器，且能实现AF设备代理内网的内网上公网。用户网络拓扑如下所示。



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eht2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。

步骤1.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。

步骤2.设置外网接口。在[网络/接口/区域/物理接口]中，选择eth2作为外网接口，点击eth2，选择透明类型，区域选择自定义的外网，勾选WAN属性，连接类型为Access 1，如下图所示。

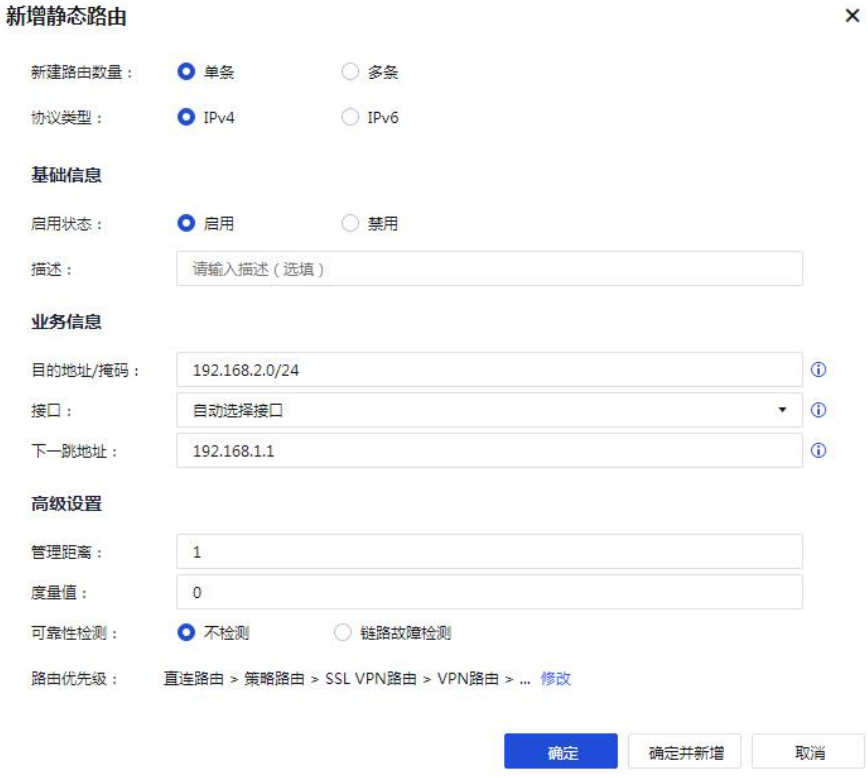


步骤3.设置服务器区接口。在[网络/接口/区域/物理接口]中，选择eth1作为服务器区接口，点击eth1，选择透明类型，区域选择自定义的外网，连接类型为Access 1，如下图所示。

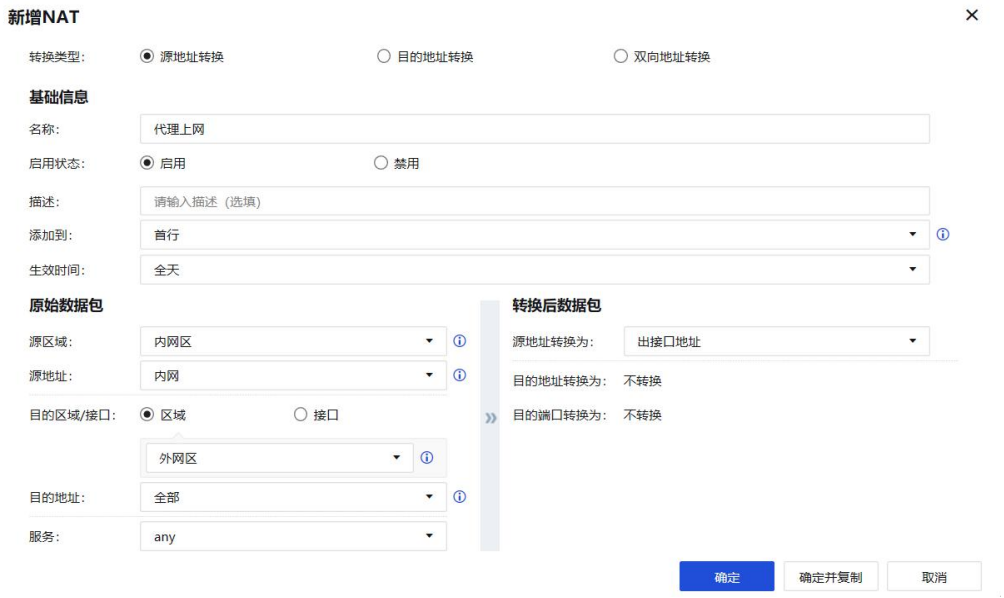
步骤4.设置内网接口。在[网络/接口/区域/物理接口]中，选择eth1作为服务器区接口，点击eth3，选择路由类型，区域选择自定义的内网，并填写IP 192.168.1.2/24，如下图所示。

步骤5.设置VLAN接口。在[网络/接口/区域/VLAN接口]中，点击<新增>，VLAN ID为1，区域为自定义外网，填写IP 1.2.1.2/24，下一跳网关为1.2.1.1，如下图所示。

步骤6.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，进入[网络/路由/静态路由]进行配置，点击<新增>静态路由，配置默认路由目的地址/掩码为 0.0.0.0/0，下一跳地址 1.2.1.1，回包路由目的地址/掩码为192.168.2.0/24，下一跳地址192.168.1.1。如下图所示。



步骤7.配置代理内网，进入[策略/地址转换/IPv4地址转换]，点击<新增>，，配置源地址转换，源区域选择自定义的内网区，源地址选择自定义的内网，目的区域选择自定义的外网区，目的地址为全部，服务为any，源地址转换为出接口地址。如下图所示。



步骤8.配置应用控制策略，放通内网用户上网权限，进入[策略/访问控制/应用控制策略]，点击<新增>，放通内到外的数据访问权限，源区域选择自定义的内网区，源地址选择自定义的内网，目的区域选择外网区，目的地址为全部，服务为any，应用为全部。如下图所示。

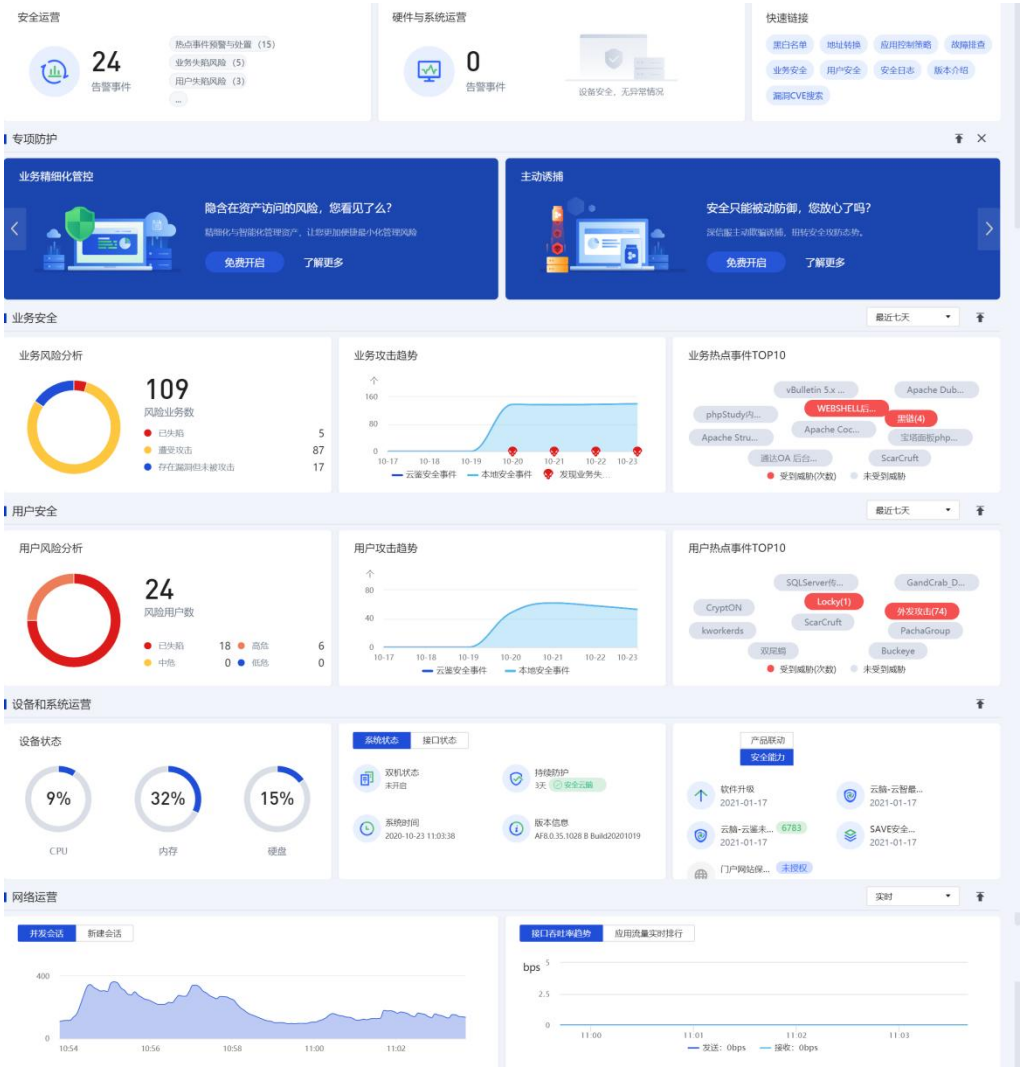
步骤9.配置应用控制策略，放通所有区域访问服务器的服务，源区域选择any，源地址为全部，目的区域选择服务器区，目的地址为自定义的服务器根据实际情况

配置相关的服务，如http。如下图所示。

步骤10.以上步骤设置完毕，则可以将设备接eth2口接外网线路，eth1口接服务器区，eth3口接内网交换机。

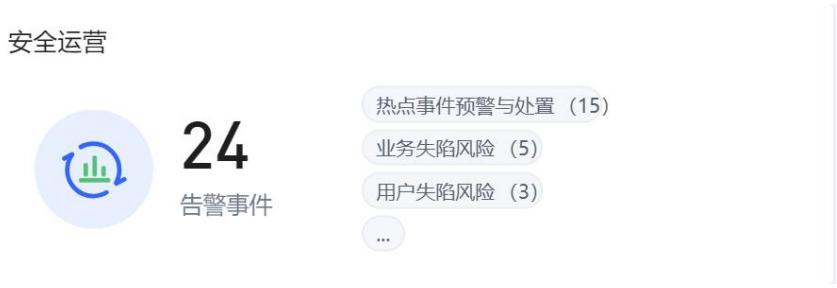
3. 首页

首页功能主要统计并展示设备的运行情况、业务和用户安全状态和风险提示等，从而对用户访问行为进行可视可控，如下图所示。



3.1. 安全运营

[安全运营]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，点击下图可跳转到安全运营中心页面。



3.2. 硬件与系统运营

[硬件与系统运营]主要显示硬件与系统运营告警、规则库和授权有效性、系统直通风险和日志合规提醒四个方面的信息，点击下图可跳转到安全运营中心页面。

3.3. 快速链接

[快速链接]主要用于快速进入相关功能页面或使用快捷功能。主要包括黑白名单、地址转换、 应用控制策略、故障排查、业务安全、用户安全、安全日志、版本介绍、漏洞CVE搜索。

3.4. 专项防护

[专项防护]主要显示AF部分特色专项防护的功能，包括：办公网安全防护、高级威胁与检测和云蜜罐诱捕，点击对应图中按钮会进入相应的防护功能配置界面。

点击 ，可以将此栏置顶显示,点击 ，可以将[专项防护]界面关闭不显示。

3.5. 勒索专项防护

[勒索专项防护]主要显示AF勒索专项防护的数据，点击后会进入相应的防护功能配置

界面。

3.6. 业务安全

[业务安全]提供迅速掌握业务整体的安全状况（业务风险分析、业务攻击趋势、业务热点事件TOP10）。如下图所示。

点击 ，可以将此栏置顶显示。

点击下拉框，可以选择最近七天、最近两天和今天的时间范围的信息。

3.7. 用户安全

[用户安全]提供迅速掌握用户整体的安全状况（包括用户风险分析、用户攻击趋势、用户热点事件TOP10）。如下图所示。

点击 ，可以将此栏置顶显示。

点击下拉框，可以选择最近七天、最近两天和今天的时间范围的信息。

3.8. 设备和系统运营

[设备和系统运营]主要显示设备状态、系统状态、接口状态、安全能力和产品联动的基本信息。

设备状态：显示设备的CPU、内存和硬盘的使用情况，便于查看设备运行是否在合理范围之内。

系统状态：显示设备的双机状态、已持续防护时间、系统时间和版本信息。

接口状态：显示当前的接口状态，绿色表明接口为UP、灰色为DOWN。

安全能力：显示设备的规则库是否开通以及过期时间。

产品联动：显示和EDR网端联动的防护功能，点击后跳转到网端联动章节。

点击 ，可以将此栏置顶显示。

3.9. 网络运营

[网络运营]显示用户网络的整体情况，其包括并发会话、新建会话、接口吞吐率趋势、应用流量实时排行四部分内容。

点击 ，可以将此栏置顶显示。

点击下拉框，可以选择最近七天、最近两天和今天的时间范围的信息。

4. 安全运营

安全运营功能用于展示设备整体安全状况，对整体安全状况进行监控和响应，提供日常维护，有效的管理运营安全服务 ，同时提供专项防护功能，并进行黑白名单的管理以及联动下一代安全体系。包括安全运营中心、物联网安全、业务安全、用户安全、专项防护、黑白名单和下一代安全体系等功能模块。

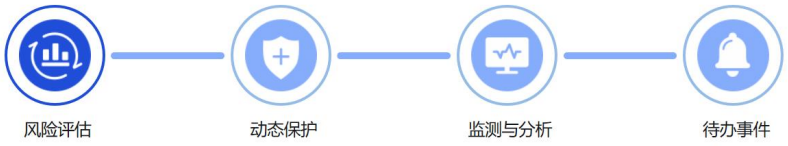
4.1. 安全运营中心

安全运营中心可以评估整体的风险，包括设备、用户和业务的风险状况，并能提供事件处置的处置向导，包括风险评估、动态保护、监测与分析和待办事件四个功能模块。

点击<评估设置>，可设置检测范围和检测选项，如下图所示。

点击<处理记录>，显示管理员处理时间、已处理的对象、类型、管理员、操作类型和备注信息等，可搜索处理记录，如下图所示。

点击<手动评估>会进行风险评估、动态保护、监测与分析和待办事件四个流程检测，如下图所示。



点击<查看详情>会跳转到对应的功能模块。

风险评估

风险评估主要分为自动评估和手动评估两种区别：

自动评估：

上架一段时间后，只要有配置过漏洞攻击防护，web应用防护或者是实时漏洞分析等，设备每小时会自动通过主动扫描，对客户网络状况进行风险评估。包括“风险评估”-“动态保护”-“监测与分析”-“待办事件”。

手动评估：

为了更实时地分析评估客户的网络状况，我们也可以通过手动评估的方式，可以更实时分析客户当前的网络风险状态，另外在我们处理完安全事件后，也建议再次手动评估一次，查看客户网络安全状况是否符合安全检查的预期。

动态保护

动态保护是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。

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。

待办事件

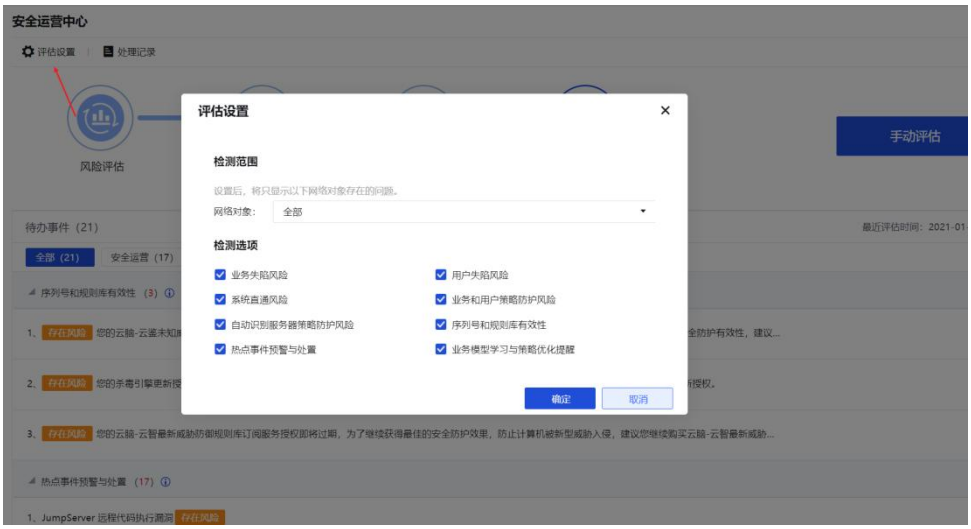
待办事件用于查看AF设备检测到的网络环境中存在的风险并对风险进行处理，可设置检测的范围和检测的选项，查看处理记录，如下图所示。

4.1.1. 案例配置

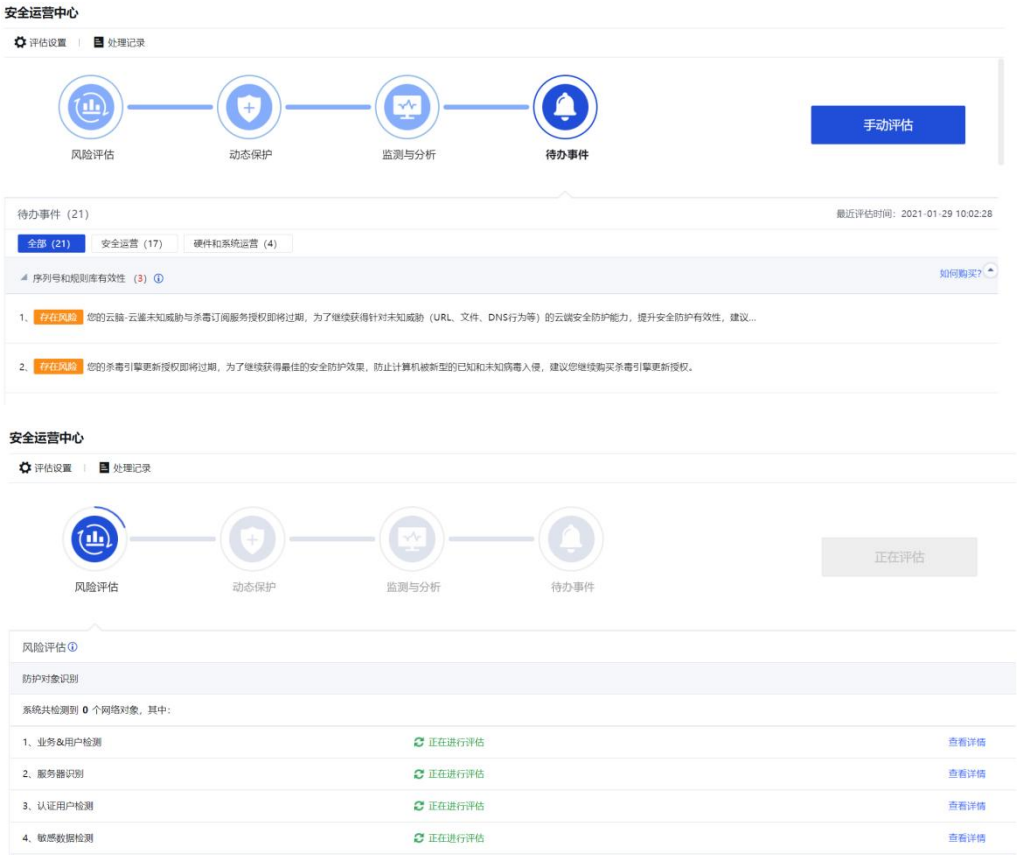
某企业部署AF已经稳定运行一段时间，现需要查看AF发现自身和业务各存在哪些风险点，从而做到事前预知，及时发现设备和业务存在的安全问题。

配置步骤：

步骤1. 点击评估设置，设置评估的范围，如下图所示。

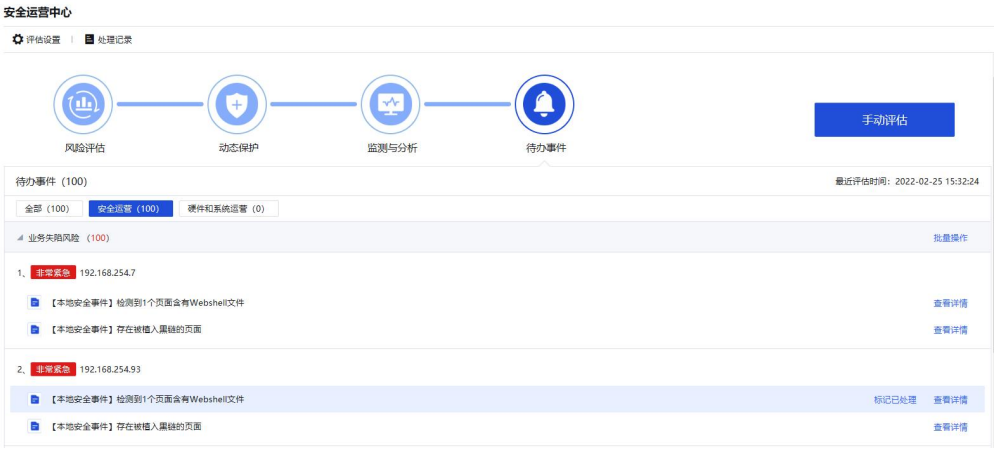


步骤2. 点击<手动评估>，对设置的评估范围进行评估，，如下图所示。



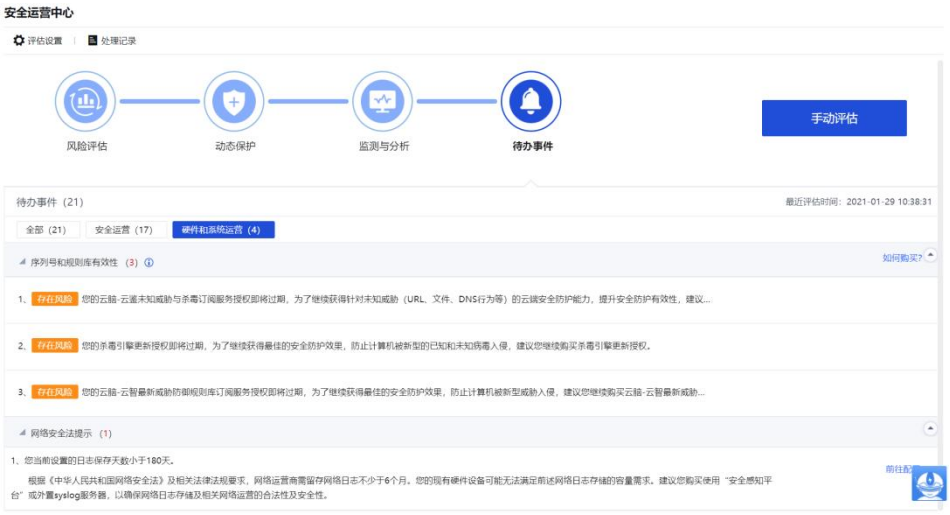
步骤3. 评估完成后，查看评估结果，如下图所示。

步骤4. 点击<安全运营>，可以查询到匹配业务失陷风险和用户失陷风险等行为，从而可以快速的发现网络中哪些业务高风险和需要及时处理的问题。如下图所示。



步骤5. 如果该事件已处理或者为误报，可以点击<标记处理>，则后续不会在产生对应的告警行为。可以在处理记录中查看已经处理的事件，如下图所示。

步骤6. 点击<硬件和系统运营>，可以查看系统自身存在的问题，比如序号即将过期等，如下图所示。



步骤7. 可根据风险提示进行相应的处置，如授权即将过期等，需要及时申请新的授权，防止过期后规则库等无法更新。

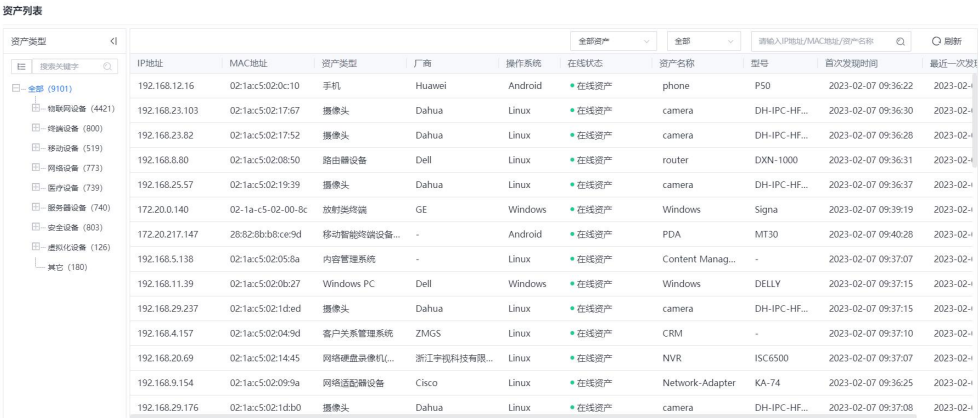
4.2. 物联网安全

物联网安全主要用于对可信资产进行入网管控，持续监测入网资产风险，可以查看当前内网接入的终端设备状态和IP使用状态，包括资产列表和资产发现设置。

4.2.1. 资产列表

资产列表中能显示的资产主要包括物联网终端、PC、移动终端、网络设备、医疗设备、共享终端和其他自定义等。其中物联网终端主要包括监控摄像头、门禁系统、打印机、3D打印机、安防设备、智能电视和企业物联网终端等。

在资产发现配置内网的网段，识别后的资产信息会在资产列表中展示，如下图所示。



4.2.2. 资产发现设置

资产发现设置主要对资产进行识别，从而获取到资产的IP、厂商、类型等信息，并在资产列表中进行展示。其中资产范围定义指的是对资产的识别范围进行限制，如果属于该范围内的资产进行识别。如果启用全网终端流量识别功能，即以被动的方式对流量进行识别该范围内的资产类型。如果启用全网终端主动扫描功能，则AF以主动发包的形式，对范围内的资产进行主动扫描，从而获取到资产的相关信息。启用全网终端流量识别功能和启用全网终端主动扫描功能建议二选一开启，不建议同时开启。

被动流量识别

在[物联网安全/资产发现设置]中，选择需要识别的资产范围，并勾选启用全网终端流量识别功能，如下图所示。

主动探测识别

在[物联网安全/资产发现设置]，选择全网终端扫描的资产范围，并勾选启用全网终端主动扫描功能，扫描完成的资产信息会在资产列表中进行展示。如下图所示。

说明：

启用全网终端主动扫描不建议在医疗场景下启用，可能会对医疗设备的正常使用产生未知风险！

点击[配置高级选项]，可以对资产的扫描速度或者清除不上线的资产进行配置，如下图所示。

表5 功能说明

功能	功能说明
定义的资产范围变化后，清除不在此范围内的资产	勾选该功能后，如果资产列表中的资产不在资产范围定义的 IP 段内，则将自动删除该资产信息
自动删除连续 30 天未发现或无流量的资产	根据设定的自动删除未发现或无流量的终端的期限，对这些已经离线的资产进行自动删除。如果与 SIP 联动，则该功能无法展示，实际自动删除则由 SIP 定义退库的时间

开启无业务流量扫描模式	默认的扫描速度并发为 50 个 IP，开启该功能后单个 CPU 扫描并发为 256 个 IP，从而大大提高资产识别速度
主动扫描全部资产的时间间隔	根据资产定义的扫描范围，当扫描完成后，进行下一轮的周期时间间隔
主动扫描单个资产的冷却时间	主动扫描出来的资产，存在冷却时间，该时间内的资产不进行主动扫描，只有等待冷却时间到期后，在匹配主动扫描全部资产的时间间隔才进行扫描
自定义资产在线状态	如果流量到 AF 或 AF 主动扫描到，会显示该资产在线
跨三层取 MAC	AF 扫描跨网段的资产，只能获取到对应的 IP、类型、厂商等信息，无获取 MAC 地址。因此，如果需要获取 MAC 地址，需要配置跨三层 MAC 识别，具体配置请参考[策略/认证/用户认证/跨三层 MAC 识别]章节

配置步骤

步骤1. 进入[安全运营/物联网安全/资产发现]，勾选<启用全网终端主动扫描>，并选择<复用已定义的资产范围>，即复用资产范围定义中的区域和地址。

步骤2. 点击<提交>，等待扫描完成。

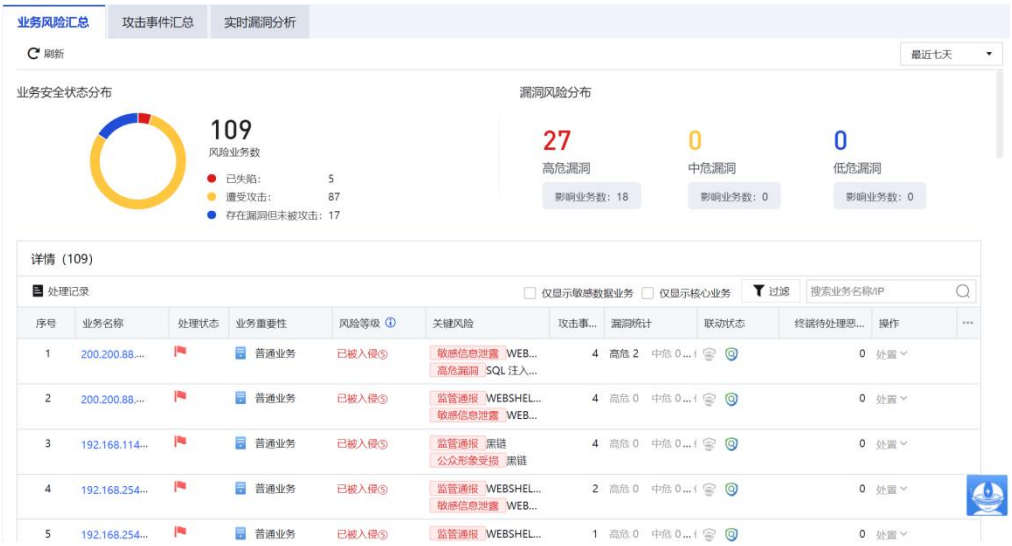
步骤3. 扫描完成后，进入资产列表中查看扫描到的资产信息。

4.3. 业务安全

业务安全是从业务角度进行安全展示，展示网络中业务相关的整体安全状况，包括业务风险汇总、安全事件汇总攻击和实时漏洞分析三个功能模块。

4.3.1. 业务风险汇总

业务风险汇总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。



关于风险等级说明，可以参考如下表。

表6 风险等级说明表

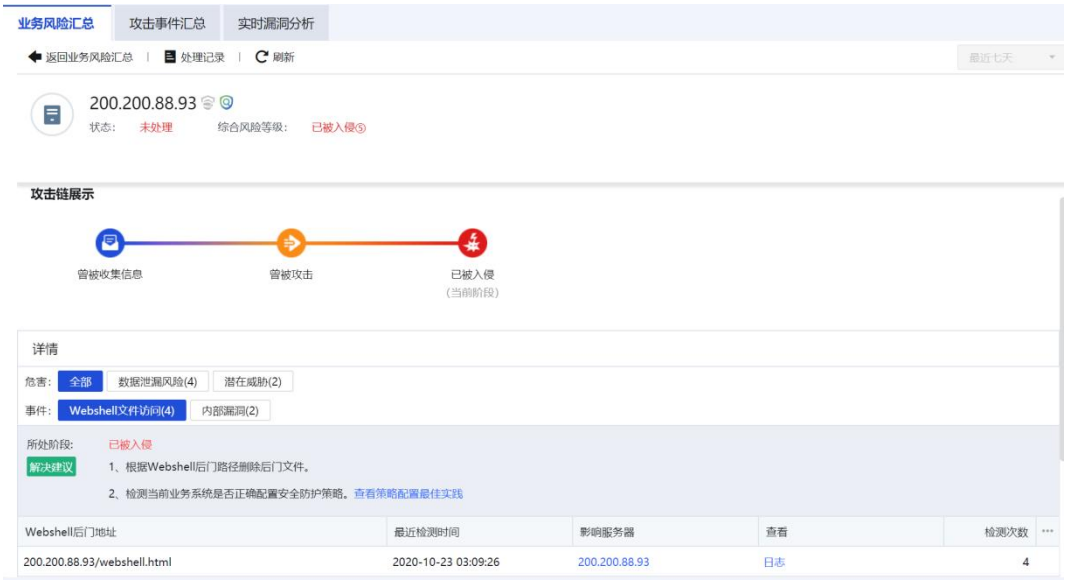
风险等级	说明
已被入侵	已有数据证明服务器已被黑，如被挂 webshell、黑链等。
曾被攻击	无数据证明服务器被黑，会存在被攻击的证据：包括 SQL 注入、暴力破解、webshell 上传等攻击类型的日志。
曾被收集信息	无数据证明服务器被黑，会记录被搜集信息的证据。
存在漏洞	无数据证明服务器被黑，无被攻击记录，说明服务器本身存在漏洞。

关键风险类型包含：监管通报、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。

点击<过滤>，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。



如图，上半部分是业务风险的总览，详情项包括：该业务当前所遭受的危害，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、外部攻击等）。

所处阶段：已被入侵；影响的服务器，解决建议，以及举证。

案例配置

某企业中，AF产生了较多业务风险告警提示，需要排查具体的业务是否存在对应的风险信息。

操作步骤：

步骤1. 点击<业务安全>，查看具体哪些业务存在风险，如果为已被入侵，则需要重点关注业务的情况，如下图所示。

步骤2. 点击业务名称，进入查看该业务的具体情况，如下图所示。

步骤3. 查看对应的事件，并点击<日志>，对具体的检测日志进行分析和判断，确认事件是不是正常的访问行为，如下图所示。

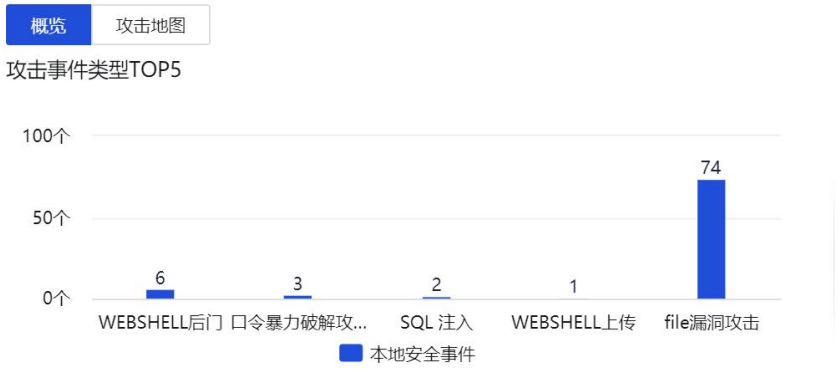
步骤4. 根据日志分析和判断之后，如果为误报，可以添加例外，后续就不会产生对应得告警。

4.3.2. 攻击事件汇总

攻击事件汇总该页面是从业务安全角度进行安全展示。可看到攻击事件类型TOP5和攻击者地图。如下图所示。

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。

攻击者地图

攻击者地图用于显示AF设备是今天/最近两天/最近七天检测到的攻击者的IP来源。

点击<投屏显示>，跳转到攻击者地图展示页面。如下图所示。

热点事件

热点事件是防火墙收集的某段时间内来自全网的排列top 10的安全事件，这些安全事件中，如果有对应的攻击威胁经过防火墙，被防火墙能识别到，则其中对应的攻击威胁会被标志为红色，如果流经防火墙的流量没有对应攻击威胁，则对应攻击威胁类型被标注为灰色。

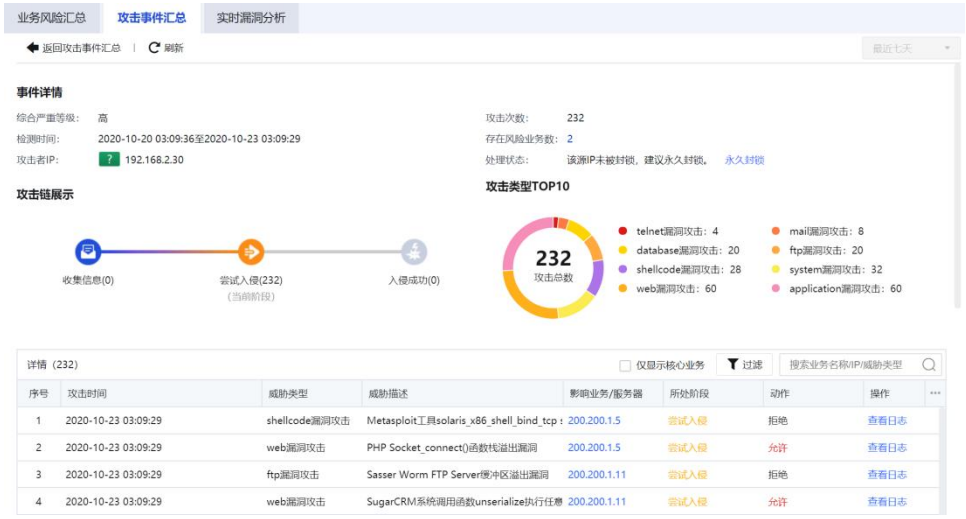
点击具体热点事件，可在表格中过滤出具体的日志。如下图所示。

受影响业务

受影响业务主要用于显示最近发生的攻击事件，如下图所示。

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、事件描述、攻击时间、状态以及操作。

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。



勾选仅显示核心业务，可只关注核心业务的安全状况。

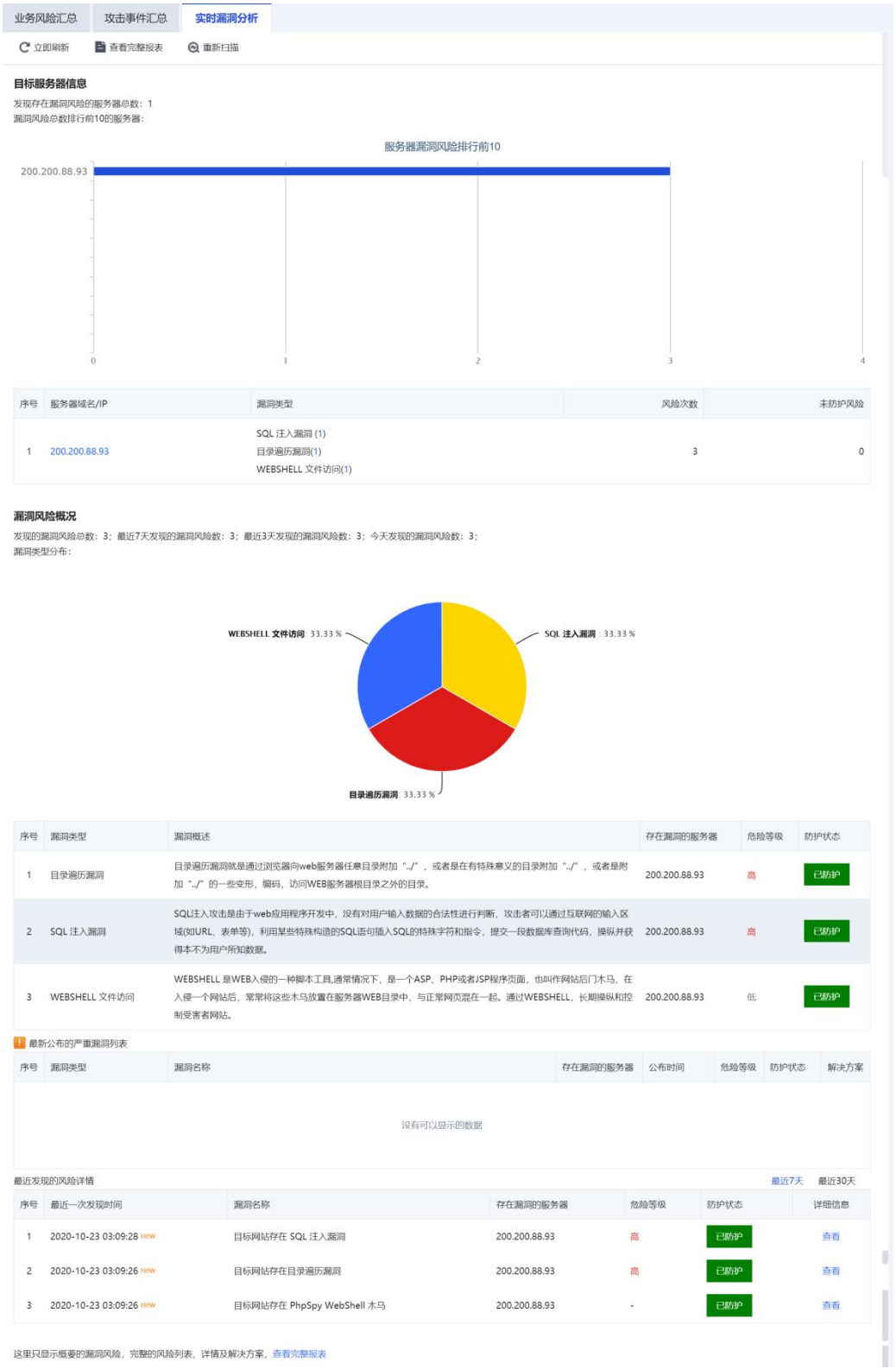
点击<过滤>，可根据检测类型、归属地和严重等级进行筛选。如下图所示。

4.3.3. 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，可以查看到业务中存在的安全漏洞风险。

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。

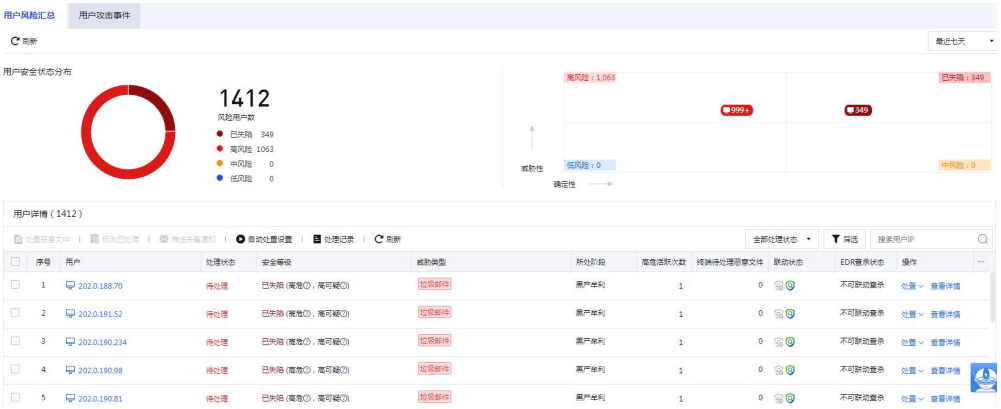


4.4. 用户安全

用户安全是从用户角度进行安全展示，掌握网络中用户端的安全状况，包括用户风险汇总和用户攻击事件两个功能模块。

4.4.1. 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。



用户安全状态分布：用于显示受影响的用户分布情况。

用户详情：用于显示最近用户发生的攻击事件。显示的内容包括：用户、安全等级、状态、威胁性、确定性、威胁类型、所处阶段、高危活跃次数、待处理文件/关联文件、联动状态、操作。

点击<查看详情>列表的用户可跳转到用户详情页面。可看到用户安全详情、攻击阶段图、解决方案。如下图所示。

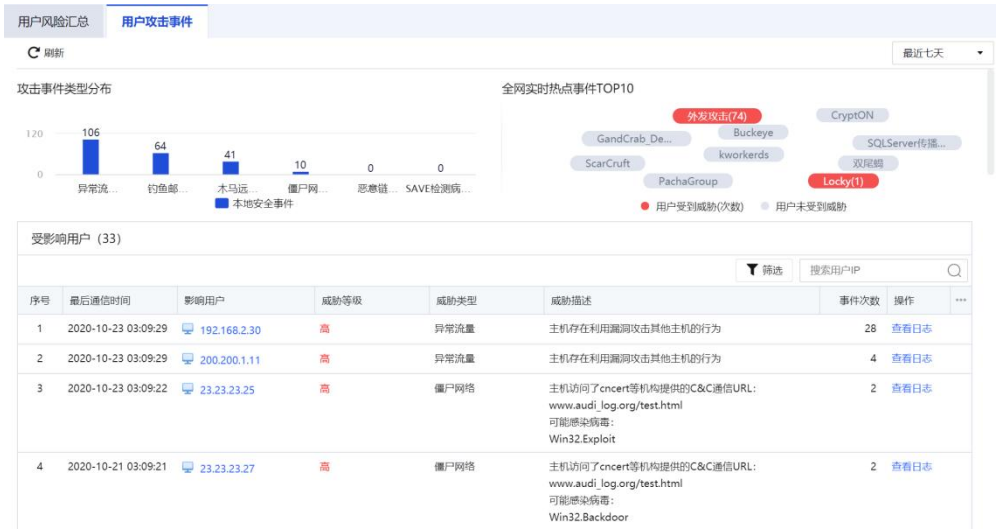
勾选仅显示核心业务，可只关注核心业务的安全状况。

点击<全部处理状态>，有全部处理状态、待处理、已处理和观察中四种状态选择。

点击<筛选>，可根据用户重要性、安全状态、EDR查杀状态、所处阶段进行筛选。

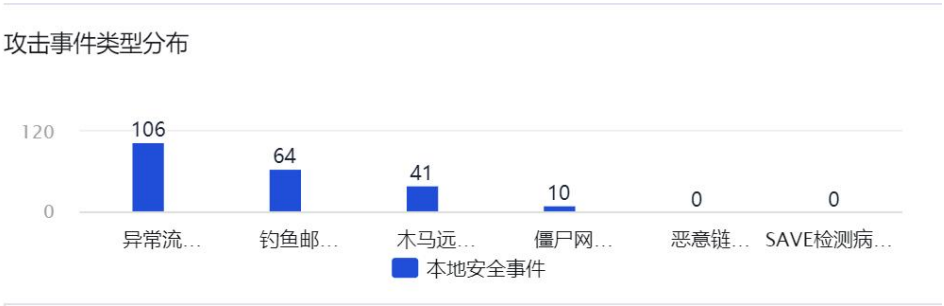
4.4.2. 用户攻击事件

用户安全事件是从攻击类型的角度进行用户安全展示，可以收集来自全网热点事件中，流量经过AF，AF识别的用户风险，如果匹配中其中的热点事件，则标注为红色，没有改风险类型则标注为灰色。

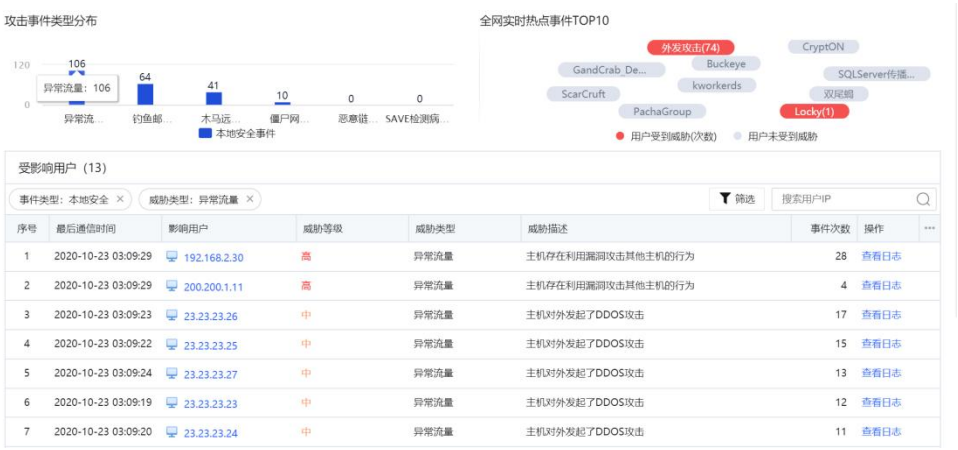


攻击事件类型分布

攻击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。

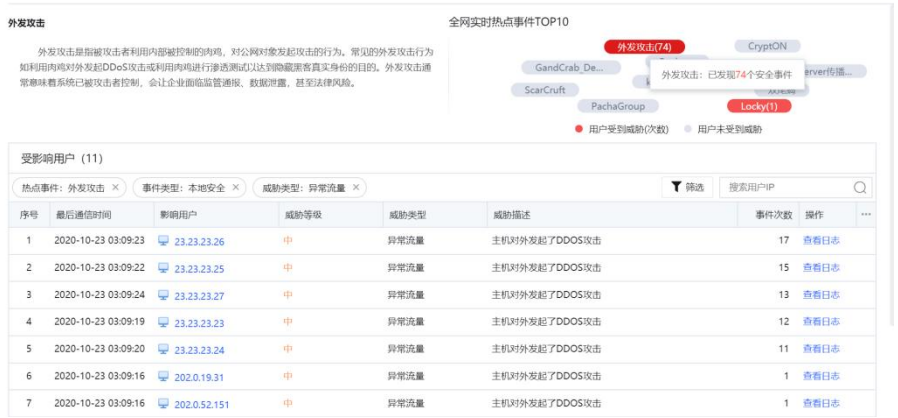


序号	最后通信时间	影响用户	威胁等级	威胁类型	威胁描述	事件次数	操作
1	2020-10-23 03:09:29	192.168.2.30	高	异常流量	主机存在利用漏洞攻击其他主机的行为	28	查看日志
2	2020-10-23 03:09:29	200.200.1.11	高	异常流量	主机存在利用漏洞攻击其他主机的行为	4	查看日志
3	2020-10-23 03:09:23	23.23.23.26	中	异常流量	主机对外发起了DDOS攻击	17	查看日志
4	2020-10-23 03:09:22	23.23.23.25	中	异常流量	主机对外发起了DDOS攻击	15	查看日志
5	2020-10-23 03:09:24	23.23.23.27	中	异常流量	主机对外发起了DDOS攻击	13	查看日志
6	2020-10-23 03:09:19	23.23.23.23	中	异常流量	主机对外发起了DDOS攻击	12	查看日志
7	2020-10-23 03:09:20	23.23.23.24	中	异常流量	主机对外发起了DDOS攻击	11	查看日志

全网实时热点事件TOP10

全网实时热点事件TOP10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，灰色表示业务未发生。如下图所示。

点击具体热点事件，可在表格中过滤出具体的日志。如下图所示。



序号	最后通信时间	影响用户	威胁等级	威胁类型	威胁描述	事件次数	操作
1	2020-10-23 03:09:23	23.23.23.26	中	异常流量	主机对外发起了DDOS攻击	17	查看日志
2	2020-10-23 03:09:22	23.23.23.25	中	异常流量	主机对外发起了DDOS攻击	15	查看日志
3	2020-10-23 03:09:24	23.23.23.27	中	异常流量	主机对外发起了DDOS攻击	13	查看日志
4	2020-10-23 03:09:19	23.23.23.23	中	异常流量	主机对外发起了DDOS攻击	12	查看日志
5	2020-10-23 03:09:20	23.23.23.24	中	异常流量	主机对外发起了DDOS攻击	11	查看日志
6	2020-10-23 03:09:16	202.0.19.31	中	异常流量	主机对外发起了DDOS攻击	1	查看日志
7	2020-10-23 03:09:16	202.0.52.151	中	异常流量	主机对外发起了DDOS攻击	1	查看日志

受影响用户

受影响用户用于显示当天/最近两天/最近七天不同时间段内发生的被攻击事件。

显示的内容包括：序号、最后通信时间、影响用户、威胁等级、威胁类型、威胁描述、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。

点击<筛选>，可根据用户重要性、威胁等级、事件类型、威胁类型进行筛选。

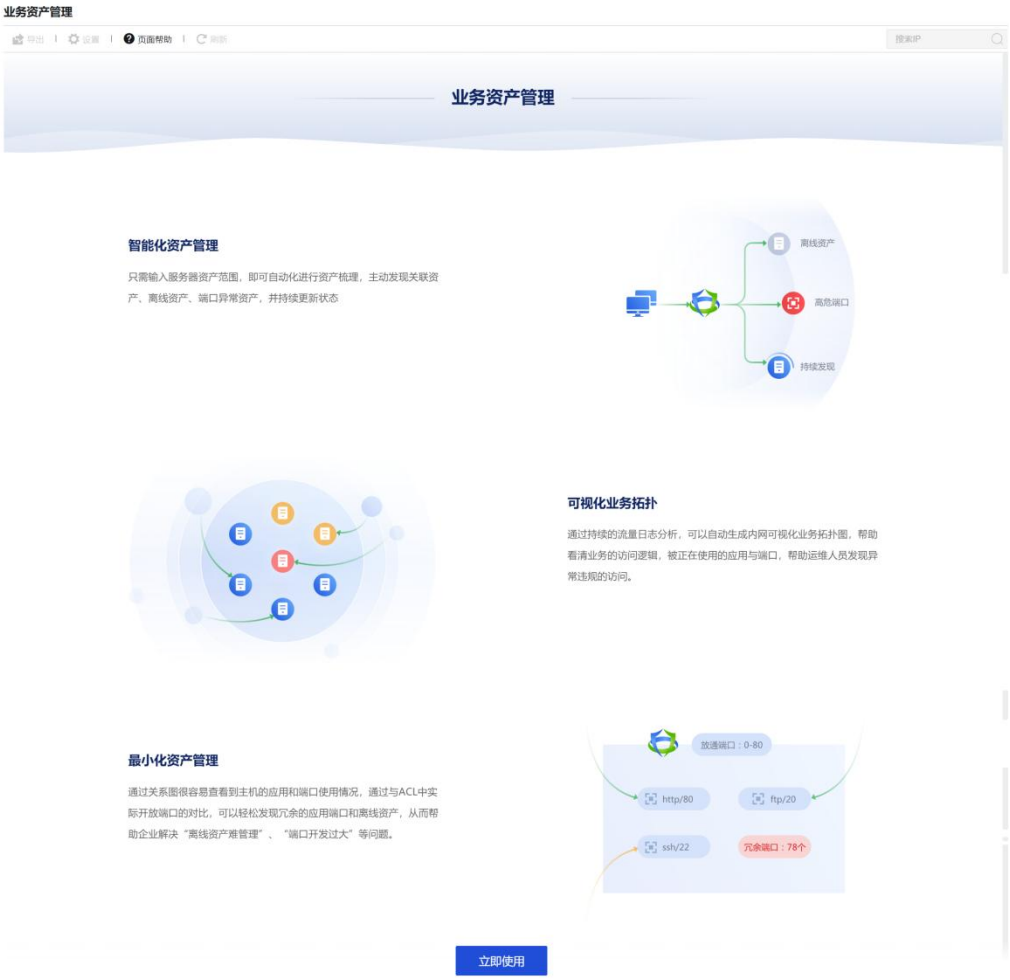
4.5. 专项防护

专项防护提供设备特有防护功能模块的展示，能够快速了解专项防护功能模块的防护情况并进行响应，包括业务资产管理、勒索专项防护、主动诱捕总览、云端黑客IP防

护和账号安全专项防护等功能模块。

4.5.1. 业务资产管理

业务资产管理是精细化管控的核心功能模块，在数据中心场景中，主要通过主动扫描，探测服务器在线的状态及端口使用情况，帮助用户梳理业务资产的访问关系，缩小策略开放端口，精简ACL策略。



点击<立即使用>弹出[配置]页面，显示功能说明。如下图所示。

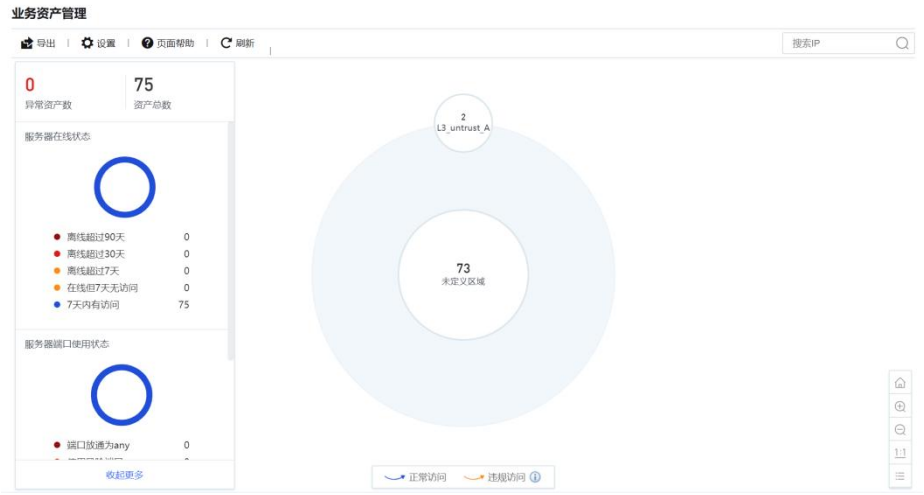
点击<下一步>进入[设置资产网段]页面，内网服务器网段和内网用户网段支持填写IPv4和IPv6单个地址、范围以及网段。业务资产管理的主动扫描，只会对填写在“内网服务器网段”内的IP地址进行扫描，即只要IP地址被填写在“内网服务器网段”内，则会被识别成服务器资产，并对这些IP地址进行主动扫描。不在这两个网段范围内，也不在私有网段范围内即为互联网网段，网段配置应该尽量准确，否则会增加扫描时间。如下图所示。

设置完成后点击<下一步>，进入[开启主动扫描]页面，如需要主动扫描，需勾选[开启并同意主动端口扫描]。开启后，设备会定期主动扫描内网服务器网段，来获取服务器活跃状态、端口和应用的使用情况。如需更改扫描时间与扫描端口，请点击<扫描时间配置>进行编辑。

点击<开始梳理>完成配置。

这在业务资产管理功能模块启用成功后，进入业务资产管理功能界面，才可点击<设置>进行主动扫描的相关配置修改。如下图所示。

资产梳理完成后，即可显示资产的梳理结果，比如服务器资产在线情况、服务器资产端口使用情况，以及资产间的访问关系拓扑图等。管理员可根据资产梳理的结果对业务资产进行管理优化。



4.5.2. 勒索专项防护

勒索专项防护是AF通过针对防护对象自动生成策略，全面防护勒索风险，过全面、可视化识别勒索风险，并提供处置建议和处置思路，让管理员敢处置勒索风险事件。勒索专项防护功能的配置入口如下。

点击<立即使用>按钮弹出[勒索防护配置]页面。如下图所示。

目的网络对象：选择内网需要进行勒索防护的业务所在IP组。

目的区域：选择需要进行勒索防护的业务所在区域。

源区域：勒索攻击发起的攻击源。

授权勒索常用端口、漏洞及弱口令的扫描权限：用于授权AF设备主动进行勒索常用端口、漏洞及弱口令的扫描，默认关闭。

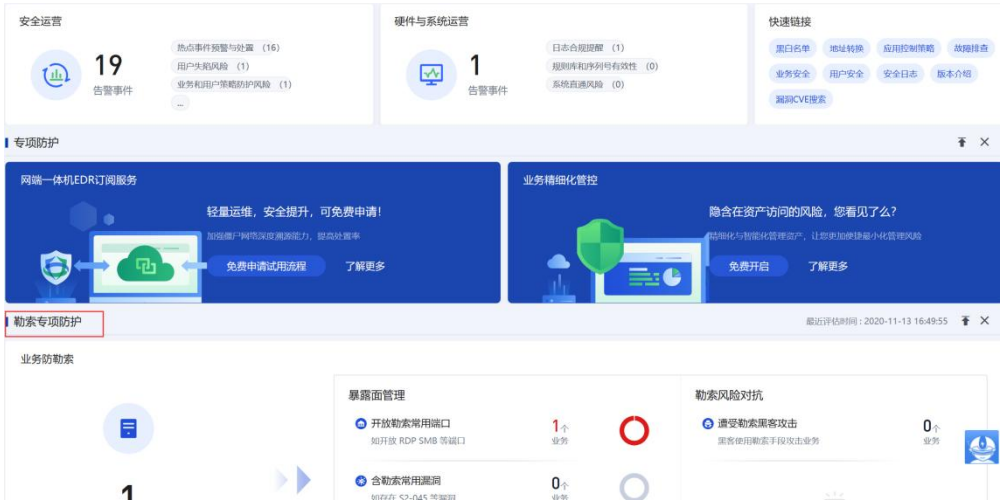
开启自动评估：用于设置AF设备主动进行勒索常用端口、漏洞及弱口令的扫描的时间，开启[授权勒索常用端口、漏洞及弱口令的扫描权限]功能，否则为灰色不可选。

自动生成安全防护策略，进行勒索病毒防护：用于生成安全防护策略，保存后会自动在[安全防护策略]页面生成策略，默认开启。并且会自动添加到安全策略列表的第一条策略。

点击<确定>后会自动进行评估，评估完成会显示勒索专项防护数据，如下图所示。

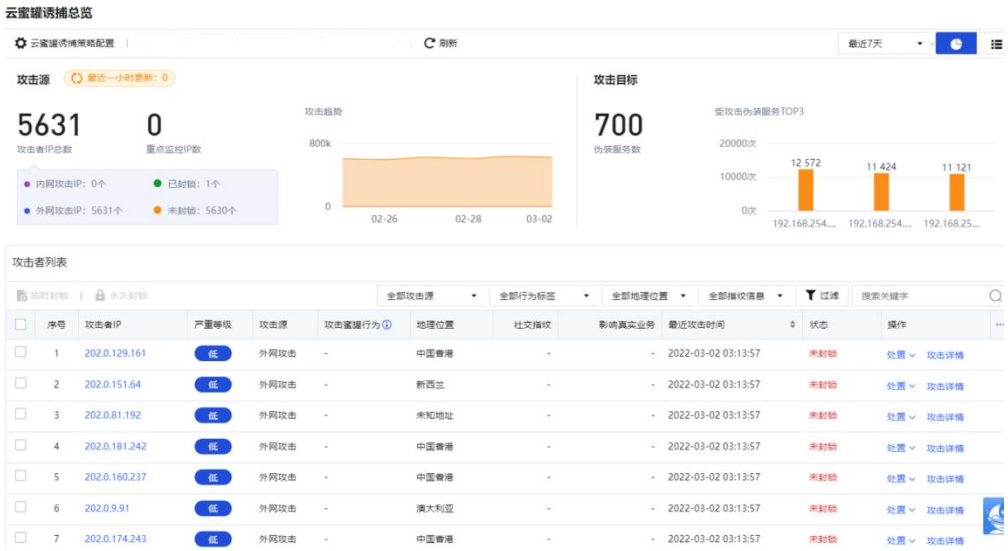
点击<模块显示设置>弹出[模块显示设置]，可以将勒索专项防护模块显示到首页中。

点击<确定>后，进入首页可以查看到[勒索专项防护]数据展示，如下图所示。



4.5.3. 云蜜罐诱捕总览

随着黑客的攻击手法变得越加隐晦，提高了攻击溯源的难度，传统的产品是基于规则、引擎、甚至云脑威胁情报等防护识别方式，已很难百分百识别拦截所有的攻击行为，所以我们可通过云蜜罐诱捕功能，设置蜜罐服务，一方面可达到转移黑客攻击的效果，另一方面可以实现云蜜罐诱捕黑客攻击，从中了解黑客所使用的工具与方法，推测黑客的攻击意图和动机，也可通过窃听黑客之间的联系，掌握他们的社交网络行为，从而能够让防御方清晰地了解其所面对的安全威胁，并通过技术和管理手段来增强真实业务系统的安全防护能力。



点击<处置>,可选择临时封锁、永久封锁和忽略三种动作。

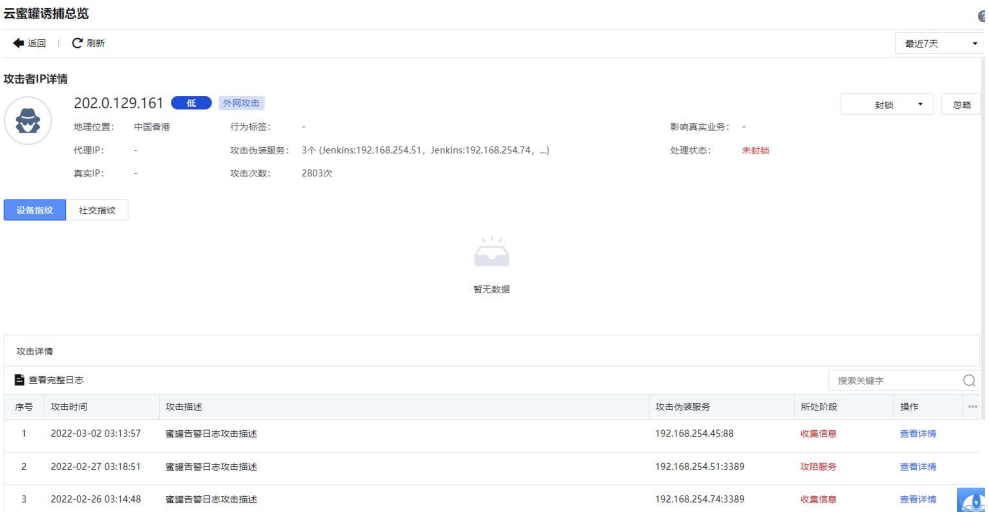
点击<临时封锁>进入[新增临时封锁IP]界面，可以对该攻击者IP设置临时封锁时间，设置完成后会将攻击者IP加入[安全运营/黑白名单/黑名单/临时封锁名单]中。

点击<永久封锁>会将攻击者IP加入[安全运营/黑白名单/黑名单/永久封锁名单]中。

点击<忽略>后添加到[云蜜罐忽略名单]中，不会在总览界面显示，不会触发联动封锁。

点击<攻击详情>会显示该攻击者IP的详细攻击情况。

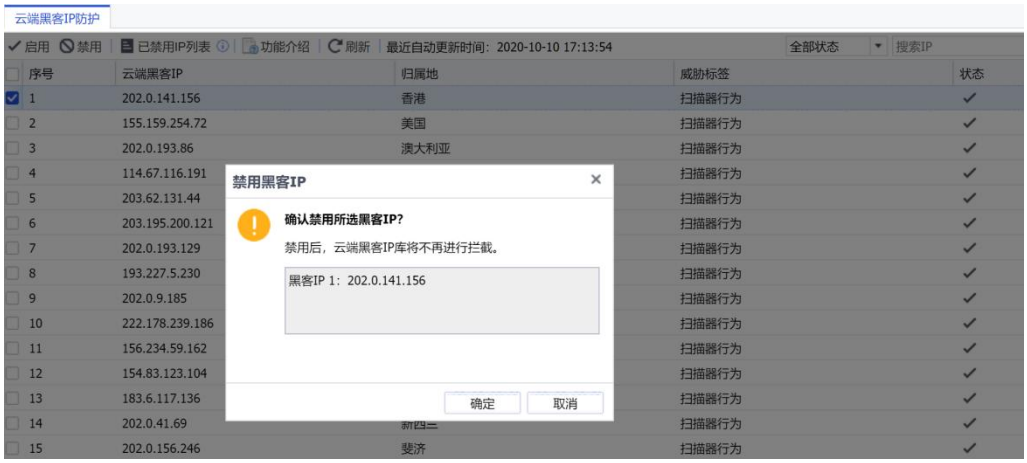
可获取到设备指纹和社交指纹信息，从而捕获黑客IP硬件信息、黑客账号信息等，通过分析黑客攻击特征，从而可通过策略调优、客户业务调优等方式，增强真实业务系统的安全防护能力。



4.5.4. 云端黑客 IP 防护

云端黑客IP防护是AF连接到云端，通过主动拉取云端的黑客IP同步到本地，对防护列表中黑客IP进行防护。当黑客IP流量经过AF后，匹配成功的源IP将自动拦截。若存在误报情况，可禁用该IP；禁用后，云端黑客IP库将不再对该IP进行识别拦截。云端黑客IP库每隔2小时自动更新，保证最新情报信息。

如果存在误报，勾选对应得IP，点击<禁用>，弹出确认按钮，点击<确定>，即可禁用该黑客IP。如下图所示：



说明：

如需要开启云端黑客 IP 防护，需要 AF 能够连接到互联网。

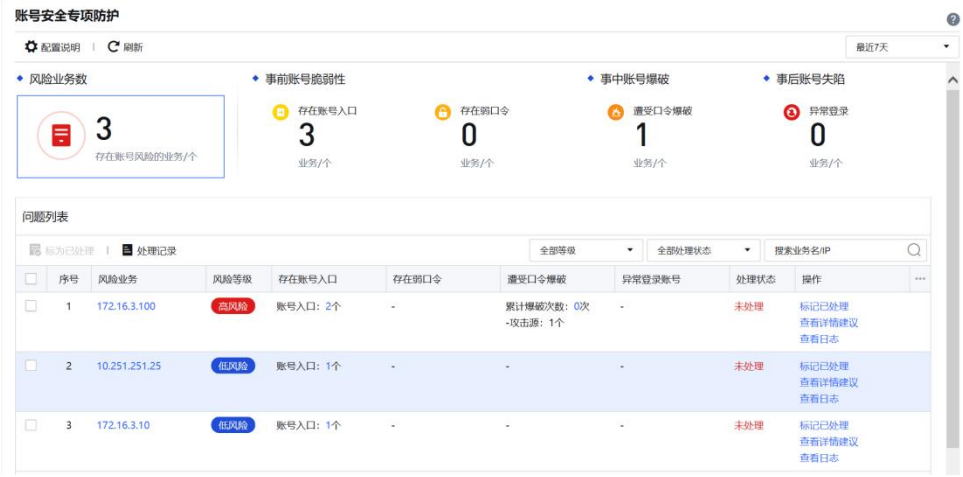
4.5.5. 账号安全专项防护

账号安全是以客户的业务对象为视角，通过分析该个业务对象是否存在账号安全的风险，比如是否存弱口令、是否遭受过口令爆破攻击、是否存在过账号异常登录等异常现象，帮助客户可视化地分析账号的相关安全风险，并给予对应的修复防护意见，从源头阻断攻击行为，从而大大降低客户业务的安全风险。另外，还可帮助客户梳理所有业务资产的账号入口都有哪些，帮助客户可视化地分析内网业务是否开发了什么不必要的账号登录入口，并给予对应账号登录入口的管理建议，帮助客户有效梳理账号入口，减少资产暴露面。

该功能前提条件：

1. 先在[对象/安全策略模板/漏洞攻击防护]中业务保护模板勾选[口令暴力破解]选项。
2. 在[对象/安全策略模板/Web应用防护]的模板中勾选[口令防护]选项，确保在已开启所有弱口令检测功能，
3. 在[策略/安全策略/安全防护策略]关联以上两个模板，检测到对应数据后才会有具体效果展示。首次使用该功能，会出现如下界面。

点击<立即使用>后，会出现具体的效果展示界面，如下图所示。



存在账号入口：要有登录的行为，不管是否有登录成功，AF都会记录为“存在账号入口”，AF会记录下具体的账号登录入口地址，从而帮助客户梳理登录入口资产，界面主要展示入口的协议及入口地址；

弱口令：主要帮助客户梳理存在弱口令的业务资产，帮助管理员具体定位是哪个账号存在弱口令，界面主要展示账号类型、名称及登录入口等，同时也支持弱口令的导出及模糊搜索。

遭受口令爆破：登录账号存在多次尝试登录并且登录失败的异常行为，AF会记录为“遭受口令爆破”，AF主要记录具体的攻击源及爆破手段等，在AF界面可支持对源IP的永久封锁，从而对爆破源进行及时的封锁阻断；

异常登录账号：通过多次账号爆破，实现爆破成功并且登录成功的行为，AF会记录为“异常登录账号”，AF主要展示了异常登录的账户，攻击源和爆破次数等

4.6. 黑白名单

黑白名单用于设置被设备信任的白名单和被设备不信任的黑名单，通过黑名单进行全局封锁，通过白名单进行全局放行，包括黑名单和白名单两个功能模块。

4.6.1. 黑名单

黑名单用于设置被设备封锁的名单地址，分为永久封锁名单和临时封锁名单。

4.6.1.1. 永久封锁名单

永久封锁名单用于封堵一些需要禁止访问外网的内网地址或一些访问攻击服务器的公网地址设置，被永久封锁。管理员可对封锁名单进行如下操作。

表7 永久封锁名单说明表

操作	说明
编辑	选择需要编辑的封锁名单进行修改地址和描述，点击<确定>即可。
删除	选择需要删除的封锁名单，点击<删除>即可。
清除所有封锁地址	会清除永久封锁名单中所有地址。
导入/导出	对封锁名单进行导入、导出操作。
刷新	刷新当前列表的页面数据。
搜索	可针对某个地址进行搜索查询。

点击<新增>弹出[新增永久封锁名单]页面，输入封锁名单和描述，点击<确定>提交。

封锁名单：可以填写IPv4、IPv6地址、域名和URL，包括支持单个地址、IP网段和IP范围等。

4.6.1.2. 临时封锁名单

临时封锁名单用于查看当漏洞攻击防护规则和Web应用防护规则，APT检测启用联动封锁时，封锁了哪些源IP以及是哪个安全策略触发的封锁或手动添加的封锁地址，自定义封锁时间，到时间期限后自动解锁。管理员可对临时名单进行如下操作。

表8 临时封锁名单说明表

操作	说明
删除	选择需要删除的封锁名单，点击<删除>即可。
清除所有封锁地址	会清除永久封锁名单中所有地址。
移入到永久封锁名单	用于将地址加入到永久封锁名单，移入永久封锁名单中的地址的通信都会被永久拒绝。
移入白名单	用于将地址加入到白名单，所有移入白名单的 AF 将不会对此对象进行拦截。
刷新间隔	刷新间隔可以设置临时封锁名单刷新的间隔，可设置：不刷新、5 秒、10 秒、20 秒、30 秒。或者自定义设置。
搜索	可针对某个地址进行搜索查询。

点击<新增>弹出[新增临时封锁名单]页面，选择封锁类型、源IP、目的IP方向，IP地址、封锁时间，点击<确定>。

封锁类型：设置需要封锁地址的类型。

- IP 地址：可选择源 IP、目的 IP 进行填写。
- 域名：可输入域名
- URL：可输入具体的 URL 地址

封锁时间：设置选择封锁的时间，到达时间期限，解除封锁，最短3分钟，最长15天。

点击<联动封锁时间设置>弹出[联动封锁时间设置]，用于设置触发安全策略联动封锁的时间。

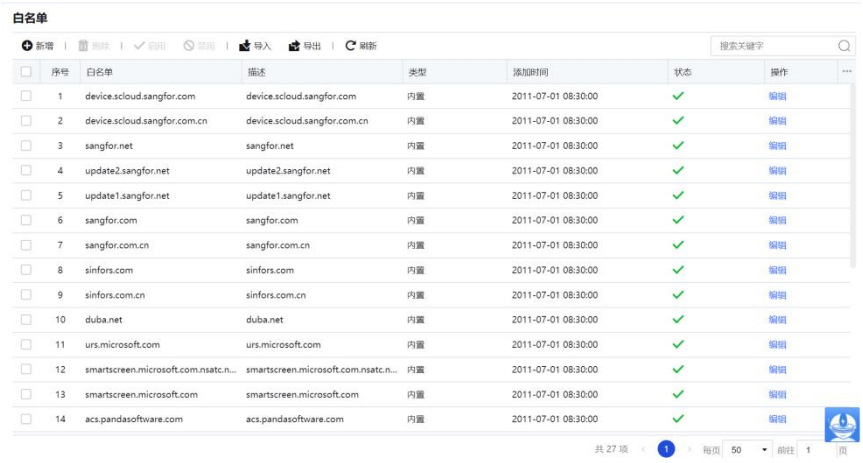
4.6.2. 白名单

白名单用于放行指定地址，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IP、域名和URL。管理员可对白名单进行如下操作。

表9 白名单说明表

操作	说明

编辑	选择需要编辑的白名单进行修改和描述，点击<确定>即可。
删除	只能删除自定义的白名单，内置的白名单，不能删除。
启用/禁用	对需要启用和禁用的白名单进行相关操作。
导入/导出	对封锁名单进行导入、导出操作。
刷新	刷新当前列表的页面数据。
搜索	可针对某个白名单进行搜索查询。



点击<新增>弹出[新增白名单]页面。输入自定义白名单和描述，点击<确定>提交。

自定义白名单：可以填写IPv4、域名和URL格式，支持单个地址、IP网段和IP范围。

4.7. 下一代安全体系

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，包括网云联动、网端联动、

高级威胁检测与防护和安全防护能力功能模块。

4.7.1. 联动方案总览

联动方案总览用于展示目前AF可以联动相应的产品示意图，包括云鉴、云图和EDR。

4.7.2. 网云联动

网云联动用于设置设备与云端的联动操作，包括云网接入设置、云鉴检测与防护两个功能模块。

4.7.2.1. 云网接入设置

云网接入设置目前AF可以联动响应的云端产品，包括云鉴、云图。如下图所示。

云鉴

深信服云鉴是基于云端沙箱、行为分析、威胁情报等多引擎的综合检测与防护订阅服务，开通后用户可以获得云端强大的安全能力，构建对于包含高级变种威胁、最新威胁等传统规则签名无法防护的未知威胁的云端检测与防护能力。

设备可以访问互联网，同时已开通云脑-云鉴订阅服务，即可完成AF与云脑-云鉴平台的对接。

云图

深信服云图结合云端大数据分析能力和用户内网业务特点，一站式集中展示安全风险及联动云网端安全产品实现快速处置，提前防御潜在威胁行为、检测内网安全问题。

在云图平台完成企业注册，同时获取到企业ID、设备名称、接入密码信息后，即可在AF设备上完成云图对接。如下图所示。

点击<立即接入>即可完成接入云图平台。如下图所示。

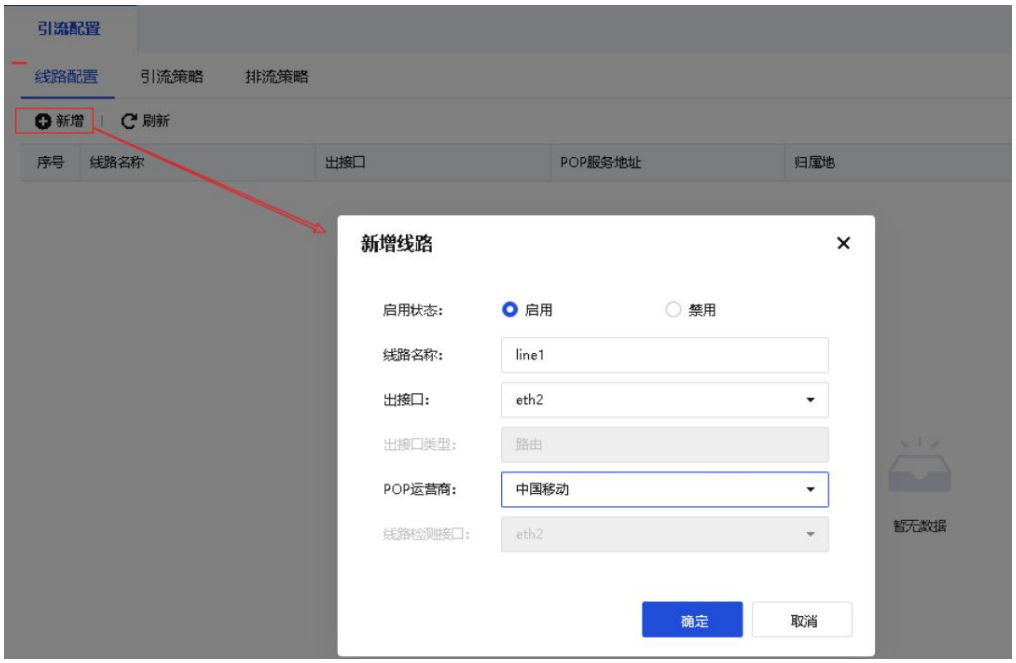
4.7.2.2. 云安全访问服务

云安全访问服务是AF通过对接安全访问服务（SASE）可实现引流，通过POP点的v-AC进行审计及管控，并且能够通过SASE运营中心进行统一管理。接入方式包括通过云图账号接入和通过引流接入码接入。

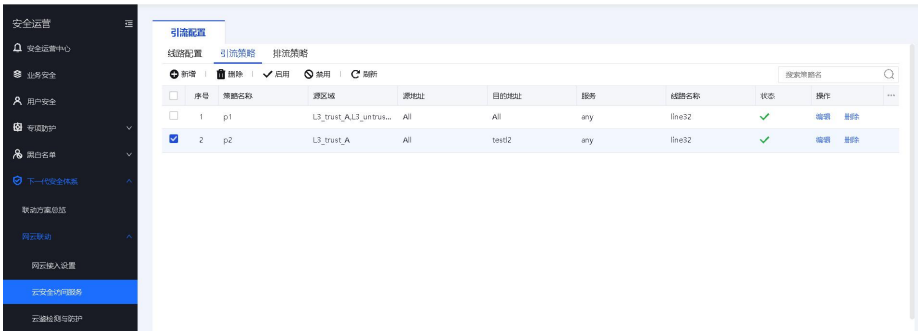
配置步骤

步骤1. 通过云图账号接入或者引流接入码配置接入。

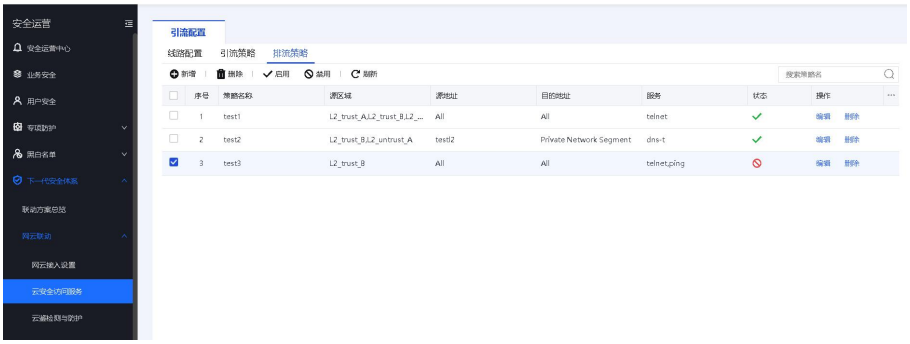
步骤2. 配置线路。POP服务器地址由云端下发，只需配置接口和希望的运营商。



步骤3. 配置引流策略。匹配到引流策略的流量才会引到SASE。



步骤4. 配置排流策略（如有流量不需要进行引流）。排流策略优先级高于引流策略，一个流量同时匹配到引流、排流策略，最终流量不被引流。排流策略对不引流的流量无影响。

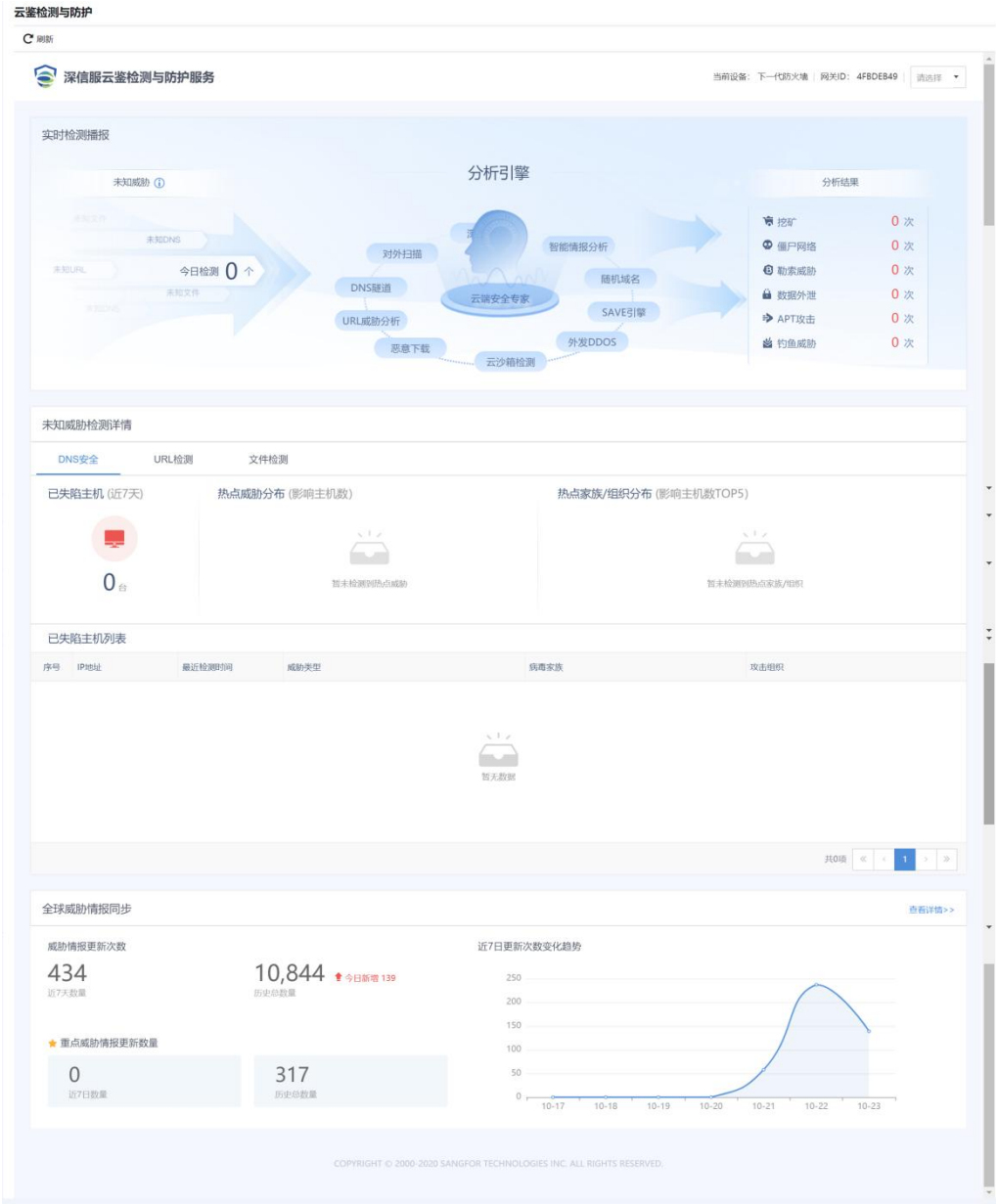


4.7.2.3. 云鉴检测与防护

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，保障用户的网络安全。

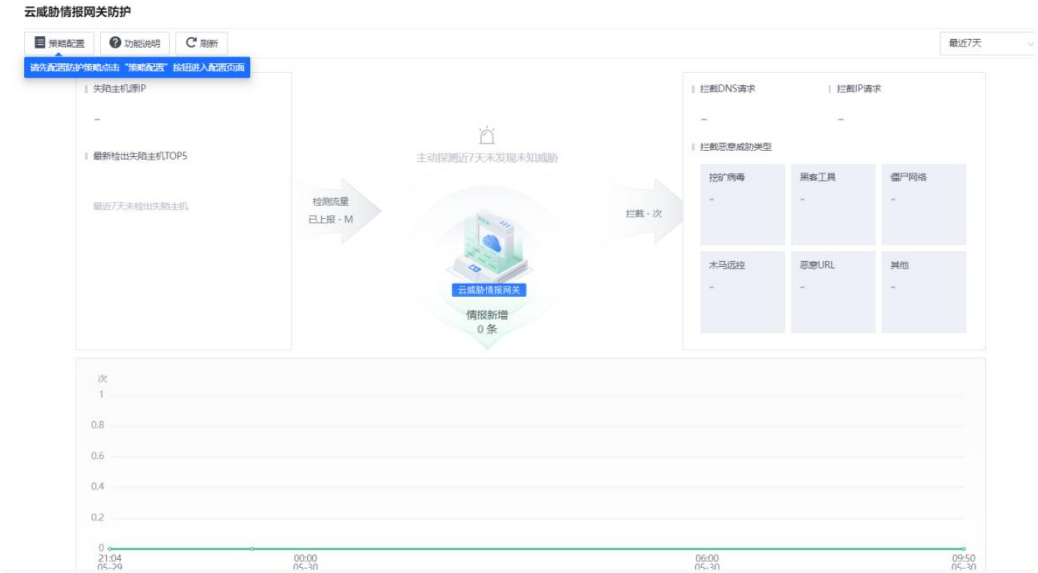
设备可以访问互联网，同时已开通云脑相应授权，设备可以自动完成云脑-云鉴的接入，此处无需额外设置。接入后，可以通过此模块查看威胁情报相关内容。如下图示。



4.7.2.4. 云威胁情报网关防护

云威胁情报网关防护，通过独创的主动探测引擎+现网海量威胁情报，对威胁流量进行实时检测&拦截，所有流量在转发前均经过威胁情报的检测并已明确结果，实现恶意流量在转发前被阻断，保护资产安全。

点击<进入监控页面>，会进入展示失陷IP和拦截恶意数据的监控页面，该页面展示的数据需要先配置完成[云安全访问服务]功能后才会有数据产生。



4.7.3. 网端联动

网端联动可以使EDR与AF共享安全信息，进而实现网络和端点的安全信息进行关联，从而能够使得威胁更可视，处置更便捷。

4.7.3.1. 网端接入设置

网端接入设置EDR和AF联动。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，AF可与EDR进行协同联动、自动处置，形成多层次立体化威胁防御体系。

EDR接入设置包括云端EDR管理平台接入和本地EDR管理平台接入两种方式。

云端EDR管理平台接入

云端管理平台接入是将EDR管理平台部署在云图上，AF和EDR需要和云图绑定后实现联动。如下图所示。

本地EDR管理平台接入

本地EDR管理平台接入是将EDR管理平台部署在本地上，直接输入IP接入，实现AF和EDR的联动。如下图所示。

4. 7. 3. 2. 终端管理

终端管理用于查看EDR客户端信息，包括终端名称、IP、终端状态、联动操作数、操作和最近更新时间，一个小时刷新一次列表信息，可以根据IP地址进行搜索。

点击<隔离主机>弹出[提示]页面进行隔离操作。

点击<确定>，隔离该主机使其无法访问任何网络，在确认刚主机已中病毒防止影响网络，可使用该操作进行隔离。

点击<解除隔离主机>恢复该主机访问网络权限。

4.7.3.3. 联动日志

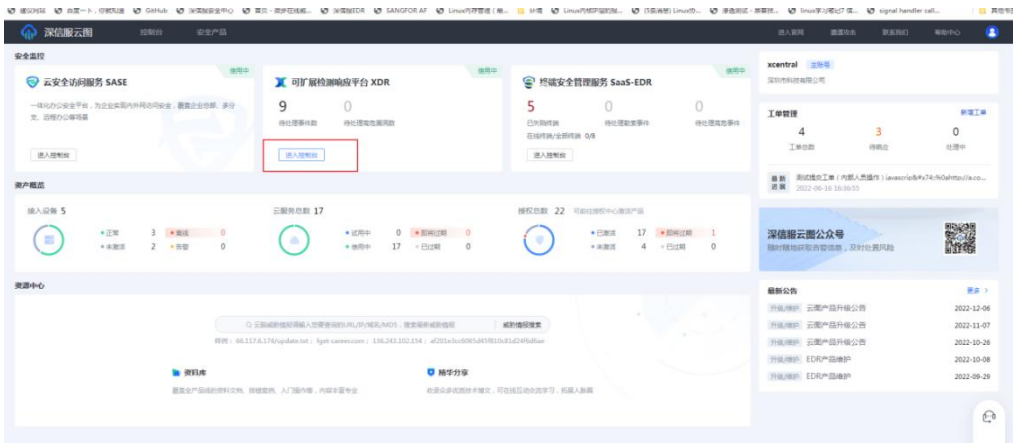
联动日志用于记录AF联动EDR对终端文件的操作日志。如下图所示。

4.7.4. 智能运营

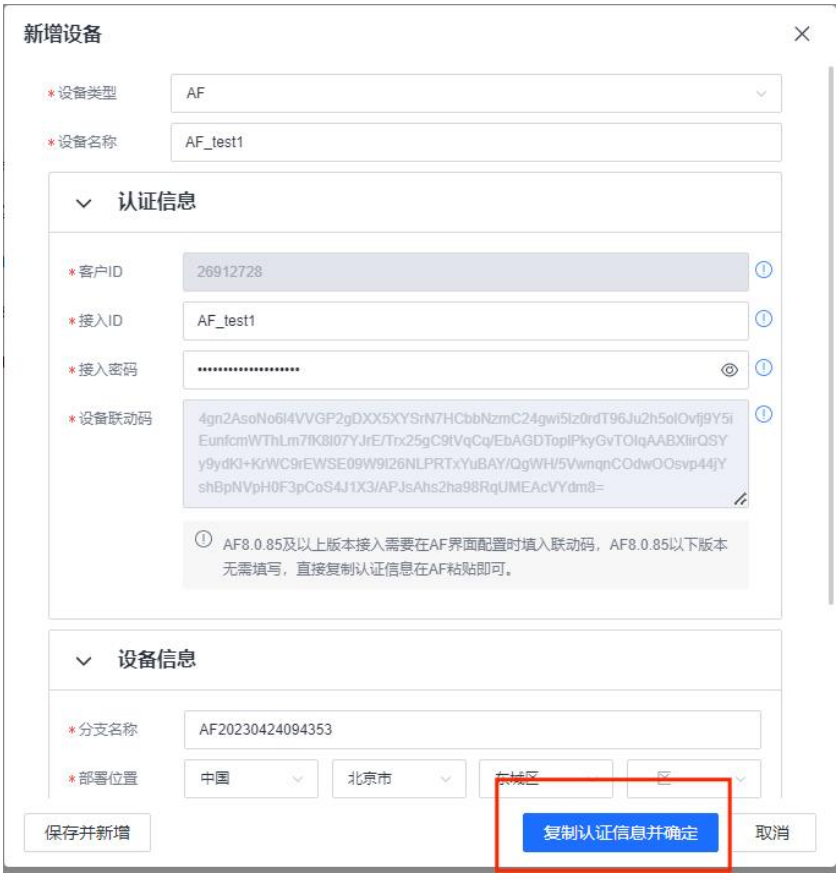
智能运营是AF配合深信服XDR平台构建高级威胁检测与响应服务，通过深度收集网络流量、端点行为、API访问等数据进行全面深入的威胁分析，实现集中式、跨场景、可扩展的高级威胁检测与响应。如下图所示。

配置步骤

步骤1. 登录云图，点击XDR可扩展检测响应平台，云图单点登录跳转到XDR。

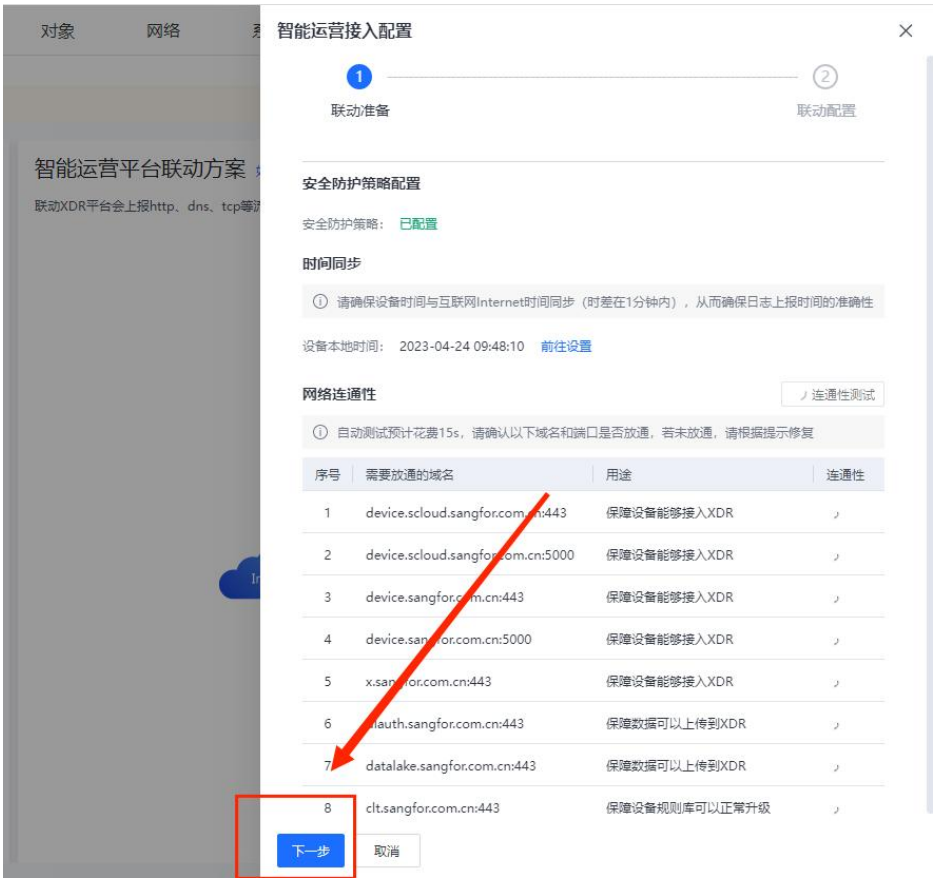


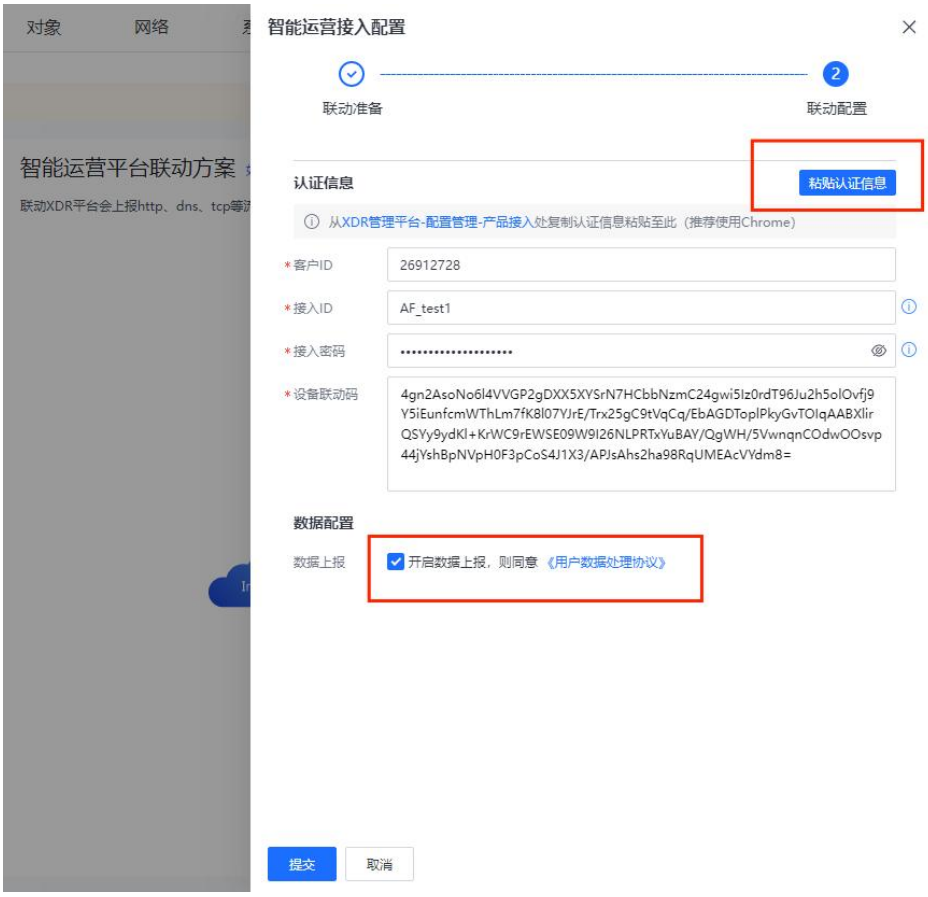
步骤2. 进入智能运营平台，[配置管理/产品接入]上，点击新增，配置AF接入账号，并复制认证信息。



步骤3. 在AF[安全运营/下一代安全体系/高级威胁检测与防护]点击<智能运营管理平台接入>。

步骤4. 点击后右侧弹出接入配置，待网络连通性测试通过后点击下一步。粘贴从智能运营平台自动复制的认证信息，并勾选数据上报功能。


对象
网络
智能运营平台联动方案
联动XDR平台会上报http、dns、tcp等
智能运营接入配置
1
联动准备
2
联动配置
安全防护策略配置
安全防护策略：
已配置
时间同步
请确保设备时间与互联网Internet时间同步（时差在1分钟内），从而确保日志上报时间的准确性
设备本地时间：
2023-04-24 09:48:10
前往设置
网络连通性
连通性测试
自动测试预计花费15s，请确认以下域名和端口是否放通，若未放通，请根据提示修复
序号
需要放通的域名
用途
连通性
1
device.scloud.sangfor.com.cn:443
保障设备能够接入XDR
2
device.scloud.sangfor.com.cn:5000
保障设备能够接入XDR
3
device.sangfor.com.cn:443
保障设备能够接入XDR
4
device.sangfor.com.cn:5000
保障设备能够接入XDR
5
x.sangfor.com.cn:443
保障设备能够接入XDR
6
auth.sangfor.com.cn:443
保障数据可以上传到XDR
7
datalake.sangfor.com.cn:443
保障数据可以上传到XDR
8
clt.sangfor.com.cn:443
保障设备规则库可以正常升级
下一步
取消


对象
网络
智能运营平台联动方案
联动XDR平台会上报http、dns、tcp等
智能运营接入配置
联动准备
2
联动配置
认证信息
粘贴认证信息
从XDR管理平台-配置管理-产品接入处复制认证信息粘贴至此（推荐使用Chrome）
*客户ID
26912728
*接入ID
AF_test1
*接入密码
*设备联动码
4gn2AsoNo6l4VVGP2gDXX5XYSrN7HCbbNzmC24gwi5Iz0rdT96Ju2h5olOvfj9
Y5iEunfcmWThLm7fK8l07YJrE/Trx25gC9tVqCq/EbAGDToplPkyGvTOlqAABXlir
QSYy9ydKl+KrWC9rEWSE09W9l26NLPRTxYuBAY/QgWH/5VwnqnCOdwOOsvp
44jYshBpNVpH0F3pCoS4J1X3/APJsAhs2ha98RqUMEAcVYdm8=
数据配置
数据上报
开启数据上报，则同意《用户数据处理协议》
提交
取消

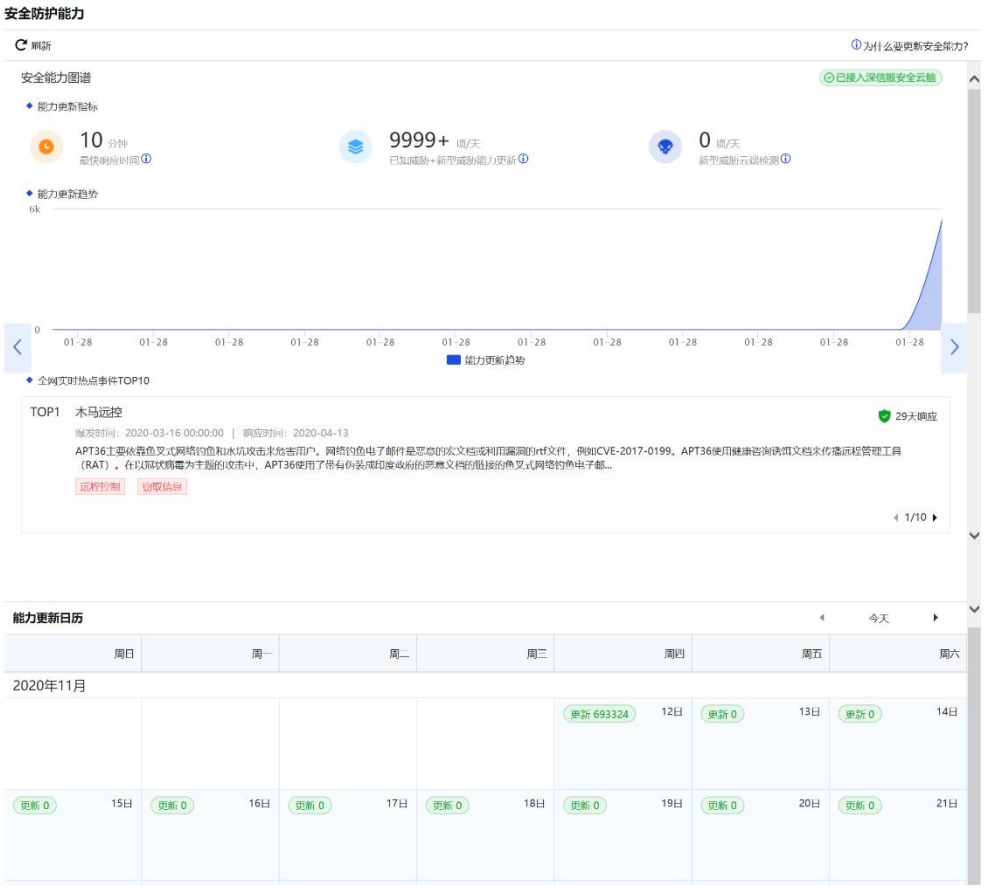
步骤5. 点击<提交>后完成智能运营平台接入。

步骤6. 登录XDR平台，在[设置/推送设置]里面设置微信推送设置。

步骤7. 微信扫描上图二维码，关注云图公众号，登录成功完成绑定，后续可通过微信公众号进行AF的简单运营。

4.7.5. 安全防护能力

安全防护能力用于展示设备的更新能力，包括安全能力图谱、能力更新指标、能力更新趋势、全网实时热点事件Top10和能力更新日历五部分内容。



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“事后风险检测能力”的实时更新。

能力更新趋势：以趋势图的方式展示持续更新的能力和相关热点事件的实时数据。

全网实时热点事件TOP10：以TOP10排名方式展示互联网安全实时热点事件。

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。

5. 监控

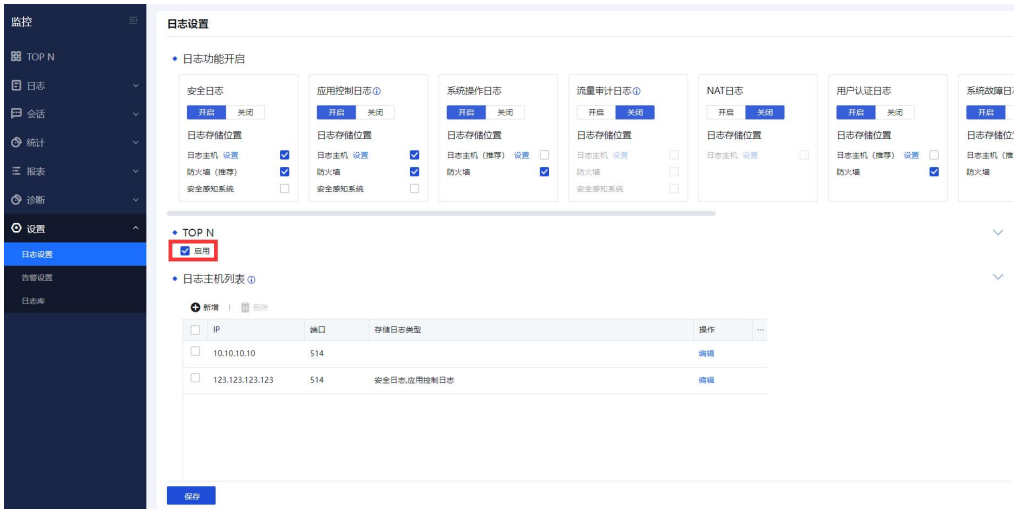
监控功能可以查看设备产生的所有日志，是AF的日志中心。同时，可以根据所产生的日志，生成对应的报表，从而提高了人员的分析效率。监控功能包括：TOPN、安全日志、行为日志、系统日志、会话、统计、报表、设置等功能

5.1. TOPN

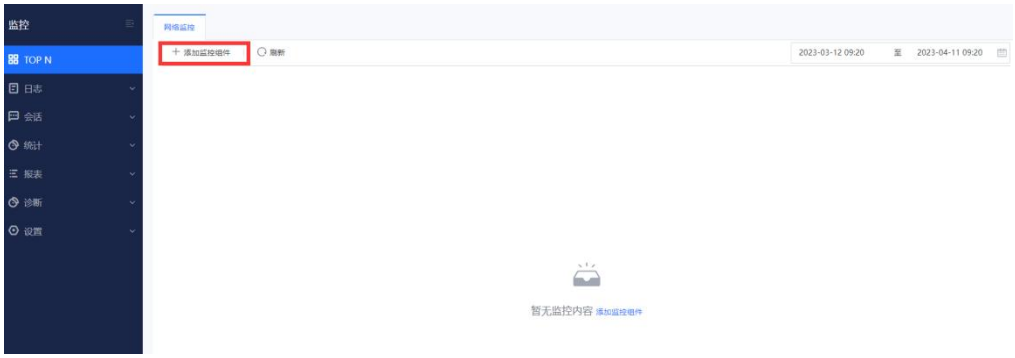
TOPN功能是按照设备、应用、源IP、目的IP和接口，依据流量和新建会话数两个维度，对网络活动进行统计排行。

配置步骤

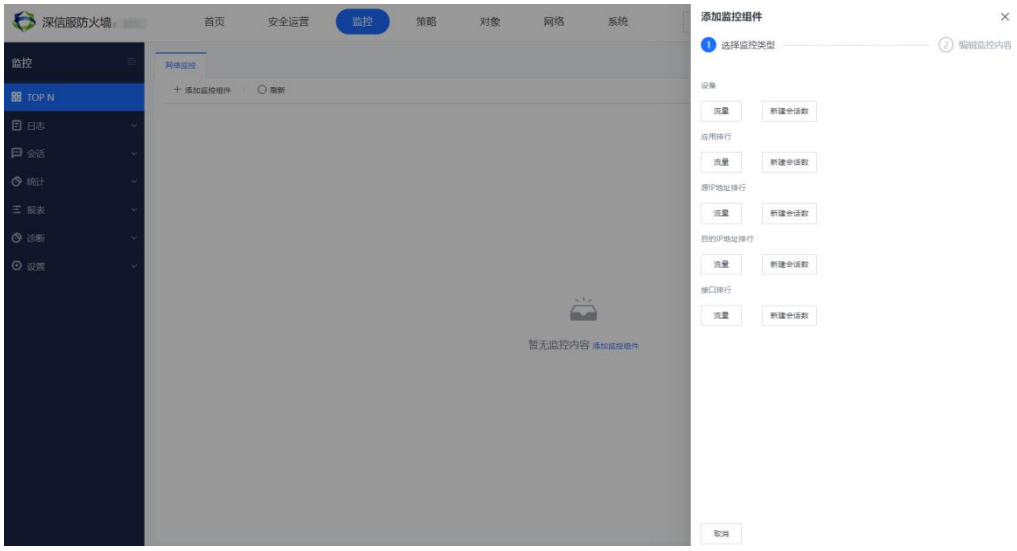
步骤1. 启用TOPN。进入[监控/设置/日志设置]TOPN选项处勾选<启用>，然后点击<保存>。



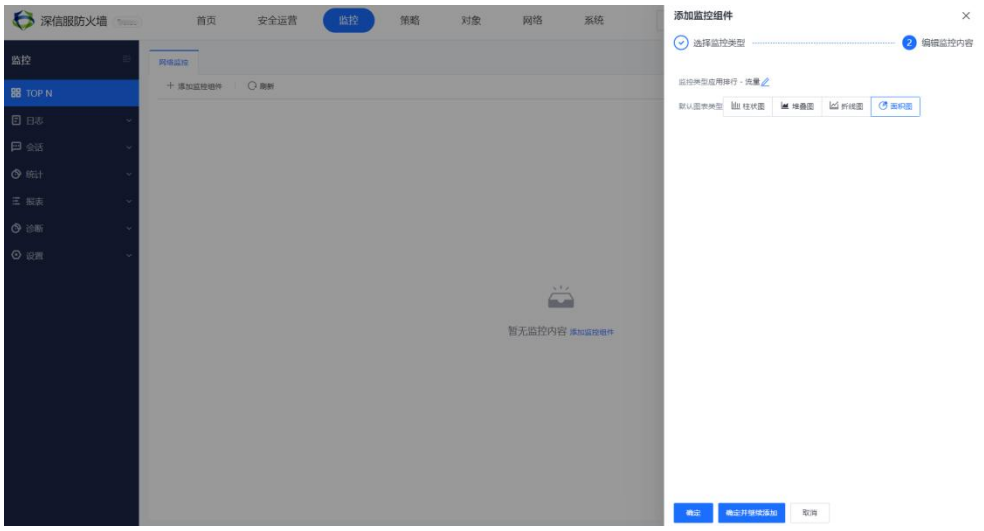
步骤2. 添加监控组件。在[监控/TOPN/网络监控]中点击<添加监控组件>。



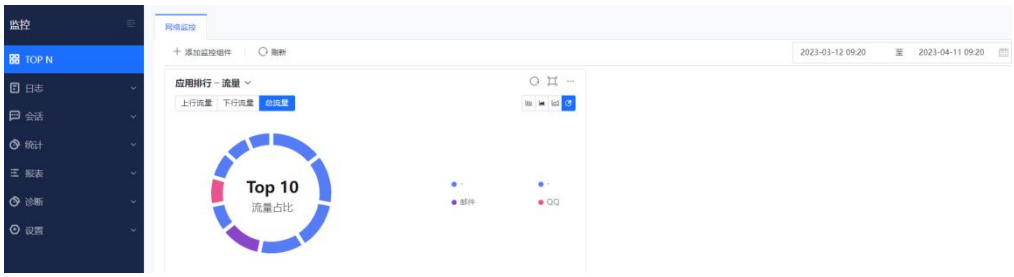
步骤3. 选择监控维度和排序维度。监控维度可选设置设备、应用、源IP、目的IP和接口，排序维度可选流量、新建会话数。



步骤4. 选择展示图的类型，可选择柱状图、堆叠图、折线图和面积图。



步骤5. 点击<确定>，完成一个监控组件的添加。如需添加其他组件重复以上步骤即可。



5.2. 日志

在安全设备运行中，会产生大量的系统、安全和运行等日志。日志功能主要记录设备产生的安全、行为和系统日志。方便用户对日志进行查看、分析。日志存储方式有防火墙（本地）、态势感知系统和syslog三种方式，防火墙默认存储日志在本地上，主要受设备磁盘大小制约。为了满足合规要求推荐防火墙加态势感知系统的形式存储日志，一是满足合规备份存储的需求，二是态势感知系统能够存储海量日志和帮助溯源分析等。

5.2.1. 安全日志

安全日志功能主要记录设备产生的安全攻击事件，包括安全防御日志和云蜜罐诱捕日志。

5.2.1.1. 安全防御日志

安全防御日志主要记录业务攻击的行为，包括Web应用防护、漏洞攻击防护、僵尸网络、网站访问、邮件安全和Dos攻击。攻击威胁触发安全策略，则会被记录安全日志，如果判断该攻击事件是误判，则可以对这个攻击事件进行添加例外排除，如果判断为真实攻击威胁，则可根据日志详情中提供的“解决方案”指引对攻击事件进行处置。可以对日志进行导出，然后进行分析或者在搜索框中输入IP/域名进行搜索对应得日志信息。

检索案例

某企业网络管理员发现Web服务器正遭受攻击，需要查看Web防护日志、确定攻击的IP和攻击使用的手段等信息。

步骤1. 点击<查询条件>，根据需求选择搜索的条件，如下图所示。

表10 日志查询条件说明

查询条件	说明
起始/结束时间	选择查询开始至结束的时间
源区域	日志来源的区域
源地址	攻击者的来源 IP

目的区域	攻击目的 IP 的区域
目的地址	攻击者攻击的 IP
日志类型	可以根据不同的日志类型进行筛选
严重等级	根据不同的安全级别进行筛选
动作	根据日志的动作进行筛选

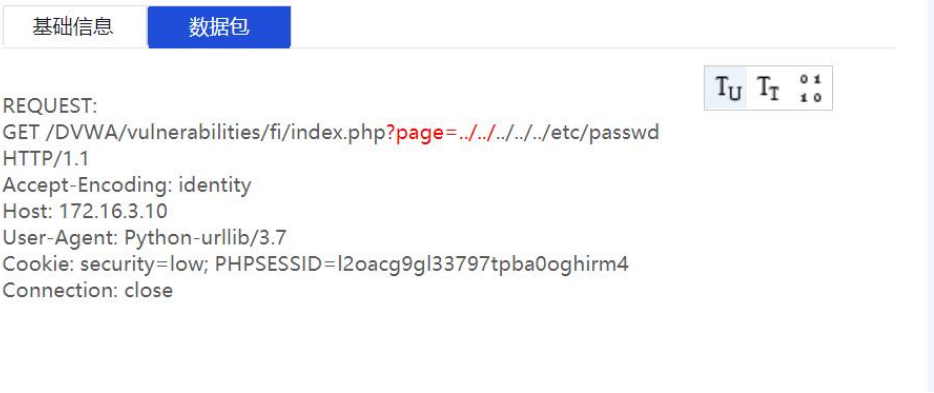
步骤2. 根据需求选择对应的时间日期，勾选Web应用防护，查看Web应用防护日志，如下图所示。

步骤3. 查看Web应用防护日志，如下图所示。

步骤4. 点击<查看详情>，查看攻击行为是否为误报，如下图所示。

基础信息：描绘该攻击行为的一些信息，如匹配的规则ID、请求方式等；

数据包：记录该数据包完整的请求信息，标红部分为攻击的特征。



可以根据查看日志的详细信息判断是否为误报，如果为误报则添加到例外。例外添加在日志最右端操作界面上，点击<更多>，选择添加例外，弹对话框。

URL：需要匹配的URL。

排除例外：对匹配上的源目IP、目的端口、规则ID进行添加例外。

仅排除参数值符合以下特征需求：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。

5.2.1.2. 云蜜罐诱捕日志

云蜜罐诱捕日志功能主要记录AF诱捕到黑客踩到蜜罐的日志，通过诱捕的形式诱惑黑客进行攻击，从而发现黑客的攻击行为。触发诱捕日志的时候会记录源IP、访问的伪装服务区地址端口、攻击次数、严重等级等信息。还可以对这些日志进行导出分析。

检索案例

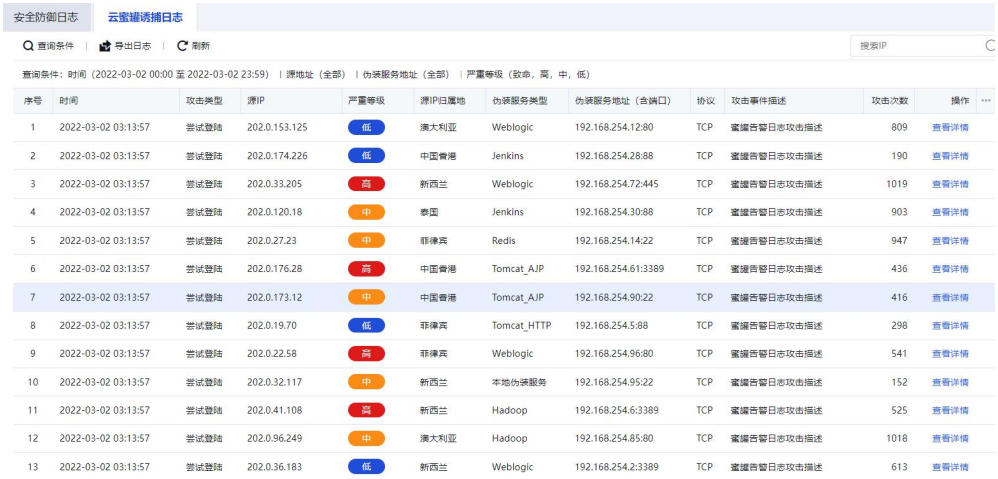
某企业互联网部署了一台AF，并开启了云蜜罐诱捕策略，对黑客的行为进行诱捕，从而及时发现黑客在对内部服务器进行攻击。现需要查看诱捕日志发现黑客的行为。

步骤1. 点击<查询条件>，根据需求进行筛选诱捕日志的信息,如下图所示。

表11 诱捕日志查询条件说明

查询条件	说明
起始/结束时间	选择查询开始至结束的时间
源地址	攻击者的来源 IP
服务地址	伪装服务的地址
严重等级	根据严重等级进行筛选

步骤2. 选择所有IP和服务地址，查看最近的诱捕情况，如下图所示。



5.2.2. 行为日志

行为日志主要记录用户/IP流量到达AF后的处理结果，应用控制日志记录能匹配的ACL信息情况。行为日志包括应用控制日志、用户登录/注销、SSL用户日志和工控审计日志。

5.2.2.1. 应用控制日志

应用控制日志一般用于查看流量匹配了什么应用控制策略，方便故障排查。

检索案例

某企业网络中，需要对某条策略进行最小化收缩，需要知道具体的访问端口。因此，在防火墙应用控制策略中开启记录日志后，在应用控制策略中进行搜索日志。

步骤1. 进入查询页面，根据需求进行源目IP等筛选，如下图所示。

步骤2. 根据搜索的结果进行判断该端口和服务是否正常，如下图所示。

步骤3. 点击<查看>可以查看日志详情，如下图所示。

说明：

应用控制策略开启的方式：

1. 在监控/设置/日志设置/日志功能开启，开启应用控制策略，勾选防火墙，如有外接设备可以选择其他的存储方式。
2. 在策略/访问控制策略/应用控制策略，选择对应得应用控制策略开启记录日志功能。

5.2.2.2. 用户登录/注销

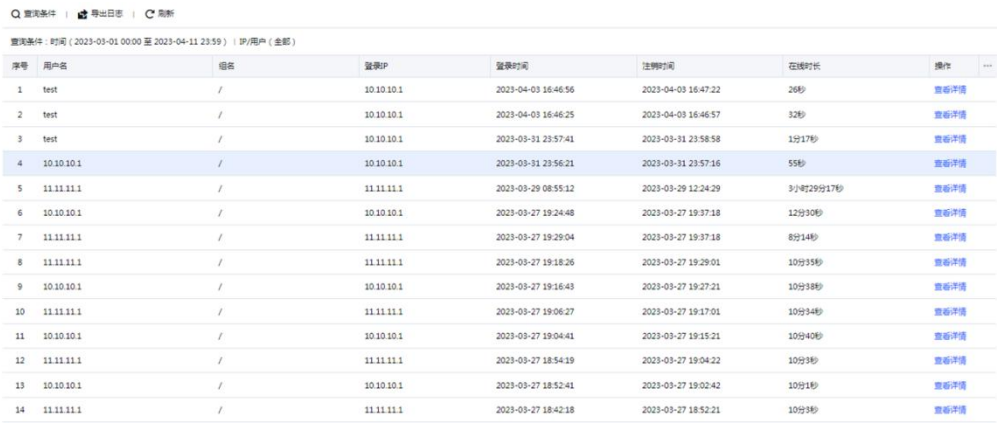
用户登录/注销主要是用于查询AF开启认证系统模块后，记录用户通过AF的认证模块的登录和注销信息。可以导出日志，进行分析。

检索案例

某企业对办公内网PC进行上网行为认证，只能通过认证的终端才能够访问互联。先需要查找用户最近的认证情况。

步骤1. 进入查询页面，根据需求对日志进行筛选，如下图所示。

步骤2. 查找结果记录了设备登录时间、注销时间和在线时长等信息，如下图所示。



序号	用户名	组名	登录IP	登录时间	注销时间	在线时长	操作
1	test	/	10.10.10.1	2023-04-03 16:46:56	2023-04-03 16:47:22	26秒	查看详情
2	test	/	10.10.10.1	2023-04-03 16:46:25	2023-04-03 16:46:57	32秒	查看详情
3	test	/	10.10.10.1	2023-03-31 23:57:41	2023-03-31 23:58:58	1分17秒	查看详情
4	10.10.10.1	/	10.10.10.1	2023-03-31 23:56:21	2023-03-31 23:57:16	55秒	查看详情
5	11.11.11.1	/	11.11.11.1	2023-03-29 08:55:12	2023-03-29 12:24:29	3小时29分17秒	查看详情
6	10.10.10.1	/	10.10.10.1	2023-03-27 19:24:48	2023-03-27 19:37:18	12分30秒	查看详情
7	11.11.11.1	/	11.11.11.1	2023-03-27 19:29:04	2023-03-27 19:37:18	8分14秒	查看详情
8	11.11.11.1	/	11.11.11.1	2023-03-27 19:18:26	2023-03-27 19:29:01	10分35秒	查看详情
9	10.10.10.1	/	10.10.10.1	2023-03-27 19:16:43	2023-03-27 19:27:21	10分38秒	查看详情
10	11.11.11.1	/	11.11.11.1	2023-03-27 19:06:27	2023-03-27 19:17:01	10分34秒	查看详情
11	10.10.10.1	/	10.10.10.1	2023-03-27 19:04:41	2023-03-27 19:15:21	10分40秒	查看详情
12	11.11.11.1	/	11.11.11.1	2023-03-27 18:54:19	2023-03-27 19:04:22	10分3秒	查看详情
13	10.10.10.1	/	10.10.10.1	2023-03-27 18:52:41	2023-03-27 19:02:42	10分1秒	查看详情
14	11.11.11.1	/	11.11.11.1	2023-03-27 18:42:18	2023-03-27 18:52:21	10分3秒	查看详情

5.2.2.3. SSL 用户日志

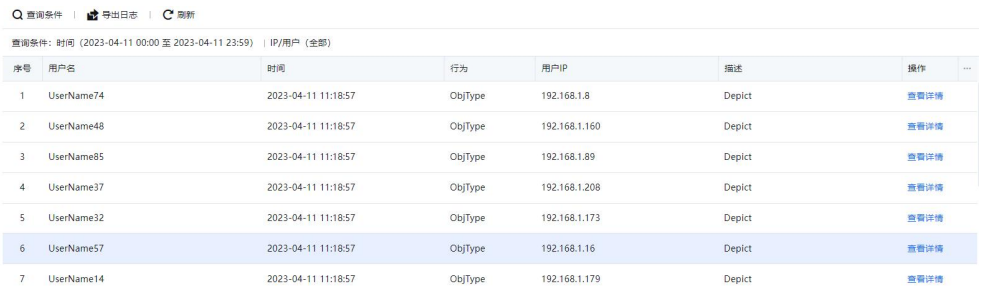
记录SSL用户的登录、注销和终端PC版本等信息，方便管理员对异常用户行为进行排查。可以进行导出SSL用户日志进行分析。

检索案例

某企业管理员，发现有用户存在异常，需要检索用户的最近登录情况。

步骤1. 进入查询页面，查找用户最近登录的情况，如下图所示。

步骤2. 查询结果可以看到登录时间、行为和用户IP等信息，如下图所示。



序号	用户名	时间	行为	用户IP	描述	操作
1	UserName74	2023-04-11 11:18:57	ObjType	192.168.1.8	Depict	查看详情
2	UserName48	2023-04-11 11:18:57	ObjType	192.168.1.160	Depict	查看详情
3	UserName85	2023-04-11 11:18:57	ObjType	192.168.1.89	Depict	查看详情
4	UserName37	2023-04-11 11:18:57	ObjType	192.168.1.208	Depict	查看详情
5	UserName32	2023-04-11 11:18:57	ObjType	192.168.1.173	Depict	查看详情
6	UserName57	2023-04-11 11:18:57	ObjType	192.168.1.16	Depict	查看详情
7	UserName14	2023-04-11 11:18:57	ObjType	192.168.1.179	Depict	查看详情

5.2.2.4. 工控审计日志

工控审计日志主要记录工控设备协议的日志，可以基于时间，IP和协议类型对的日志

进行过滤，方便各类审计需求，目前支持的协议类型：opcda，s7，s7-plus，modbus，iec104，profinetIO。

检索案例

某企业管理员，需要检索工控终端的交互信息。

步骤1. 进入查询页面，根据根据需求进行筛选，如下图所示。

步骤2. 查询结果可以看到记录时间、源IP、源端口、目的IP、目的端口、协议类型和协议详情等信息，如下图所示。


查询条件 | 导出日志 | 刷新

查询条件：时间（2023-04-12 00:00 至 2023-04-12 23:59） | 源IP（所有） | 目的IP（所有） | 协议类型（全部）

序号	记录时间	源IP	源端口	目的IP	目的端口	协议类型	协议详情
1	2023-04-12 10:19:03	202.0.36.38	41061	192.168.254.55	29789	MODBUS	协议:tcp 功能码:Read_Holding_Registers 起始地址:2 结束地...
2	2023-04-12 10:19:03	202.0.53.103	27433	192.168.254.87	50748	OPCDA	协议数据单元标识类型:REQUEST 操作类型:IOPCServer 操作码...
3	2023-04-12 10:19:03	202.0.15.195	4588	192.168.254.38	24992	S7-Plus	协议版本号:V3 操作码:Notification
4	2023-04-12 10:19:03	202.0.36.135	16387	192.168.254.58	19090	OPCDA	协议数据单元标识类型:REQUEST 操作类型:IOPCAsyncIO2 操...
5	2023-04-12 10:19:03	202.0.23.28	62617	192.168.254.29	60907	profinetIO	操作类型:PNIODevice 功能码:PNIO_OPNUM_READ_IMPLICIT ...
6	2023-04-12 10:19:03	202.0.110.109	59798	192.168.254.98	30530	MODBUS	协议:tcp 功能码:Read_Holding_Registers 起始地址:2 结束地...
7	2023-04-12 10:19:03	202.0.36.145	40612	192.168.254.78	55027	S7	协议数据单元标识类型:Job 操作类型:Read 数据类型:BYTE 数...
8	2023-04-12 10:19:03	202.0.175.82	20266	192.168.254.48	46612	profinetIO	操作类型:PNIODevice 功能码:PNIO_OPNUM_READ_IMPLICIT ...
9	2023-04-12 10:19:03	202.0.126.88	63827	192.168.254.76	33921	profinetIO	操作类型:PNIODevice 功能码:PNIO_OPNUM_READ_IMPLICIT ...

5.2.3. 系统日志

系统日志主要记录设备管理员对设备的操作日志、设备遭受攻击时的本机安全日志和本机访问控制日志。这些日志都可以导出来提供给相关人员进行分析，如下图所示。

5.2.3.1. 系统操作日志

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。

检索案例

某企业网络中，需要检索近期哪些管理员账号配置NAT的情况。

步骤1. 点击<查询条件>，对NAT的配置情况进行检索，如下图所示。

步骤2. 查看检索结果，列出了进行NAT配置的管理员账号、操作时间、主机等信息。

5.2.3.2. 本机安全日志

AF自身有抵御渗透攻击的功能，当本机遭受到恶意攻击时，可以查看本机安全日志进行分析，该日志记录AF被攻击的详情信息。

检索案例

某企业中需要对本机安全进行防护，而管理员需要周期性的查看设备是否被攻击，因此需要查看所有的本机安全日志，确定设备是否存在异常。

步骤1.点击<查询条件>，根据需求对日志进行筛选，如下图所示。

步骤2.查看具体的攻击信息，如下图所示。

步骤3.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。

说明：

本机安全日志开启的方式：

1. 在策略/安全策略/DOS/DDOS 防护，选择本机 DoS 防护，勾选启用。
2. 选择扫描攻击类型、DOS/DDOS 防护，并勾选记录日志等功能。

5.2.3.3. 本机访问控制

AF有对自身的访问控制策略，本机访问控制用于终端访问AF所匹配的访问控制策略，

可以根据日志排查终端访问AF匹配了那条策略等。

检索案例

某企业中需要查看有哪些终端访问AF，并确定是否为正常的访问关系。

步骤1. 点击<查询条件>，根据需求对日志进行筛选，如下图所示。

步骤2. 查询结果可以了解具体访问的源目IP等信息，点击<查看详情>，可以查看到具体的信息，如下图所示。

说明：

本机访问日志开启的方式：

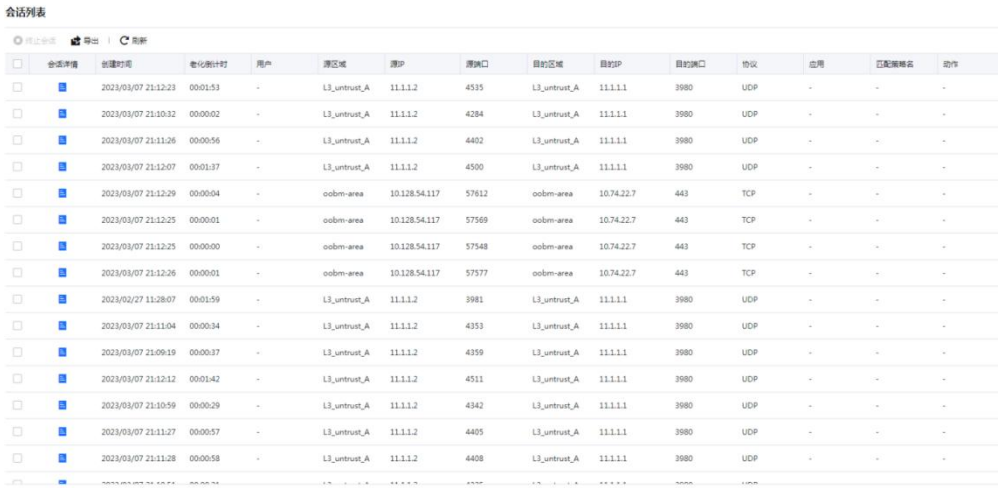
1. 在监控/设置/日志设置/日志功能开启，开启本机访问控制，勾选防火墙，如有外接设备可以选择其他的存储方式。
2. 在策略/访问控制/本机访问控制，根据需求对对应的策略进行勾选记录日志。

5.3. 会话

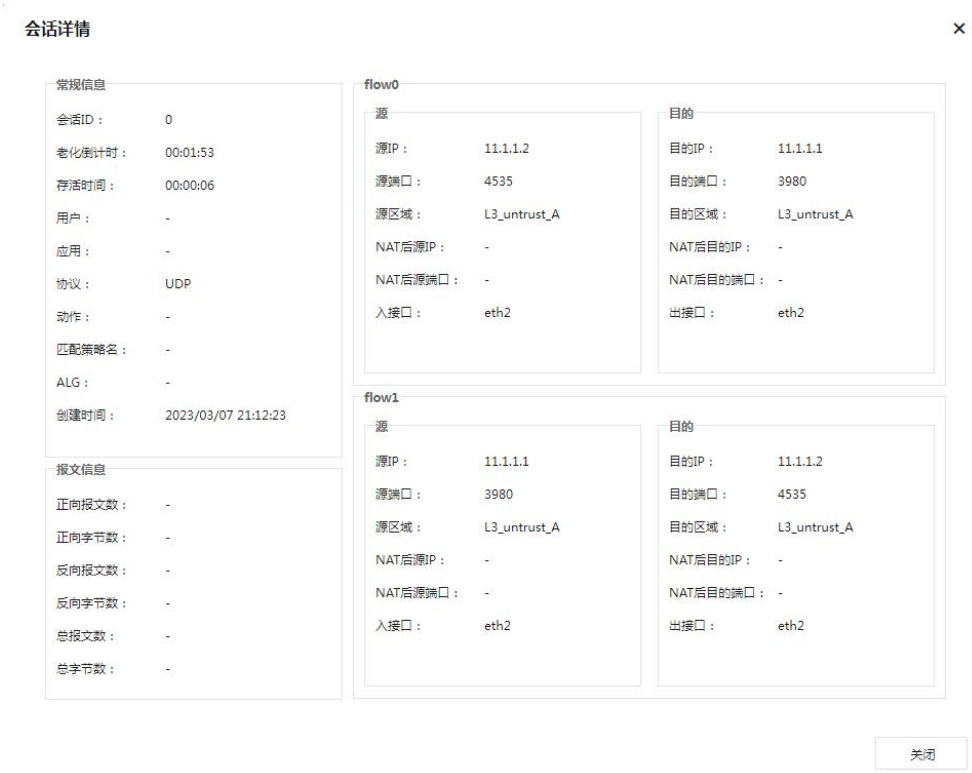
会话功能主要记录业务流量所产生的会话数、产生的流量大小和触发异常的流量。并对会话数进行排行区分IP所创建的会话数。会话功能包括：会话列表、流量排行、异常流量、会话排行和流量管理状态。

5.3.1. 会话列表

会话列表用于展示经过防火墙建立的每条会话信息，支持实时会话查询，可多维度进行会话条件筛选，并支持批量导出及批量终止异常会话，界面如下。



点击会话详情下每条会话的按钮，可以查看具体会话信息，界面如下。



5.3.2. 流量排行

流量排行主要根据用户、应用和IP对流量进行统计，包括用户流量排名、应用流量排名、IP流量排名和IP流量趋势。

5.3.2.1. 用户流量排行

用户流量排行主要对通过上网认证的用户统计其流量进行排名，即显示在线用户的使用带宽的情况，界面如下。

用户流量排名查看案例

某企业网络中，管理员需要查看sangfor用户在办公时间访问那些应用。

步骤1. 点击<过滤条件>，可以指定用户流量排名的过滤条件。如下图所示。

选择线路：选择具体需要查看的线路。

应用类型：用于指定需要查看是应用服务。

过滤对象：过滤对象是用来设置具体的用户或者IP。

步骤2. 查看检索结果，如下图所示。

根据用户的总流速进行排名来显示内容分别包含：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。点击<冻结>，用于将对应的用户冻结上网；在获取机器名：点击<获取>，用来获取对应用户计算机名；在流量构成：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。

步骤3. （可选）冻结用户上网，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，如下图所示。

步骤4. （可选）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<已冻结用户>，此时会跳转到在线用户管理的页面，如下图所示。

在这里找到被冻结的用户，选择该用户点击<解冻>即可。

5.3.2.2. 应用流量排行

应用流量排行用于统计业务流量经过设备实时的应用流量排名情况，可以查看当前业务流量的应用统计，也可以根据过滤条件进行筛选，界面如下。

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。

⚠ 注意:

1.应用流量排行支持 IPv6 环境中的应用流量统计排行。
2.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.应用流量排行开启需要在日志设置中开启控制日志开关。

5.3.2.3. IP 流量排行

IP流量排名用于显示在线IP的使用带宽情况，如下图所示。

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，显示该IP具体的应用流量。

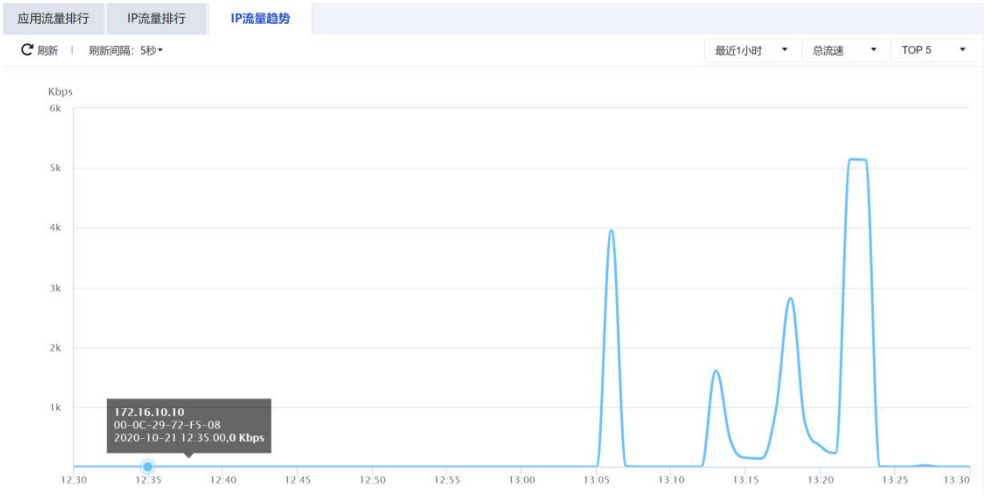
点击<刷新间隔：5秒>用于设置页面上的排行刷新时间间隔；

点击<立即刷新>可以立即进行刷新。

IP流量排行支持查看IPv6环境中的IP地址流量排行情况。

5.3.2.4. IP 流量趋势图

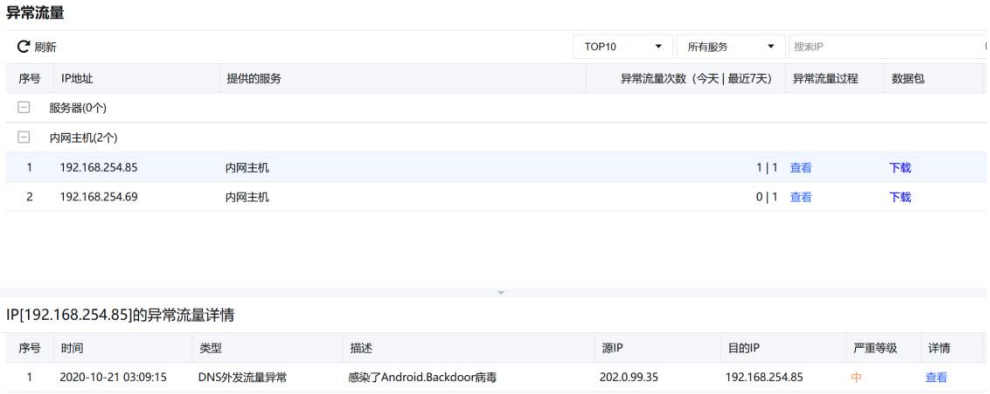
IP流量趋势图主要用于统计IP的流量趋势情况。



如图，根据IP的最近流速的趋势显示Top5或者Top10的IP。

5.3.3. 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，如下图所示。



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、描述及详情的信息。

5. 3. 4. 会话排行

会话排行用于查看业务流量通过AF设备时，创建的会话数情况，并可以根据IP进行会话排名和对会话进行查询等。

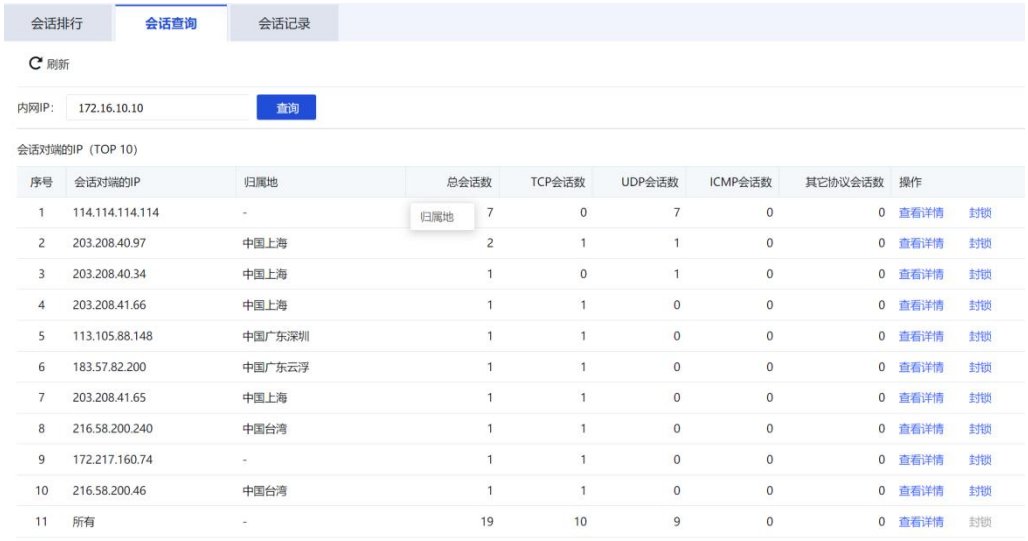
5. 3. 4. 1. 会话排行

会话排行用于查看业务流量通过AF设备时，创建的会话数情况，界面如下。

点击<查看详情>即可切换到[会话查询]页面查看该IP的具体会话信息，如下图所示。

5.3.4.2. 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。



点击<查看>，可以查看会话详情，如下图所示。

点击<封锁>，可以封锁会话IP，如下图所示。

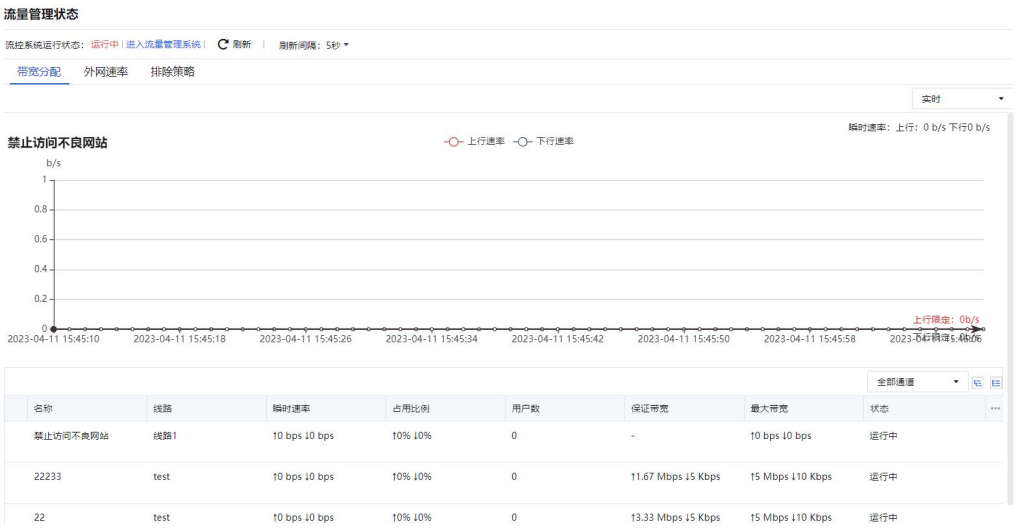
5. 3. 4. 3. 会话记录

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。

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。

5.3.5. 流量管理状态

流量管理状态是在启用流量管理系统后才会显示的页面，用于展示流量管理系统下的通道和流量情况，如下图所示。

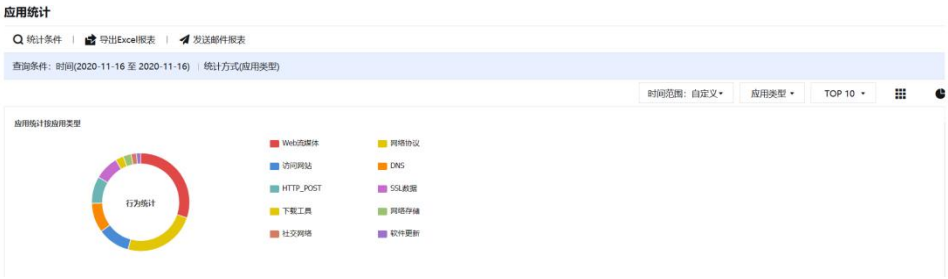


5.4. 统计

统计功能主要是统计业务的流量数据，并根据业务流量进行识别应用，来对应用的类型进行分类和排名。从而能够快速的发现业务中存在哪些应用，并查看这些应用触发的流量的情况。

5.4.1. 应用统计

应用统计主要用于对业务流量进行识别对应的应用，并根据这些应用进行排名。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。

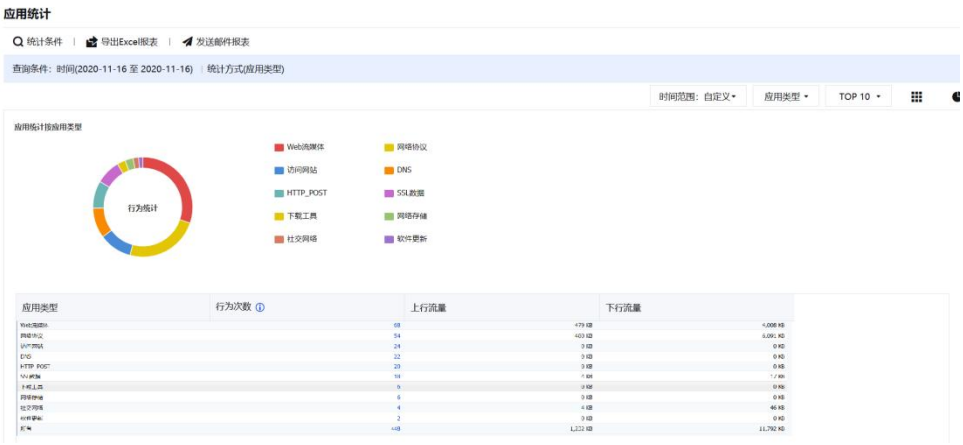


应用统计查询案例

某企业网络中，管理员需要对应用流量进行统计分析来了解哪些占用的带宽比较大从而知道哪些应用占用较大的带宽。

步骤1. 点击<统计条件>，根据需求进行筛选应用，如下图所示。

步骤2. 查看查询结果，列出哪些应用行为次数最多，如下图所示。



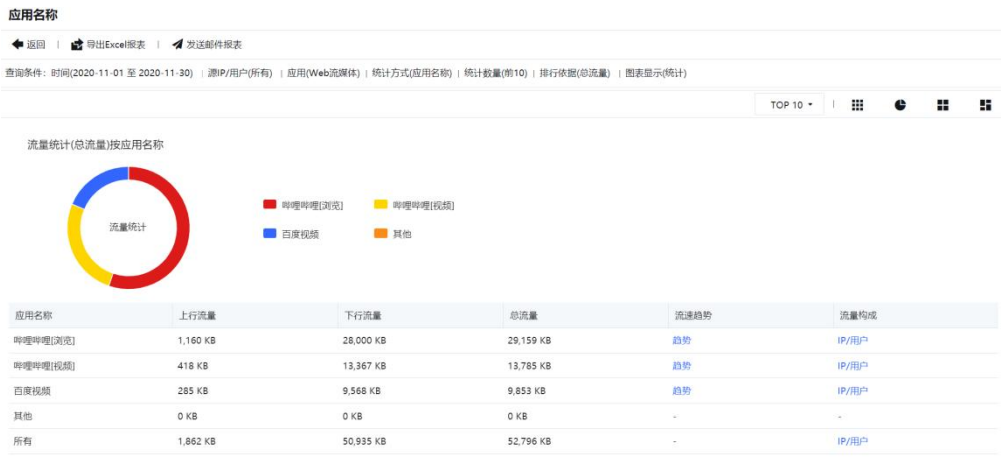
步骤3. 点击<行为次数>，可以查看到该应用所触发应用控制日志。

说明：

应用统计需要对应用控制策略中的策略进行勾选日志记录，才能够进行记录到。

5.4.2. 流量统计

流量统计用于统计应用的流量，并根据应用触发的流量进行排名。从而可以更加直观的查看哪些应用所触发的流量最多，哪些最少，并能够快速区分业务中存在哪些流量。

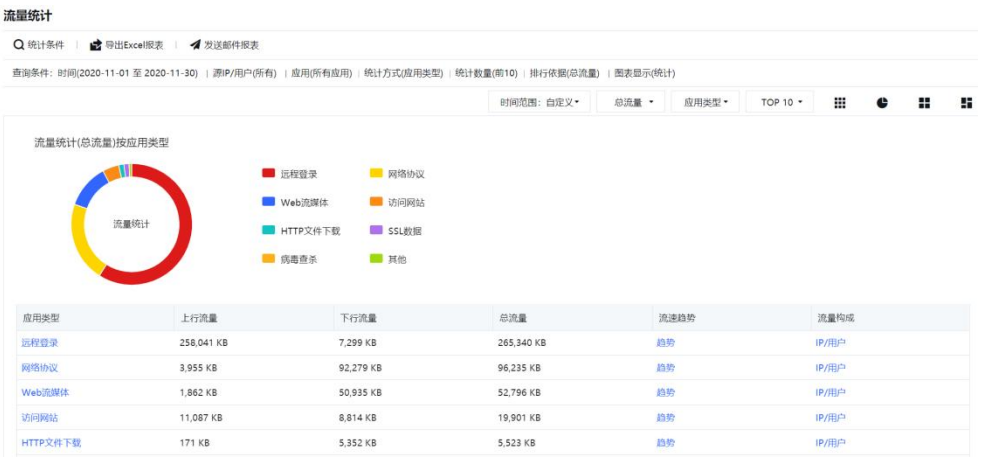


流量统计查看案例

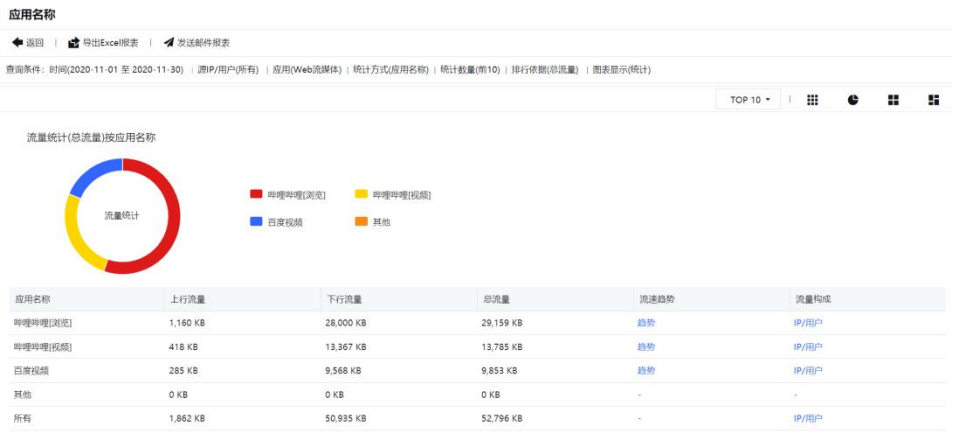
某企业管理员，需要经常性的查看业务流量中的应用占比，查看到Web流媒体类型的应用使用较多的流量，需要对该流量进行分析。

步骤1. 根据需求设置制定的条件，如下图所示。

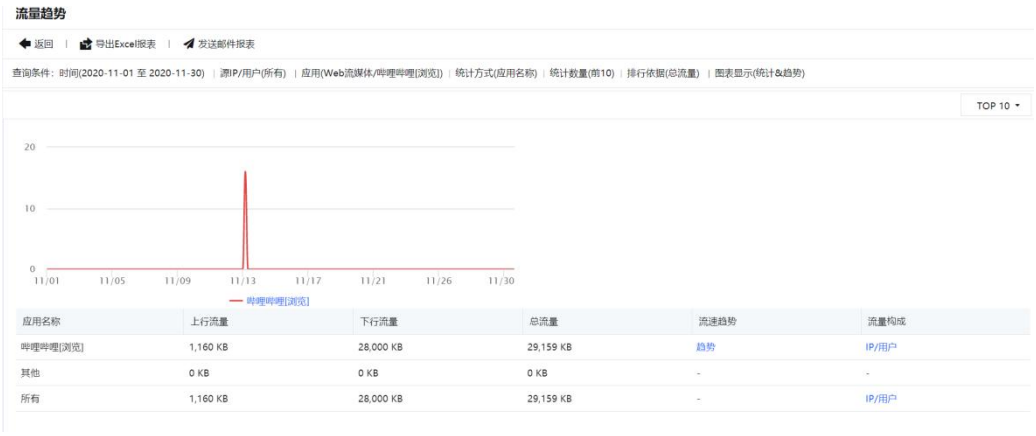
步骤2. 查看查询结果，可以查询寻到应用类型、上下流量和总流量等，如下图所示。



步骤3. 点击<Web流媒体>，从而查看具体的应用占比和流量大小，如下图所示。



步骤4. 点击<趋势>，可以查看到具体的流量趋势图，如下图所示。



步骤5. 点击<IP/用户>，可以查看具体的IP访问该应用，从而快速定位到具体的人员，如下图所示。

说明：

流量统计功能启用步骤：

1、在对应的接口中，需要勾选 WAN 属性。

2、需要在日志功能中，勾选流量审计日志。

5.5. 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：安全风险报表、报表订阅。

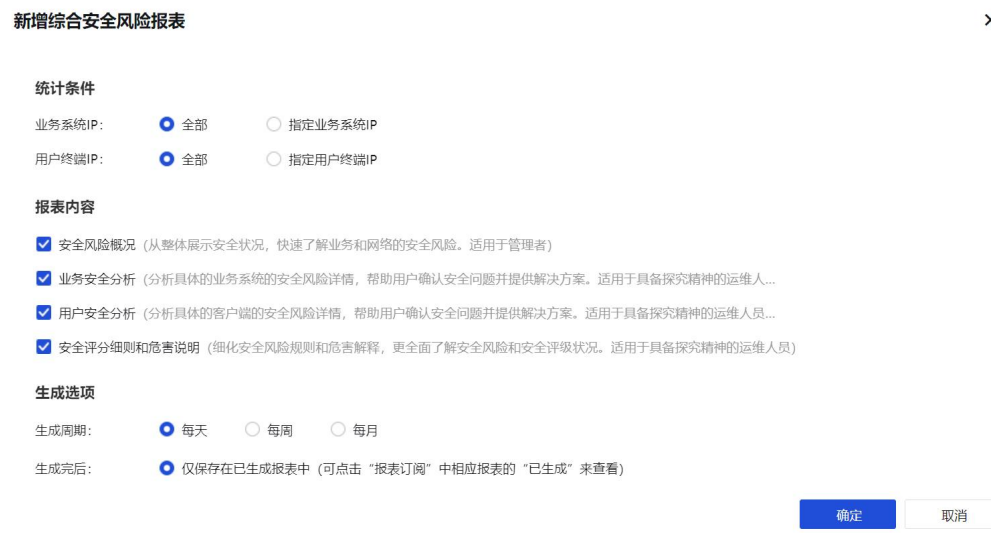
5.5.1. 安全风险报表

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。如下图所示：

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。

5.5.2. 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。其中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。



报表生成设置：可以根据设置生成报表生成的时间等，如下图所示。

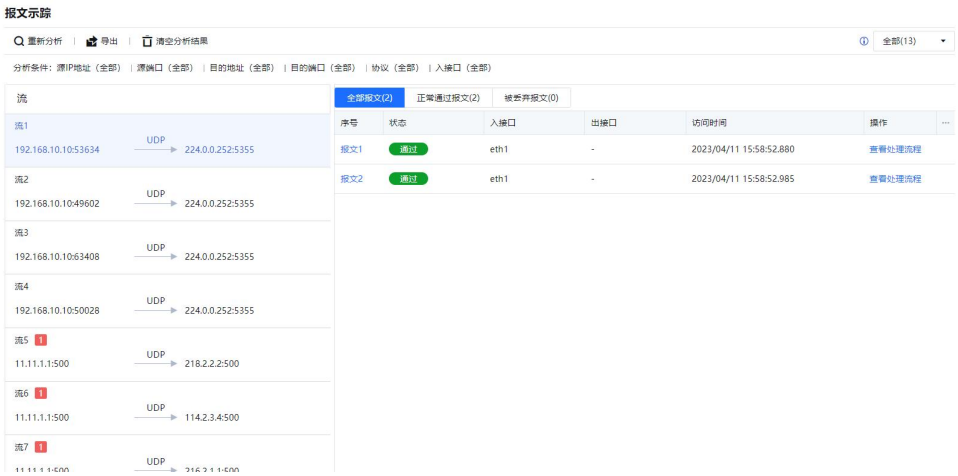
5.6. 诊断

诊断功能主要用于排查经过防火墙的数据包详情，主要包括报文示踪功能。

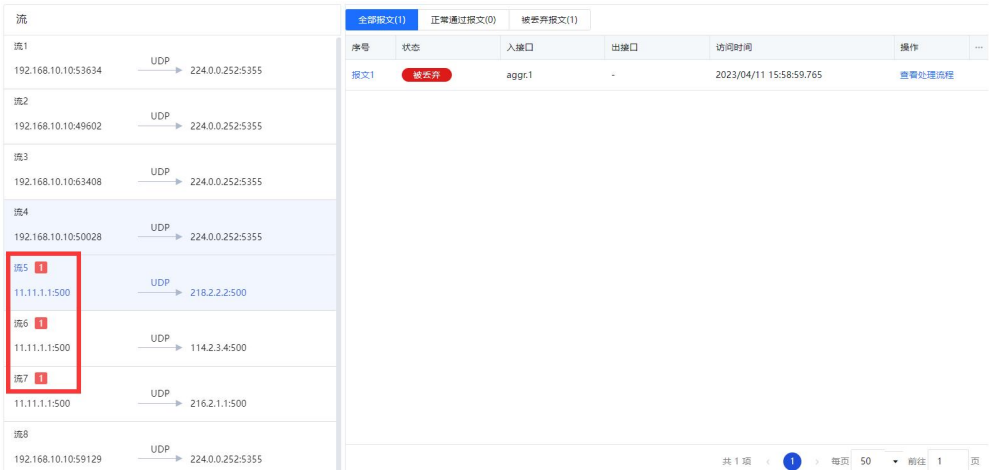
5.6.1. 报文示踪

报文示踪功能主要用于排查报文处理流程和数据包丢包原因，如下图所示。

设置好分析条件后，点击<开始分析>，会展示具体报文信息，如下图所示。



有被丢弃的数据包，会显示红色图标，同时显示被丢弃的数量，如下图所示。



点击<查看处理流程>可以查看具体数据包经过防火墙各个模块的处理情况，如有被丢弃会显示出在具体哪个模块丢包以及丢包可能原因，如下图所示。

5.7. 设置

设置功能主要对日志存储功能进行设置，并对日志是否告警配置等，是一个日志功能开关的集合。

5.7.1. 日志设置

日志设置功能主要控制设备日志的启停，并控制着设备产生的日志存储到第三方设备上。从而满足日志存储的合规要求。

5.7.1.1. 日志功能开启

日志功能开启后，设备才能够记录日志到指定的位置，如日志主机、防火墙、安全感知系统。可记录安全日志、应用控制日志、系统操作日志、流量审计日志、NAT日志、用户认证日志、系统故障日志、SSL VPN用户日志、本机访问控制日志和工控设计日志等。个别默认是关闭的，如果需要开启，需要在页面中勾选相应的选项开启。页面如下。

默认推荐只开启安全日志存储到本地，如需开启其他日志，可以根据实际需求进行修改。应用控制日志、流量审计日志、NAT日志、本机访问日志产生的量都较大，如需开启建议使用第三方存储设备进行存储。

5.7.1.2. TOPN

勾选启用后，可在[监控/TOPN]页面中进行设置。

5.7.1.3. 日志主机列表

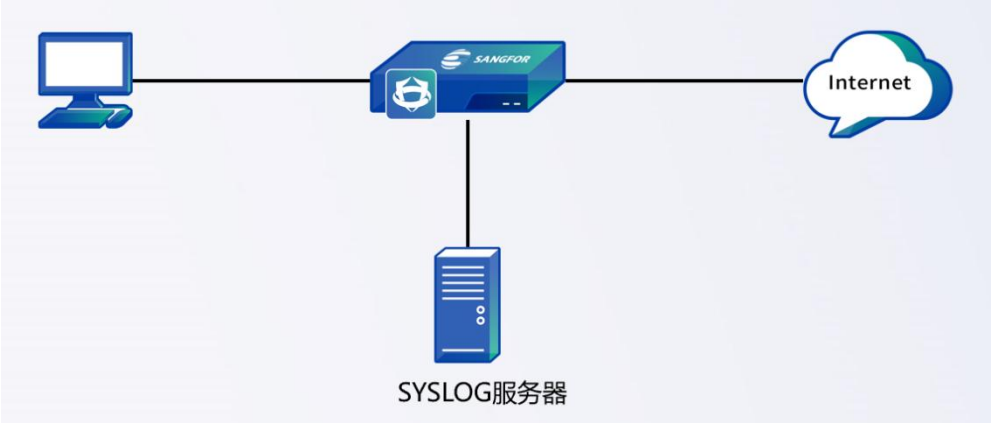
在安全设备运行中，会产生大量的系统、安全和运行等日志。而安全设备本身的存储空间无法满足日志的存储，易造成日志覆盖或者丢失，导致无法进行攻击溯源分析和

满足监管要求。因此，安全设备与Syslog服务器对接成功后，安全设备发送日志给Syslog服务器，从而减轻了安全设备的日志存储压力和满足监管的合规要求。

Syslog用于将设备日志发送到Syslog服务器进行存储，需要设置Syslog服务器的IP和端口信息。

配置案例

某企业互联网出口，部署了一台AF。为满足监管要求，需要把安全日志发送到日志服务器上进行存储，且该服务器只能接收UDP514的数据包。



步骤1. 开启安全日志通过syslog的形式发送给日志主机，如下图所示。

点击<设置>，可以在此直接添加日志主机，同时可以选择最小日志级别，如下图所示。

步骤2. 配置日志主机syslog服务器，并以UDP514的形式发送日志给日志服务器，在日志主机列表点击<新增>，选择需要同步的安全日志，可以设置多个syslog服务器，如下图所示。

步骤3. 查看AF产生安全日志,查看日志详情，并是否把日志发送给syslog服务器，如下图所示。

步骤4. 日志能够发送到syslog服务器。

说明：

1.SYSLOG 仅支持 UDP 方式连接，UTF-8 的编码方式。

2.SYSLOG 服务器最多支持同时接入 5 个。

5.7.1.4. 防火墙日志设置

用于设置设备存储日志的自动删除选项，页面如下。

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。

⚠ 注意：

已删除的日志无法找回，建议增加 syslog、安全感知系统等进行日志备份

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。

日志导出限制：允许导出的日志条数，导出的日志过多会消耗大量内存和CPU等资源。

5.7.1.5. 安全态势感知平台和全流量威胁分析系统设置

该功能主要用于设置设备与安全感知系统和全流量威胁分析系统联动，联动后AF的日志会同步的态势感知平台上，态势感知平台在进行日志进一步溯源分析等。态势感知平台也可以下发指令给AF，AF收到指令后执行对应的动作。AF与态势感知系统联动配置如下图所示。

服务器地址：是安全感知系统和全流量威胁分析系统的地址。

通讯端口：默认4430端口。

同步账号：接入安全感知系统和全流量威胁分析系统的账号信息。

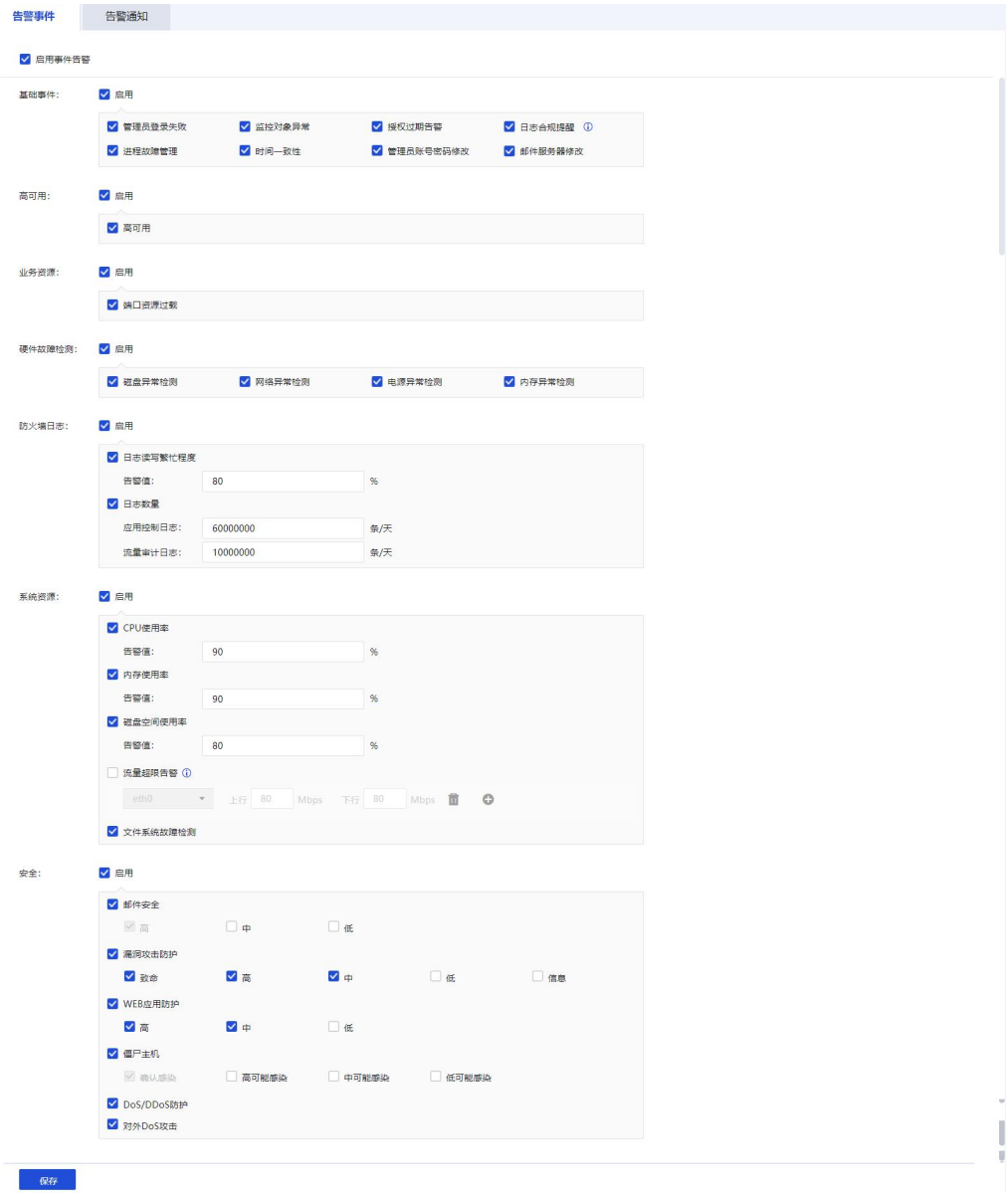
密码：接入安全感知系统和全流量威胁分析系统的密码信息。

5.7.2. 告警设置

当设备发生异常行为或者存在攻击行为进行时，以邮件和短信的方式进行告警，从而能够让客户快速感知到目前的网络情况。

5.7.2.1. 告警事件

选择需要开启告警的事件，勾选即开启告警，如下图所示。



5.7.2.2. 告警通知

对触发告警的事件，根据设置的通知方式进行告警。目前支持邮件告警和短信告警，如下图所示。

邮件通知设置

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。

短信通知设置

用于设置将告警信息以短信的形式发送到管理员手机上。AF的短信告警仅支持用户登录权限访问功能。

短信模板ID：需要复制短信模板到服务商通过审核，获取ID后填写。

短信模板：配置完短信服务器后填写短信模板。

手机号码：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。

5.7.2.3. 邮件告警设置案例

某企业互联网出口中，部署了一台AF，先需要对高危的安全事件进行邮件告警，从而使管理员能够快速的响应。

步骤1. AF能够访问互联网，且配置邮件服务器，如下图所示。

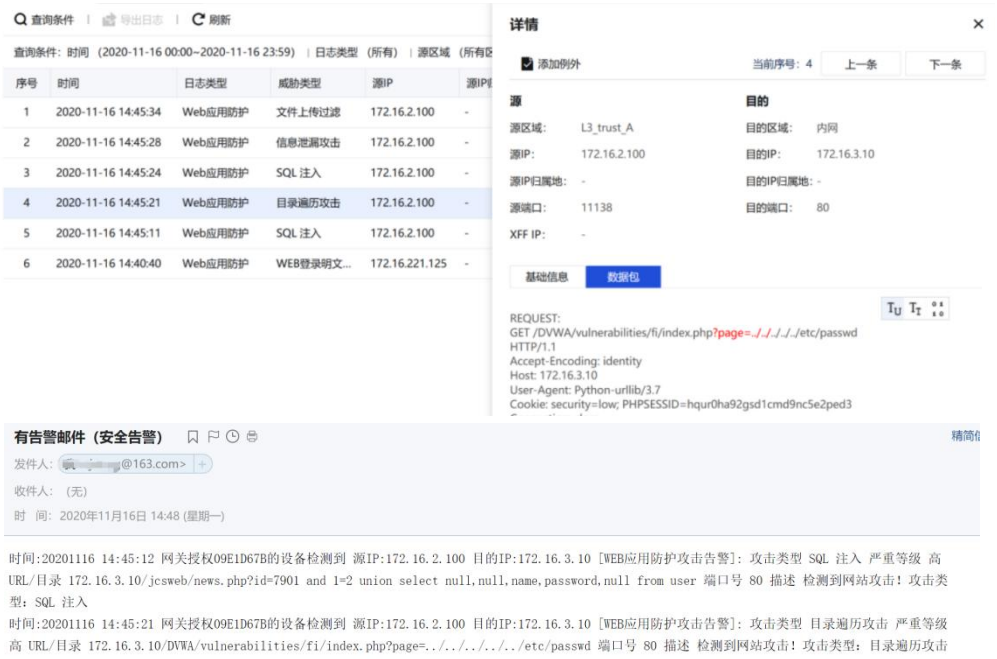
⚠ 注意：

若您配置的发件邮人邮箱已启用第三方客户端授权码，SMTP 的密码框输入授权码。

步骤2. 在[监控/设置/告警事件]开启告警功能，并对安全事件只勾选高危的功能，如下图所示。

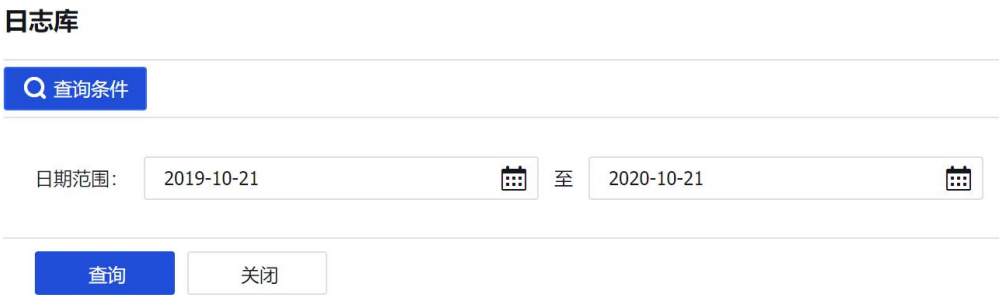
步骤3. 设置邮件告警，并填写对应的告警邮箱。

步骤4. 查看遭受攻击后，收到的告警内容，如下图所示。

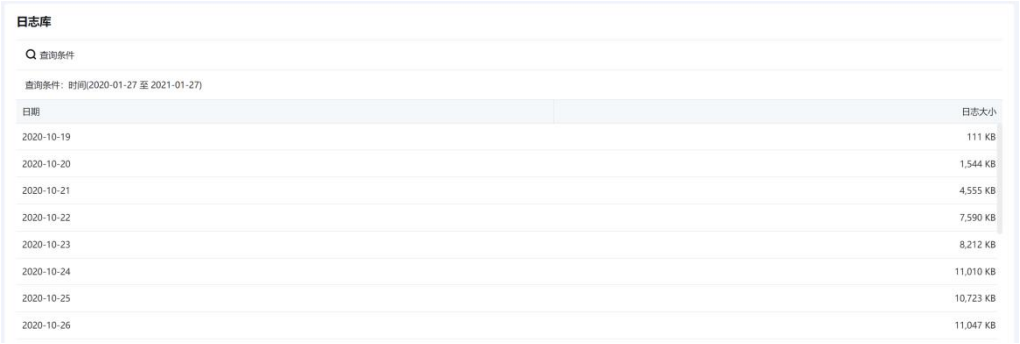


5.7.3. 日志库

用于查询指定时间内的日志文件大小。



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。



6. 策略

策略作为设备的主要功能模块，提供完整的安全防御体系，确保安全防护不存在短板，针对经过设备的数据包根据策略进行检测和控制，包括访问控制、地址转换、安全策略、解密、流控、认证和页面定制等功能模块。

6.1. 访问控制

访问控制主要是通过规则特征去控制经过设备的一些报文进行一系列的控制。包括应用控制策略、地域访问控制、本机访问控制、连接数控制、网页关键字检测和协议命令控制等功能模块。

6.1.1. 应用控制策略

应用行为控制常用于企业内部对内部用户的上网（HTTP）行为、FTP行为和IM行为、工具类等行为进行精细化控制。在企业内部通常需要对内网用户的上网的行为进行管理，不同的用户访问网络资源需要不同的权限，同一用户在不同的时间段具有的权限往往也不同。AF的应用控制能满足以上的需求。

该模块的设置需要引用[网络]里面的区域和[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。

在[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。

6.1.1.1. 策略配置

策略配置用于新增、修改和调整应用控制策略。鼠标移到策略组名上，相应策略组后方显示[...]的标示，点击该标识，管理员可对策略组进行相应编辑。

表12 策略配置功能参数说明表

操作	说明
删除	可删除当前的策略组。
编辑	可重新编辑该策略组名称。
上方插入	可以当前策略组上方插入一条新的策略组。
置顶	把当前策略组的顺序移至最上方。

上移	可对当前策略组的顺序上移一条。
下移	可对当前策略组的顺序下移一条。
移动到自定位置	可把当前策略组顺序移动到一条指定的位置。

在策略配置页面点击<新增>，进入[新增应用控制策略]页面，设置如下。

基础信息设置：

名称：定义规则名称。

状态：设置该策略为启用或者禁用状态。

描述：非必选项，添加规则的描述。

策略组：定义规则所属的策略组。

策略位置：设置策略的优先级，可以设置该策略在某条策略之前或者之后。

标签：非必选项，定义规则的标签，可用做显示区域，及过滤筛选时使用。

源：

源区域：选择需要控制的数据的源区域，默认为“any”区域，即代表所有区域。

源地址：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：

目的区域：选择需要控制的数据的目的区域。默认为“any”区域，即代表所有区域。

目的地址：选择需要控制的数据的目的IP组。如果要针对内网用户上外网数据进行控制，则此处目标IP一般可以选择“全部”。

服务：选择需要做控制的服务。该处是调用[对象/服务]中定义的服务。

应用：选择需要做控制的应用。该处是调用[对象/内容识别库/应用识别库]里的应用特征。

⚠ **注意：**

服务和应用都需要填写，两者都满足才能匹配上该策略。

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>进去[高级选项]界面。如下图所示。

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。

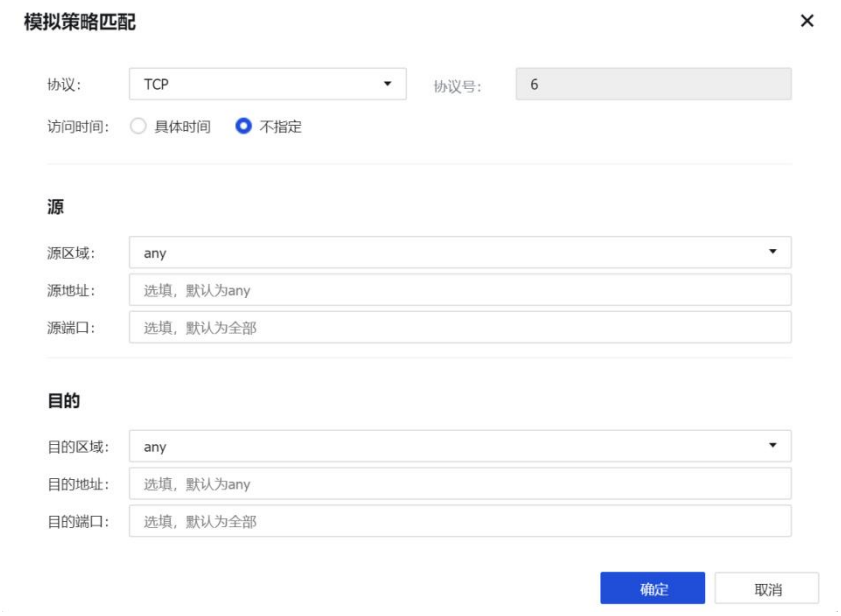
日志选项：默认未开启应用控制日志记录，需要提前在[系统/日志设置]中，开启“应用控制日志”，同时选择保存应用控制日志的存储位置。勾选“记录日志”，则把控制行为记录到所选择的存储位置中。应用控制日志过大将导致系统磁盘读写缓慢，建议使用外置数据中心或syslog存储该日志。

点击<更多操作>选择[辅助工具]可配置失效策略检查、模拟策略匹配、标签管理和策略变更原因记录。

标签管理：可以设置标签的相关操作，包括新增、编辑和删除等操作。如下图所示。

策略变更原因记录：启用后，将在新增或修改策略时显示变更原因输入框，方便记录变更原因，未启用则只自动记录变更内容和类型，点击<前往查看>会进入策略生命周期管理页面。

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。



失效策略检查：可以检查已失效的策略。

实时冲突策略检查：在新增、修改和移动策略时，实时对策略的冲突进行检测并提醒。该功能启用后，可能在策略数量过多时造成页面加载延迟。

应用控制策略配置案例

某企业不允许研发部门的人员在上班时间使用IM聊天工具，当有研发人员使用IM工具，设备会拒绝，可在AF上配置应用控制策略。

操作步骤

步骤1.在[策略/应用控制策略]点击<新增>进入[应用控制策略]界面。

基础信息的相关参数配置如下：

名称：不允许使用 IM 工具

状态：选择启用

描述：可自定义，如“不允许研发部门的人员使用 IM”

策略组：选择默认策略组

策略位置：设置优先级在限制下载 P2P 之前。

标签：可自定义，也可选择默认。

步骤2.源区域选择自定义的内网区，区域的定义可以参考区域配置，源地址选择

自定义的研发部，用户组的定义可以参考用户管理配置。

⚠ 注意：

当前策略中选择了用户组，需要启用认证功能，且该用户已配置相关认证策略，如未启用认证策略，会导致策略不生效。

步骤3.配置目的信息，目的区域选择自定义的外网区， 目的地址选择全部，服务选择any，应用选择IM。

步骤4.生效条件设置，动作选择拒绝，生效时间选择自定义的上班时间。如需要查看日志，需要在高级选项的设置，勾选记录日志。

步骤5.点击<确定>完成配置。

步骤6.当研发部门的人员使用终端登陆IM工具，会出现网络异常，不能正常登陆该IM工具，访问其他网址不受影响。

步骤7.可在[监控/日志/行为日志]中可查询到拒绝的日志的详细信息。

6.1.1.2. 策略优化

策略优化功能，针对当前所配置的应用控制策略，进行系统分析，给出目前策略配置不合理的相关提示信息。在大批量应用控制策略的情况下，可以快速优化当前的应用

控制策略，以最小范围放通为原则，做到精细化的管控目的。

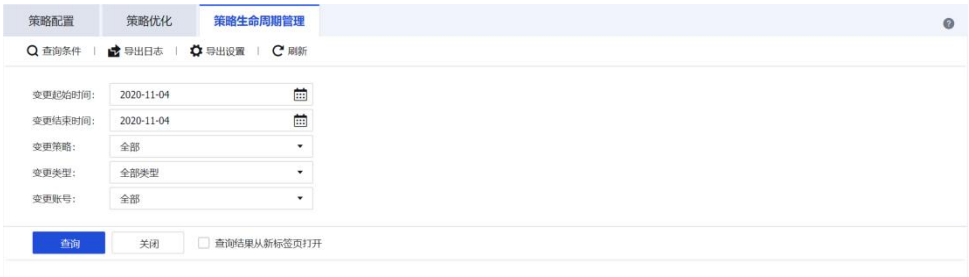
点击<开始分析>。系统自动进行策略的优化分析，分析结束后，得到如上图的当前风险列表。

点击待优化事件操作的“忽略”。选择对该事件的一定时间内的忽略，即指定时间内，不再检测该条应用控制规则的事件。

点击待优化事件操作的“查看详情”。可弹出关于该事件的具体详情描述，是解决方案建议，如下图所示。

6.1.1.3. 策略生命周期管理

策略生命周期管理，即对应用控制策略在指定查询范围内的操作，进行变更的记录和展示，方便对日常的维护工作有相应的记录和溯源。



变更起始时间：设置变更查询的起始时间。

变更结束时间：设置变更查询的结束时间。

变更策略：设置变更查询的指定某条应用控制策略，默认查询全部策略的变更情况。

变更类型：设置变更查询的类型，包括“新增”、“编辑”、“删除”三种类型。

变更账号：设置查询指定账号的变更操作，默认查询全部账号的变更情况。

管理员可以对以上的选项进行设置后，点击<查询条件>会显示如下内容。

导出日志：可对变更查询的结果，进行导出，导出为.cve格式的表格。

导出设置：可设置要导出日志的展示内容，默认导出是全部，可根据需求自行设置不需要导出的项目。

日志详情：对查询出来的变更记录，点击“操作”列的查看详细，可弹出该变更的详细情况，如下图所示。

6.1.2. 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。管理员可进行如下操作。

表13 地址转换功能参数说明表

参数	说明
新增	可以新增地域访问控制策略
排除列表	可以添加不受地域访问控制的 IP 地址
已拒绝 IP	显示被地域访问控制策略拒绝的 IP 地址记录
纠错反馈	将错误的 IP 地址和归属地记录反馈到深信服厂家

归属地查询	可以输入 IP 地址查询对应的归属地
更新地址库	可以手动更新 ISP 地址库

地域访问控制案例

某企业内网有服务器提供给外网访问，但业务只针对国内的，为了避免被国外地址恶意访问，需要限制只有中国大陆的地址可以访问内网服务器，需要在AF进行设置。

步骤1.在[策略/地域访问控制]点击<新增>进入[地域访问控制]界面。如下图所示。

步骤2.输入策略名称：“只允许中国大陆访问”，启用状态选择启用，描述可自定义，源的外网区域选择：“外网区”，区域的定义可以参考区域配置。

步骤3. 网络对象选择自定义的服务器，网络对象的定义可以参考网络对象配置，也可以直接点击<新增>进行添加。

步骤4.控制方式选择只允许以下国家/地区访问，[国家/地区]选择亚太地区/中国大陆。如下图所示。

步骤5.点击<确定>完成配置即可只允许中国大陆的地址能够访问内网服务器。

步骤6.通过非中国大陆的地址去访问内网服务器发现无法访问成功，通过中国大陆的地址去访问内网服务器能够正常访问。

6.1.3. 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，如下图所示。

本机访问控制配置案例

某企业使用AF做网关部署，开启了DNS代理功能，为了安全考虑，需要关闭外网区域访问DNS服务的53端口权限。

步骤1.点击<新增>按钮，进入[本机访问控制配置]界面。

定义名称：拒绝外网 DNS。

源地址选择：全部。

源区域：选择自定义的外网。

端口选择：全部。

目的地址选择：全部。。

服务选择：内置的 DNS 相关服务。

动作选择拒绝。

步骤2.点击<确定>保存配置生效。

步骤3.内网电脑能正常使用AF进行DNS解析，外网地址telnet测试AF外网接口DNS服务的53端口不通。

6.1.4. 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，影响网络设备的性能，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。

目的IP连接数控制：针对目标IP控制并发连接数。

双向IP连接数控制：针对双向IP控制并发连接数。

连接数配置案例

某企业管理员希望针对内网用户限制最高会话数，单用户最高并发500个会话。

步骤1.点击<新增>选择[源IP连接数控制]进行配置。

步骤2.输入名称，源的区域选择自定义的内网区，网络对象选择自定义的内网，网络对象的定义可以参考网络对象配置，每IP最大并发连接数填写：500。如下图所示。

步骤3.点击<确定>即可生效。

步骤4.当内网有终端新建TCP并发连接数超过500时会无法再建立TCP连接。

⚠ 注意：

连接数控制仅针对 TCP 连接有效。

6.2. 地址转换

地址转换支持源地址转换（SNAT）和目的地址转换（DNAT），实现内网地址转换成公网地址后进行网络通信，将对外网地址的访问映射为对内网地址访问，支持将对一个公网地址的访问映射为内网多个地址，实现内网服务器的负载均衡访问，同时支持目的端口转换。包括IPv4地址转换、IPv6地址转换、NAT64转换和DNS-Mapping四个功能模块。

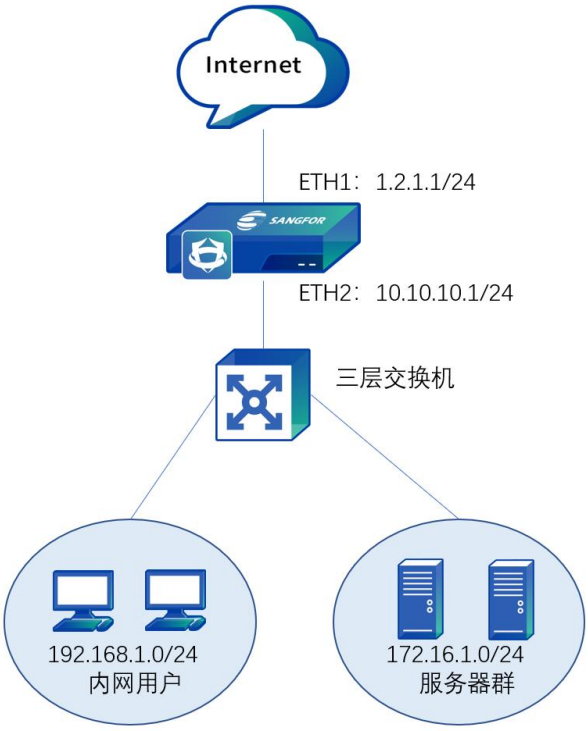
6.2.1. IPv4 地址转换

IPv4地址转换用于IPv4网络环境，是针对IPv4地址类型进行NAT转换，包括源地址转换、目的地址转换和双向地址转换。管理员可对IPV4地址转换进行如下操作。

表14 IPv4地址转换功能参数说明表

操作	说明
删除	可以删除勾选的策略
启用/禁用	启用或者禁用勾选的策略
移动	移动策略的位置，调整优先级，在上面的策略优先级高
清除匹配数	清楚选中策略的匹配数据，归为 0
模拟匹配	模拟源和目的数据包，是否 有匹配策略
导入/导出	支持将策略导入或者导出
刷新	刷新该页面，显示当前最新的数据
搜索关键字	通过策略名称进行搜索

本章节所有案例均使用如下拓扑，内网用户网段是192.168.1.0/24，服务器网段是172.16.1.0/24，AF做网关部署在公网出口，ETH1口IP地址1.2.1.1/24，ETH2口IP地址10.10.10.1。



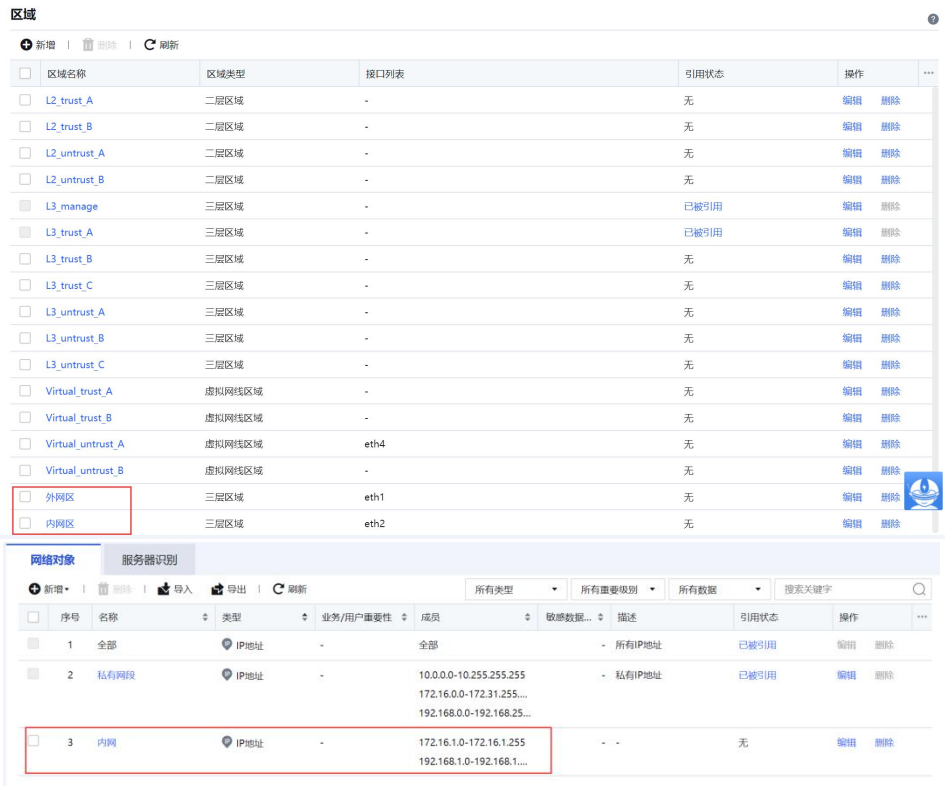
6.2.1.1. 源地址转换

源地址转换具体作用是将IP数据包的源地址转换成另外一个地址，内网地址访问外网时，将发起访问的内网IP地址转换为指定的IP地址，内网的多台主机可以通过同一个有效的公网IP地址访问外网，因此可以认为，源地址转换在一定程度上，能够有效的解决公网IPV4地址不足的问题，并能够达到隐藏内网的作用。源地址转换主要应用于网关设备代理上网的场景，如内网有多个私网网段的终端需要同时使用一个或者多个相同的公网IP地址访问公网服务。

源地址转换配置案例

某企业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。

步骤1. 定义内外网区域。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，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]。



步骤2. 新增NAT，在[地址转换/IPv4地址转换]页面点击<新增>，弹出[新增NAT]页面，默认选择[源地址转换]，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，添加到转换规则的位置以及生效时间。

步骤3. 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]，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]，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“any”即可。

步骤4. 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。

转换模式：选择IP范围后，可以设置转换模式，包含动态转换和静态转换。

Sticky：选择IP范围或者网络对象后，可以设置Sticky模式，Sticky nat逃逸功能，是在sticky nat申请端口失败时，尽可能到配置的IP中去申请端口，保证流量能正常通过；

进入逃逸功能时，会输出告警日志，提示用户当前的网络环境进入过sitcky nat逃逸模式，包含Strict模式和Loose模式。Strict模式即为严格模式，通过报文的源ip作为key从ip范围或ip对象中查找ip，所以来自同一源ip的报文会转成同一个ip，但当端口资源申请失败时，打印错误日志，进入droplist流程处理。Loose模式即为宽松模式，在sticky申请端口资源失败时，会在配置的ip范围内，从失败的ip（a.b.c.d）向后找到一个ip，去申请端口资源，若申请成功，则返回找到的资源，若申请端口资源失败，则再向后一个ip申请端口资源，直到配置范围的最大值；若达到配置范围的最大值，申请端口资源还没有成功，则失败的ip(a.b.c.d)向前找到一个ip，去申请端口资源，若申请成功，则返回找到的资源，若申请端口资源失败，则再向后一个ip申请端口资源，直到配置范围的最小值；若在配置的ip范围内，申请端口都失败，则打印错误日志，进入droplist流程处理。

高级选项：选择IP范围、指定IP和网络对象后，可以设置高级选项。

点击<设置>可进行端口的预分配，如下图所示。

步骤5. 保存配置。最后点击<确定>，完成源地址转换规则的配置。

步骤6. 放通内网到外网的应用控制策略后，当使用内网网段PC去访问外网，能够正常访问。

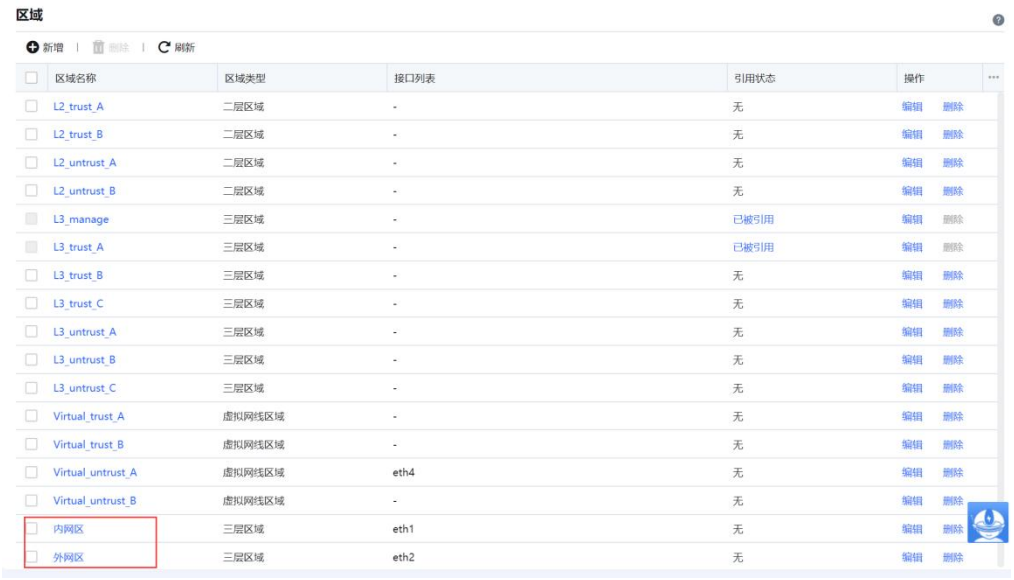
6.2.1.2. 目的地址转换

目的地址转换也称为反向地址转换、地址映射或端口映射，是一种单向的针对目标地址的地址转换，具体作用是将IP数据包的目的地址转换为另外一个地址。目的地址转换主要用于内部服务器以公网地址向外网用户提供服务的场景，可以指定特定的端口服务给公网用户访问，避免服务器直接全部暴露在公网，一定程度上可以保护服务器。

目的地址转换配置案例

某企业内网有一台Web服务器172.16.1.100的80端口提供http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，此处需要使用目的地址转换规则来实现。

步骤1. 定义内外网区域。在配置目标地址转换规则之前，首先要在[网络/接口/区域]定义好接口所属的[区域]。此案例中将ETH2定义为[外网区]，ETH1定义为[内网区]。



步骤2. 新增NAT。在[地址转换/IPv4地址转换]页面点击<新增>弹出[新增NAT]页面，选择[目的地址转换]，在“基础信息”的[名称]中填写规则的名称，自定义好描述信息，添加到转换规则的位置以及生效时间。

步骤3. 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，设置区域为外网区。

源地址：指明从哪个源地址访问过来的数据才进行目标地址转换。

目的地址：指明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”。

服务：设置进行目的地址转换的服务。本案例中服务类型需要选择 http，服务可以直接新增或者在网络对象中定义。

步骤4. 设置转换后数据包匹配条件。

转换后数据包：源地址不转换，需要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http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。

⚠ 注意：

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]设置端口为 8080。

步骤5. 放通应用控制策略。 [放通策略]里默认选择[放通后台ACL]，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，如不选择需要自行在应用控制策略中进行放通。最后点击<确定>，则完成配置。如下图所示。

步骤6. 外网用户输入http://www.xxx.com能访问到内网172.16.1.100服务器。

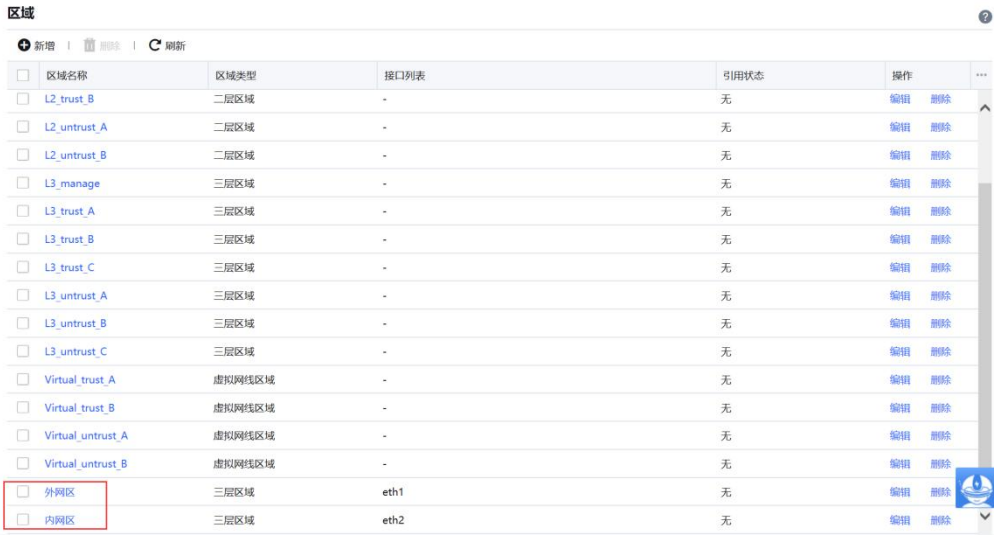
6.2.1.3. 双向地址转换

双向地址转换用于对经过设备的数据做源地址和目标地址都进行转换。常应用于发布服务器，将内网服务器的服务映射到公网，使外网用户和内网用户都可以通过公网地址访问到网络内部服务器。

双向地址转换配置案例

某企业内网有一台Web服务器172.16.1.100的80端口提供http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，此处需要使用双向地址转换规则来实现。

步骤1. 定义内外网区域。在配置目标地址转换规则之前，首先要在[网络/接口/区域]定义好接口所属的[区域]。此案例中将ETH2定义为[内网区]，ETH1定义为[外网区]。



步骤2. 新增NAT。在[地址转换/IPv4地址转换]页面点击<新增>弹出[新增NAT]页面，选择[双向地址转换]，在“基础信息”的[名称]中填写规则的名称，自定义好描述信息，添加到转换规则的位置以及生效时间。

步骤3. 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]和[内网区]。

源地址：指明从哪个源地址访问过来的数据才进行目标地址转换。

目的地址：指明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”。

服务：设置进行目的地址转换的服务。本案例中服务类型需要选择 http，服务可以直接新增或者在网络对象中定义。

步骤4. 设置转换后数据包匹配条件。

转换后数据包：需要将源地址转化为出接口地址，然后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http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。

步骤5. [放通策略]里默认选择[放通后台ACL]，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，如不选择需要自行在应用控制策略中进行放通。最后点击<确定>，则完成配置。如下图所示。

步骤6. 外网用户和内网用户都可以通过访问http://www.xxx.com访问到内网172.16.1.100服务器。

6.2.2. IPv6地址转换

NAT66是指IPv6地址之间的转换。使用NAT66不仅可以保护私网IPv6用户的隐私，而且可以降低IPv6网络维护和管理成本。根据转换方式的不同，NAT66可以分为NPTv6和静态NAT66。源地址或者目的地址经过NPTv6转换后，IPv6的网络前缀会被新的网络前缀替换，同时IPv6地址的接口ID部分会根据RFC6296规定进行调整，具体算法请参考RFC6296。而源地址或者目的地址经过静态NAT66转换后，IPv6的网络前缀会被新的网络前缀替换，IPv6地址的接口ID部分不会发生改变。因此，在IPv6数量较多且对转换后的IP地址不敏感的场景下，一般采用NPTv6转换方式，如大量IPv6私网用户访问Internet。在IPv6地址数量较少且对转换后的IP地址敏感时，一般采用静态NAT66方式，如IPv6公网用户访问内部服务器。

本章节所有案例均使用如下拓扑，内外网都是IPv6网段，内网服务器的IP是2001::1/128，AF网关部署在公网出口，ETH1口IP地址2003::1/128，ETH2口IP地址2001::2/128。

表15 IPv6地址转换功能参数说明表

操作	说明
删除	可以删除勾选的策略
启用/禁用	启用或者禁用勾选的策略
移动	移动策略的位置，调整优先级，在上面的策略优先级高
刷新	刷新该页面，显示当前最新的数据

6.2.2.1. 源地址转换

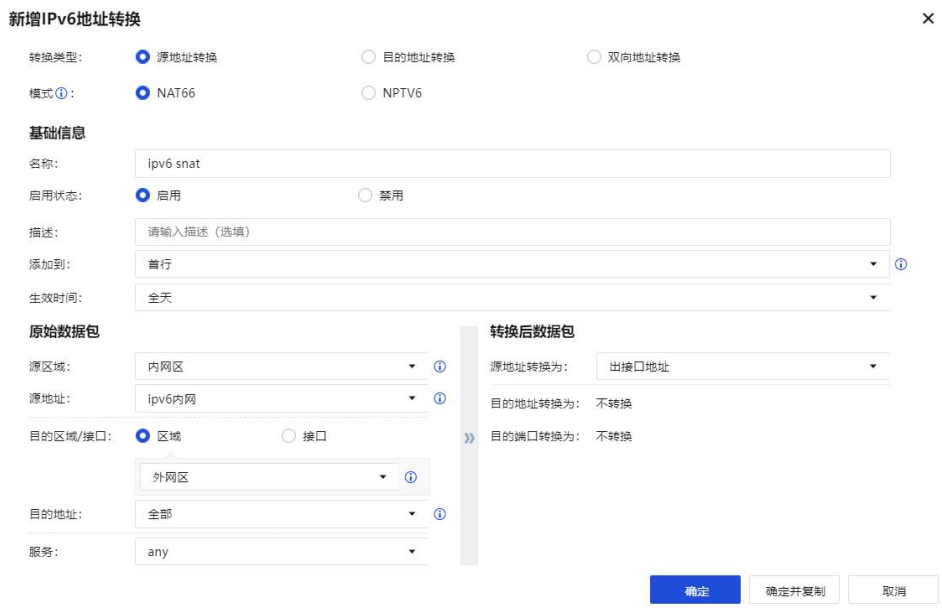
源地址转换具体作用是将IP数据包的源地址转换成另外一个地址，内网地址访问外网时，将发起访问的内网IP地址转换为指定的IP地址，内网的多台主机可以通过同一个有效的公网IP地址访问外网，达到隐藏内网的作用。源地址转换支持NPTv6转换方式。

源地址转换配置案例

某企业内外网都是IPv6网段，内网服务器的IP是2001::1，AF网关部署在公网出口，ETH1口IP地址2003::1，ETH2口IP地址2001::2，现需要对外网隐藏内网地址，要用到源地址转换成AF的ETH1口IP地址上外网。

步骤1. 定义内外网区域。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]，案例中将ETH1定义为[外网区]，ETH2定义为[内网区]。如下图所示。

步骤2. 新增源地址转换。在[地址转换/IPv6地址转换]页面点击<新增>，选择[源地址转换]，配置名称。



步骤3. 保存配置。最后点击<确定>，完成源地址转换规则的配置。如图。

步骤4. 放通内网到外网的应用控制策略后，通过服务器访问外网，源地址会转换为AF的外网口ETH1口地址。

6.2.2.2. 目的地址转换

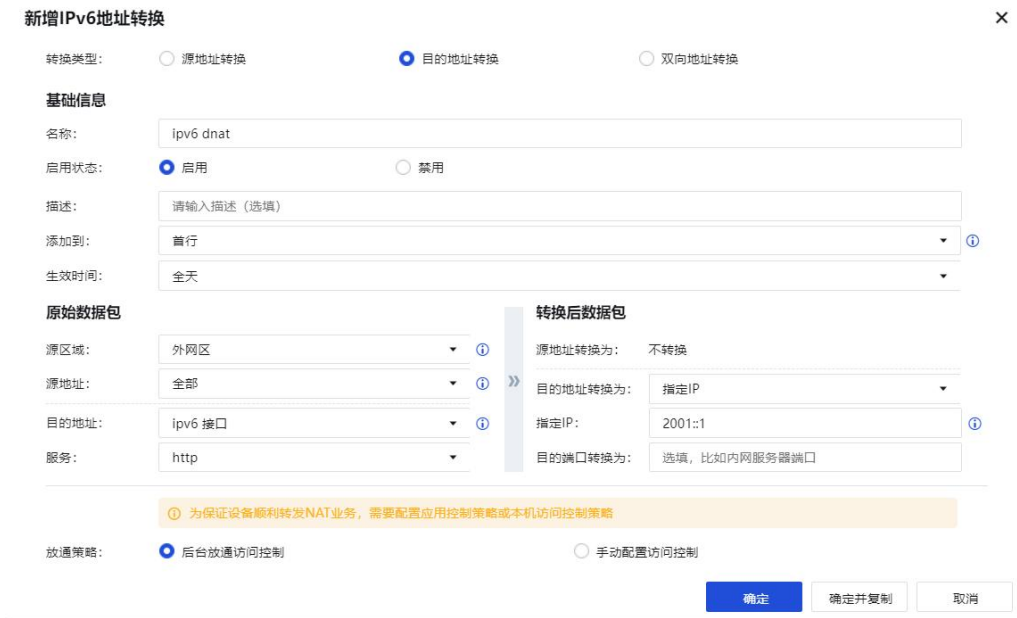
目的地址转换也称为反向地址转换、地址映射或端口映射，是一种单向的针对目标地址的地址转换，具体作用是将IP数据包的目的地址转换为另外一个地址。目的地址转换主要用于内部服务器以公网地址向外网用户提供服务的场景，可以指定特定的端口服务给公网用户访问，避免服务器直接全部暴露在公网，一定程度上可以保护服务器。

目的地址转换配置案例

某企业内外网都是IPv6网段，内网服务器的IP是2001::1，AF网关部署在公网出口，ETH1口IP地址2003::1，ETH2口IP地址2001::2，现需要将内网服务器发布web服务到外网，外网用户可以通过AF出口ETH1口IP地址访问到内网服务器。

步骤1. 定义内外网区域。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]，详细配置，例中将ETH1定义为[外网区]，ETH2定义为[内网区]。如下图所示。

步骤2. 新增目的地址转换。在[地址转换/IPv6地址转换]页面点击<新增>，选择[目的地址转换]，填写相关信息。



步骤3. 保存配置。最后点击<确定>，完成目的地址转换规则的配置。如图。

步骤4. 放通外网到内网的web服务应用控制策略后，通过外网访问http://[2003::1]，能够访问到内网服务器。

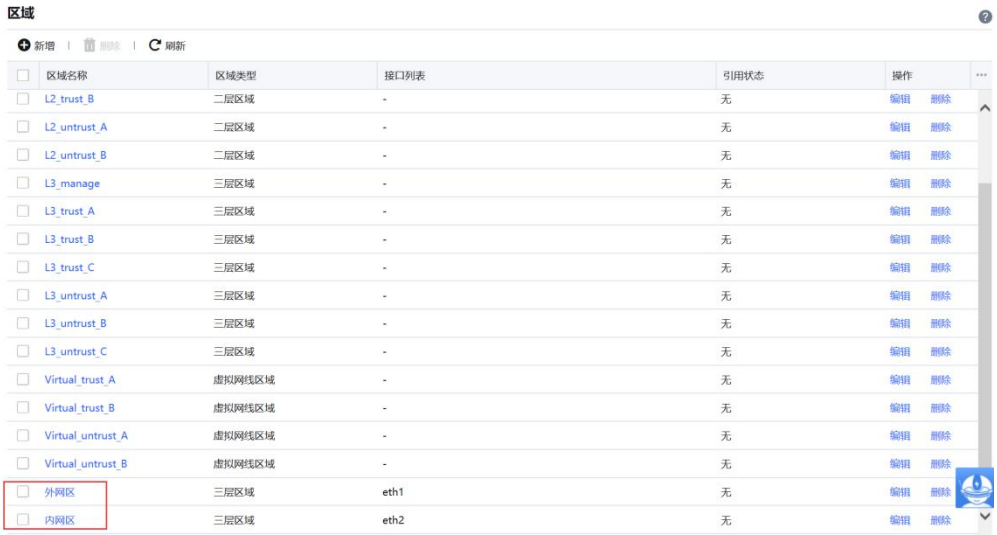
6.2.2.3. 双向地址转换

双向地址转换用于对经过设备的数据做源地址和目标地址都进行转换。常应用于发布服务器，将内网服务器的服务映射到公网，使外网用户和内网用户都可以通过公网地址访问到网络内部服务器。

双向地址转换配置案例

某企业内网有一台Web服务器2001::1的80端口提供http服务，并且已经申请了一个域名www.xxx.com指向2003::1。客户希望外网用户输入http://www.xxx.com能访问到内网2001::1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2001::1服务器，此处需要使用IPv6双向地址转换规则来实现。

步骤1. 定义内外网区域。在配置目标地址转换规则之前，首先要在[网络/接口/区域]定义好接口所属的[区域]。此案例中将ETH2定义为[内网区]，ETH1定义为[外网区]。



步骤2. 新增双向地址转换。在[地址转换/IPv6地址转换]页面点击<新增>，选择[双向地址转换]，填写相关信息。

步骤3. 保存配置。最后点击<确定>，完成双向地址转换规则的配置。如图。

步骤4. 外网用户和内网用户都可以通过访问http://www.xxx.com访问到内网2001::1服务器。

6.2.3. NAT64 地址转换

NAT64是一种有状态的网络地址与协议转换技术，用于将IPv6地址转换为IPv4地址，并将IPv4地址转换为IPv6地址。一般只支持通过IPv6 网络侧用户发起连接访问IPv4侧网络资源。但NAT64也支持通过手工配置静态映射关系，实现IPv4 网络主动发起连接访问IPv6网络。因此允许 IPv6 客户端访问IPv4 服务器，并允许IPv4客户端访问IPv6服务器。NAT64可实现TCP、UDP、ICMP 协议下的IPv6与IPv4网络地址和协议转换。管理员可对NAT64地址转换进行如下操作。

表16 NAT64地址转换功能参数说明表

操作	说明
删除	可以删除勾选的策略
启用/禁用	启用或者禁用勾选的策略
移动	移动策略的位置，调整优先级，在上面的策略优先级高
导入/导出	支持将策略导入或者导出

刷新	刷新该页面，显示当前最新的数据
搜索关键字	通过策略名称进行搜索

6.2.3.1. IPv4 to IPv6 地址转换

新增IPv4 to IPv6地址转换用于对访问IPv4地址的协议请求，转换成IPv6地址的协议进行通信。实现IPv4协议到IPv6协议的访问。

IPv4 to IPv6地址转换配置案例

某企业内网是IPv6网络，内网服务器地址是2003::1/128，外网是IPv4网络，AF的ETH1口IP地址是1.2.1.1/24，现在需要将内网服务器的Web服务发布到IPv4网络，让IPv4网络用户可以通过http://1.2.1.1访问到内网服务器。具体拓扑如下图所示。

步骤1.定义内外网区域。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，例中将ETH1定义为[外网区]，ETH2定义为[内网区]。如下图所示。

步骤1.新增IPv4 to IPv6地址转换。在[地址转换/NAT64地址转换]页面点击<新增>，选择[新增IPv4 to IPv6地址转换]，填写好相关信息。

步骤2.保存配置。最后点击<确定>，完成NAT64地址转换规则的配置。如图。

步骤3.外网用户通过访问http://1.2.1.1可以访问到内网服务器。

6.2.3.2. IPv6 to IPv4 地址转换

新增Pv6 to IPv4地址转换用于对访问IPv6地址的协议请求，转换成IPv4地址的协议进行通信。实现IPv6协议到IPv4协议的访问。

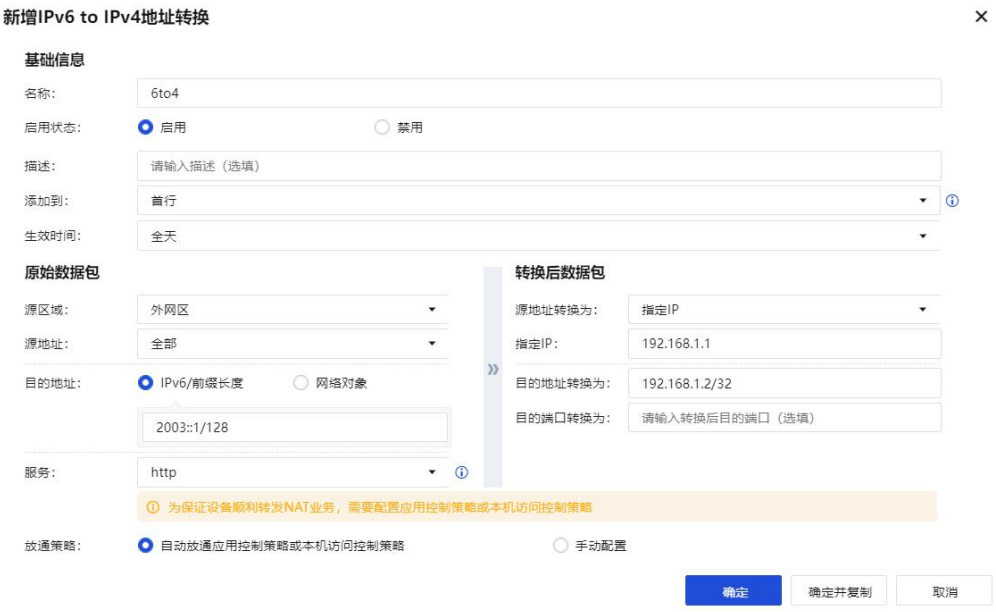
IPv6 to IPv4地址转换配置案例

某企业内网是IPv4网络，内网服务器地址是192.168.1.2/24，外网是IPv6网络，AF的ETH1口IP地址是2003::1/128，现在需要将内网服务器的Web服务发布到IPv6网络，让IPv6网络用户可以通过http://[2003::1]访问到内网服务器。具体拓扑如下图所示。

步骤1.定义内外网区域。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，例中将ETH1定义为[外网区]，ETH2定义为[内网区]。如下图所示。

步骤2.新增IPv6 to IPv4地址转换。在[地址转换/NAT64地址转换]页面点击<新增>，选择[新增IPv6 to IPv4地址转换]，填写好相关信息。



步骤3.保存配置。最后点击<确定>，完成NAT64地址转换规则的配置。如图。

步骤4.外网用户通过访问http://[2003::1]可以访问到内网服务器。

6.2.4. 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，内网用户PC发出的DNS解析请求得到的DNS服务器响应包到达防火墙的公网出接口时，防火墙在接口上查找到DNS-Mapping映射表项后，将内网服务器的地址替换解析到的公网地址返回给内网用户PC，内网用户PC实际是直接访问了服务器的内网IP，没有经过规则转换。

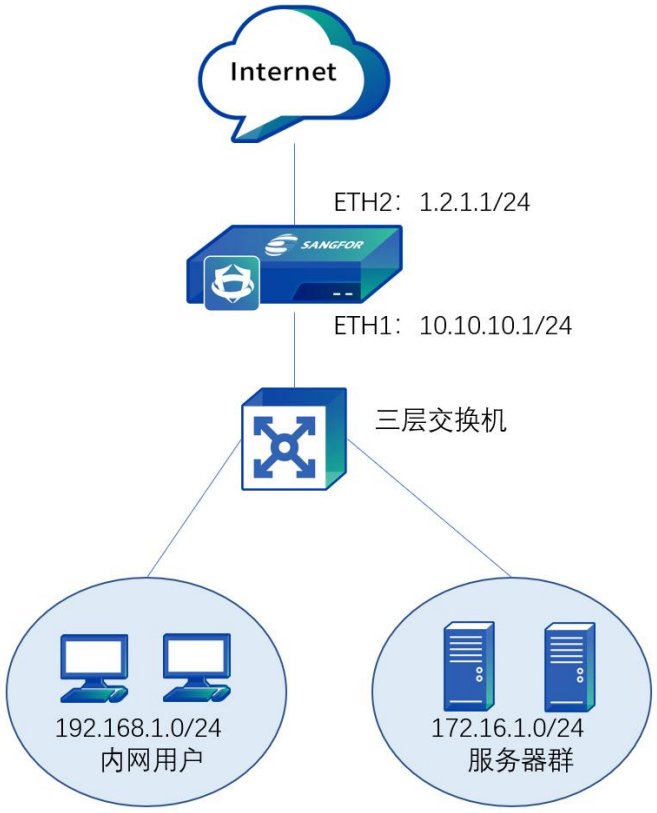
DNS Mapping与双向地址转换的区别是：

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。

DNS Mapping配置案例

某企业拓扑如下，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。



步骤1.进入[网络/地址转换/DNS Mapping]菜单，点击<新增>。

步骤2.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。

步骤3.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。

6.3. 安全策略

安全策略是AF的核心功能之一，能够对经过AF的流量进行安全检测，并对恶意行为进行阻断和联动封锁等。并通过事前风险预知、事中安全防护和事后检测及响应，从而建立一个闭环的机制。安全策略主要包括Web应用防护、漏洞攻击防护、内容安全、僵尸网络和DDOS防护等。

6.3.1. 安全防护策略

安全防护策略是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、僵尸网络等6大安全功能。

可以对安全防护策略进行新增、删除、启用、禁用、上移、下移、移动、刷新、高级设置和筛选操作。

安全防护策略是通过流量方向进行精确防护，因此流量方向的正确性关系到对应的攻击行为是否能够检测出来。

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。

源地址：

区域：选择攻击数据发起的方向所在的区域。

网络对象/用户：选择攻击数据发起的方向所在区域的源IP地址。

目的地址：

区域：选择数据访问方向所在目的区域。

网络对象/用户：选择数据访问方向所在区域的目的IP地址。

6.3.1.1. 业务防护策略

业务保护策略主要对用户的业务进行保护，从而防止业务服务器遭受攻击，提高网络的安全性。业务防护策略主要有实时漏洞分析、漏洞攻击防护、内容安全、Web应用防护、僵尸网络和联动封锁模块组成。

点击<新增>，选择业务防护策略，如下图所示。

网络配置参考安全防护策略，需要注意源地址和目的地址方向。

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。

说明：

CDN（内容分发网络）是构建在现有网络基础之上的智能虚拟网络，依靠部署在各地的边缘服务器，通过中心平台的负载均衡、内容分发、调度等功能模块，使用户就近获取所需内容，降低网络拥塞，提高用户访问响应速度和命中率。如果边缘服务器无该服务内容，则会使用本地的 IP 向中心服务器进行资源请求，从而边缘服务器起到一个代理的作用。

点击<下一步>，配置安全评估，即实时漏洞分析，如下图所示。

实时漏洞分析：被动流量观测，实时发现业务系统存在的漏洞、配置、账号弱口令等事前风险。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潜在风险和解决办法展现给用户，可在[安全运营/业务安全/实时漏洞分析]中进行查看。

点击<下一步>，进入防御配置。如下图所示。

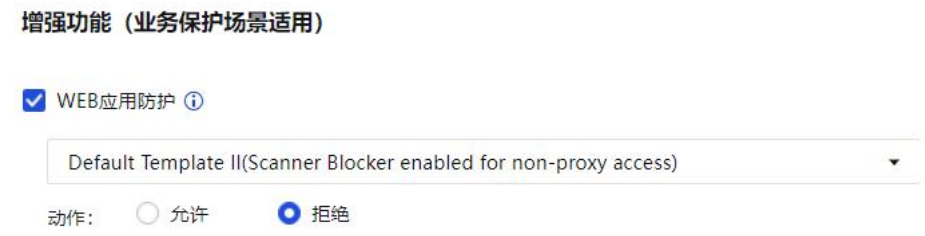
基础防御：

漏洞攻击防护：选择是否启用漏洞攻击防护，这里可以调用漏洞攻击防护模板。识别针对系统漏洞、应用漏洞的攻击行为，以及针对账号的暴力破解行为。

内容安全：选择是否启用内容安全，这里可以调用内容安全策略模板。包含邮件安全、URL过滤、文件安全三大功能，对网络通信内容中存在的威胁进行有效识别并防御。

动作：设置满足上述定义的条件的数据包是允许还是拒绝。如果为允许，则只对数据包进行检测，实际上不拒绝；如果为拒绝，则会根据规则库定义的动作进行拒绝或者允许。

增强功能：



Web应用防护策略：选择是否启用Web应用防护策略，且选中引用相关的Web应用防护模板。专门针对Web服务器设计的防攻击策略，可以防止系统命令注入、SQL注入、XSS攻击等各种针对Web应用的攻击和泄密行为。

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，可以引用僵尸网络模板。

内网是否存在DNS服务器：如果内网存在DNS服务器时，检测到的恶意域名会进行重定向。恶意域名解析的IP地址将会被替换成以下的重定向IP地址，监听对该IP地址的访问，即可定位内网感染僵尸网络病毒的真实主机IP。

记录日志：勾选记录日志，触发攻击行为会记录相应日志到安全日志中。

响应：

联动封锁：点击<设置>选项，开启联动封锁，当漏洞攻击防护规则、WAF规则和内容安全模块，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。

说明：

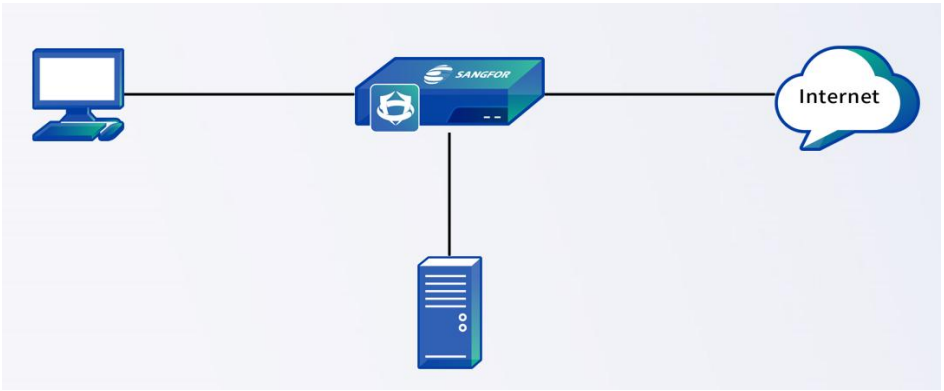
1．高危行为联动封锁：漏洞攻击防护、WAF、DOS 部分指定的高等级规则；

2．任意攻击行为联动封锁：漏洞攻击防护、WAF、DOS 中存在“阻断”事件会触发联动封锁；

3．触发 IPS 口令爆破、WAF 漏洞防扫描、CC 攻击和后门防扫描、DDOS 攻击都会自动封锁，无需开启联动封锁。

实时漏洞分析、WAF、IPS、内网安全配置案例：

某企业Web服务器对互联网提供服务，经常遭受来自互联网的恶意攻击，导致业务异常。因此，为了业务的连续性，需要部署一台AF来防护互联网的攻击，并保护业务的安全。同时，需要对服务器的漏洞进行风险分析，能够检测到服务器存在的风险问题。



步骤1.（可选）创建漏洞攻击防护、内容安全、Web应用防护、僵尸网络和网络对象模板，方便提供给业务防护策略进行调用和方便后续对策略的调整等。

步骤2.点击<新增>，选择业务防护策略，填写源目地址、区域等，如下图所示。

步骤3.点击<下一步>，选择开启实时漏洞分析，如下图所示。

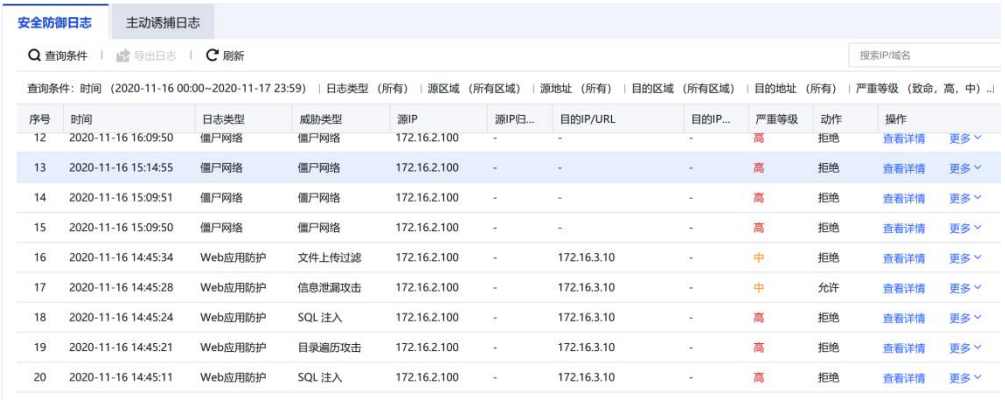
步骤4.点击<下一步>，选择对应的IPS、内网过滤和WAF等功能，并对攻击行为进行阻断，如下图所示。

步骤5.点击<下一步>，配置僵尸网络、联动封锁等，如下图所示。

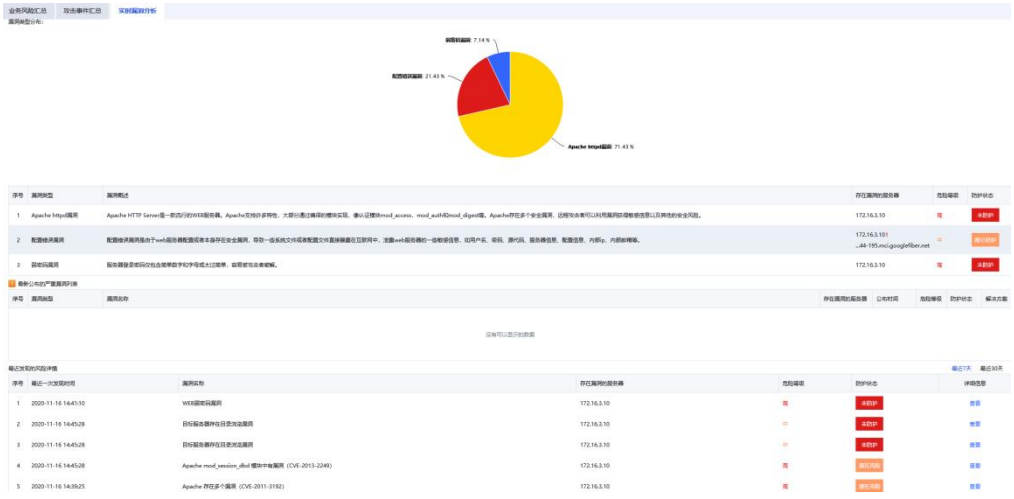
步骤6.配置完成结果如下图所示。

步骤7.在外网方向对内网方向的服务器进行攻击测试，如使用Xhack工具来测试。

步骤8.查看安全日志，能够检测WAF、IPS和僵尸网络等恶意攻击行为，如下图所示。



步骤9.查看实时漏洞分析，在[安全运营/业务安全/实时漏洞分析]中查看，如下图所示。

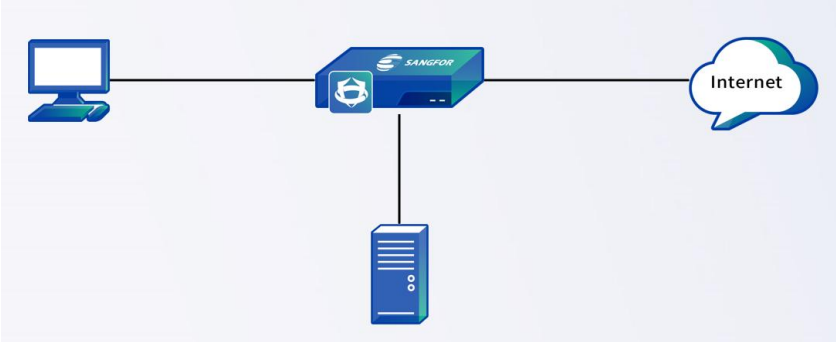


6.3.1.2. 用户防护策略

用户保护策略主要对客户的终端用户进行保护，防止终端遭受攻击，提高内网的安全性。用户保护策略主要有漏洞攻击防护、内容安全和僵尸网络等功能。

配置案例

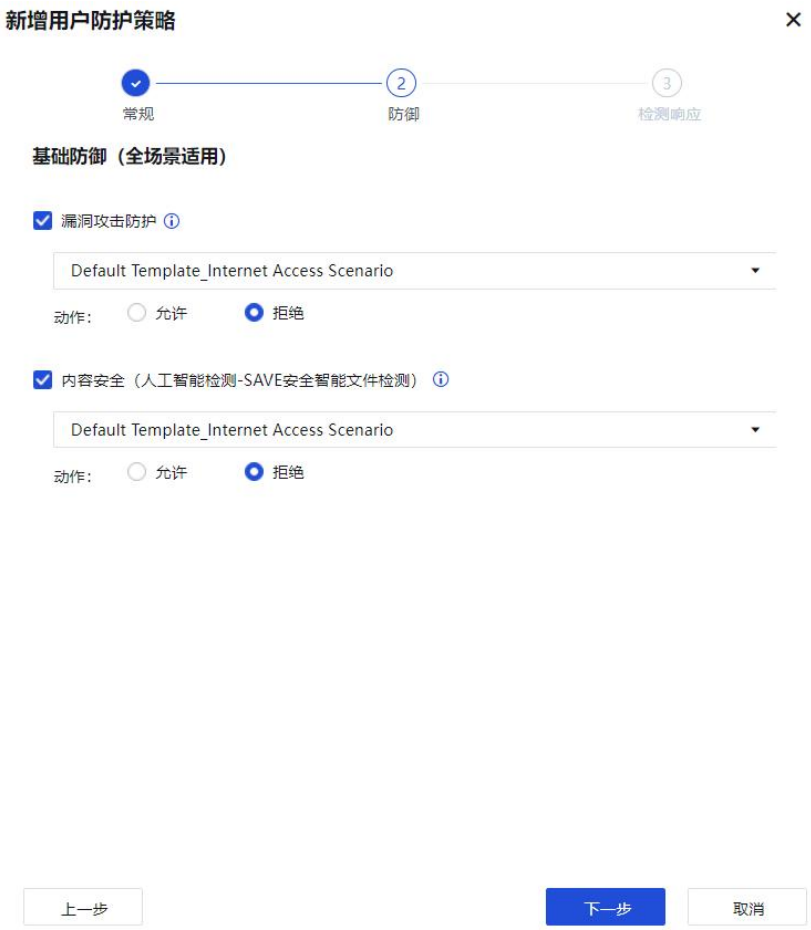
某企业办公网环境中，为了防止内部人员对互联网进行攻击，从而带来一定的法律风险。因此，需要对用户的上网进行管控。



步骤1.（可选）创建漏洞攻击防护、内容安全、僵尸网络和网络对象模板，方便提供给业务防护策略进行调用和方便后续对策略的调整等。

步骤2.点击<新增>，选择用户防护策略，填写源目地址、区域等，如下图所示。

步骤3.点击<下一步>，进行安全防御的配置，如下图所示。



步骤4.点击<下一步>，进行检测响应的配置，如下图所示。

步骤5.点击<确定>，保存该配置生效。

步骤6.测试结果如下图所示。

6.3.1.3. 高级设置

高级配置功能主要是对于影响业务或者误报的规则进行添加例外。添加例外后的规则不在进行检测且不告警。添加例外的规则包括僵尸网络、漏洞攻击防护、实时漏洞、Web智能语义、内容安全、邮件安全和文件杀毒等。

点击<高级设置>，弹出高级设置页面，如下图所示。

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。

启用内网DNS服务器场景优化：内网存在DNS服务器时必须进行配置，主要用于定位内网感染僵尸网络主机的真实IP地址。

点击<配置恶意域名重定向>，可以把恶意域名解析的IP地址将会被重定向成以下的蜜罐IP地址，监听对蜜罐地址的访问，即可定位内网感染僵尸网络病毒的真实主机IP。

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。若出现正常业务无法访问，建议将业务的域名添加到白名单中。

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。

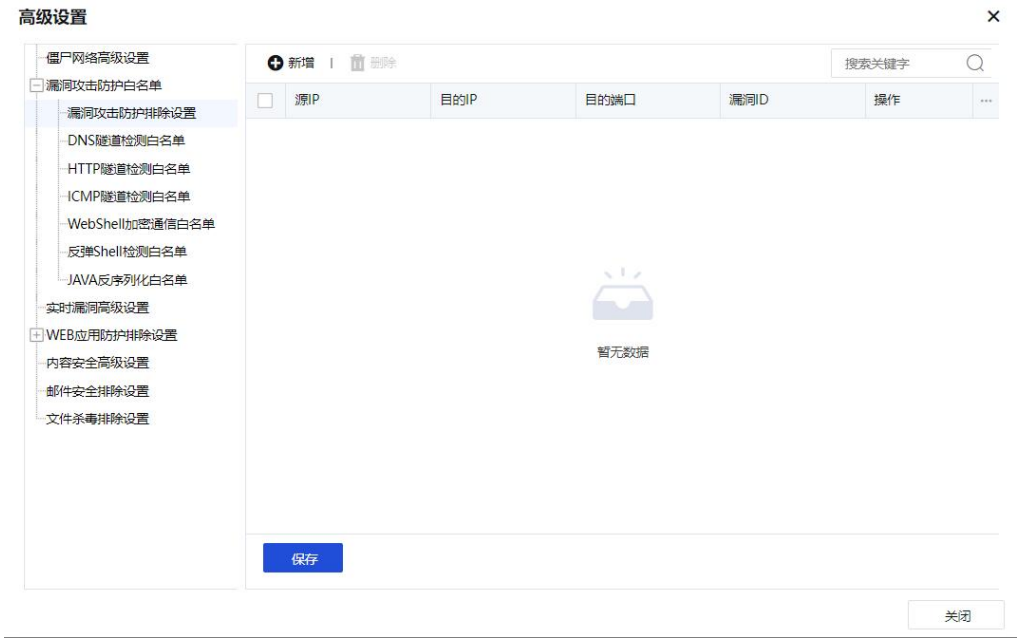
僵尸网络行为检测：通过配置的可疑行为做检测，定位出疑似僵尸网络的主机，但所有规则不阻断数据通信，只做检测并记录日志。

点击<保存>，对僵尸网络高级设置进行保存。

漏洞攻击防护白名单：

用于设置漏洞攻击防护不需检测或者误报的进行例外排除数据，包含漏洞攻击防护排除设置、DNS隧道检测白名单、HTTP隧道检测白名单、ICMP隧道检测白名单、WebShell加密通信白名单、反弹Shell检测白名单和JAVA反序列化白名单。

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数据，如下图所示。



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。

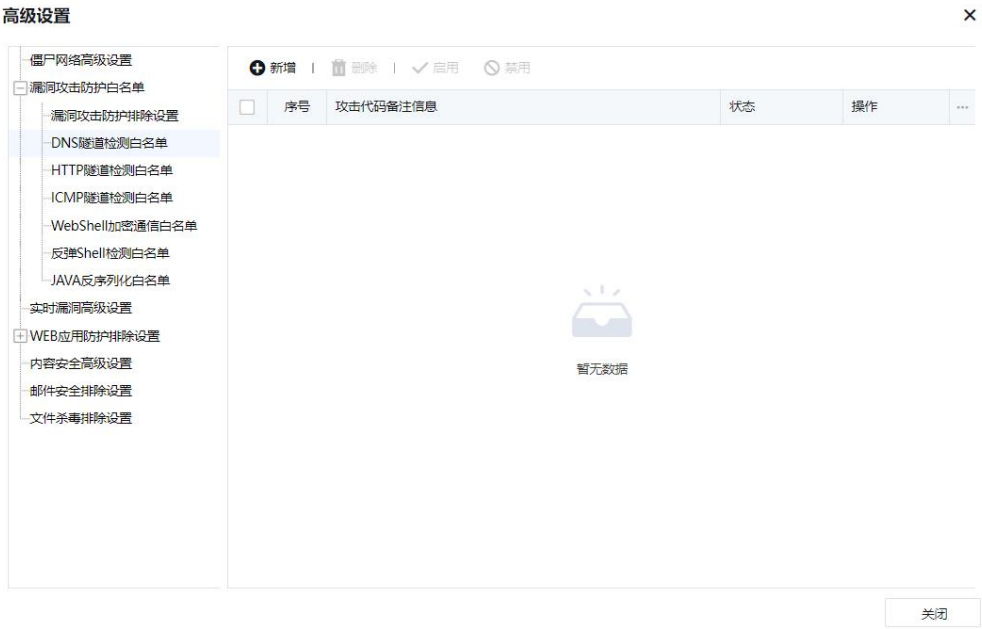
目的端口：定义目的端口。

漏洞ID：定义漏洞ID。

点击<确定>，提交设置。

点击<保存>，对漏洞攻击防护排除设置进行保存。

DNS隧道检测白名单、HTTP隧道检测白名单、ICMP隧道检测白名单、WebShell加密通信白名单、反弹Shell检测白名单和JAVA反序列化白名单等都是用于添加对应威胁类型的白名单，如下图所示。



点击<新增>后跳转到安全日志页面显示对应类型的日志，如下图所示。

再点击<更多>即可选择<添加例外>，如下图所示。

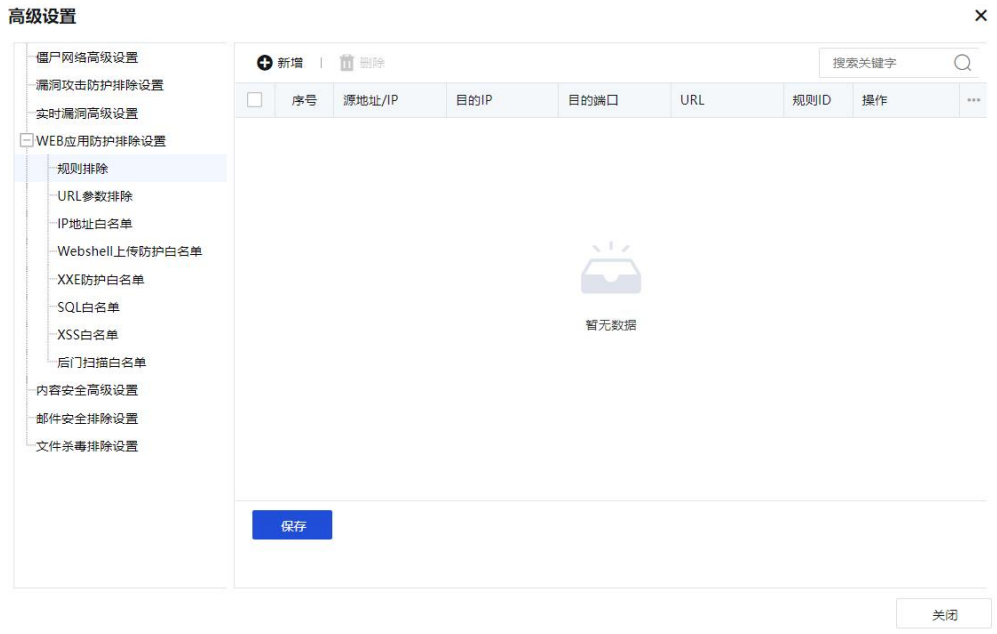
实时漏洞高级设置：

可以启用排除域名/IP/端口/URL和企业OA端口设置。

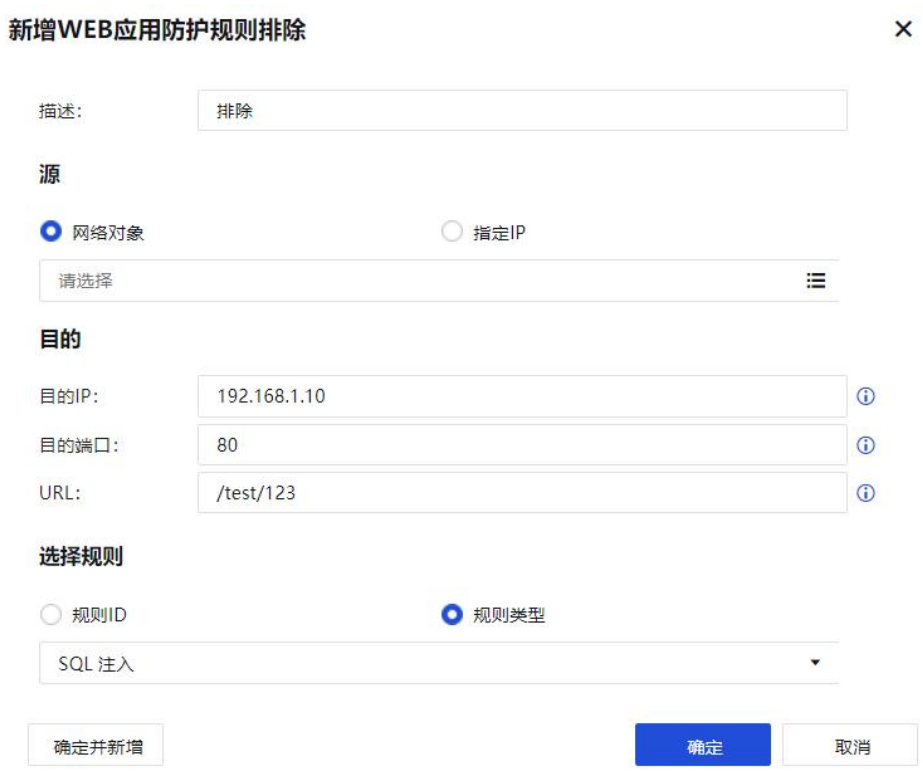
点击<保存>，对实时漏洞高级设置进行保存。

Web 应用防护排除设置:

可以对Web检测中存在误报的规则添加例外，包括规则排除、URL参数、IP地址、Webshell上传防护、XXE防护、SQL、XSS和后门扫描等添加例外，从而减少误报的发生，如下图所示。



规则排除：对Web检测出的误报规则进行排除，从而减少业务受到影响。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。

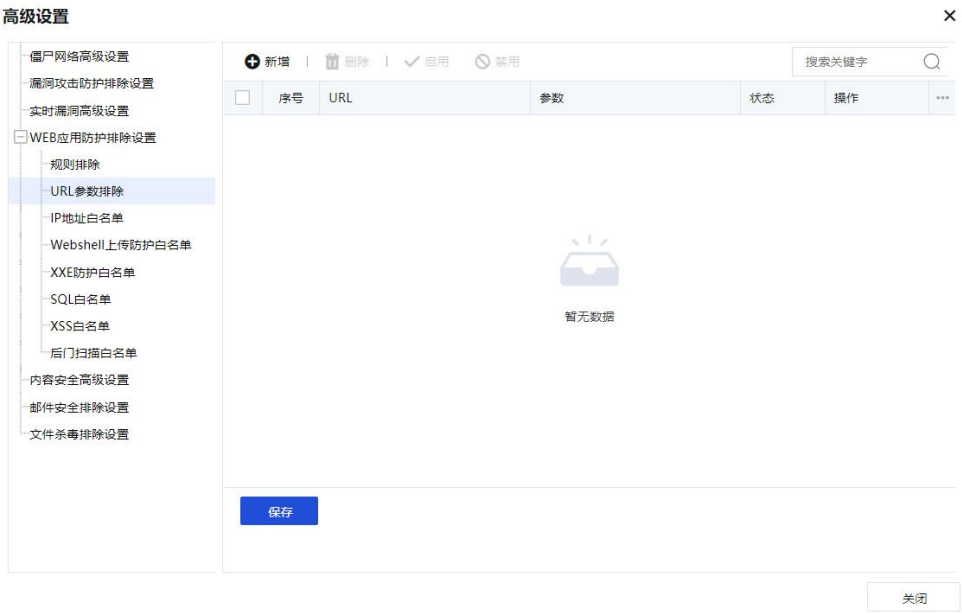
规则ID：定义规则ID。

规则类型： 定义规则类型，对某一类规则添加例外。

点击<确定>，提交配置。

点击<保存>，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。

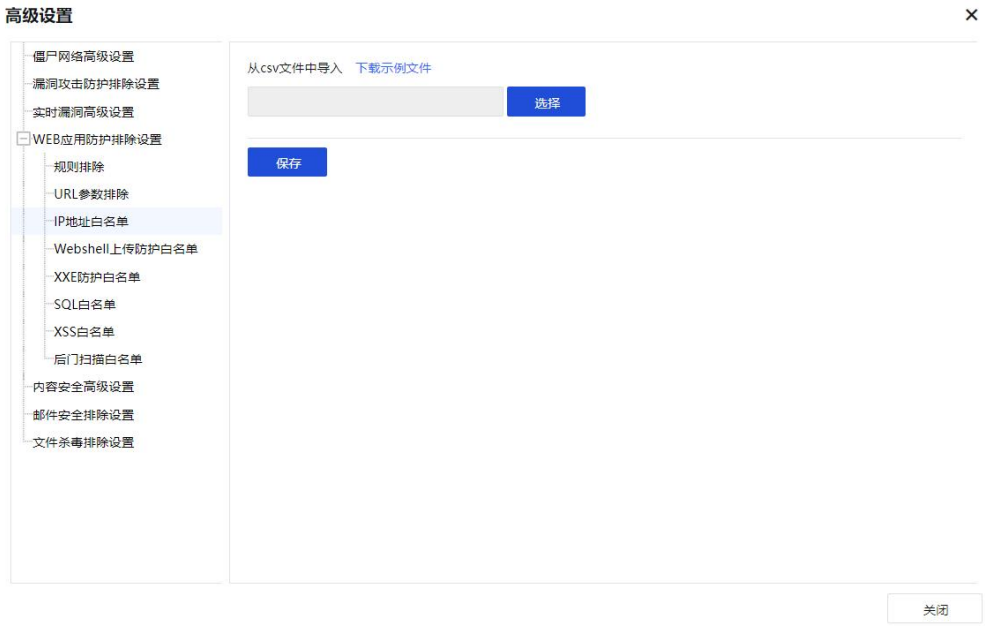
URL：定义URL。

参数：定义参数信息。

点击<确定>，提交配置。

点击<保存>，对URL参数排除设置进行保存。

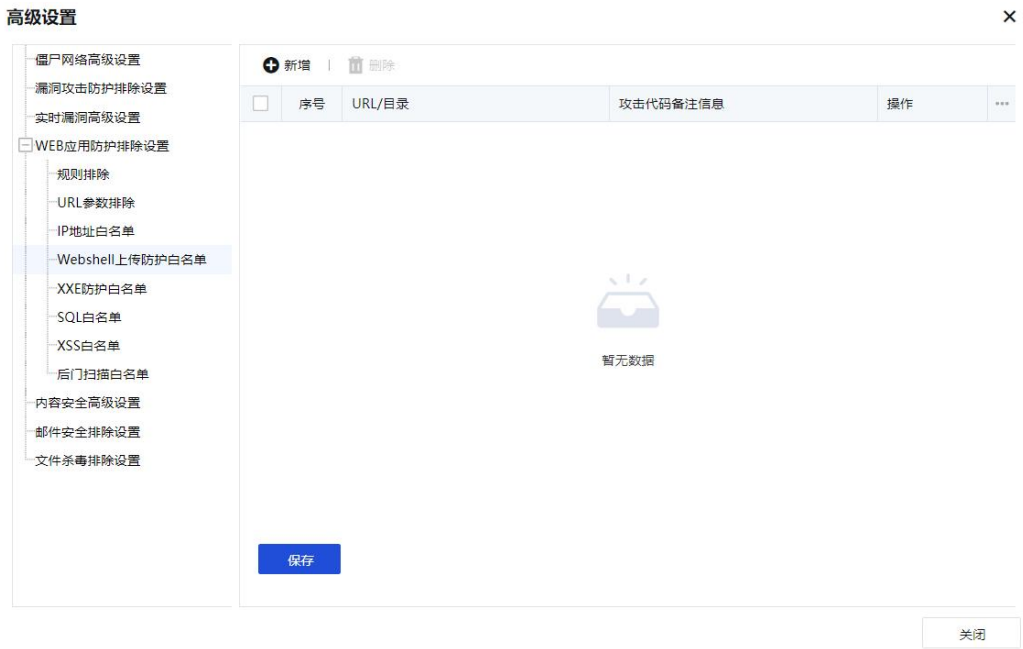
IP地址白名单：可对IP地址进行排除。如下图所示。



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。

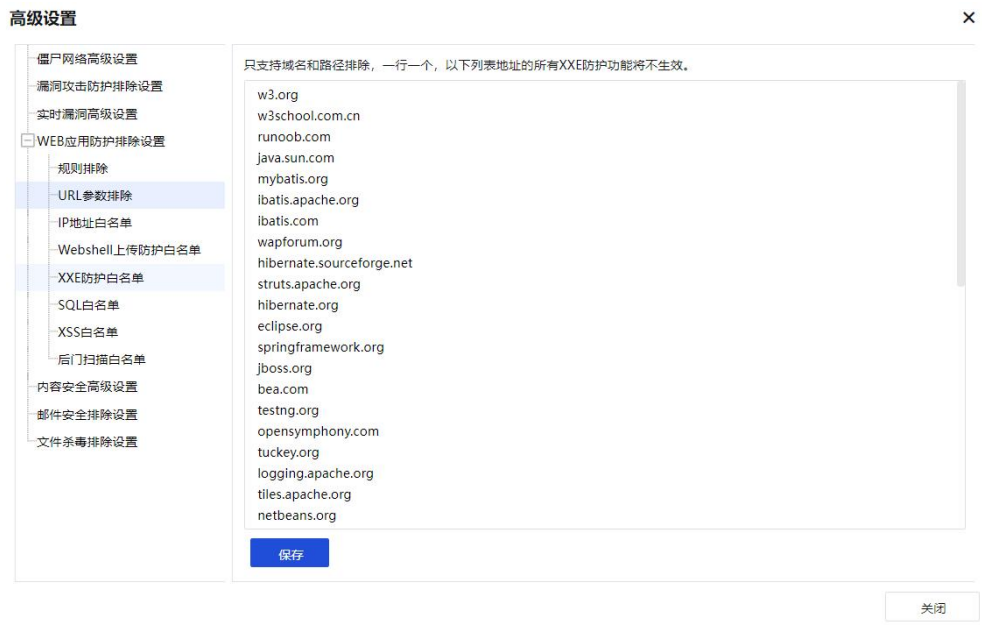
点击<保存>，对IP地址白名单设置进行保存。

Webshell上传防护白名单：针对Web智能引擎检测出来的Webshell上传出现误报时，可以对Webshell上传的防护加入白名单，从而减少误报造成的影响。如下图所示。



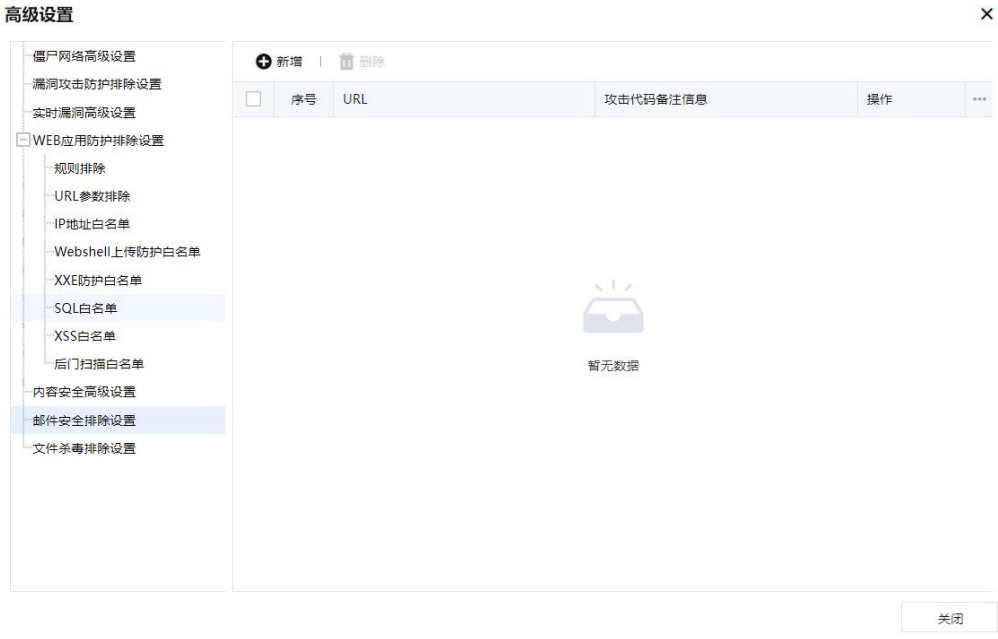
点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

XXE防护白名单：针对Web智能引擎检测出来的XEE出现误报时，对XXE的防护添加到对应的白名单中，如下图所示。



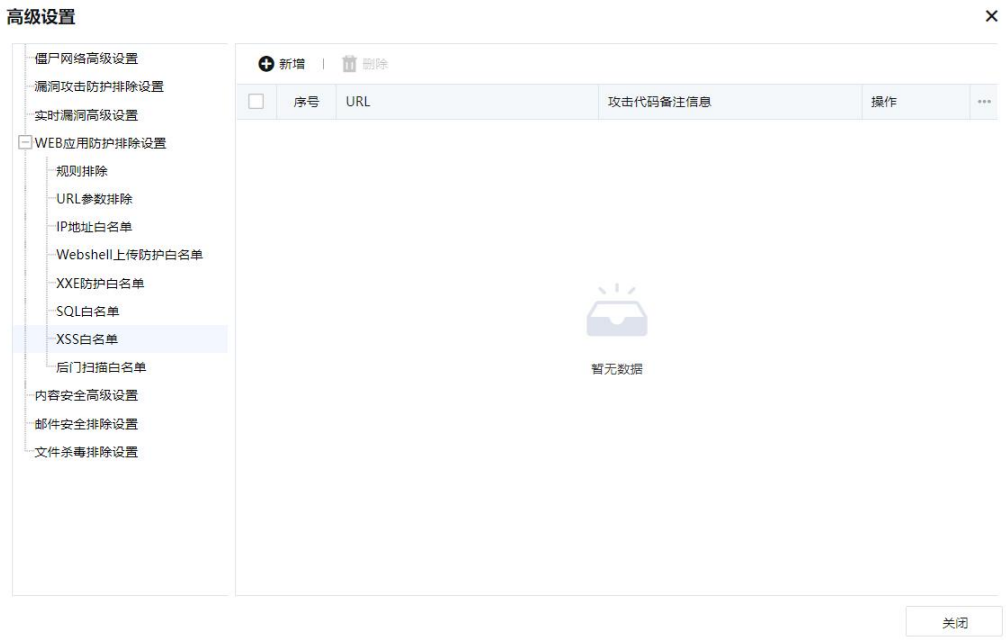
输入对应的域名即可，点击<保存>生效。

SQL白名单：针对Web智能引擎检测出来的SQL语义出现误报时，可以对SQL注入的防护加入白名单，从而减少误报造成的影响。如下图所示。



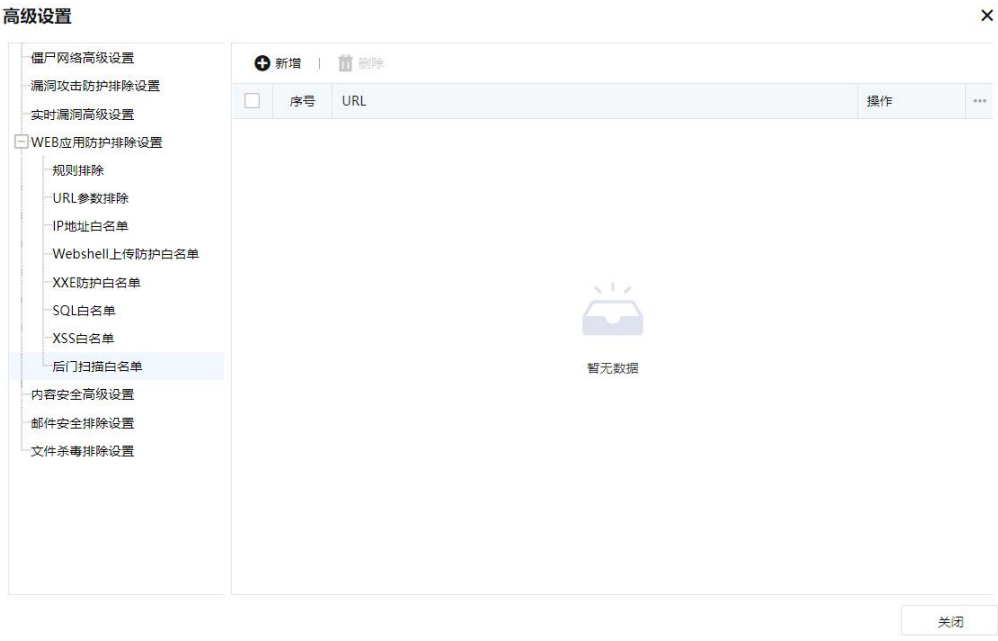
点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

XSS白名单：针对Web智能引擎检测出来的XSS语义出现误报时，可以对XSS注入的防护加入白名单，从而减少误报造成的影响。如下图所示。



点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

后门扫描白名单：针对Web智能引擎检测出来的后门扫描出现误报时，可以对后门扫描加入白名单，从而减少误报造成的影响。如下图所示。



点击<新增>，跳转到安全日志界面，需要在安全日志后添加例外，可加入到白名单中。

内容安全高级设置

主要对病毒文件的检测内容进行限制，如文件大小、压缩程度，可以进行对应的调整。如下图所示。

杀毒文件大小限制：限制杀毒文件的大小，默认为10M，最大支持20M。如下图所示。

配置文件类型

序号	类型组名	文件后缀	杀毒限制
1	电影	*.rm *.rmvb *.avi *.asf *.wmv ...	10M
2	音乐	*.mp3 *.wma *.ogg *.wav	10M
3	图片	*.jpg *.gif *.bmp *.tiff *.png	10M
4	文本	*.cpp *.c *.txt * h	10M

关闭

点击对应的类型组名，可以对检测的文件大小进行修改，如下图所示。

压缩层级限制：配置需要解压文件的层级，对解压的文件进行病毒检测。模式为4级，最大支持16级。

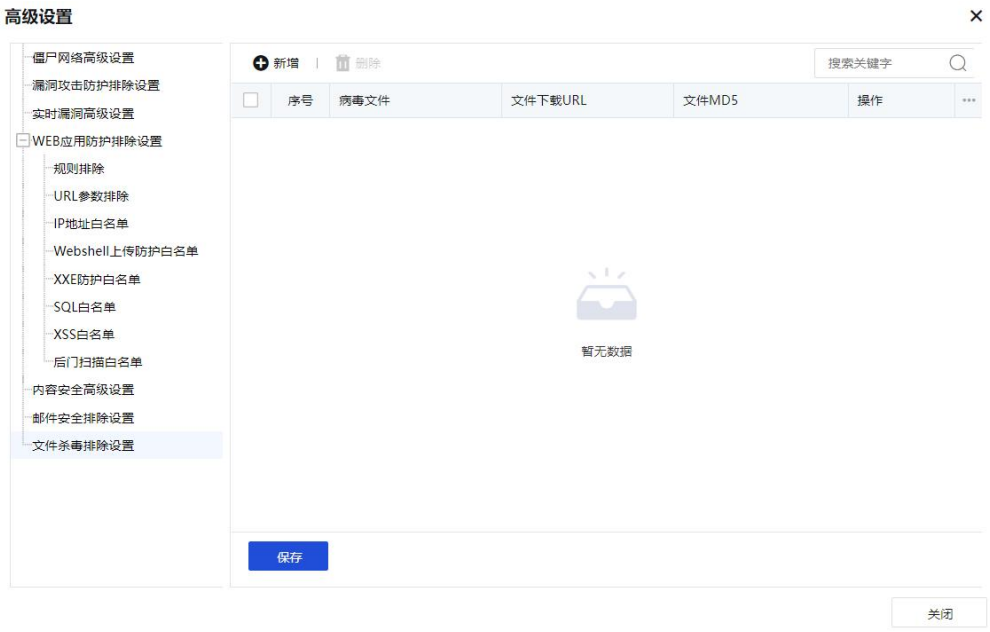
邮件安全排除设置

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>，对邮件安全排除设置进行保存。

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可选其一。

描述：该对象的描述信息。

点击<确定>，提交配置。

点击<文件杀毒排除设置>，对文件杀毒排除设置进行保存。

6.3.2. 云蜜罐诱捕策略

主动诱导攻击者攻击“假”目标，延长对抗时间，保护真实资产安全。捕获到攻击IP后进行自动封锁，进而防止攻击者对内外网进行扫描等攻击行为。通过云端蜜罐深度

溯源指纹信息、社交信息、位置信息等数据，精准勾勒攻击者画像，从攻击源头切断攻击。当检测到内部主机对不该访问的伪装业务发起恶意扫描，即可快速定位内网失陷主机，自动封锁，防止横向扩散感染核心业务。如下图所示。

点击<新增>，创建蜜罐策略，如下图所示。

策略名称：填写对应的策略名称。

描述：填写对应的描述信息。

状态：启用或禁用该策略。

应用场景标签：用来标记告警提示时是诱捕外网攻击还是诱捕内网扩散。

云端分析能力：开启云端高级捕获与分析技术，可以获取攻击方的指纹信息、工具、手法、攻击轨迹等，汇总形成攻击者画像，有效溯源分析攻击者行为。开启后可在配置伪装服务时选择云端伪装服务类型。开启该功能需要设备能够连接网络且开通相应的授权。

说明：

连接到云端获取更多的伪装服务，目前有 SSH、RDP、SMB、VNC 等，本地值提供 tcp 连接功能，并记录访问日志，不支持应用层服务。

配置伪装服务

IP类型：选择是伪装IP还是真实业务IP。

伪装IP：伪装出来的IP，实际业务中不存在，且AF无法ping通该IP，则AF会模拟ARP响应报文回给攻击端，使攻击端感知到该业务的存在。

真实业务IP：真实存在的IP，AF能够ping通该IP，则AF收到该IP响应的ARP包，才会回包给攻击端，使攻击端感知到该业务的存在。

IP/IP段：根据需求填写IP/IP段；

伪装服务区类型：如果勾选云端能力分析，则可以选择多个伪装服务，否则只能选择本地HTTP伪装服务。选择后，可以点击<编辑>，对端口进行修改。

说明：

1、尽量配置与真实业务的 IP 和端口，以增大诱捕率，但不要和真实业务重合，否则将影响正常业务的访问；
2、单个策略的伪装服务之和最大支持 50 个；
3、为使本云蜜罐联动功能生效，AF 设备部署时必须同时保证：
（1）访问者能与 AF 设备成功建立 TCP 连接，否则流量无法进入 AF，云蜜罐诱捕功能失效；
（2）AF 设备与外网连通，否则流量无法发送至云端，云蜜罐服务失效；
4、在线伪装服务相比本地伪装服务，由于其能够真实访问，因此获取到的黑客信息更为丰富，业务针对性强，建议用户配置在线伪装服务；
5、云蜜罐诱捕策略只支持路由、透明模式部署、虚拟网线部署；
6、AF 与攻击者只进行三次握手，如果是本地伪装服务，则三次握手后的数据包将进行丢弃，不进行解包分析；如果是在线伪装服务，则三次握手后的数据包直接转发到云端分析。

联动处置

自动联动封锁：启用或者禁用联动封锁功能，对诱捕到的恶意行为进行联动封锁。

联动对象：对所有访问伪装服务的源IP进行封锁或者有恶意攻击行为的源IP进行封锁。

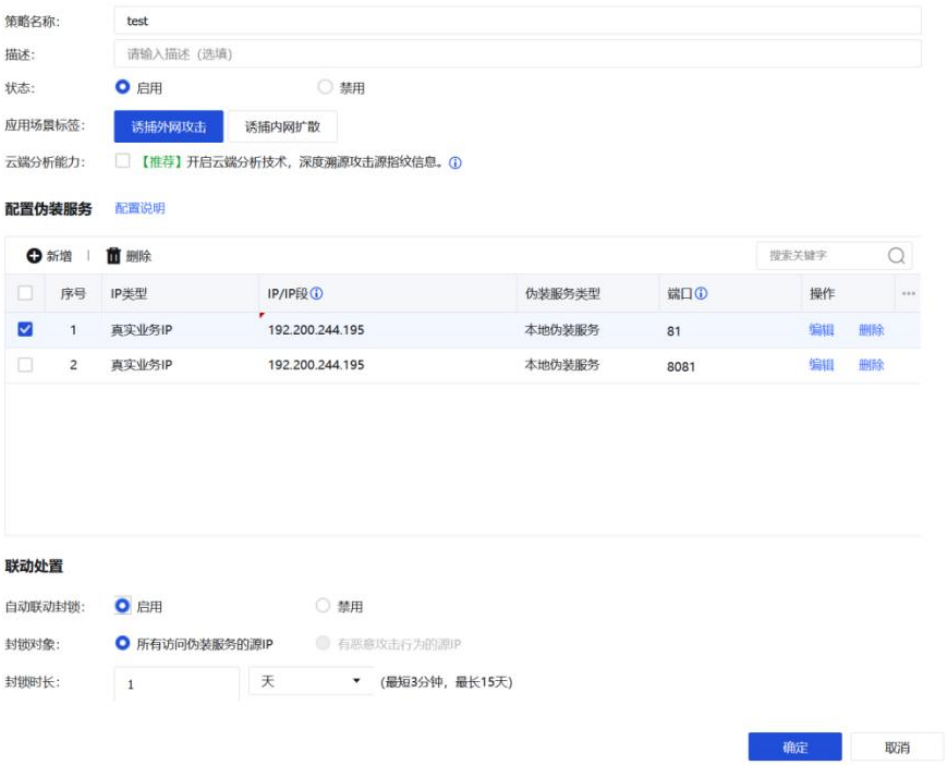
封锁时长：联动封锁的时长，最长15天。

配置案例

某企业的内网业务系统，对外提供业务服务，经常遭受到互联网的攻击扫描，因此，业务系统一旦被攻陷，将带来巨大的损失。所以，需要诱捕的方式找到真实的攻击者，

从而对黑客IP进行更加准确的封禁。客户对外的真实业务为192.200.244.195:80，需要伪装服务192.200.244.195:8080和192.200.244.195:81。当存在访问伪装业务的IP时，对其进行自动封锁。

步骤1. 点击<新增>，创建蜜罐策略，如下图所示。



步骤2. 点击<确定>，完成配置。

步骤3. 访问蜜罐页面，查看告警结果，如下图所示。

6.3.3. 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。深信服AF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。可以对DDOS防护策略进行新增、删除、启用、禁用、上移、下移、移动和刷新等操作。

6.3.3.1. 外网对内攻击防护策略

外网对内网发起DOS攻击，从而消耗服务器资源，严重影响业务的连续性。因此，外网的DOS攻击成为了一个主流的DOS攻击手段。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<新增>，选择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。

源

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。

防护配置

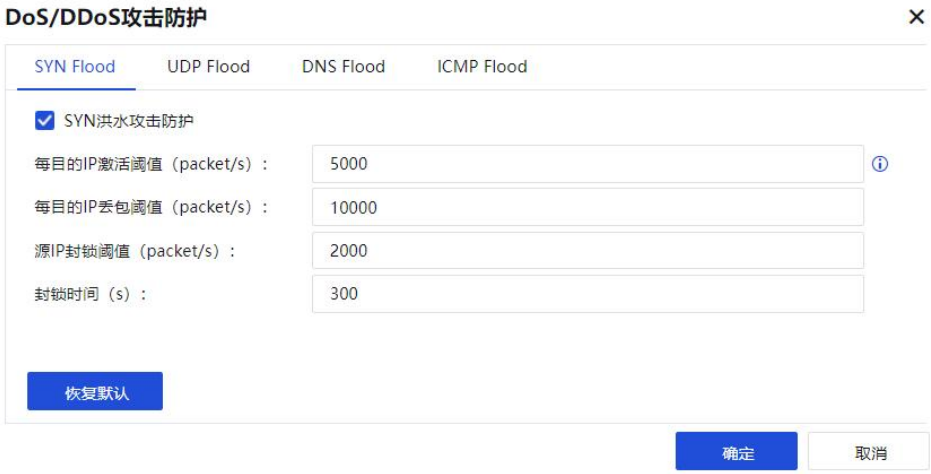
扫描攻击类型：可开启IP地址扫描防护和端口扫描防护。如下图所示。

IP地址扫描防护：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：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。

网络对象：需要防护的对象，一般为目的IP。

DoS/DDoS攻击类型：点击<已选防护:SYN洪水攻击防护...>，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0~100000000。

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。

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

未知协议类型防护：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：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：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。

⚠ 注意：

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：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：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：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：当ICMP报文大于1024时，被认为是攻击。

IP协议报文选项

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

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。

最后点击<确定>，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。

说明：

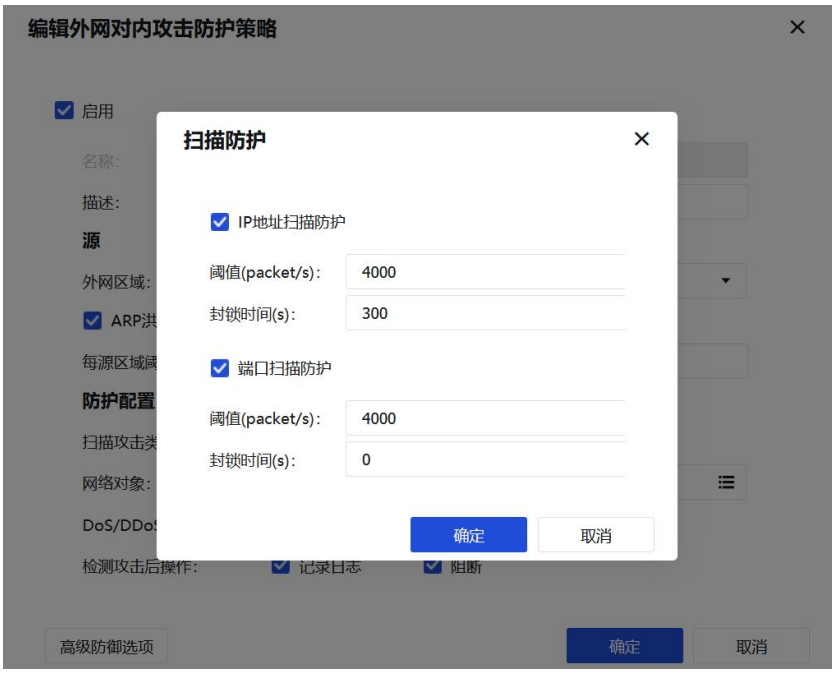
1.数据包匹配是由上往下匹配的，当匹配到任何一个攻击行为被丢弃之后，都不会往下匹配。如果数据包没有匹配到前面的攻击，则会继续匹配下面设置的攻击行为是否符合。
2.设置了扫描防护，最好再设置 DoS/DDoS 攻击防护里的 ICMP 攻击防护等信息。这个主要是由黑客的攻击行为特征决定的。黑客的入侵一般情况下是首先扫描 IP 地址是否存在，扫描到 IP，然后是扫描端口。当扫描到 IP 和端口之后，则会进行<下一步>攻击行为。也有一些黑客本来就知道 IP 和端口，不需要扫描，直接发起攻击行为。所以最好是两处都进行设置，才能有效地防范攻击行为。

配置案例

某企业服务器，经常出现业务访问缓慢现象，排查发现服务器的一些资源使用率比较高。抓包发现导致这一现象为某些互联网IP发送大量的SYN包、UDP包等，占用了大量的资源。因此，需要在互联网出口的AF配置DDOS攻击防护解决该问题。

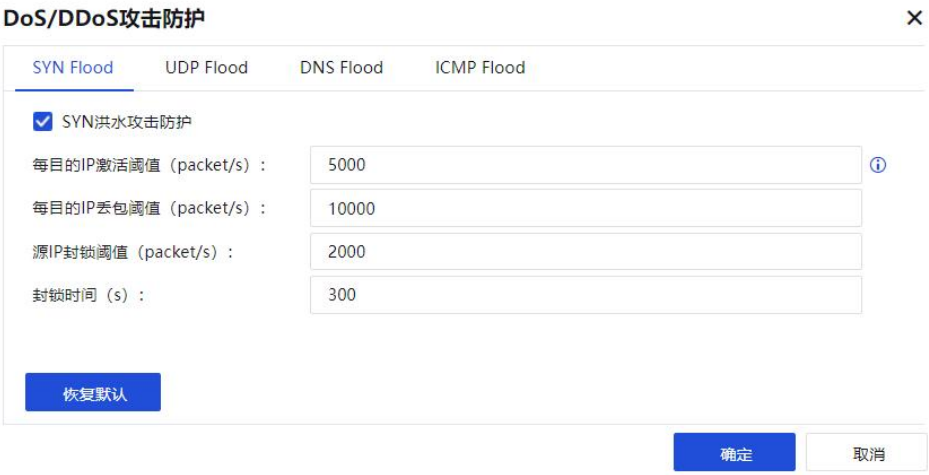
步骤1. 点击<新建>，选择外网对内网攻击防护，如下图所示。

步骤2. 点击<已选防护：IP地址扫描防护，端口扫描放>，开启扫描攻击防护，如下图所示。



步骤3. 选择网络对象，对特定的IP进行防护，如无需求选择全部即可。

步骤4. 点击<已选防护：SYN洪水防护保护...>，对DDOS攻击防护进行配置，如下图所示。



根据实际需求配置SYN、UDP、DNS、ICMP等的FLOOD参数。

步骤5. （可选）点击<高级防御>，选择对特定的攻击进行防护，如下图所示。

步骤6. 测试结果如下图所示。

6.3.3.2. 内网对外攻击防护策略

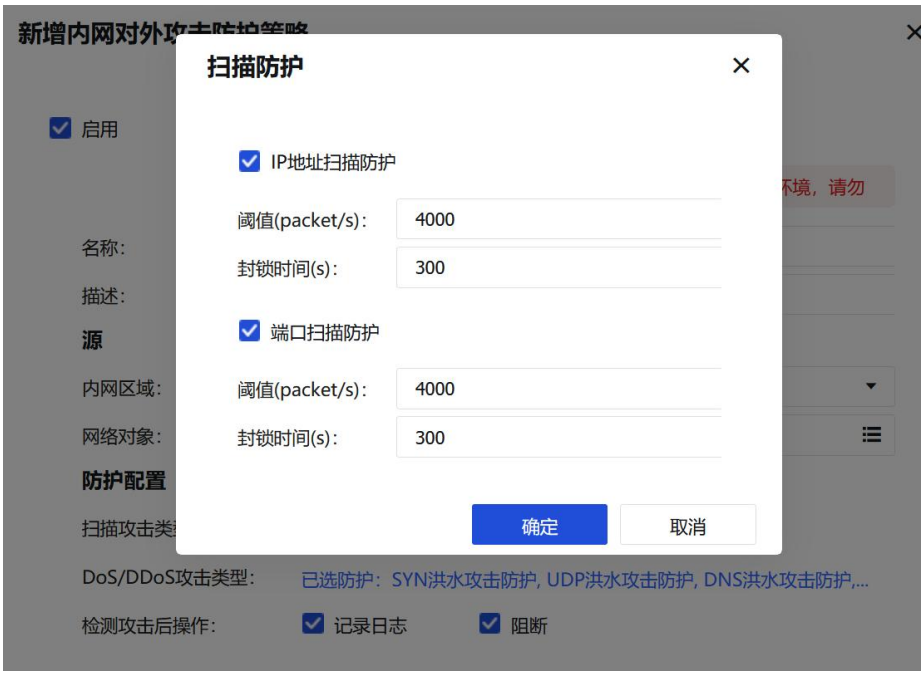
内网对外网攻击防护是为了防止内网主机变成肉机对外网进行攻击，从而带来一定的法律风险。

配置案例

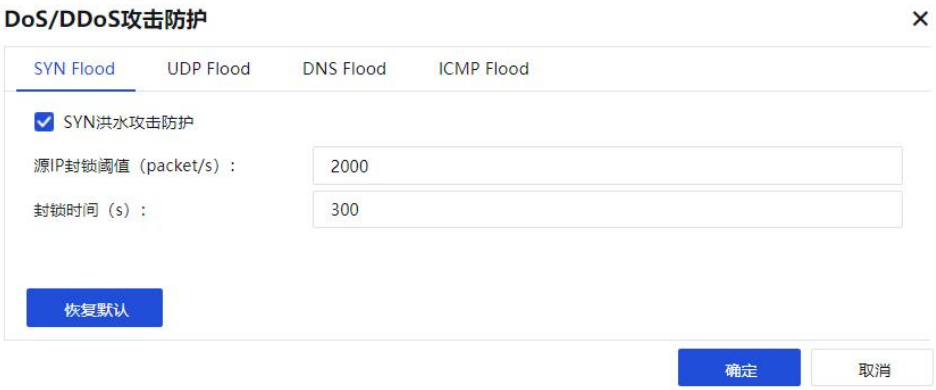
某企业办公网环境中，在互联网出口经常发些某几个终端使用过高的带宽，导致内网上网缓慢。登录终端查看，发送该终端一直对某个IP发送SYN、UDP报文。为了防护这种情况的再次发生，需要在AF上配置内网到外网的攻击防护。

步骤1. 点击<新建>，选择内网对外网攻击防护，如下图所示。

步骤2. 点击<已选防护：IP地址扫描防护，端口扫描放>，开启扫描攻击防护，如下图所示。



步骤3. 点击<已选防护：SYN洪水防护保护…>，对DDOS攻击防护进行配置，如下图所示。



根据实际需求配置 SYN、UDP、DNS、ICMP 等的 FLOOD 参数。

步骤4. （可选）点击<高级防御>，选择对特定的攻击进行防护，如下图所示。

步骤5. 配置结果如下图所示。

步骤6. 攻击效果如下图所示。

6.3.3.3. 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。

6.3.3.4. 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。

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>，

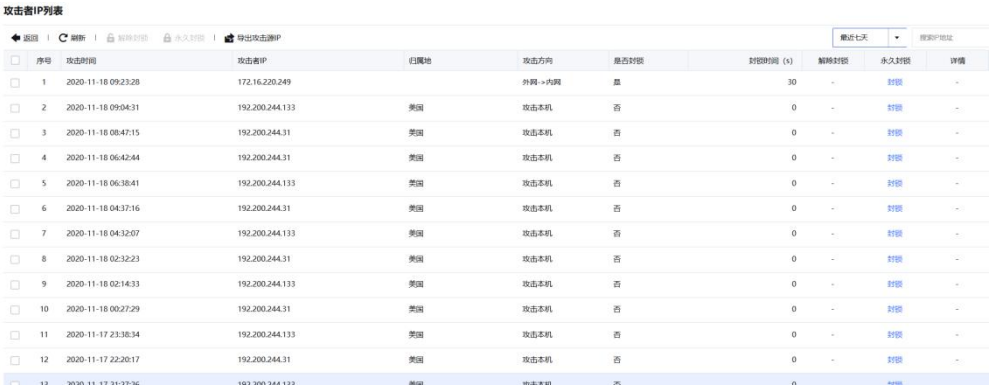
跳转到[地域访问控制]的设置页面。

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。

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。

6.3.3.5. 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。



6.4. 解密

解密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授权开启。

6.4.1. 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，对服务器的流量进行检测，从而保护服务器防止被攻击。如下图所示。

配置案例：

某企业内网发布Web应用服务器，对内外提供服务，而Web应用服务器是使用HTTPS协议传输。因此，为了防止Web服务器遭受攻击，需要对HTTPS流量进行检测，从而保护服务器的安全。

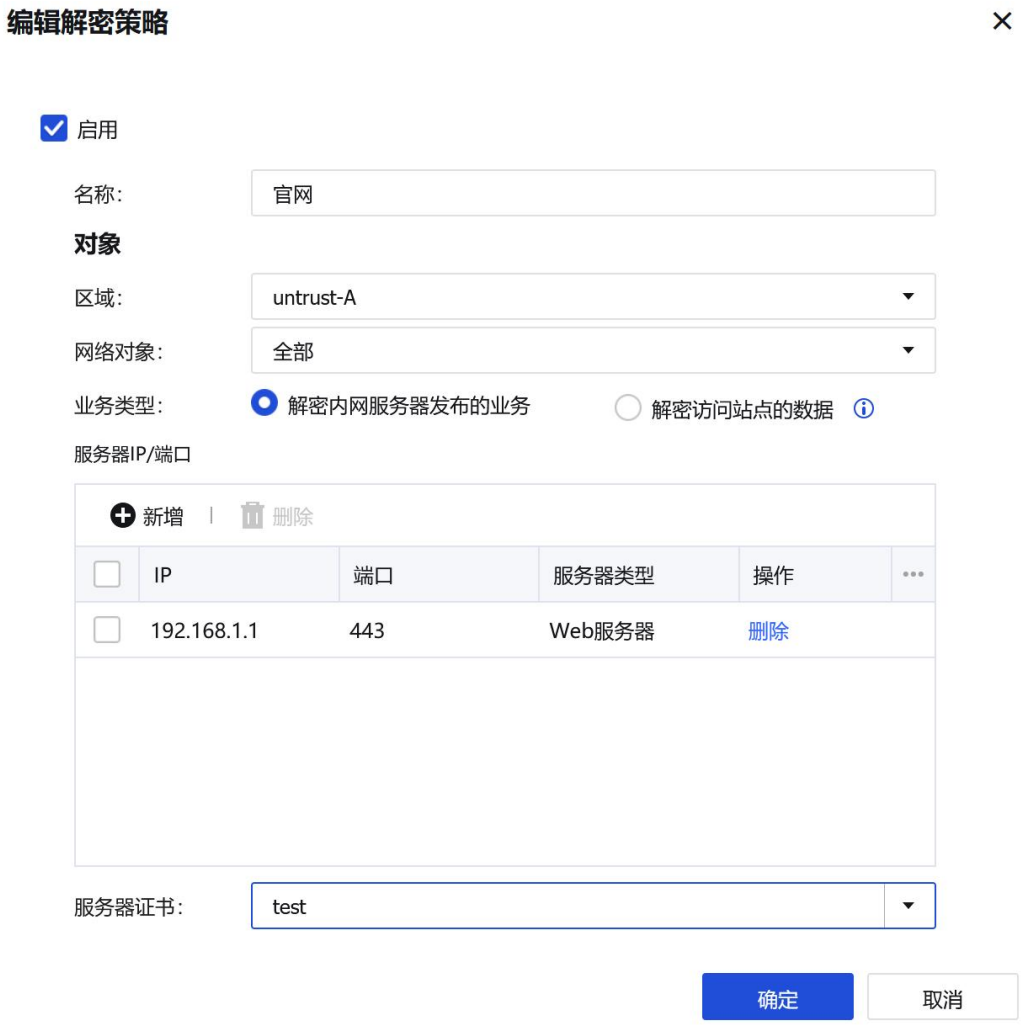
步骤1. 导入HTTPS服务器证书，点击<服务器证书>，弹出添加证书对话框，点击<

新增>，创建服务器证书，如下图所示。

表17 证书格式说明

证书格式	说明
导入一个证书文件	导入后缀为 pfx、p12 的证书文件，该文件包含公钥、私钥和密码，导入时需要输入密码对该文件进行解密。
自签名证书	根据自定义生成的证书信息。需要自己手动录入名称、国家、颁发给、密钥长度、有效期。其余为可选项。填写完成后，可以生成自签名证书。
导入一对公私钥	导入公私钥证书，公钥支持后缀为 PEM、DER 的文件，私钥支持后缀为 PEM、DER、PVK 的文件，导入完成后点击确定即可。

步骤2. 点击<新增>，创建解密策略，填写对应的信息，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。支持Web服务器、邮件服务器、FTP服务器和其他服务器。

服务器证书：选择该加密服务器的证书。需要在[服务器证书]页面导入服务器证书，可以支持选择多个服务器证书，最多支持8个。

步骤3. 点击<确定>，提交。

6.4.2. 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。

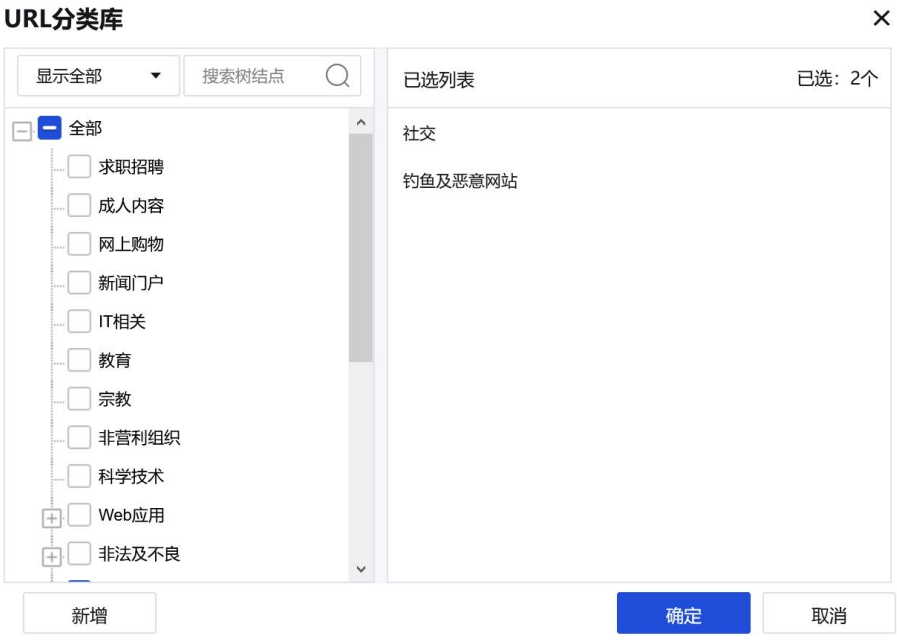
名称：填写便于识别的策略的名称。

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，从URL分类库选择需要解密的网站分类。



根证书下载：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，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。

6.4.3. 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。

说明：

1、该功能请不要随意开启，会对设备造成一定的性能压力。
2、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策略中设置即可。
3、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。

6.5. 流控

流控是通过建立流控通道对各种上网应用的流量大小进行控制。

流控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。

基本概念

流量通道：在某条线路上将整个线路带宽按百分比分割为若干份，根据应用类型或者用户组来分配不同比例的带宽资源。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：对通道的最大带宽进行设置，可设置最小带宽。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。

流量通道匹配及优先级

当流控系统处于启用：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。

6.5.1. 通道配置

6.5.1.1. 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。

保证通道设置

某公司租用了一条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。

步骤1.进入[流控/通道配置]，勾选[启用流控系统]，启用流控。

步骤2.进入[流控/虚拟线路配置]，配置虚拟线路列表和虚拟线路规则，设置方法见虚拟线路配置章节。

步骤3.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。

步骤4.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。

步骤5.勾选[启用通道]，该通道是启用状态，不勾选则为禁用状态，流控功能不生效。

通道名称：输入该通道的名称。

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，需要事先在虚拟网线通道设置中设置，关于虚拟网线通道设置参见虚拟线路配置章节。

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：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。

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。

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，点击<确定>，完成保证通道的设置。

步骤6.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。

⚠ 注意:

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%，第一条实际分配到 90/（90+30）%，即 75%。

优先级：当实际带宽有空余，优先级越高越先占用空闲带宽。

6.5.1.2. 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。

限制通道设置

某公司租用了一条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，通过流控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。

步骤1.进入[流控/通道配置]，先启用流控系统。

步骤2.勾选[启用流控系统]，启用流控。

步骤3.进入[流控/虚拟线路配置]，配置虚拟线路列表和虚拟线路规则。

步骤4.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>，新增一级通道，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：可设置生效线路、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，当数据走此条线路时才会匹配到此通道。

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。

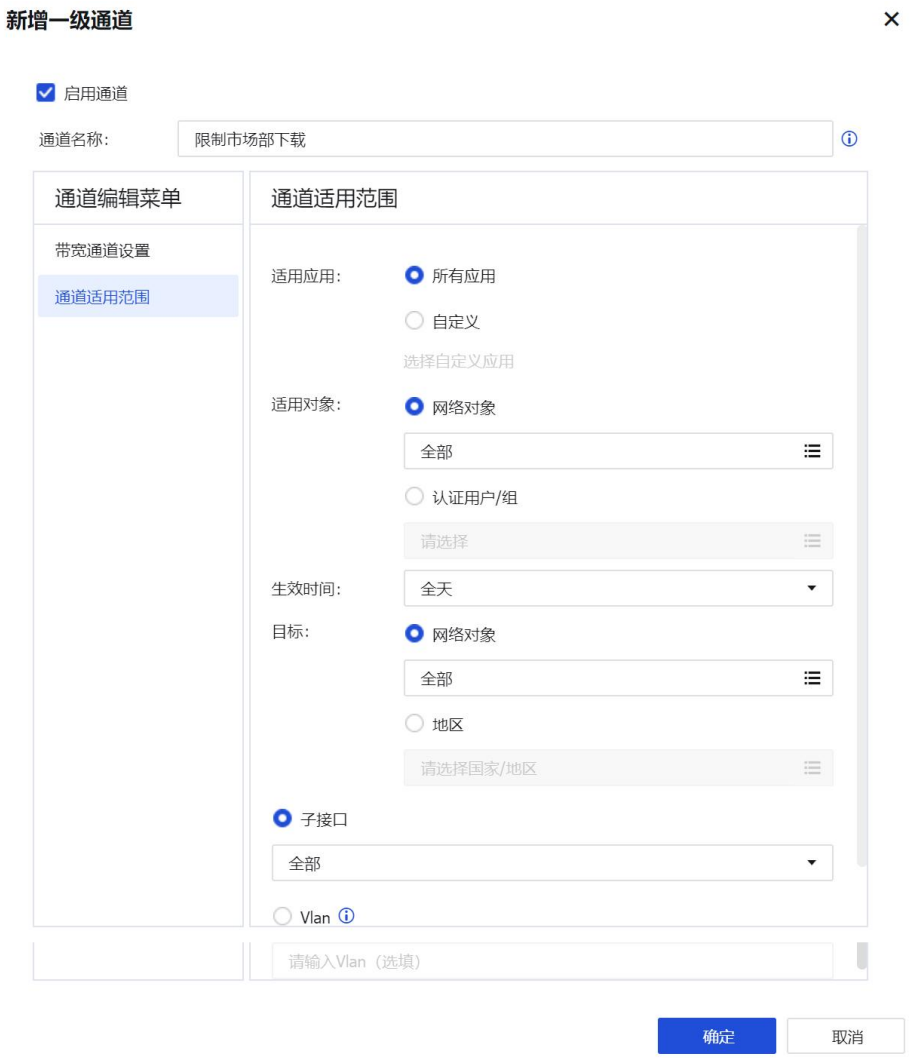
启用限制单IP最大带宽：用于限制匹配到此通道的单个IP占用的带宽值，此例中需要对市场部每个用户P2P、下载等数据的占用带宽限制在30KB/s，在[上行]、[下行]中分

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。



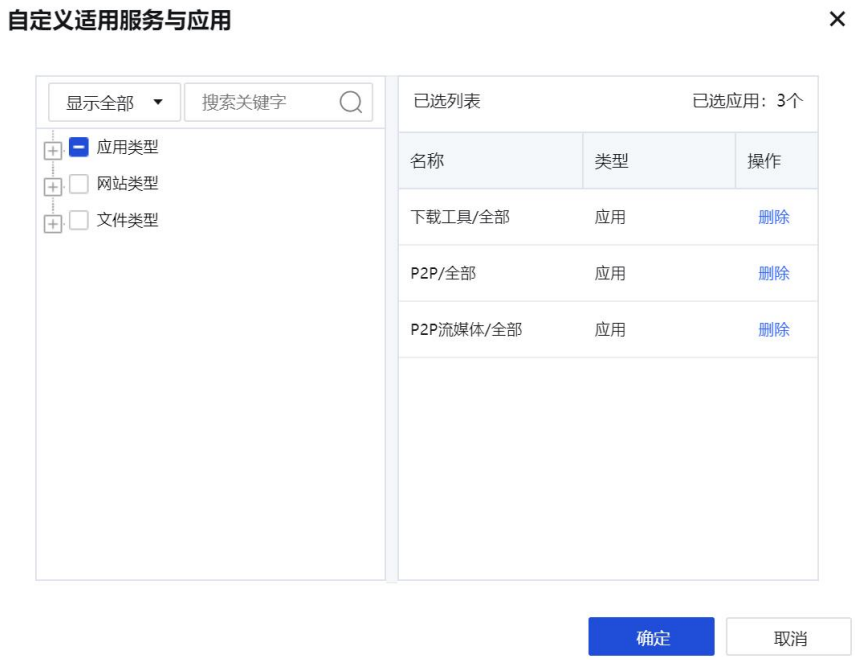
适用应用：用于设置应用类型。

所有应用:表示针对所有类型的数据有效。

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。

设置完成后，点击<确定>，完成限制通道的设置。

步骤5.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。

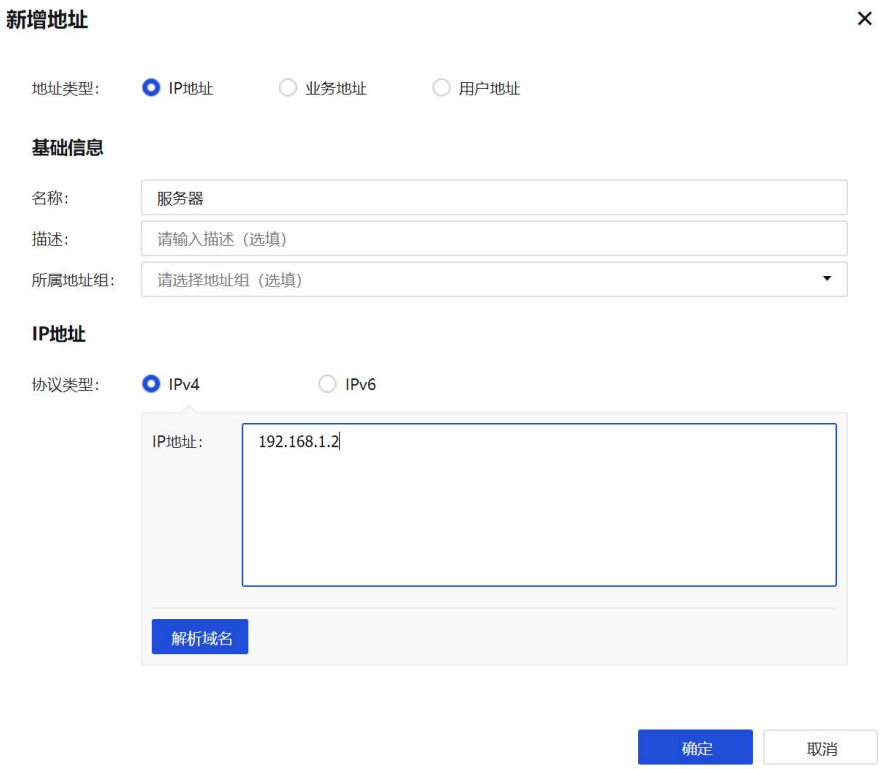
6.5.1.3. 排除策略

排除策略用于设置某些类型的数据不匹配任何流控通道，设置排除策略的目的在于排除部分数据不受流控策略的限制，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控，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。

排除策略用户设置

当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。

步骤1. 在[对象/网络对象]新增IP组，将需要排除的IP地址添加进去。



步骤2. 点击进入[流控/通道配置/排除策略]，点击<新增>，添加排除策略。

步骤3. 设置排除策略。填写策略名称，应用类型选中全部，目标IP组选择步骤1中设置的[服务器]。

步骤4. 点击<确定>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。

6.5.2. 虚拟线路配置

6.5.2.1. 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。

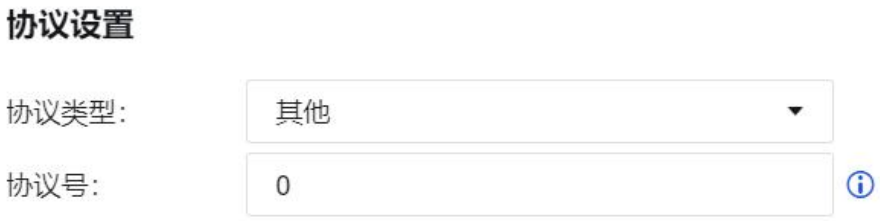
⚠ 注意:

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。

6.5.2.2. 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/流控/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，设置如下图所示。



协议设置：用于指定数据包的协定；其中包括的协议类型有：TCP、UDP、ICMP，如果还有其他类型的选择其他，且在协议号输入协议号范围。

内网范围：用于设置数据包的源IP和源端口的条件；包括IP地址和内网端口，IP地址包括IPV4和IPV6，输入具体IP地址或者IP范围即可。

外网范围：用于设置数据包的目标IP和目标端口条件，包括IP地址和外网端口，IP地址包括IPV4和IPV6，输入具体IP地址或者IP范围即可；端口可选择所有端口或者指定

端口和范围。

目标线路：指定匹配该虚拟线路规则的数据包匹配那条虚拟线路，即从哪个接口转发。

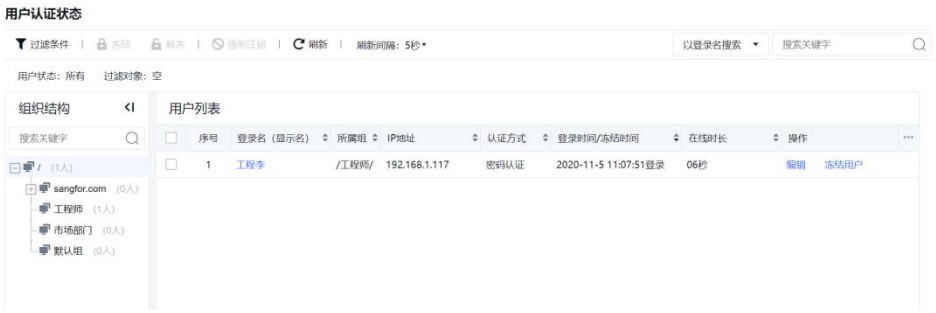
当虚拟线路成为某条虚拟线路规则的目标线路后，针对该线路作为流控通道才生效。

6.6. 认证

介绍用户管理和用户认证的定义、认证方式和使用方法。

6.6.1. 用户认证状态

用户认证状态主要用于管理已经通过设备认证的在线用户，如下图所示。



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。

表18 用户认证功能说明表

参数	说明
过滤条件	过滤条件有用户状态和对象可选，用户状态分为所有、冻结和活跃可选，对象有用户名称和 IP 可选。
冻结/解冻	选择一个或多个用户，点击<冻结>来冻结用户，使其不能上网，设置冻结的时间，超过设置的时间后用户能正常上网； 选择被解冻的用户，点击<解冻>来解冻被冻结的用户能正常上网；
强制注销	管理员可强制注销在线用户，但不能对不需要认证和临时用户进行注销。
搜索	以登录名或者 IP 地址来搜索指定用户来进行定位。

6.6.2. 用户管理

用户管理的作用是管理所有访问互联网的用户，用户是指访问网络资源的主体，是“谁”在进行访问，是网络访问行为的重要标识。

管理员可以通过[组/用户]页面来对上网用户进行统一管理。FW上的用户包括上网用户和接入用户两种形式：

- 上网用户

内部网络中访问网络资源的主体，如企业总部的内部员工。上网用户可以直接通过FW访问网络资源。

- 接入用户

外部网络中访问网络资源的主体，如企业的分支机构员工和出差员工。接入用户需要先通过SSL VPN、IPSec VPN或PPPoE方式接入到FW，然后才能访问企业总部的网络资源。

6.6.2.1. 组/用户

为了实现基于用户管理，需要对访问网络的用户进行身份认证，来对所有用户进行上网行为的管理。

用户类型

1. 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。

2. 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）。

组/用户

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。

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。

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：点击 » 选择[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地址和按MAC地址三种可选条件。

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。

6.6.2.2. 组/用户管理

管理员可对用户组和用户进行新增、删除、批量编辑、导入导出等操作。

表19 组/用户管理功能说明

功能项	说明
删除组/用户	当不需要的组或用户删除，选择需要删除的[组/用户]，勾选<删除>即可。当[认证策略|LDAP 自动同步|应用控制策略|流量管理|安全防护策略]关联了需要删除的用户/组，则此用户/组将无法直接删除，需要先把引用关系解除，才能将该用户/组删除。
编辑/批量编辑	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高级属性中的终端绑定，即 IP、MAC 绑定。因为这一项设置具有唯一性，不能编辑多用户时设置。
导入/导出	可以将组/用户的数据批量导入或者导出设备。 以通过 CSV 的文件导入用户，通过一个 CSV 的文件导入用户，导入用户时可以同时导入显示名、所属组、密码、允许登录的 IP 范围、是否公用账号、自定义属性等。如果导入用户时指定的所属组不存在，也会自动建立用户组。 直接勾选需要导出的组和用户。当某个用户组没有用户时，此用户组不支持单独导出。

高级搜索	可以设置查询条件和范围：IP 和 MAC 进行筛选，其他选项可以自己定义来查询。
上移/下移/移动到	本地的用户和用户组，支持移动。可以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并且使用目标组的上网策略。对于普通管理员而言，可能只有管理部分组的权限，在移动组/用户时，无法移动到没有权限管理的用户组。

6.6.2.3. 新增用户/组

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。

新增子组

设备默认自带的组为root组(根组)，不能进行删除和编辑，新增的组都是root组的子组。根组是一级组，根组下新增的组是二级组，依此类推，本地组最多支持16级组织架构，包括根组。这样的设计更符合公司的组织架构，方便管理。例如：在根组下新增一个工程师组。

步骤1. 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，选择新增类型组。

步骤2. 进入新增组页面。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。

步骤3. 点击<确定>，完成子组添加。

6.6.2.4. 常用案例 1

企业内网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。

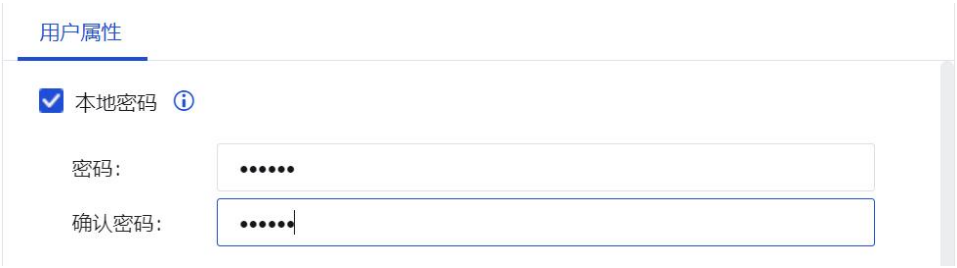
步骤1. 企业需求是：192.168.1.0/255.255.255.0网段的计算机全部采用用户名密码的认证方式。所以首先需要设置这个网段用户的认证方式。

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。区域的定义请参考区域配置。

步骤2. 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，选择新增类型用户。

步骤3. 进入[新增用户]窗口。启用该用户，填写登录名、描述、显示名和当前所属组。

步骤4. 设置[用户属性]，用户属性设置包括：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。



步骤6.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]。

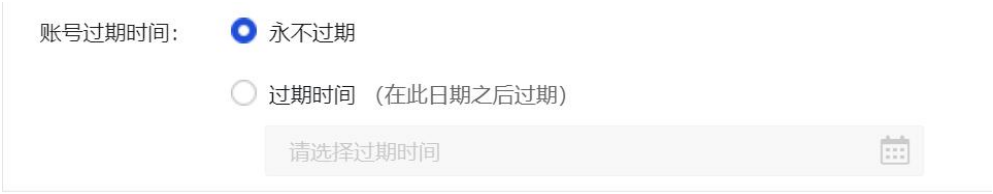
勾选[绑定IP]，在输入框中填入192.168.1.2-192.168.1.100。

步骤7.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。

步骤8.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。

步骤9.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。

过期时间：用于设置该用户的过期时间。



步骤10.完成用户属性的编辑后，点击<确定>，完成用户的添加。

步骤11.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。

⚠ 注意：

[绑定 IP/MAC 地址]：分两种绑定方式分别为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，并且指定的地址只能是该用户使用。

6.6.2.5. 常用案例 2

企业内网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192.168.1.117/00-0C-29-7F-0B-47（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）。

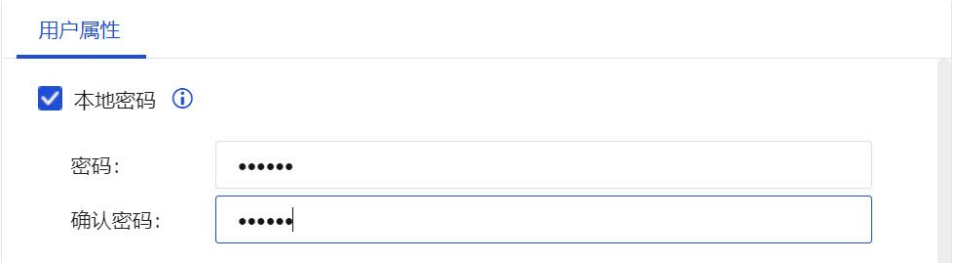
企业需求是：192.168.1.0/255.255.255.0网段的计算机全部采用用户名密码的认证方式。所以首先需要设置这个网段用户的认证方式。

步骤1.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。

步骤2.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。

步骤3.进入[新增用户]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。

步骤4.设置[用户属性]，勾选本地密码，在密码：输入用户登录认证的密码。



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/ 00-0C-29-7F-0B-47（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）。

步骤5.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(00-0C-29-7F-0B-47)。

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[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。

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。

过期时间：用于设置该用户的过期时间。

步骤6.完成用户属性的编辑后，点击<确定>，完成用户的添加。

步骤7.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，提示如下图所示。

其他用户在此IP/MAC认证，也会提示认证不通过。

⚠ 注意：

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 地址或者计算机名作为用户名。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。

6. 6. 2. 6. 常用案例 3

在“/工程师”组设置一个用户为主管，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(00-0C-29-7F-0B-47)。

步骤1.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。

步骤2.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，选择新增类型[用户]。

步骤3.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。

步骤4. [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/ 00-0C-29-7F-0B-47（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）。

步骤5.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(00-0C-29-7F-0B-47)。

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。

过期时间：用于设置该用户的过期时间。

步骤6.完成用户属性的编辑后，点击<确定>，完成用户的添加。

步骤7.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。

6.6.3. 用户导入

[用户导入]用于把用户批量导入，提供CSV格式文件导入、扫描IP导入、从外部LADP服务器上导入用户三种方式。

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，那么同时也可以自动创建对应的用户组。

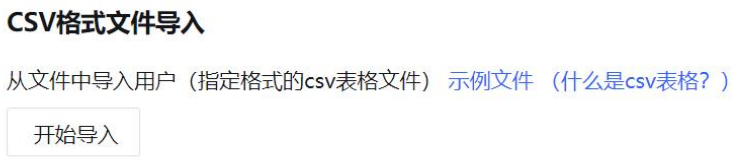
扫描 IP 导入：当导入 IP/MAC 绑定的用户时，可以通过[扫描 IP 导入]：扫描内网用户的 MAC 地址，方便此类用户的导入。通过此方法导入的用户默认都属于根组，并且认证方式是不需要认证，绑定 IP/MAC，用户名是通过扫描得到的机器名。当导入的用户 IP 和已有的用户绑定的 IP 有冲突时，无法导入此用户。

从外部 LADP 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。当使用域用户导入时，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。

6.6.3.1. 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。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。

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。



步骤1. 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					
11	李四		/总部/研发/	本地密码为空		10.0.10.10		N	N	
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		##########

步骤2. 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。

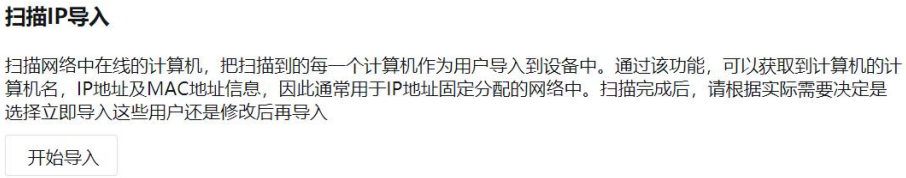
勾选[用户所属组不存在时，自动创建]：表示导入用户指定的用户组不存在时，设备会自动新建该组，反之不勾选则不会新建该组，用户会默认导入到根组。

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，更新此用户的属性；选择跳过，不导入该用户：表示当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。

6.6.3.2. 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。



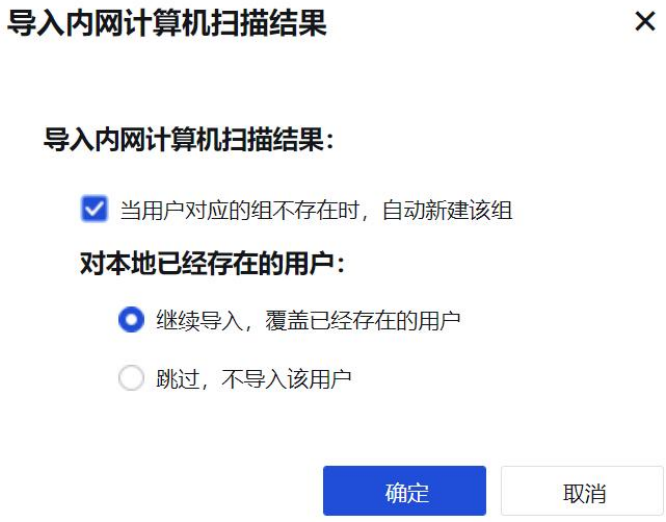
6.6.3.3. 扫描 IP 配置案例

扫描内网192.168.1.100-192.168.1.200范围内的计算机，并导入到用户列表中。

步骤1. 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。

步骤2. 点击<开始扫描>，扫描出192.168.1.100-192.168.1.200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。

步骤3. 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。

步骤4. 点击<确定>按钮，用户将被导入到根组中。

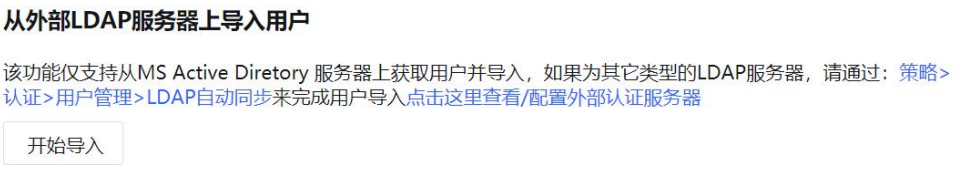
⚠ 注意:

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。

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 Diretory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。

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]）。



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。

6.6.4. LDAP 自动同步

[LDAP自动同步]主要是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，设备每天会与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。

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。

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。

6.6.4.1. LDAP 自动同步案例

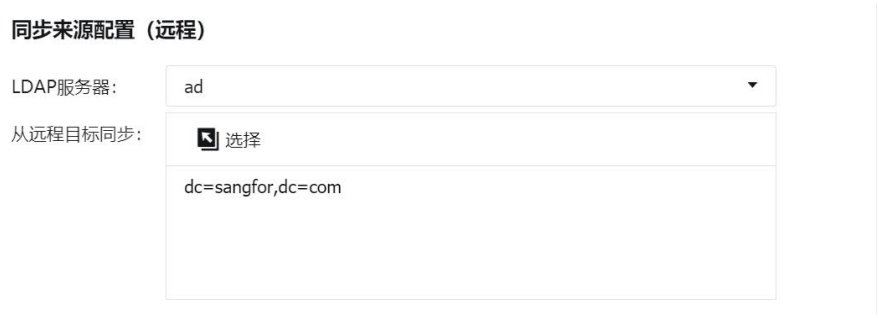
某企业需要将LDAP服务器中的组织结构同步到设备中，并保持和LDAP服务器同步，需要AF配置LDAP自动同步。

步骤1. 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，具体请参考外部认证服务器配置。

步骤2. 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。

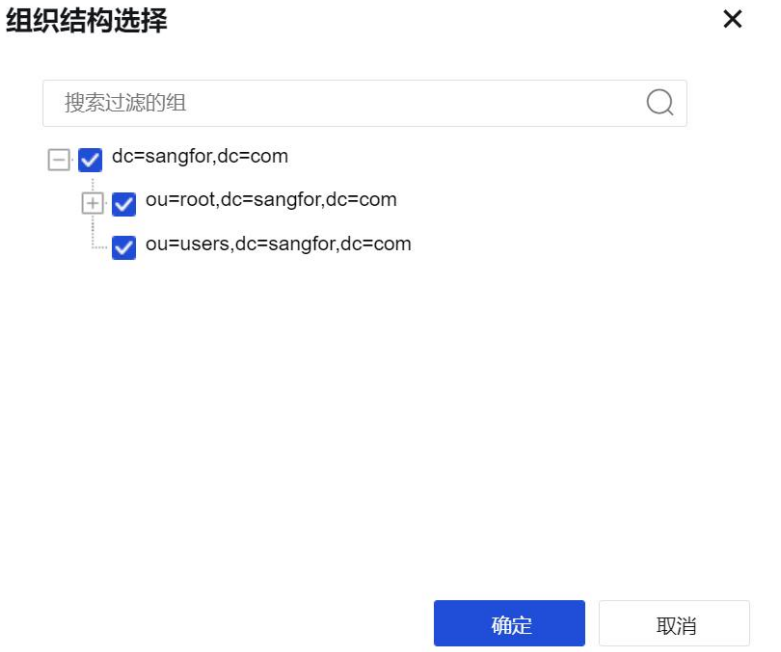
步骤3. 在[LDAP同步]窗口中，设置策略名称、策略描述、同步工作模式、自动同步。[同步工作模式]选择按组织结构（OU）同步，自动同步选择启用，自动同步一天同步一次。

步骤4. 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。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。

步骤5. [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，根据需求进行选择。

同步 LDAP 的 OU 组织结构和用户到本地：表示将 OU 作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。

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。

同步 LDAP 的 OU 组织结构到本地，不导入用户：表示只将 OU 作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。

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。

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。在[组织结构选择]窗口选择相应的组，选择完成点击<确定>。

步骤6. 设置完同步策略，点击<确定>，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，或等到自动一天一次进行同步。

步骤7. 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]，如下图所示。此时导入的OU和用户同LDAP服务器中的完全一致。

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。

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。

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。

6.6.5. 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。

根据认证方式，可以分为以下几种类型：

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。

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，降低了用户对上网的体验。

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，通过计算机的名称来识别用户。

优点：用户访问网络前不会在浏览器中弹出认证框输入用户名，密码。因用户不会感知到设备的存在；

缺点：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。

6.6.5.1. 认证策略

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。

管理员可以对所有的认证策略进行删除操作、批量编辑、启用和禁用、导入、上移/下移等操作，也能进行过滤选择。

表20 认证策略界面说明

字段名称	说明
新增策略	认证策略列表页面，可点击新增一条新的认证策略。
删除策略	认证策略列表页面，可点击删除相应的策略。
编辑/批量编辑	在认证策略列表页面，勾选需要编辑的认证策略，点击认证策略名称，设备会弹出认证策略的编辑页面，修改选中策略的相关信息。 批量编辑：勾选多个自定义的认证策略，可编辑策略的适用对象，其他信息不可以修改。
导入	支持认证策略的导入，点击导入，选中需要导入的认证策略文件，即可进行导入。
启用/禁用	选中已禁用的策略，点击启用，该策略即可生效，选中已启用的策略，点击禁用，该策略会失效。
上移/下移	由于策略是自上而下进行匹配，所以可以选中相应的策略，点击上移或者下移，或自定义移动，来进行优先匹配策略。

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。

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。

创建不需要认证的用户是方式：

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）。

在[认证策略]中设置不需要认证，并以 IP 地址或者 MAC 地址或者计算机名作为用户名。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。

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。

步骤1. 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。

步骤2. 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。

步骤3. 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。

认证的顺序是先本地认证，再外部认证。

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。

步骤1. 对指定的网段设置认证策略为：必须使用单点登录

步骤2. 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。

步骤3. 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：[认证策略]选择不需要认证，新用户选择以IP地址作为用户名或者以MAC地址作为用户名或者以计算机名作为用户名；单点登录用户；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。

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。

步骤1. 勾选[开启用户认证]按钮；

步骤2. 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。

6.6.5.2. 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）

步骤1. 设置[外部认证服务器]，设置LDAP认证服务器。

步骤2. 设置[用户认证/认证策略]，点击<新增>，弹出[认证策略]窗口。名称：填写认证策略的名称，必填项，描述：填写对策略的描述，补充说明，可选项。

策略适用IP/MAC范围：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。

步骤3. 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，勾选[本地密码认证/外部密码认证/单点登录]。

步骤4. 设置[认证策略/新用户选项]，设置对新用户的处理方式。

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]中设置未通过认证用户权限。

步骤5. 设置其他网段用户的认证策略，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]。

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，设置顺序如下图所示。

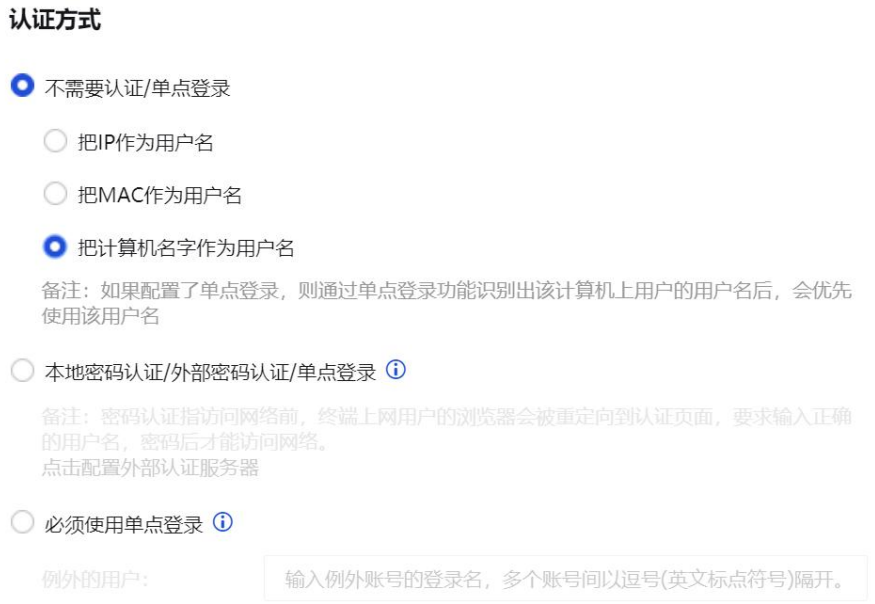
6.6.5.3. 认证策略配置案例 2

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。

步骤1. 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。

步骤2. 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。

步骤3. [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]。



步骤4. [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。

步骤5. 点击<确定>按钮，完成策略编辑。

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看到，不会加到指定的本地组中。

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。

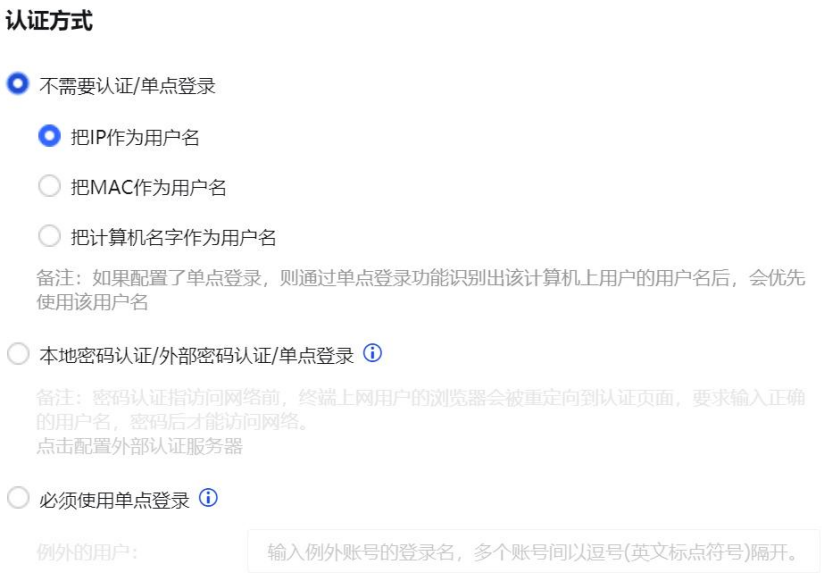
6.6.5.4. 认证策略配置案例 3

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”。

步骤1. 设置[外部认证服务器]和[LDAP自动同步]。

步骤2. 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。

步骤3. 认证方式选择[不需要认证/单点登录]，勾选[把IP作为用户名]。



步骤4. [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。

步骤5. 点击<确定>按钮，完成策略编辑。

6.6.5.5. 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。

单点登录选项

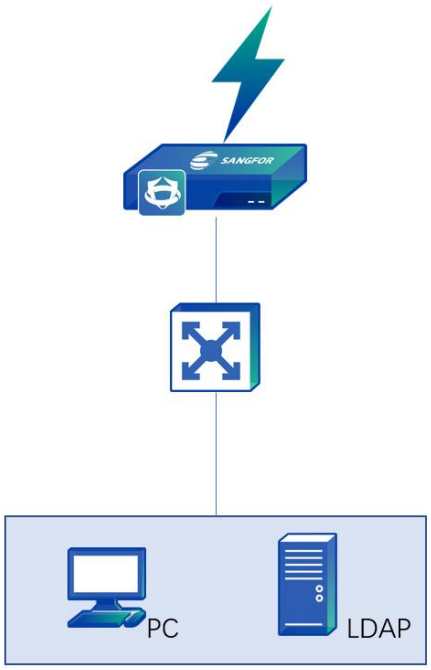
当客户有自己的第三方认证服务器对内网用户进行认证时，单点登录可以实现在内网用户通过第三方认证服务器认证时同时通过设备的认证，并且获取到相关的权限上网。设备上使用和第三方认证服务器同一套用户名密码。目前设备支持的单点登录类型包括：AD域单点登录、Proxy单点登录、POP3单点登录和Web单点登录。此处设置的是只是实现单点登录的基本方法，完成单点登录的配置还需要配置用户、认证服务器以及用户的认证方式，分别在用户管理、外部认证服务器、认证策略中设置。

域单点登录

如果企业的网络中已有一台微软AD域服务器做用户管理，并且企业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，即终端用户登录域即可上网，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）。

6.6.5.6. 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。



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防火墙设备。

配置步骤

步骤1. 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。

步骤2. 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：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，下载脚本用于步骤3，步骤4的设置。

⚠ 注意：

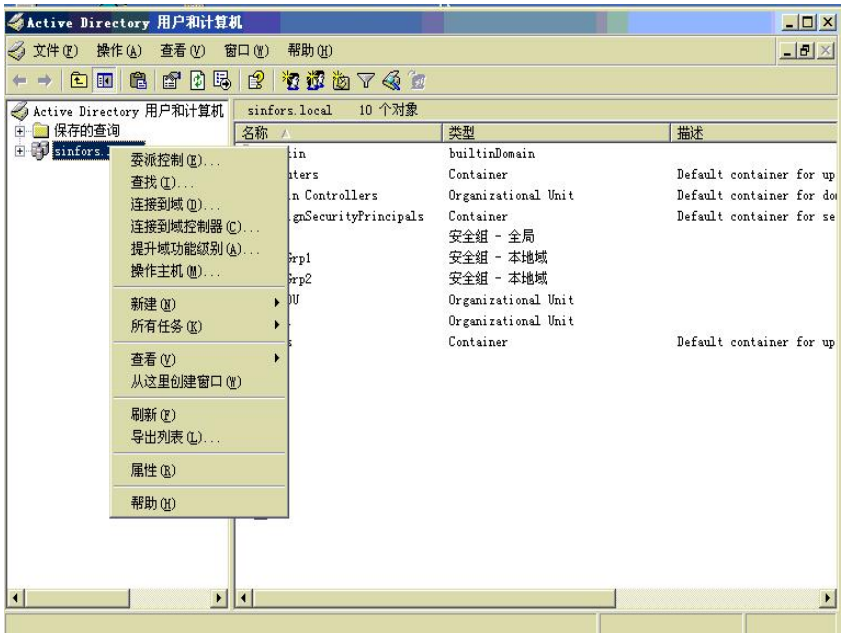
此处支持 AC11.0R2 及以上版本，同步认证信息到 AF，端口为 1775。

步骤3. 在AD域服务器上配置登录脚本程序。

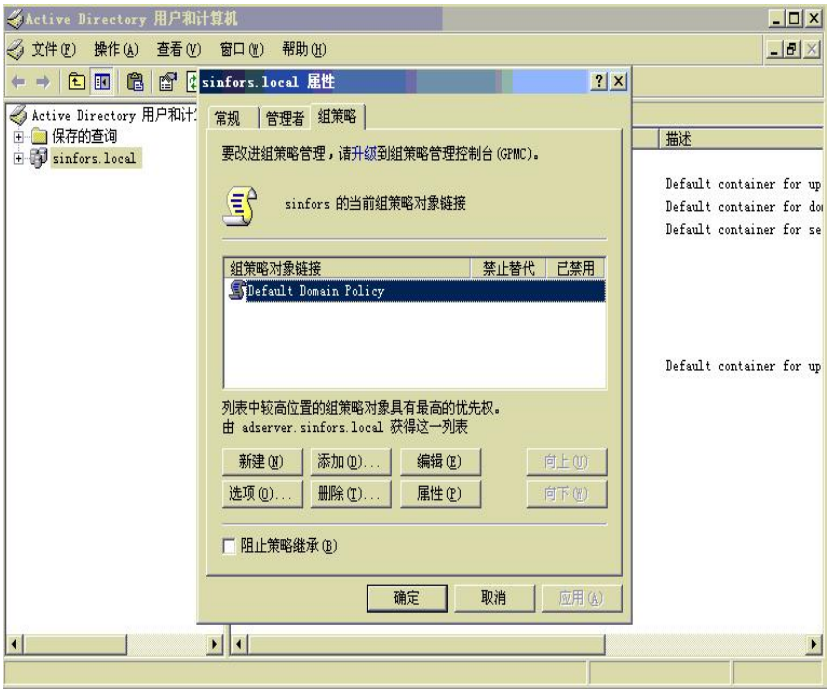
1. 登陆域服务器后，打开“管理您的服务器”菜单，如下图所示。

2. 选择“管理Active Directory中的用户和计算机”选项。

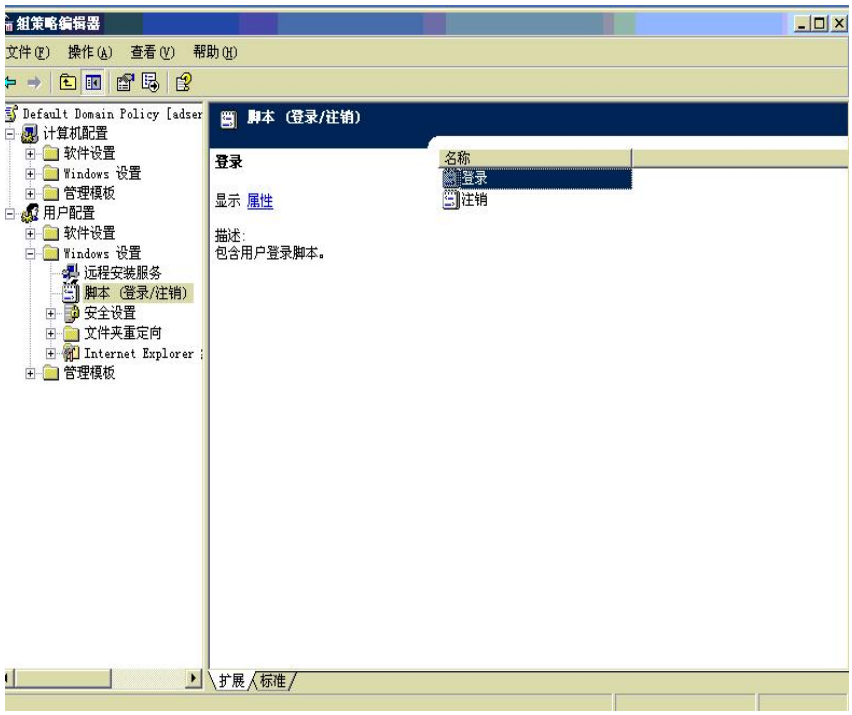
3. 在弹出的窗口中右键所要监控的域，选择属性。



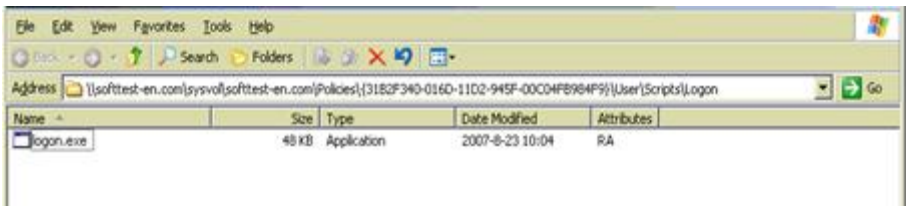
4. 在弹出的窗口中，点击组策略选项，在组策略窗口中，双击其中的组策略“Default Domain Policy”。



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(登陆/注销)”。

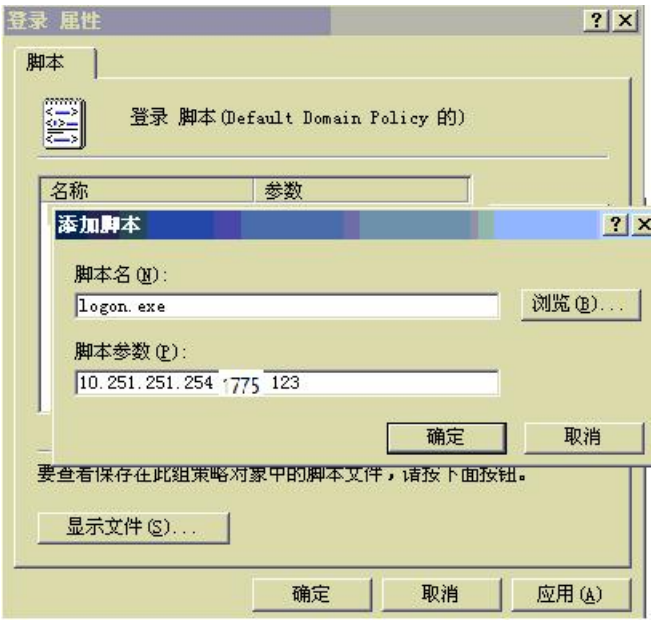


6. 双击右边的“登陆”选项，在弹出的登陆脚本编辑窗口左下脚点击“显示文件”，将打开一个目录然后将登陆脚本文件保存在该目录下，关闭该目录。

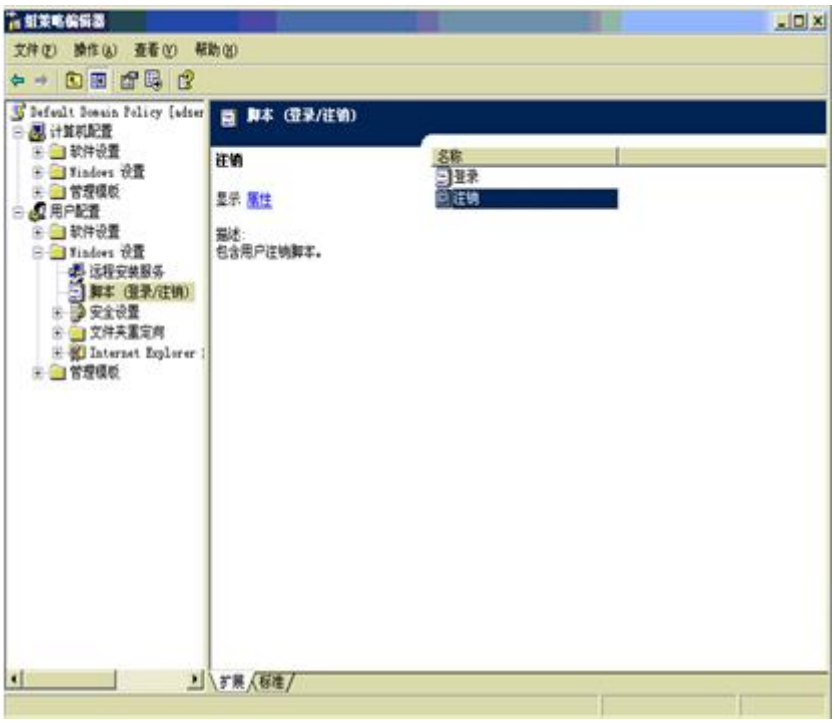


7. 在弹出的登陆脚本编辑窗口中单击添加按钮，在添加脚本窗口中，点击浏览，选择保存的登陆脚本文件(即logon.exe)，并在脚本参数中输入IP(IP是属于设备端的

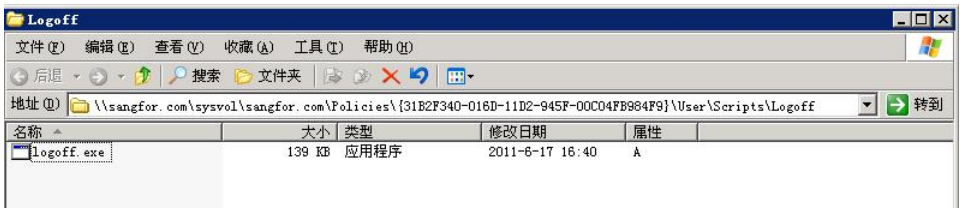
IP)，端口号(固定是1775)，密钥(必须与设备端设置的密码一致)。注意每个参数以空格分隔，后点击应用后点击确定，依次关闭所有组策略属性页面布局。



8. 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。
9. 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。



10. 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。



11. 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。

12. 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。

步骤4. 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。

步骤5. 用PC登录域，登录域成功后即可上网。

13. 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。
14. 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。
15. 要求域服务器IP，设备IP以及用户PC能够相互通信。
16. AF和与服务器通信使用的是1775端口。

6.6.5.7. 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和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<确定>，保存配置。

6.6.5.8. 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和勾选启用集成windows身份验证。

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<确定>。

高级选项中可配置认证失败后重定向间隔。

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。

⚠ 注意：

1.在域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证框)

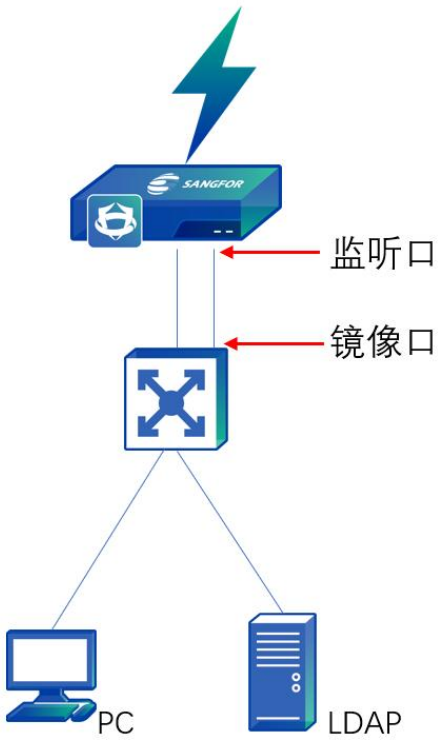
3.kerberos 认证不会踢密码认证的用户

4.含有`~!#$%^&*+\|{};:“” ‘’ ,/<>?等特殊字符的域账号登陆时，不支持认证（仅 AF 不支持）

6.6.5.9. 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登陆域的整个过程都会被设备监听到。

2. 如果用户登陆域成功，则自动通过设备认证。

配置步骤

步骤1.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。

步骤2.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。

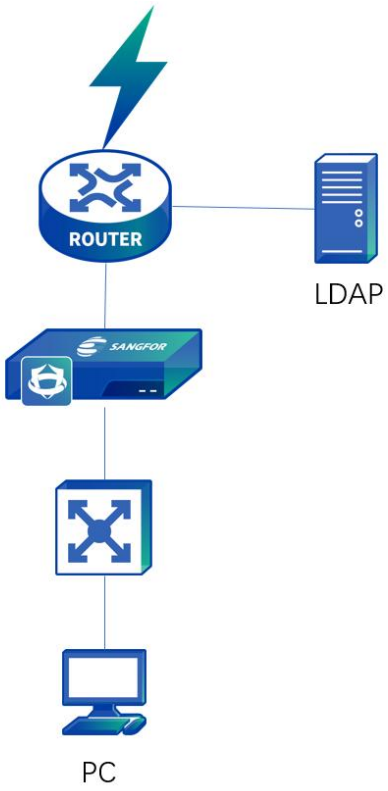
步骤3.勾选[监听计算机登录域的数据，获取登录信息]，表示使用监听模式实现单点登录。在[监听的域控制器地址列表]：中输入域服务器的IP和监听端口，如果有多个域服务器，则一行一个IP和端口，如下图所示。

步骤4.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。

步骤5.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。

步骤6.PC登录域，登录成功后即可上网。

第二种情况：域服务器在WAN口方向



数据流过程如下。

3. PC登陆域可穿透设备。
4. 设备的内网接口同时作为监听口，无需再设置监听口。

配置步骤

步骤1. 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。

步骤2. 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。

步骤3. 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。

步骤4. PC登录域，登录成功后即可上网。

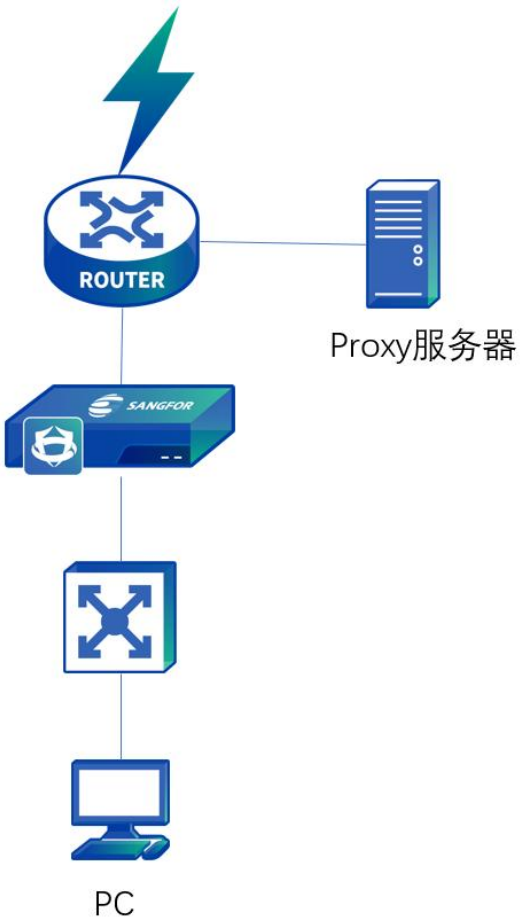
⚠ 注意：

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。

6.6.5.10. 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WAN口方向，如下图所示。



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。

配置步骤

步骤1. 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。

步骤2. 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。

步骤3. 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。

步骤4. PC登录Proxy服务器，登录成功后即可上网。

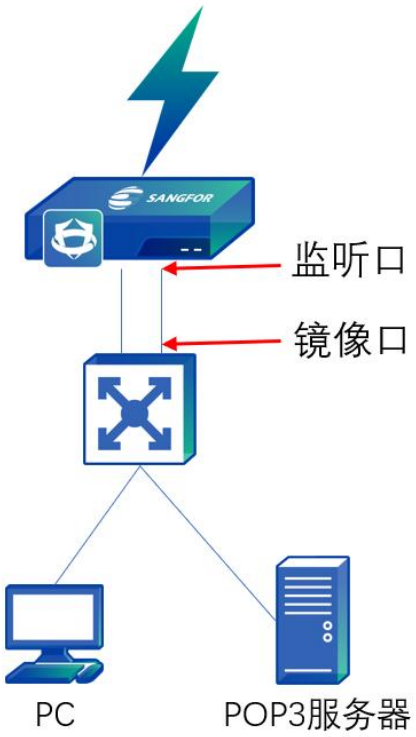
如果Proxy服务器在外网，要启用自动认证，则必须在根组中开放访问Proxy这个服务

器的权限，并在[认证选项/其他认证选项]中勾选[未通过认证用户可以访问基本服务（HTTP除外）]。如下图所示。

6.6.5.11. POP3 单点登录

企业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，上网不需要再次需入密码。
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。

配置步骤

步骤1.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。

步骤2.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。

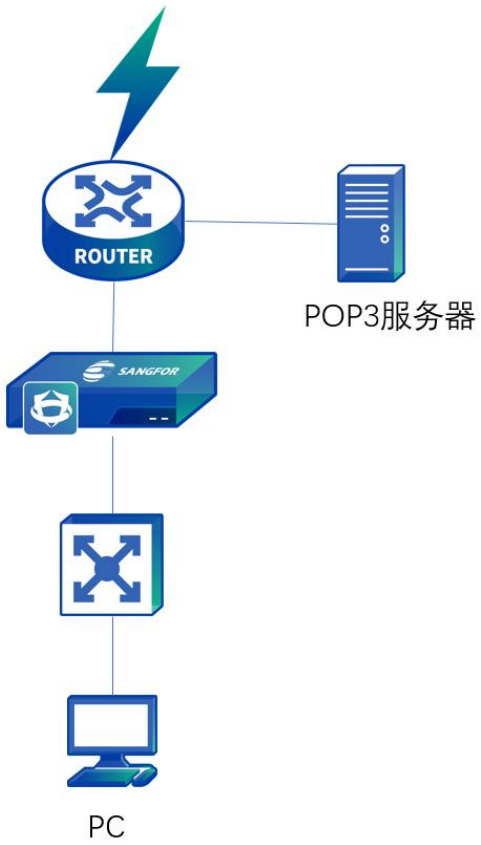
勾选[启用POP3单点登录]：启用POP3单点登录功能，在[邮件服务器地址列表]：中输入POP3服务器的IP和监听端口，如果有多个POP3服务器，则一行一个IP和端口，此处的端口设置POP3认证的端口（一般默认是TCP110）。

步骤3.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。

步骤4.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。

步骤5. 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WAN口方向。



数据流过程如下：

1. PC登陆P0P3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。

配置步骤

步骤1.设置认证POP3服务器，进入[用户认证/认证选项/外部认证服务器]进行设置。

步骤2.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。

步骤3.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。

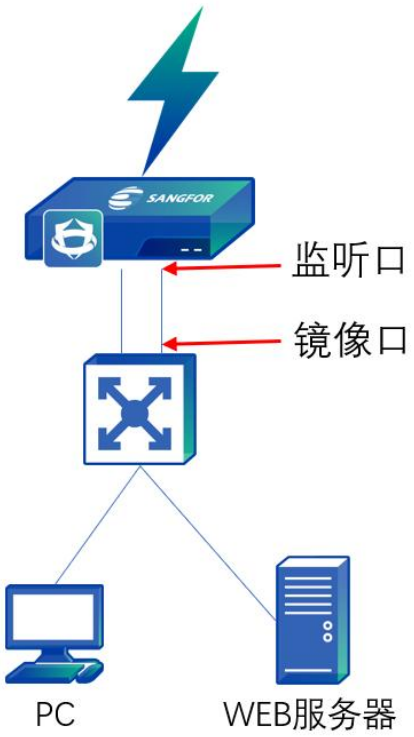
步骤4.PC通过邮件客户端收发一次邮件，登录POP3成功后即可上网。

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/其他认证选项]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。

6.6.5.12. 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，且账户信息均保存在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：

3. 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。
4. 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。

配置步骤：

步骤1.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[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]。

步骤2.在[Web认证服务器]：中填写Web认证服务器地址。

步骤3.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。

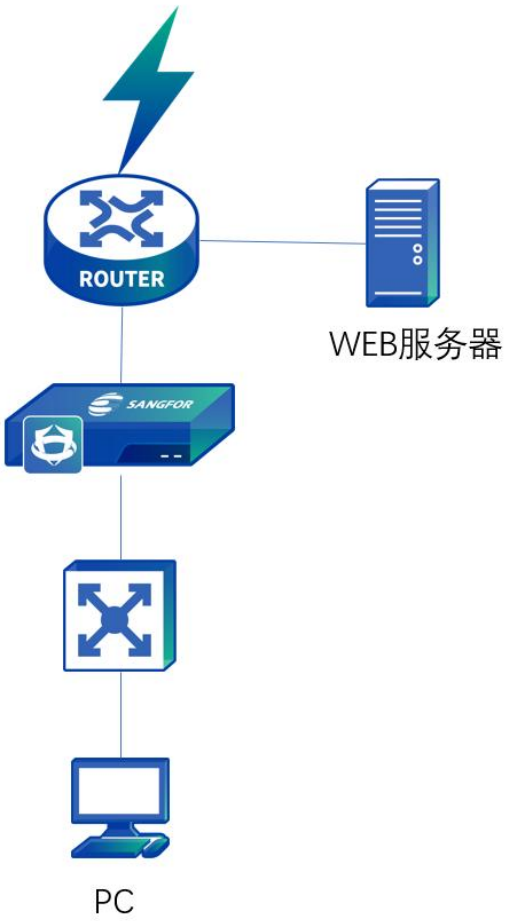
步骤4.填写[用户表单名称]，用来填写Web认证时，向服务器提交用户名表单名称。

步骤5.选择[认证成功关键词]：或者[认证成功关键词]，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。

步骤6.设置监听口，点[其他选项]，勾选[设置监听镜像网口]，选择监听口。

步骤7.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WAN口方向。



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。

配置步骤

步骤1.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[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]。

步骤2.在[Web认证服务器]：中填写Web认证服务器地址。

步骤3.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。

步骤4.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

步骤5.选择[认证成功关键词]：或者[认证成功关键词]，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。

步骤6.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。

6.6.5.13. 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]：填写Radius服务器的地址。

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。

6. 6. 5. 14. 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。

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。

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。

认证冲突

[认证冲突]用于不允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。如下图所示。

6.6.5.15. 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：AF设备会定期发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。

配置步骤

步骤1.在三层交换机上开启SNMP功能。

步骤2.点击进入[用户认证/认证选项/跨三层MAC识别]进行设置，在设备接口勾选[启用SNMP设置]，启用SNMP功能。

步骤3.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。

步骤4.在[SNMP服务器列表]添加服务器，点击<新增服务器>，会弹出[新增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。如下图所示。

步骤5.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。

步骤6.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，需手动设置SNMP服务器信息。

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，配置页面如下图所示。

3. 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
4. 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。
5. 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。
6. 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和HTTPS服务外的根组权限。
7. 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。
8. 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。
9. 登录页面需要安装根证书后，才允许用户登录：解密功能通过此选项安装SSL证书。

6.6.5.16. 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。

LDAP服务器

在[策略/认证/用户认证/外部认证服务器]页面， 点击<新增>，选择[LDAP服务器]，会弹出[外部认证服务器（LDAP）]窗口，填写服务器名称。

基本配置：

服务器地址：填写对接AC的LDAP服务器地址。

认证端口：LDAP服务器连接的端口。例如AD域在未启用SSL/TLS加密时默认端口为389。

超时：设定认证请求的超时时间。当AC把认证请求转发到LDAP服务器后，如果超过这个时间无回应，则视为认证失败，如果AF到LDAP服务器间的网络比较慢，可尝试把超时时间延长（例如10秒）。

BaseDN：指定域搜索路径的起点，该起点决定了该条LDAP规则的生效范围。如果用户在指定的BaseDN以外，则该用户无法做外部服务器认证，所配置的策略对该用户也不会生效。所以可以通过BaseDN来划分不同管理员的所属区域。

同步配置：

类型：MS Active Directory[OPEN LDAP、SUN LDAP、 IBM LDAP、OTHER LADAP。

匿名搜索：如果LDAP服务器支持匿名搜索时，则可以使用此选项。

域用户：AF将使用该账号到LDAP服务器去查询以及同步的内网的用户账号。

用户密码：域用户对应的密码。

用户组属性：指定LDAP服务器上，唯一标识用户的属性字段。例如AD域上sAMAccountName属性标识了用户，而在Novell LDAP上uid属性标识了用户。

用户组过滤：指定LDAP服务器的用户过滤条件，即通过这条件可以确定某个节点是否为用户。例如AD域上可以通过填写“(|(objectClass=user)(objectClass=person))”来过滤某个节点是否为用户。

搜索配置：

分页搜索：使用扩展 API 对 LDAP 服务器进行搜索，建议保留默认配置。
页面大小：LDAP 分页时返回的大小，0 表示无限制，建议保留默认配置。
大小限制：同步 LDAP 时的 size limit 选项，这里建议保留默认配置。

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）。

RADIUS服务器

在[策略/认证/用户认证/外部认证服务器]页面，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，填写服务器名称。

服务器名称：用于设置 Radius 服务器名称。

IP 地址：填写 Radius 服务器的 IP 地址。

认证端口：设置 Radius 服务器的认证端口，默认是 1812。

超时时间：设置认证请求的超时时间。

共享密钥：设置 Radius 协商密钥。

采用协议：设置Radius协商协议，不加密的协议PAP、质询握手身份验证协议Microsoft CHAP、Microsoft CHAP2、EAP_MD5。

POP3服务器

在[策略/认证/用户认证/外部认证服务器]页面，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，填写服务器名称。

POP3服务器配置：

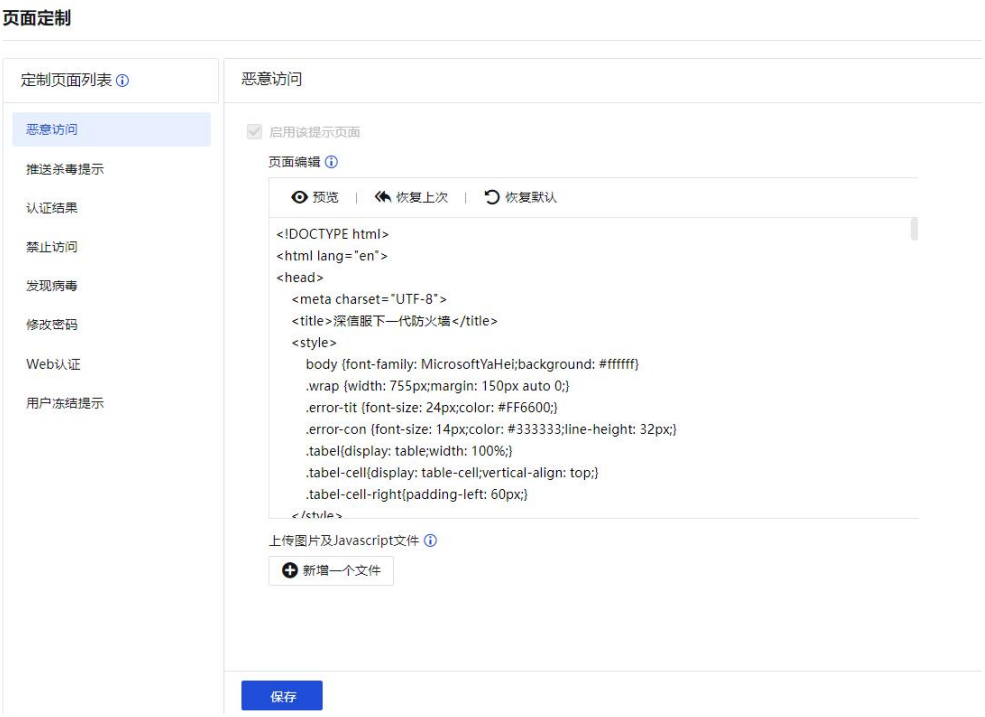
服务器地址：填写pop3服务器的地址。

认证端口：填写认证端口号。

超时（秒）：设定认证请求的超时时间。

6.7. 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。



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。

7. 对象

对象定义中的各种对象是设备做安全防护的基础设置，漏洞攻击防护、Web应用防护、僵尸网络和内网安全等都是基于对象来引用的。对象定义中包括应用内容识别库、安全防护规则库、IP地址库、时间计划、网络对象、服务等。

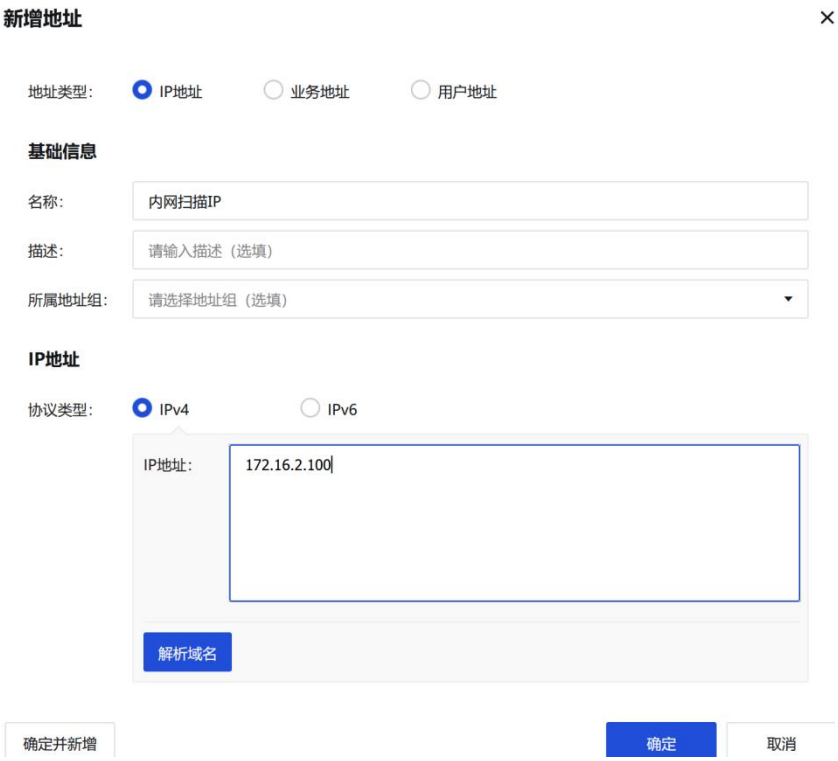
表21 对象定义功能说明

功能类别	功能说明
网络对象	用于设置地址或者地址组，方便在应用控制策略、安全防护策略等引用。
服务	用户可通过端口号和协议等条件设置服务，并且通过数据包的端口和协议来对数据进行控制。
安全策略模板	用户可以设置安全模板的内容，安全模板提供给安全策略引用。安全策略模板包括漏洞攻击防护、Web 应用防护、僵尸网络和内容安全。
安全防护规则	用户可以查找对应的安全规则，也可以自定义规则。这些规则汇总起来提供给安全模板进行引用。
内容识别库	识别流量中的内容，提供应用、URL 和文件的识别，提供安全模板进行引用
网络服务	用户可通过端口号和协议等条件设置网络服务，并且通过数据包的端口和协议来对上网数据进行控制。
IP 地址库	用于导入 ISP 地址段或者更改 IP 地址的归属地，提供选路时进行引用等。
时间计划	于设置时间计划，设备上的大部分控制都是可以基于时间段来进行控制的，用户可以在此处设置时间段，方便在控制策略中调用。

7.1. 网络对象

用于定义一个包含某些IP地址或者域名的集合，这个地址可以是内网的IP段，也可以是公网的某些IP范围，或者是全部IP，也可以是域名，这些IP集合可以重新组成一个新的集合--地址组。定义好的网络对象可提供应用控制策略等调用。可以对网络对象进行导入、导出，从而进行快速的配置，网络对象配置如下图所示。

点击<新增>，可以根据地址、域名或者地址组来进行添加网络对象，新增地址，地址类型有三种选择：IP地址、业务地址、用户地址。如下图所示。



名称：填写对应的名称。

描述：填写对应的描述信息。

所属地址组：（可选）该IP地址需要加入的组。

协议类型：选择IPv4或者IPv6。

IP地址：填写IP地址。

解析域名：用于解析域名和IP地址之间的关系，解析完成后的域名对应的IP会填写到IP地址中。

说明：

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。

选择业务地址，如下图所示。

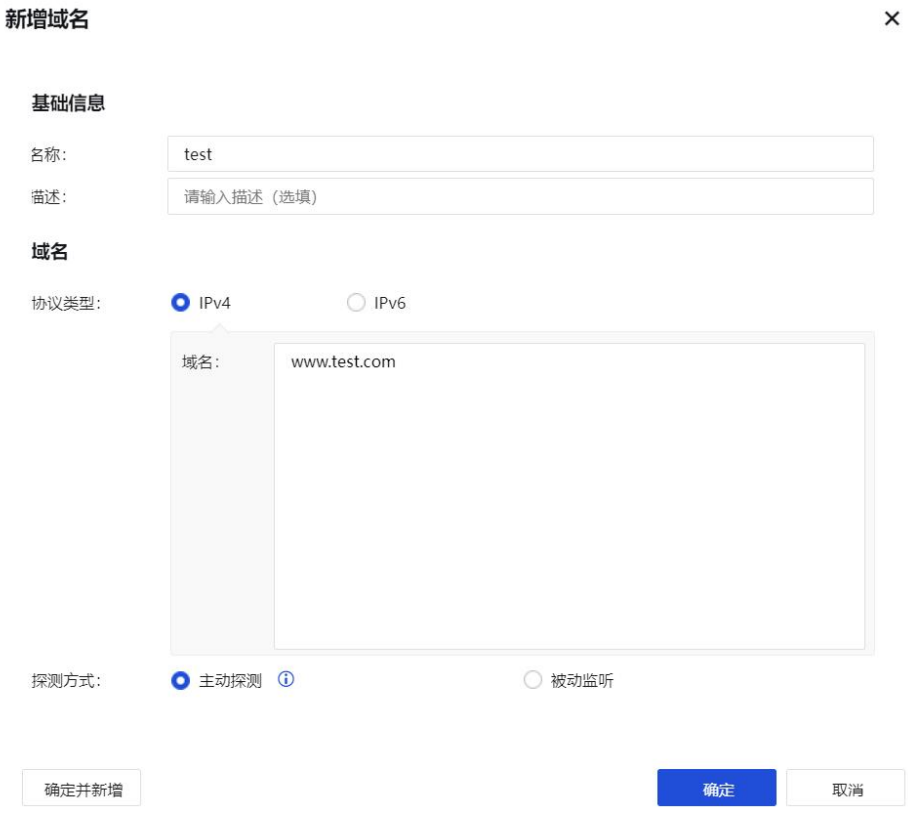
重要级别：标记业务的重要级别，方便后续优先关注或管理该业务安全问题。

敏感数据：系统自动识别存在敏感数据的业务，方便您知道网络中敏感数据在哪，也可手动标记该业务是否存在敏感数据。

选择用户地址，如下图所示。

重要级别：选择用户的重要性分别为普通业务和核心用户，可根据实际需求设置。

选择新增域名，如下图所示。



协议类型：选择IPv4或者IPv6。

探测方式：主动探测是设备主动发起DNS解析请求得到该域名的IP地址，被动监听是设备通过检测经过设备的DNS包来获取该域名的IP地址。

选择新增地址组，如下图所示。

协议类型：一个地址组内的IP组必须是同一种IP类型(IPV4和IPV6其中之一)。

引用地址或地址组：选择该地址组需要包含的IP组或地址组，可根据实际需求设置。

服务器识别

识别到的服务器信息将在该界面进行展示，展示的内容包括：开发的端口、敏感数据页面数等。如下图所示。

合并到业务：选择需要合并的业务。

忽略：对于识别出来的服务器信息进行忽略。

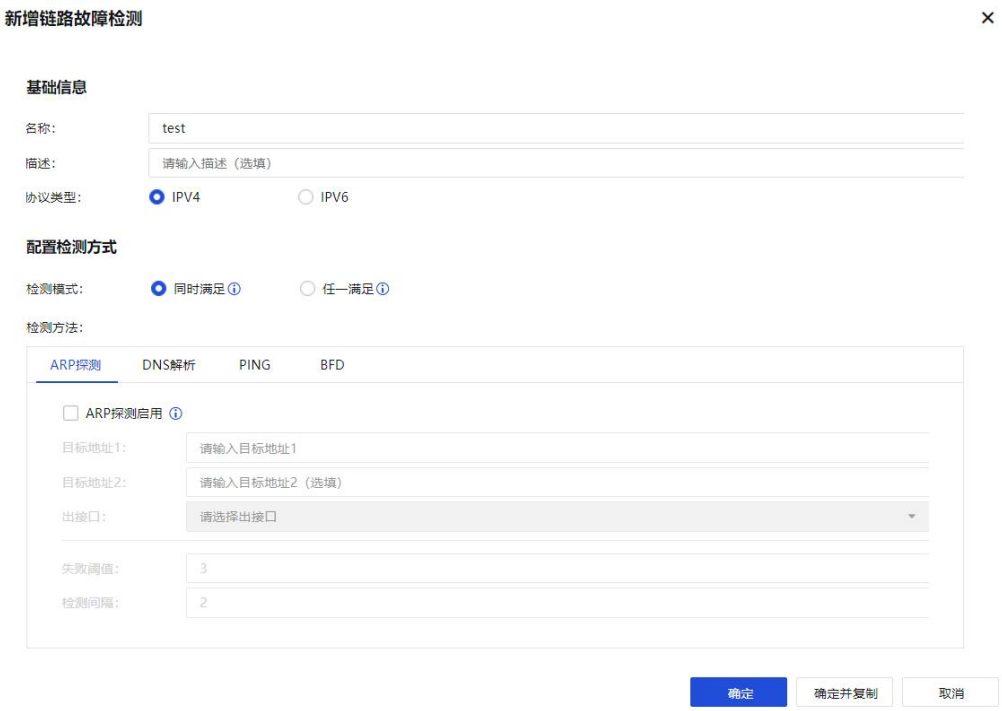
查看忽略服务器：查看添加忽略的服务器。

查看忽略页面：查看服务器忽略的页面信息。

高级设置：是否开启服务器识别的功能，是否识别数据业务。

7.2. 链路检测

链路检测：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ARP探测、DNS解析、PING和BFD的方式来检测。如下图所示。



检测模式：可以选择同时满足和任一满足。同时满足是所有的检测方法都正常时该链路即为正常；任一满足是其中一个检测方法正常时该链路即为正常。

ARP 探测：通过向指定网络设备发送 ARP 来判断链路的状态，每组目标 IP 可填写两个 IP，已逗号分隔开，向组内的所有 IP 发送 ARP 数据包。

DNS 解析：通过到指定的 DNS 服务器解析域名来判断链路状态；最多可配置两组 DNS 服务器，其中任何一组解析域名失败即判定为链路故障。

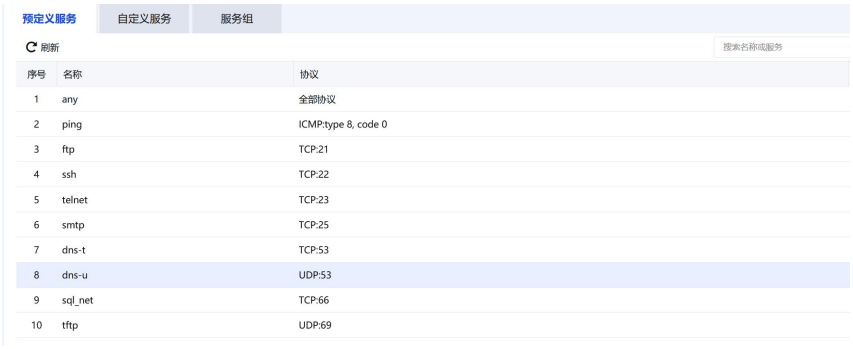
PING：通过PING指定的服务器来判断链路状态；最多可配置两组目标IP，每组目标IP可填写2个IP，以逗号分割，其中任何一组内的所有IP都PING不通的时候即判定为链路故障。

BFD：遵循rfc5880的标准，BFD需要两端都配置对应的会话才可组成一个探测系统，通过udp port 3784来标识BFD的控制报文，通过udp port 3785来标识BFD的echo报

文从而来识别链路是否正常。

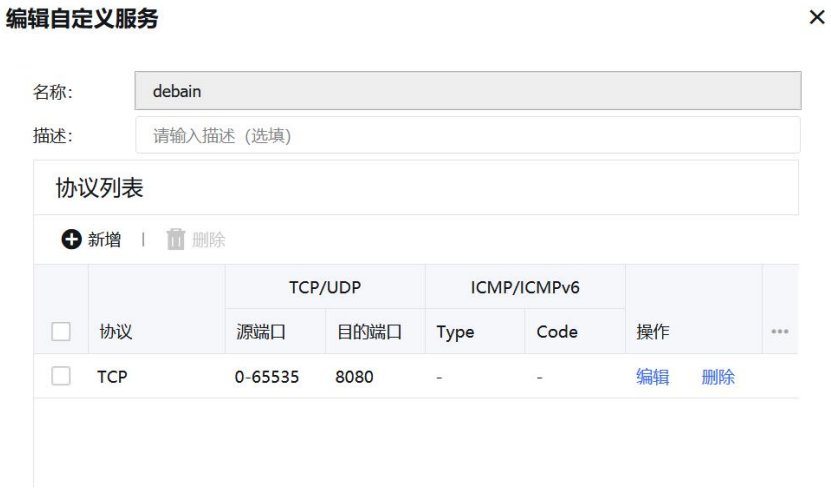
7.3. 服务

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，它可以被应用控制策略等调用，以实现对某些网络服务的允许、拒绝等控制。服务配置如下图所示。



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，如下图所示。

自定义服务：当预定义服务没有合适的时候，可以手工自定义服务，点击<新增>，创建自定义服务，如下图所示。



名称：填写对应的名称。

描述：填写对应的描述信息。

协议：支持TCP、UDP、ICMP或者其他，具体端口号可以在对应的协议下进行编写。

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，点击<新增>，创建服务器，如下图所示：

名称：填写对应的名称。

描述：填写对应的描述信息。

服务：选择需要定义好的服务。

7.4. 安全策略模板

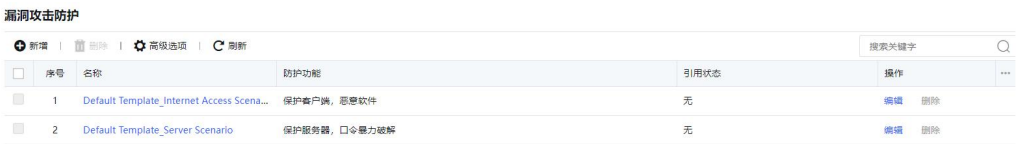
将多个安全规则整合到一个模板中，让安全策略进行调用。同时，可以对模板进行修改，以适用业务的需求。

7.4.1. 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。其中：

默认模板_客户端保护场景 Default Template_Internet Access Scenario 针对内网用户进行防护。

默认模板_业务保护场景 Default Template_Server Scenario 针对服务器进行防护。

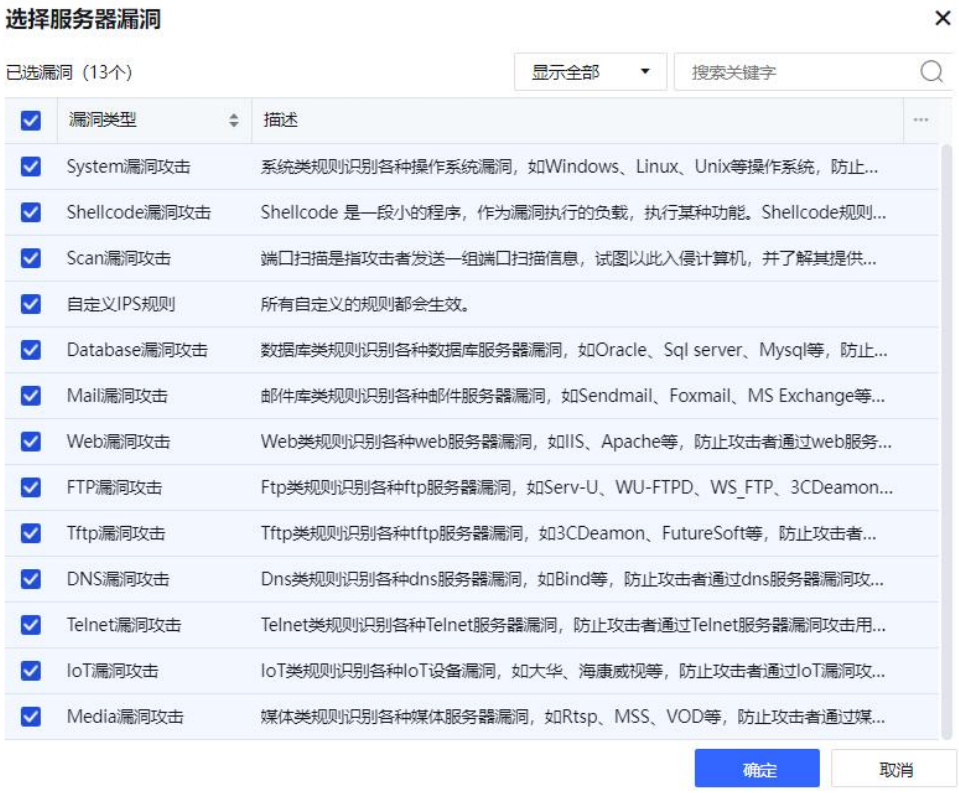


点击<新增>，创建漏洞攻击防护模板，如下图所示。

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：System漏洞攻击、Shellcode漏洞攻击等]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：System漏洞攻击、Shellcode漏洞攻击等] 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、IMAP Standard 、Rlogin、Telnet、Oracle、MS Sql2008...]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。

点击口令爆破类型，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：Worm漏洞攻击、Trojan漏洞攻击、Spyware漏洞攻击、Backdoor漏洞攻击] 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。

勾选失陷外联检测引擎，同时点击[已选失陷外联检测引擎] 弹出选择失陷外联检测引擎，勾选对应的引擎类型，则设备对这种类型失陷外联动作进行检测防护。

勾选Web智能语义引擎，同时点击[已选启用JAVA反序列化防护] 弹出Web智能语义引擎页面，勾选启用JAVA反序列化防护，并选择对应防护，则设备对JAVA反序列化攻击进行检测防护。

点击<确定>，完成漏洞攻击防护模板的创建。

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。

HTTP端口：可以将多个HTTP端口添加，用于更加准确的识别HTTP攻击。

7.4.2. Web 应用防护

Web应用防护是专门针对内网的Web服务器设计的防攻击策略，可以防止系统命令注入、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。如下图所示。

Default Template：默认开启常规的Web防护功能，但不开启“漏洞防扫描功能”。

Default Template II(Scanner Blocker enabled for non-proxy access)：默认开启常规的Web防护功能，同时开启“漏洞防扫描功能”。

点击<新增>，可以创建Web应用防护模板，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。如下图所示。

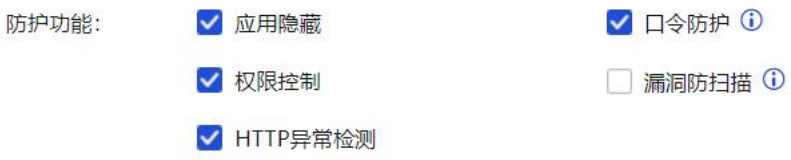
防护类型：设置针对服务器的哪些攻击行为进行防护。点击<防护类型：SQL注入、XSS攻击、网页木马等>弹出选择Web应用防护类型编辑框，勾选相应的防护类型，则设备会对这一种服务类型的相关攻击行为进行防护。

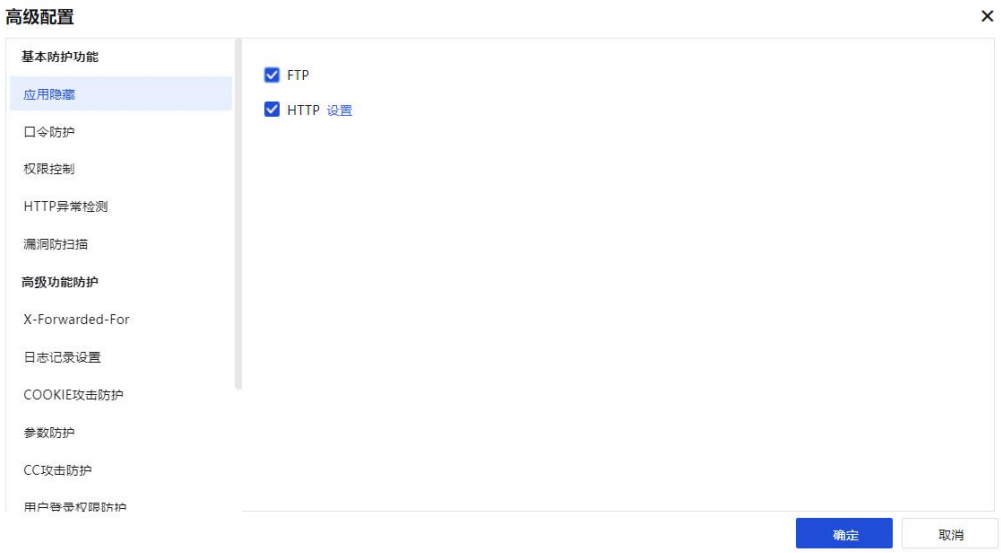
表22 Web应用防护类型说明

防护类型	说明
SQL 注入	攻击者通过设计上的安全漏洞，把 SQL 代码粘贴在网页形式的输入框内，获取网络资源或改变数据。
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。
网页木马	网页木马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。

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。
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，同时也称为网站后门木马，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，与正常网页混在一起。通过 WEHShell 来长期操纵和控制受害者网站。
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。
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。
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，当提交的文件存在恶意代码或木马时，文件中的代码和木马会以 Web 权限被成功执行。
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。
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。
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。
WebShell 后门通信	在已知Web系统漏洞情况下，攻击者利用Web系统漏洞将WebShell页面成功植入到Web系统中，攻击者通过WebShell页面访问数据库，执行系统命令并长期的操控Web系统。
自定义 WAF 规则	用户可自定义防护规则，对服务器进行防护，自定义规则在自定义规则中进行设置。

防护功能：主要功能有应用隐藏、口令防护、权限控制、HTTP异常检测、漏洞扫描，开启高级的防护功能请点击<高级配置>中进行设置。





7.4.2.1. 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。

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。

启用过滤HTTP响应报文头，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。

7.4.2.2. 口令防护

Web口令防护设置：该防护针对http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http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>保存后生效。当防火墙检测到这种弱口令会产生日志记录提醒管理员。

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。点击<设置>，可以增加弱口令的复杂度和自定义密码字典，如下图所示。

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。

Web口令防护爆破设置：该防护主要是对Web口令方爆破进行设置，点击<设置>进入方爆破设置页面，如下图所示。

高频Web口令爆破防护：利用内置的WAF口令爆破防护规则，实时检测口令爆破行为。

中低频Web口令爆破防护：针对攻击源爆破频率较低的行为，通过对一段时间内离线日志的算法分析，检测到以往很难发现的爆破攻击源IP。

严格模式：持续15分钟，每分钟登录2次；阈值设置低，较容易触发暴力破解，适用于对安全性要求高的环境。

标准模式：持续21分钟，每分钟登录4次；阈值设置适中，可以满足多数业务场景的暴力破解检测，通常选择此模式。

宽松模式：持续45分钟，每分钟登录8次；阈值设置高，较难触发暴力破解，适用于对业务连续性要求高的环境。

分布式Web口令爆破防护：在多台设备同时攻击一台服务器的情况下，通过对一段时间内离线日志的算法分析，检测到以往很难发现的爆破攻击源IP。

Web口令登录参数设置：本页面新增的自定义口令防护规则会自动同步至[对象/安全防护规则库/自定义规则库]中，点击<新增>，创建Web口令自定义防护规则，如下图所示。

7.4.2.3. 权限控制

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。

点击下拉框可以下拉选择设备内置的一些文件类型，点击+号，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。例如拒绝访问某个URL，则web应用防护针对该URL都无效，因为客户端都无法访问，更不会存在攻击。如果此处允许访问某个URL，则web应用防护该URL也无效，相当于一个白名单。勾选URL防护，点击<设置>，页面如下。

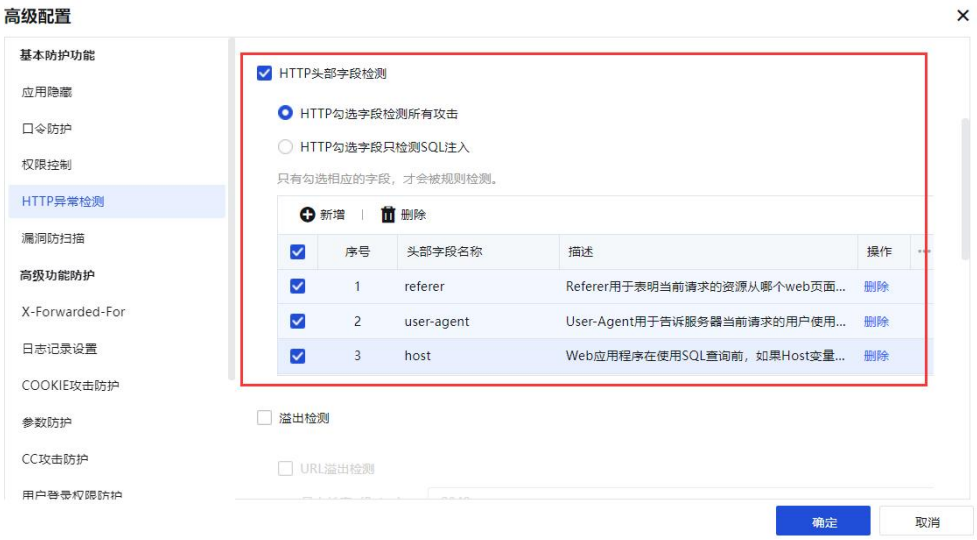
点击<新增>，增加URL过滤，如下图所示。

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 ，则此处填写/login.html，并根据需求对该URL进行拒绝或者允许访问。

7.4.2.4. HTTP 异常检测

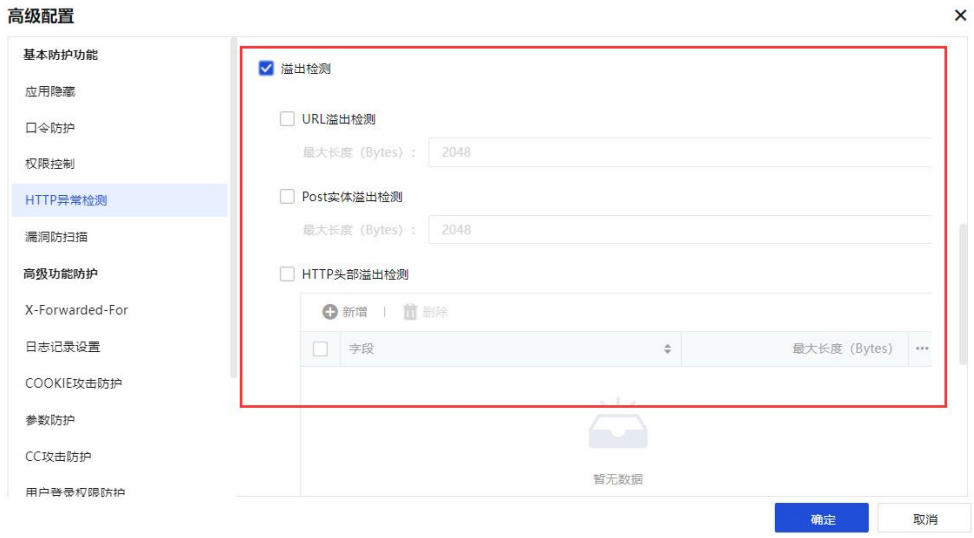
方法过滤：主要是用于设置允许的HTTP方法，启用后，该HTTP请求类型将被禁止。即勾选的HTTP方法会被策略判定为异常，进行拦截，如下图所示。

HTTP头部字段检测：可以将HTTP头部中的Referer、User-Agent、Host字段进行SQL注入等攻击的检测。注：此功能要将Web应用防护策略中的网站防护“sql注入”等启用才能生效，如下图所示。



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然是SQL注入攻击，拦截部分为HTTP数据包的头部Host字段。

溢出检测：主要防止HTTP的一些字段过长，导致溢出，如下图所示。



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。

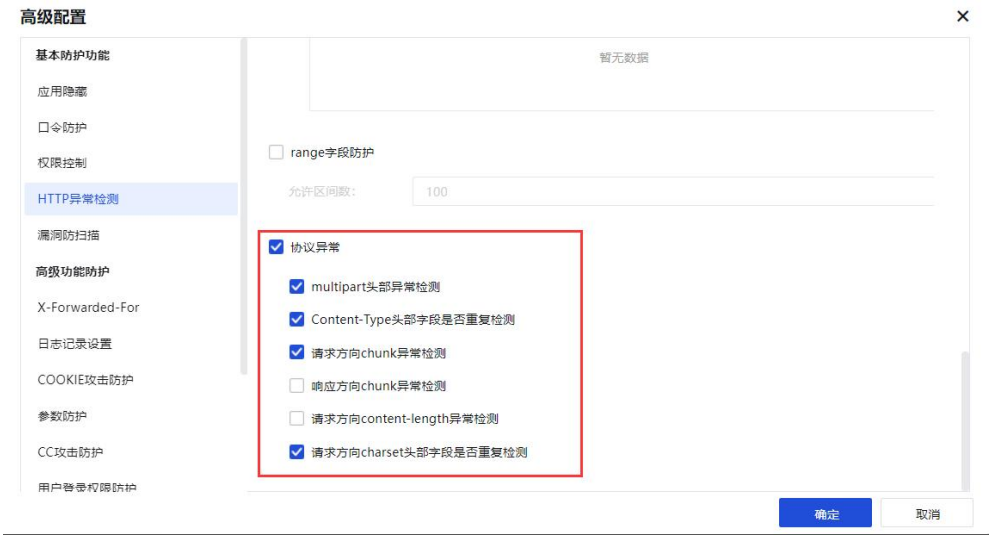
POST实体溢出检测：勾选启用Post 实体溢出检测，设置Post数据的实体部分的最大长度，防止造成服务器接收数据溢出的错误。

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。

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。

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、Content-Type头部字段是否重复检测、请求方向chunk异常检测、请求方向charset头部字段是否重复检测和请求方向content-length异常检测。



7.4.2.5. 漏洞防扫描

用于设置Web网站被扫描的行为检测，页面如下。

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：

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。

[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。

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。

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。

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。

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。

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。

⚠ 注意 ：

1. 以下两种场景不建议开启防扫描功能：
2. 对业务访问者 IP 进行源地址转换；
3. 统一使用代理服务器访问业务。

7.4.2.6. 高级功能防护

1. X-Forwarded-For

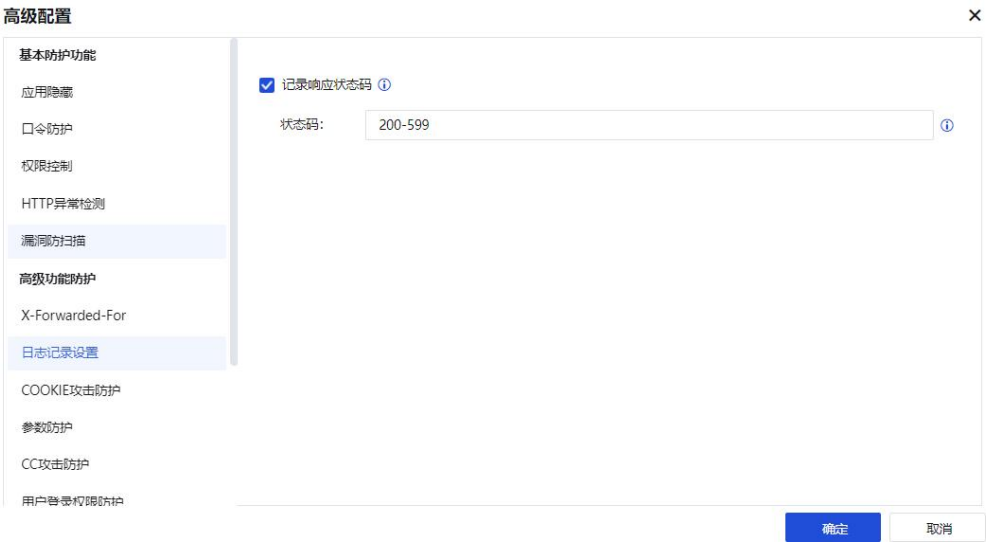
流量经过CDN或者代理等场景，一般都会在HTTP头部插入对应得X-Forwarded-For字段记录真实的源IP地址，以便服务器知道访问的真实IP。勾选启用，如下图所示。

头部字段：识别插入的HTTP头部字段，目前能够识别X-Forwarded-For、Cdn-Src-Ip和Clientip三种，也可以自定义进行配置。

代理服务器IP：如果访问经过CDN、或网络环境中部署了代理设备或负载均衡设备，请在此填写受信任的真实CDN IP或代理IP，用于进行日志记录和联动封锁。

日志记录设置

用于设置日志记录类型，页面如下。



状态码：配置范围为200-599，响应状态码记录状态码条件：

1.请求方向的攻击。

2.检测到攻击动作是允许。

⚠ 注意 ：

如果外层启用开关关闭，但记录响应状态码处于勾选状态且引用当前模板的策略启用记录日志时，功能仍旧生效

COOKIE攻击防护

COOKIE是客户端浏览某网站时，网站存储在客户端机器上的一个小文本文件。一般情况下，它会记录客户端的用户ID、密码、浏览过的网页、停留的时间等信息，当同一客户端再次访问该网站时，网站通过读取COOKIE，得知相关信息就可以做出相应的动作。当客户端访问服务器时，一些重要的信息会保留在COOKIE里，可能会被他人利用，导致信息泄露。

攻击者利用COOKIE的方式一般有两种：盗用COOKIE和篡改COOKIE，盗用COOKIE是为了伪造合法身份欺骗服务器，篡改COOKIE是为了利用服务器实现上的逻辑缺陷。

COOKIE攻击防护是根据COOKIE的属性和客户端信息来检测COOKIE是否被盗用和篡改。可以针对所有的COOKIE属性做防护，也可以针对某些属性做防护。

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。配置如下图所示。

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

自定义参数防护：可以自定义相关参数，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。

CC攻击防护

用于防止针对网站发起的CC攻击。配置如下。

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。

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。

Web登录路径

URL：Web 资源防护，即登录的 URL 的防护路径，如 192.168.1.1/login.php

非Web登录方式

预定义服务/FTP：选择需要防护的非Web资源，只支持TCP类型。

URL：主动认证的URL，访问后返回认证页面。

允许短信验证号码

手机号码：填写管理员手机号码，即认证接收的号码。

发送测试短信：发送测试短信，验证短信猫是否可用。

验证通过后有效时间：白名单时间，认证后这段时间内无需再认证。

勾选允许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。

说明：

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。

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。

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

Web智能语义引擎

通过智能语义引擎，对命令注入、PHP代码、JAVA代码、XEE攻击、Webshell上传、SQL注入、XSS攻击、后门扫描防护进行算法检测，不需要进行规则检测，从而提高

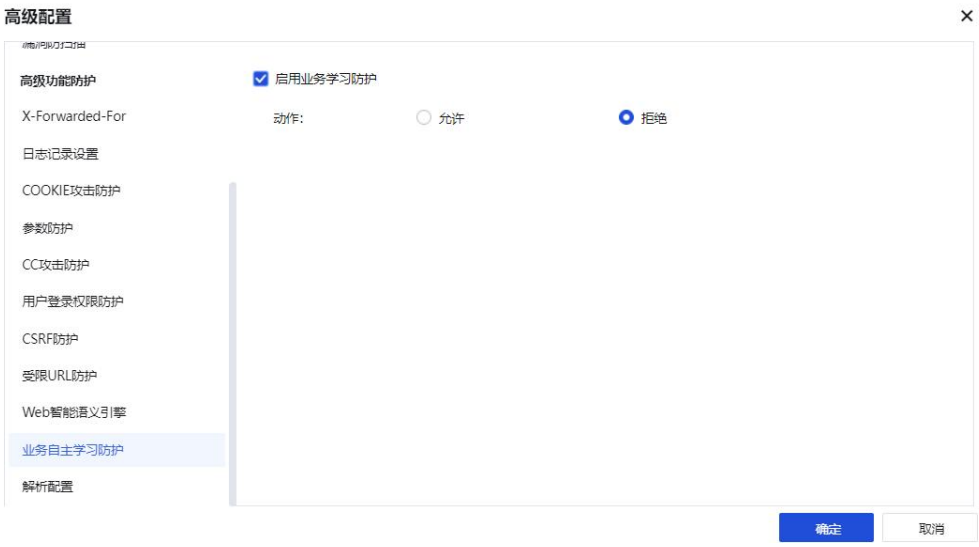
检测率。如下图所示。

表23 Web智能语义引擎说明

引擎类型	说明
命令注入防护	提高命令注入攻击检测的安全效果，如果用户对安全性要求较高，可以接受一定的误报，建议选择高检出；如果用户对业务稳定性要求高，建议选择低误报。
PHP 代码注入防护	提升对未知漏洞进行 PHP 代码注入攻击的检测能力，减少对规则的依赖，如用户对业务稳定性要求较高，可选择低误报。
JAVA 代码注入防护	增加对更多 java 表达式语言的检测能力，减少漏报。
XXE 攻击防护	XXE 安全检测引擎，通过语法进行分析检测，减少漏报以及误报，提高 AF 拦截成功率，提高 AF 安全检测能力
Webshell 上传防护	减少因为缓冲区截断而导致的漏报，如果用户对安全性要求较高，能接受一定的误报，建议选择高检出如果用户对业务稳定性要求高，建议选择低误报。
SQL 注入防护	SQL 注入防护引擎，将改进 AF 的防御效果，增加抗绕过能力和降低误报率，该功能默认启用，并选择低误报和禁用非注入型检测，适用于 SQL 业务较多的场景，在 SQL 业务较少的场景下可选择高检出和启用非注入型检测。
XSS 攻击防护	XSS 攻击防护引擎可以增强对 XSS 攻击的检测能力，降低误报率，该功能默认启用，并选择低误报，适用于后台编辑前端页面较多的场景，在安全要求较高的场景下可以选择高检出。
后门扫描防护	后门扫描防护引擎可以增强对后门扫描攻击的检测能力，该功能默认启用，并选择低误报，在安全要求较高的场景下可以选择高检出。
模板注入防护	模板注入防护引擎对用户输入未经过滤就解析，用户输入可利用模板语法将恶意 payload 注入模板中，服务端执行模板，引起 RCE 和信息泄露等危害，以模板为概念产生的漏洞问题进行防护，默认关闭，在安全要求较高的场景下可以选择高检出。
PHP 反序列化攻击防护	PHP 反序列化攻击防护引擎可以增强对 PHP 反序列化攻击的检测防护能力，该功能默认启用，并选择低误报，在安全要求较高的场景下可以选择高检出

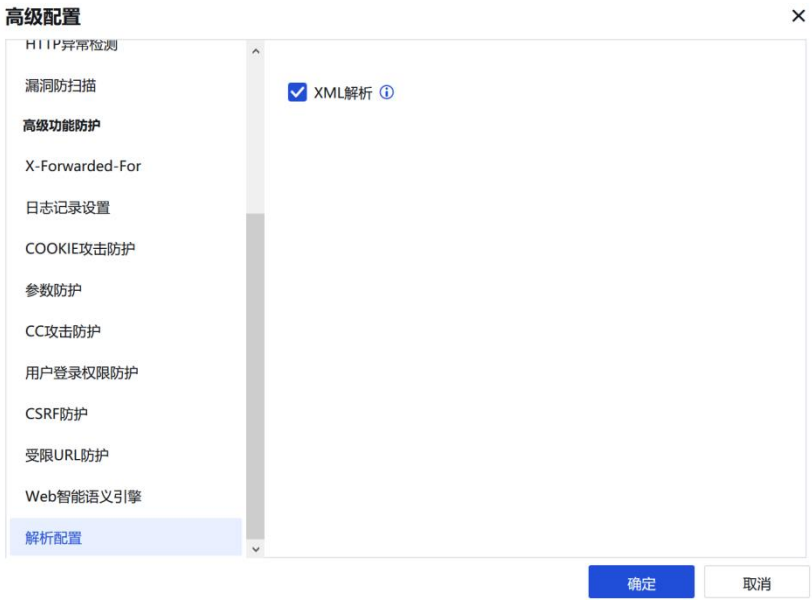
业务自主学习防护

业务自主学习防护是通过识别异常流量的方式，对客户的业务流量建立由特征模型组成的基线，从而检出异于业务的流量，针对检出的异常流量，也将尝试识别其中的已知攻击特征，从而分离出未知恶意行为和已知攻击行为。该功能默认关闭。



解析配置

XML解析引擎检测功能，增强XML攻击检测识别。能够检测http报文中的body部分，即通过XML协议传输包装的webshell的一种攻击绕过手段。如下图所示。



7.4.2.7. 云端威胁防护

云端威胁防护配置：云端黑客IP防护和云端联动封堵，主要作用是联动云脑，拉取封锁IP库数据，进行临时封堵，提供快速有效的技术手段，及时阻断攻击行为，提升AF安全效果能力。云端联动封锁是AF接入云脑后，经过云脑分析该AF的相关数据，针对该AF下发需要进行临时封锁的数据，下发的封锁数据会显示在[策略/黑白名单/黑名单/临时封锁名单]列表中。

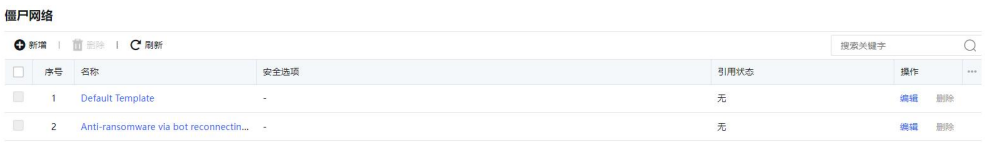
勾选即开启云端黑客IP防护，如下图所示。

说明：

开启云端黑客 IP 防护需要 AF 连接到互联网，下发的黑客 IP 可在云端黑客 IP 进行查看。

7.4.3. 僵尸网络

僵尸网络主要用于发现和隔离内网感染了病毒、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，其配置如下图所示。



点击[安全策略模板/僵尸网络]进入模板设置页面，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>，弹出新增模板如下图所示。

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。

默认检测：默认检测包含恶意域名检测，不可配置。

恶意URL检测：对恶意URL进行检测。

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。

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，如下图所示。

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。

⚠ 注意：

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。

7.4.4. 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；如下图所示。

点击[安全策略模板/内容安全]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>，弹出新增模板如下图所示。

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。

启用服务器外连下载防护：在服务器保护场景中，如服务器有主动外连外部http服务器时，对外连的下载行为进行SAVE安全智能文件检测。

7.5. 安全防护规则库

安全防护规则库主要提供给安全策略模板调用，该功能可以调用系统内置的安全规则库，也可以自定义规则，从而快速的响应，对攻击行为进行防护。

7.5.1. 安全规则库

安全规则库是AF内置的规则库，在升级授权有效期内可以更新，包含Web应用防护特征库、漏洞攻击特征识别库、僵尸网络与病毒防护库和实时漏洞分析识别库。选择不同的识别库类型进行不同的设置。

7.5.1.1. 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。

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。如下图

所示。

防护类型显示当前防护类型的规则库，点击下拉框，可以根据防护类型查看对应的规则ID，防护名称显示该防护规则对应的名称，如下图所示。

防护名称：显示该防护规则的名称。

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，如下图所示。

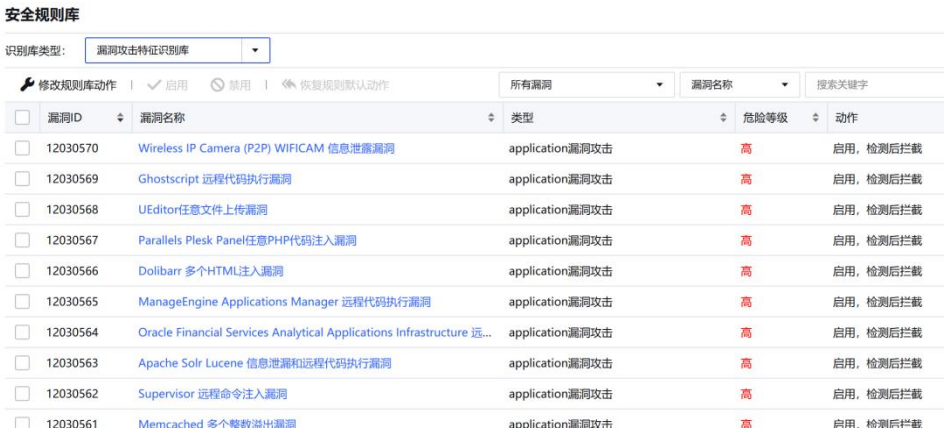
启用，检测后拦截：表示启用当前规则，当检测到此攻击的行为时，拦截相应的数据包。

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。

7.5.1.2. 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，如下图所示。



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。

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。

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：描述漏洞的危险等级，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。这个动作可以自定义，点击<漏洞名称>即可进入编辑页面，如下图所示。

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。

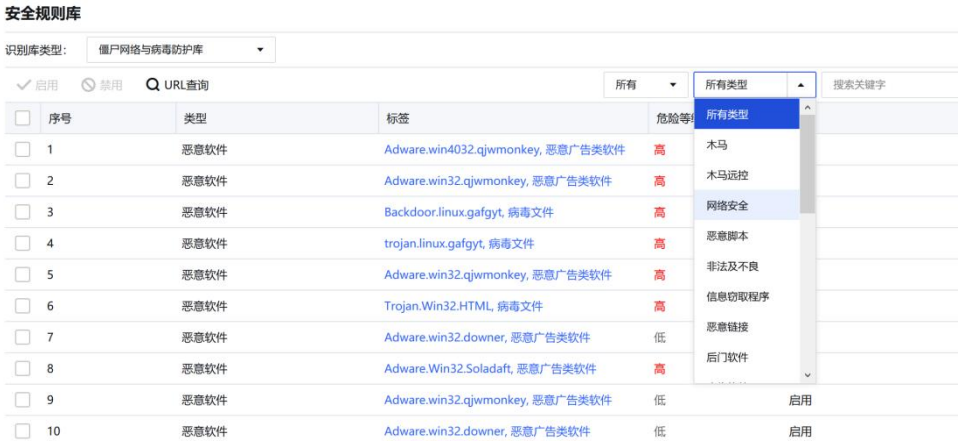
禁用：表示禁用当前规则，当规则禁用后，设备不会对该漏洞进行检测。

⚠ 注意：

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。

7.5.1.3. 僵尸网络与病毒防护库

僵尸网络与病毒防护库包含了木马、挖矿、蠕虫、非法与不良、感染型病毒、后门软件、恶意链接、广告软件、恶意软件、网络安全、间谍软件、黑客工具、恶意脚本、木马远控、勒索软件、Rootkit、流氓软件、僵尸网络这18类规则防护类型。



规则状态：可以查看所有启用或禁用状态下的规则。

类型：木马、挖矿、蠕虫、非法与不良、感染型病毒、后门软件、恶意链接、广告软件、恶意软件、网络安全、间谍软件、黑客工具、恶意脚本、木马远控、勒索软件、Rootkit、流氓软件、僵尸网络这18类规则防护类型。

启用：启用选定的规则库。

禁用：禁止选定的规则库。

7.5.1.4. 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。对指定的数据进行实时漏洞分析，如下图所示。

页面右上角，可以输入规则名称或规则ID查找规则。

在筛选中点击下拉框显示设备内置的漏洞类型，可勾选相应的类型筛选规则。

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。

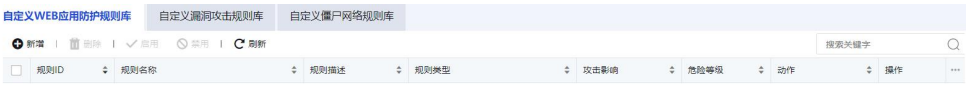
动作：包括启用和禁用两类，当漏洞禁用后，设备不会对该漏洞进行检测。

7.5.2. 自定义规则库

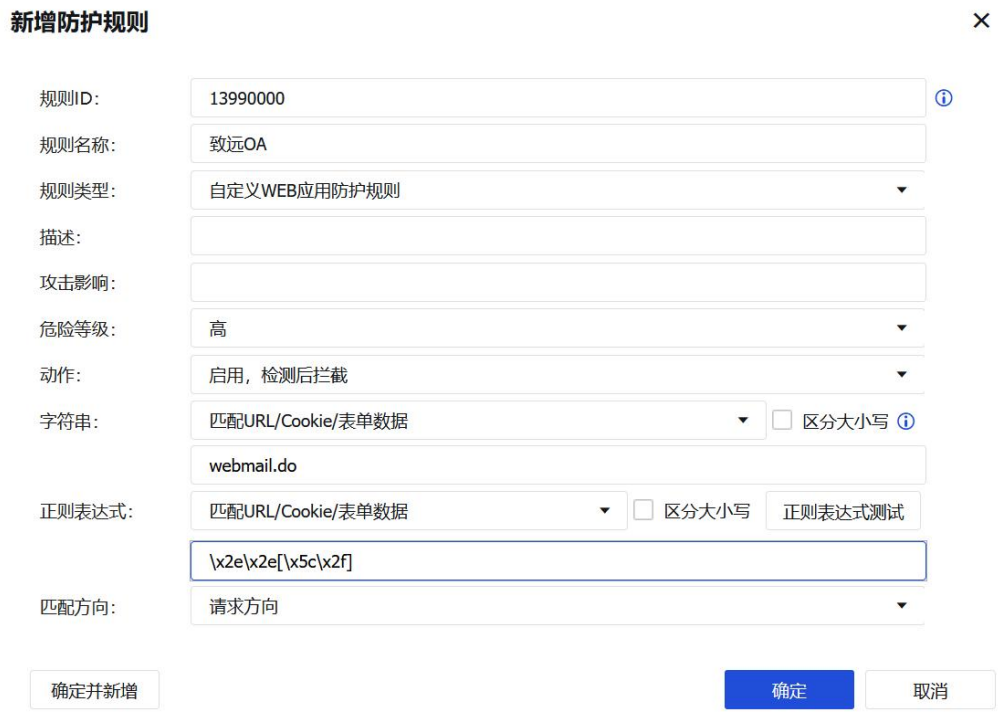
根据手工自定义规则库，能够及时的防护未发现的攻击行为。目前支持自定义Web应用防护规则库、自定义漏洞攻击规则库、自定义僵尸网络规则库和自定义敏感信息防护规则库。

7.5.2.1. 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。

规则类型：可选自定义Web应用防护规则、CC防护规则和自定义口令防护规则。

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。

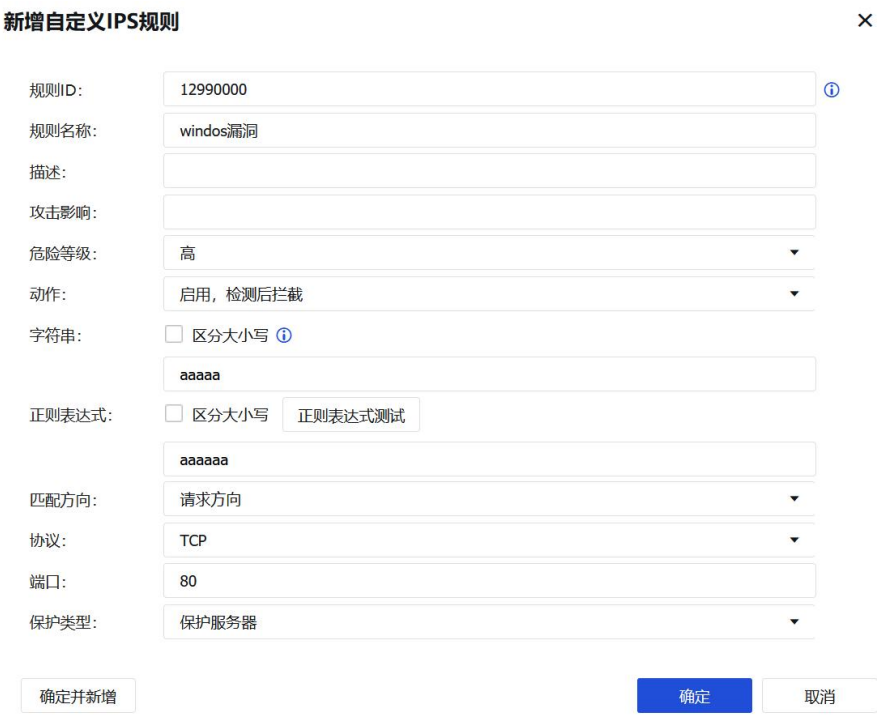
禁用：表示禁用当前规则，当规则禁用后，设备不会对该规则进行检测。

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。

7.5.2.2. 自定义漏洞攻击规则库

自定义漏洞攻击规则库用于用户自己定义哪些规则属于漏洞攻击模块需要检测和防护的，如下图所示。

在自定义漏洞攻击规则库页面，点击<新增>。



规则名称、描述、攻击影响可根据情况自己定义。

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。

7.5.2.3. 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，如下图所示。

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。

7.6. 内容识别库

内容识别库主要能够识别应用、URL、文件类型等。通过识别不同的内容，对内容进

行安全检测。

7.6.1. 应用识别库

应用识别库主要用于识别应用数据，通过识别不同的应用，对应用进行安全防护。

7.6.1.1. 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。

应用识别库分为内置库和自定义库，内置库有内置库规则与内置库应用，自定义库有自定义规则与自定义应用；内置库不可修改，由设备定时更新，更新内置库需要序号授权，保证设备能够上网；自定义库可以增加、删除、修改等，一个自定义定义可以引用多条规则。

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。

查看应用识别规则

在导航菜单页面中的[对象/内容识别库/应用识别库]，进入[应用特征识别库]页面。

应用规则总数：10481：显示的是设备当前内置的规则识别库中的应用规则总数。

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

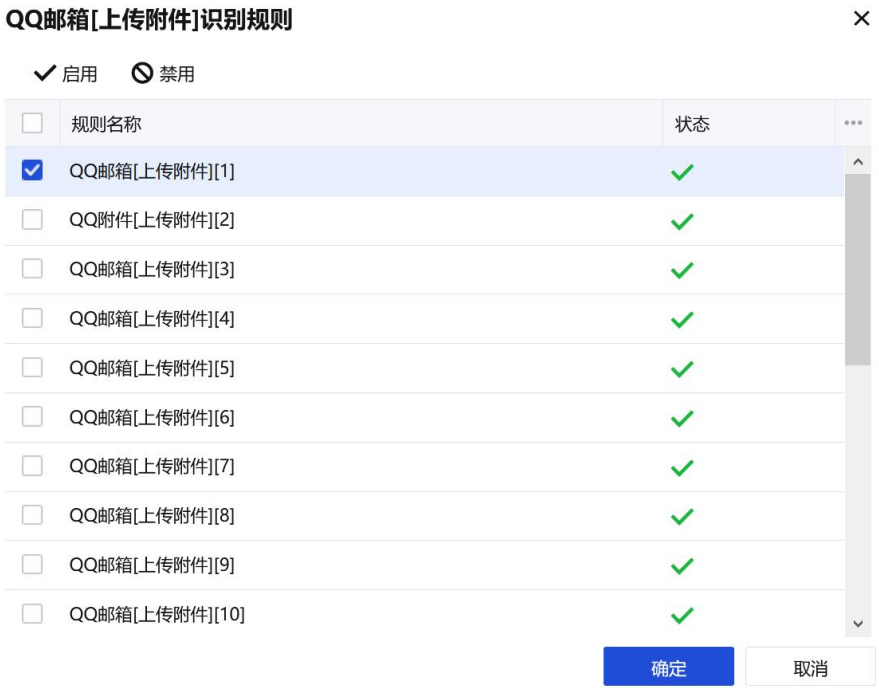
条件的规则。在搜索中需要查询的规则关键词，如筛选条件设置为“QQ”。

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/应用识别库]，进入应用特征识别库页面，先筛选出想要设置的规则，比如需要对QQ的规则进行禁用，如图筛选出QQ相关的应用：

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。



⚠ 注意：

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. 应用特征识别库支持 IPv6，可以识别 IPv6 环境中的各类常见应用。

7.6.1.2. 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、深信服VPN数据的识别、自由门，无界浏览等代理工具数据。配置如下图所示。

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/应用识别库]，右边进入应用智能识别库页面。

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。

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。

是否启用该规则：可以勾选该项，启用该规则。

其中规则名称、规则分类、规则描述三项均不能编辑。

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。智能识别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，如果有大量未识别的数据，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，设备不会对此类数据进行P2P智能识别，可以避免部分误判的情况。

7.6.1.3. 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。管理员可进行新增、删除、启用/禁用、导入/导出自定义应用操作。

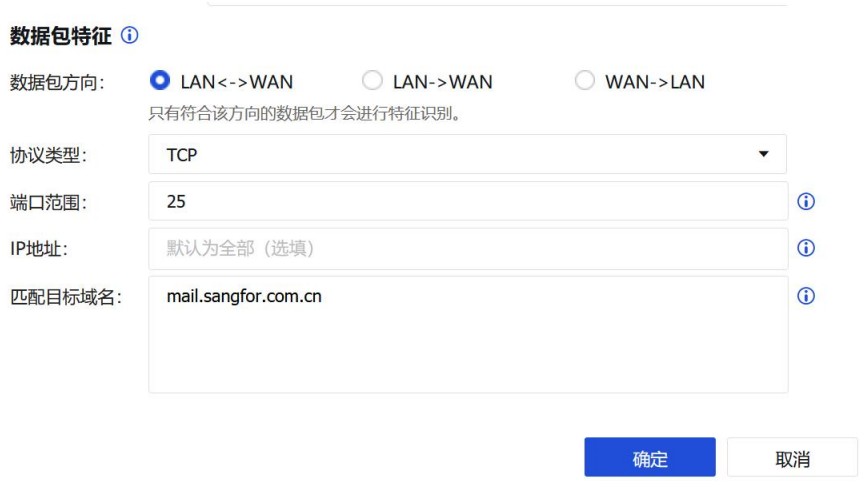
在导航菜单页面中的[对象/内容识别库/应用识别库]，右边进入[自定义应用识别规则]编辑页面。

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。

步骤1.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。

步骤2.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）。

步骤3.设置匹配数据包的类型。



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.深信服.com.cn”。

步骤4.设置完成后点击<确定>，完成此条规则的设置。

步骤5.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，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。

步骤6.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。

⚠ 注意：

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。

7.6.2. 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。

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，页面上方显示内置URL库版本以及内置URL升级的有效期。如下图所示。

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。

⚠ 注意：

1．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。

2．URL分类库不支持IPv6；

Web过滤不对IPv6环境流量中的URL进行处理，不记录IPv6网站访问的相关日志。

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。如下图所示。

编辑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和关键词，作为对内置URL库的补充。

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。

7.6.3. 文件类型组

7.6.3.1. 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/流控/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。如下图所示。

在文件类型组页面点击<新增>，则弹出新增文件类型组窗口，如下图所示。

名称：用于设置名称。

描述：用于设置文件组的描述信息。

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。

> ⚠ 注意：
>
> 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。

7.6.3.2. 邮件附件过滤类型组

邮件附件过滤类型组主要用来过滤邮件的附件类型，对于一些存在威胁行为的邮件附件，可以进行过滤，从而保护收件人的安全。如下图所示。

点击<新增>，创建邮件附件过滤类型，如下图所示。

名称：用于设置名称。

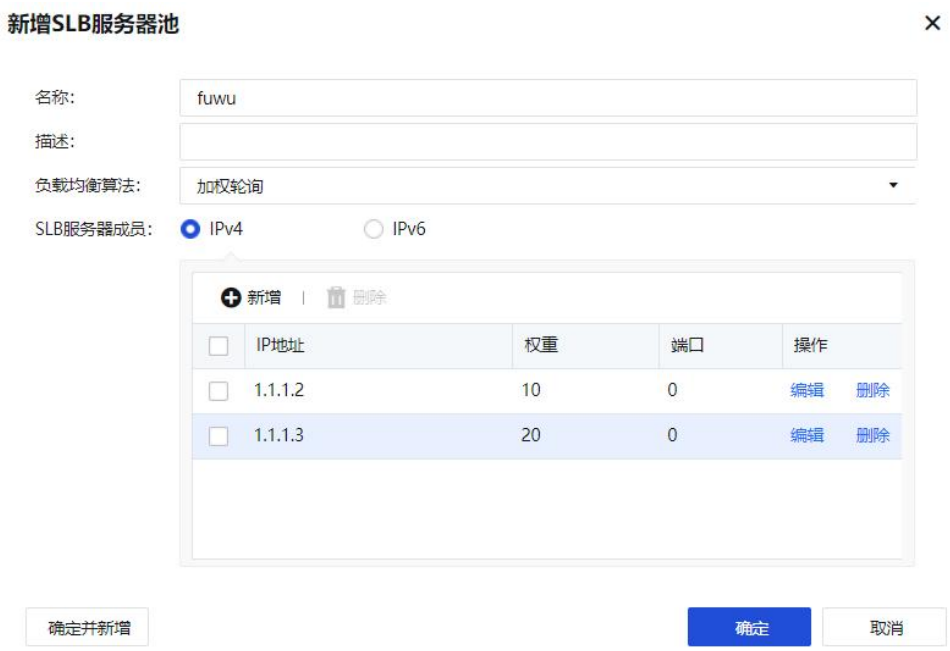
描述：用于设置附件组的描述信息。

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。

7.7. SLB 服务器池

SLB服务器池是用于加入到目的地址转换（或双向地址转换）的目标地址中，可通过加权轮询算法选出服务器池中的一个IP作为地址转换的目的地址，打到将流量均衡的负载到不同服务器的作用。

点击<新增>，进行SLB服务器池的添加，如下图所示。



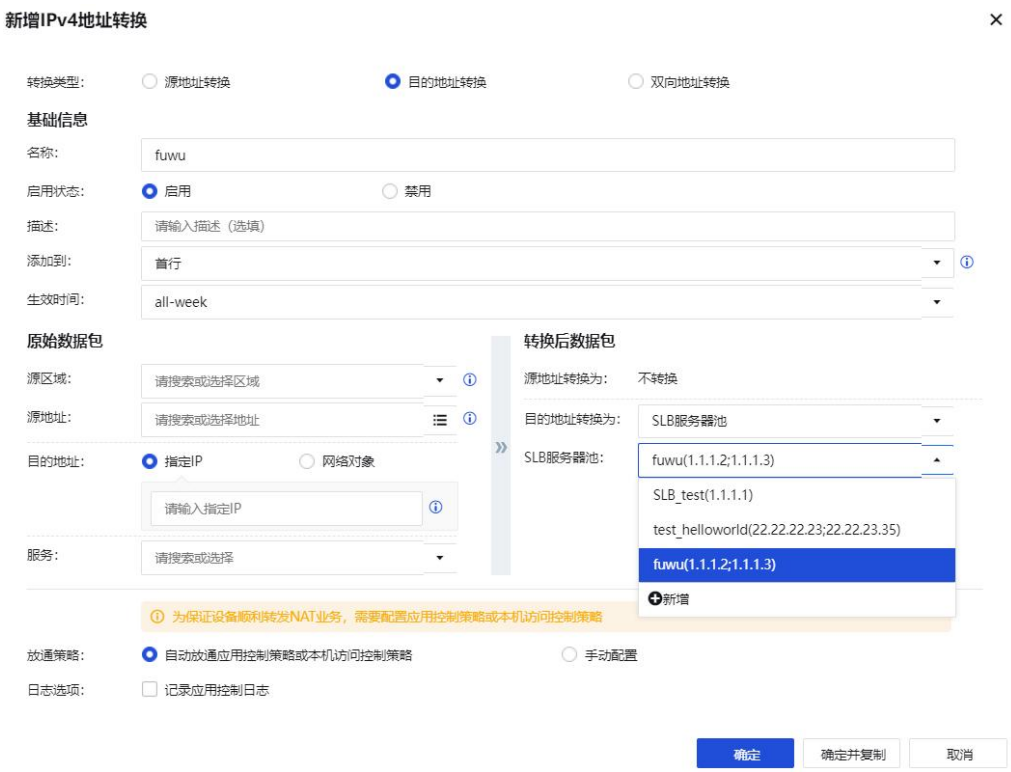
负载均衡算法：支持加权轮询算法，加权轮询是四层负载均衡中常用的负载均衡算法之一，它可以根据服务器的负载情况动态调整流量分配。加权轮询算法的原理如下：

1. 给每个服务器分配一个权重值，权重值越大表示该服务器能够处理的流量越多。
2. 依次轮询每个服务器，每次分配的流量大小为该服务器的权重值。
3. 每次分配完流量后，将该服务器的权重值减去总权重值，以便下次轮询时调整流量分配。
4. 当某个服务器的权重值减为0时，将其从轮询列表中删除，直到所有服务器的权重值都恢复到初始值

说明：

可以配置 16 个 SLB 服务器池，每个 SLB 地址池支持配置 IP+端口共 32 条。

新增SLB服务器池完成后，可以在[策略/地址转换]中新增目的地址转换或者双向地址转换中进行选择，如下图所示。



7.8. IP 地址库

IP地址库是包含所有IP地址的集合，根据IP地址的不同可以分为运营商地址、地域地址。因此，IP地址库包括ISP地址段、IP地址归属地功能。

7.8.1. ISP 地址段

ISP地址段用于设置网络运营商的IP地址段，在中文配置下默认全部、联通、电信、移动、教育网等，英文配置只有全部。此IP地址段是用在路由模式部署下调用。

点击<新增>会弹出 ISP 地址库设置窗口，需要填写名称，地址范围和 WHOIS 标志，如下图所示。

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。

点击<ISP查询>，可以查找对应的地址对应哪个运营商，如下图所示。

设备出厂时中文配置时，默认有联通、电信、中国移动、教育网四个ISP地址库。

7.8.2. IP 归属地

IP归属地主要用于纠正IP归属地错误问题、查询IP地址归属地等。从而减少IP地址归属地误报的影响，能够更加准确的展示攻击的来源等。

IP归属地纠正

当管理员检测内网的某个IP地址属于非所属区域时，可以通过IP归属地纠正来修改IP的正确区域或者是自定义IP的归属地。

点击<新增>,创建IP地址库的纠正，如下图所示。

归属地查询

当内网检测到有异常流量，管理员可以通过归属地查询去定位IP的位置然后做相应的策略。

点击<归属地查询>，查找对应的IP，如下图所示。

7.9. 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。

7.9.1. 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。如下图所示。

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。

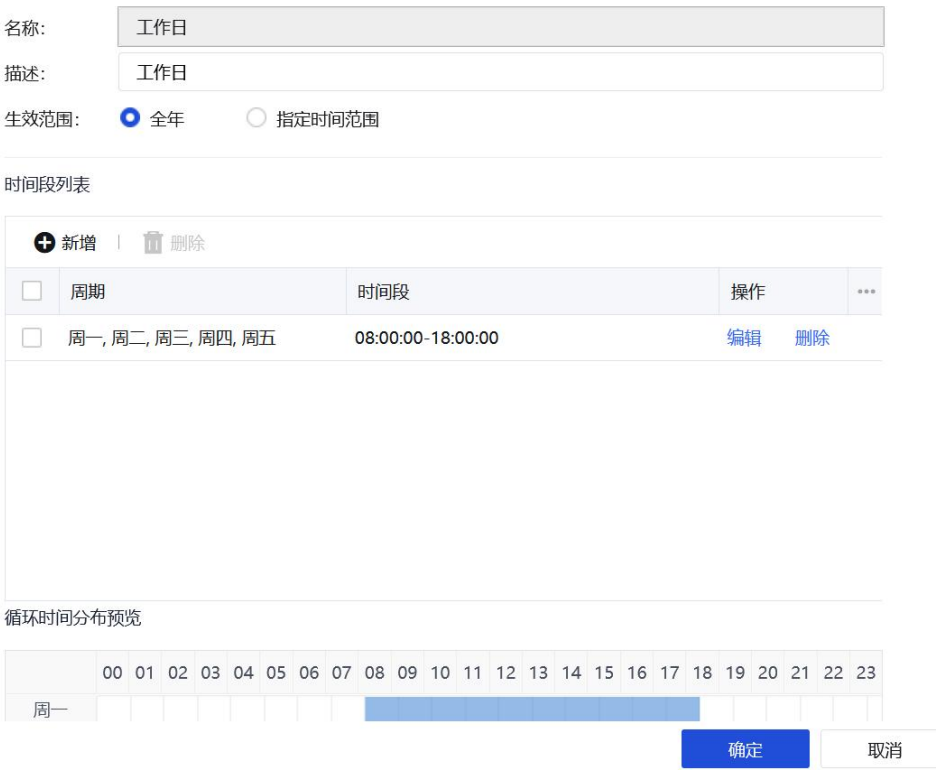
结束时间：用于设置该时间计划的结束日期和时间。

7.9.2. 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。

在循环时间计划页面点<新增>，则弹出时间组计划设置页面。



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。

生效范围：指定在生效的时间范围内。

点击<新增>可以设置具体的时间周期以及时间范围。

8. 网络

网络功能主要介绍网络相关特性的内容和配置方法。

8.1. 接口

接口用于网络中设备间的互联，其功能就是完成设备之间的数据交换。

根据部署方式的不同，接口的配置也存在较大差异。接口用于设置设备各网络接口和接口所属局域网络信息，可以设置物理接口、子接口、VLAN接口、聚合接口、GRE隧道和接口联动，如下图所示。

8.1.1. 物理接口

设备面板上的接口一一对应(如eth0为manage口)的接口，物理接口无法删除或新增，物理接口的数目由硬件决定（个别平台支持可扩展）。可以看各个接口名称、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、网口状态等，如下图所示。

接口名称：网口的名称，物理接口不支持修改名称。

网口状态：显示该网口的连接状态，其中连接状态显示绿色表示接口UP，白色显示表示接口DOWN。

WAN：显示该物理接口是否有WAN口属性，如需要配置流控等则需要开启该功能。

接口类型：显示接口所属的类型。接口类型有路由接口、透明接口、虚拟网线接口和

旁路镜像接口四种。

区域：接口所属的安全区域，eth0口默认属于带外管理区，不可修改。

连接类型：显示接口IP地址获取的类型，包括PPPoE、静态IPv4、DHCP IPv4、静态IPv6、DHCP IPv6。

IP地址：显示该网口配置的IP地址。

工作模式：显示该网口的物理网卡的工作模式，可配置物理网卡的工作模式。

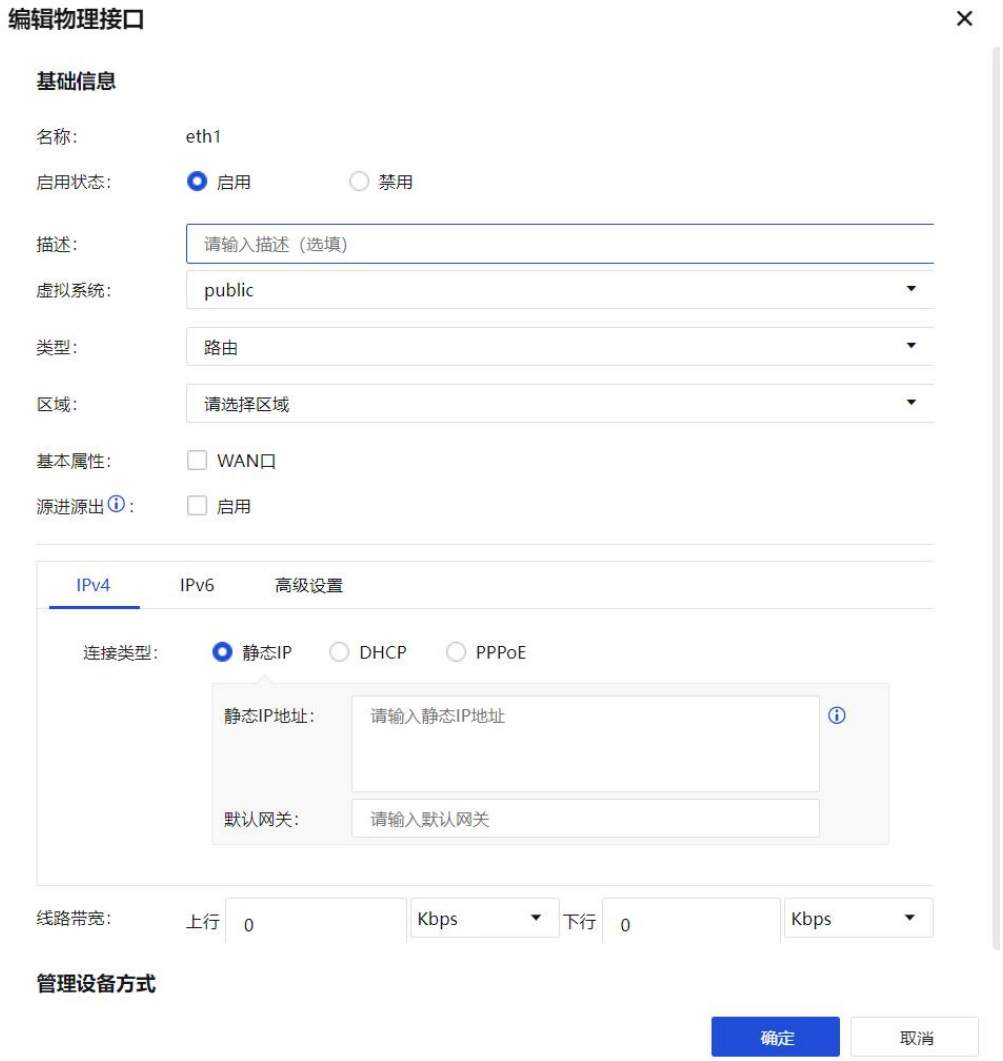
MTU(IPv4/IPv6)：显示该网口的MTU信息，可配置MTU，MTU范围：68~1796。

状态：显示接口启用的状态。

操作：编辑接口的信息。

编辑物理接口

点击接口名称<eth1>，进入到eth1的配置界面，如下图所示。



启用状态：选择接口是否启用。

类型：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，表示该接口工作在三层模式，需要配置 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。

基本属性：设置该接口的基本属性，是否为WAN口。

源进源出：用于多运营商出口场景，启用后可以保持数据包源进源出，在多运营商出口场景下进行业务发布，必须勾选防止数据包没有源进源出导致业务无法访问，启用接口WAN属性后，会自动勾选启用源进源出。

指定连接获取 IPv4 地址的方式。

选中“静态IP”，表示通过手工配置方式指定接口IPv4地址和下一跳地址。接口配置路由，需要配置上对应得IP地址。下一跳网关在勾选WAN时，必须填写，填写后不会自动生成默认路由。

选中“DHCP”，表示通过DHCP方式自动获取IPv4地址和下一跳地址。

选中“PPPoE拨号”，通过拨号的形式获取IP地址，由于运营商IP经常发生改变，所以需要勾选添加默认路由。

指定连接获取 IPv6 地址的方式。如下图所示。

如果该接口需要使用IPv6，需要先IPv6协议中选择<启用>。

选中“静态IP”，表示通过手工配置方式指定接口IPv6地址和下一跳地址。

选中“DHCP”，表示通过DHCP方式自动获取IPv6地址和下一跳地址。

高级配置：可设置接口的工作模式，MTU，以及MAC地址，也可选择是否开启巨帧功能，使该物理接口支持MTU为9000的数据包，如下图所示。

线路带宽：设置该接口的线路带宽范围，如下图所示。

管理设备方式：是否允许该接口访问设备，如HTTPS、PING、SSH、SNMP。

说明：

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，可在[系统/系统配置/通用配置/网络参数]进行修改。
3. 任何接口的 IPv4 地址不允许设置在 1.1.1.0/24 网段范围。

8.1.2. 子接口

子接口指的是在一个主接口上配置出来的多个逻辑上的虚拟接口。子接口依赖物理接口，共用主接口的物理层参数，又可以分别配置各自的链路层和网络层参数。主接口状态的变化会对子接口产生影响，特别是只有主接口处于连通状态时子接口才能正常工作。

设备支持在三层以太网接口和三层VLAN-Trunk接口下创建子接口。当三层以太网接口或VLAN--Trunk接口需要识别VLAN报文时，可通过配置子接口解决。这样，来自不同VLAN的报文可以从不同的子接口进行转发，为用户提供了很高的灵活性。

在[网络/接口/子接口]进行配置，点击<新增>，创建子接口，如下图所示。

物理接口：接口选择在那个物理接口上创建的子接口。

VLAN ID：创建的VLAN ID，说明该接口支持接收和发送对应的VALN ID。

描述：填写该子接口的描述信息。

所属区域：选择为该子接口定义的区域。

源进源出：用于多运营商出口场景，启用后可以保持数据包源进源出，在多运营商出口场景下进行业务发布，必须勾选防止数据包没有源进源出导致业务无法访问，启用接口WAN属性后，会自动勾选启用源进源出。

高级设置中MTU：显示该网口的MTU信息，可配置MTU，MTU范围：68~1500。

8.1.3. VLAN 接口

当VLAN内的主机需要与网络层的设备通信时，可以在设备上创建基于VLAN的逻辑接口，即VLAN接口。VLAN接口在功能上与普通三层物理接口基本相同，可实现配置IPv4/IPv6地址等多种三层特性。用于二层透明部署场景，以实现VLAN间的通信。

新增VLAN接口，在[网络/接口/VLAN接口]，点击<新增>，如下图所示。

VLAN ID ：为VLAN创建虚拟接口，实现三层互通。

描述：简单描述该接口的信息。

所属区域：选择该VLAN接口所属的区域。

源进源出：用于多运营商出口场景，启用后可以保持数据包源进源出，在多运营商出口场景下进行业务发布，必须勾选防止数据包没有源进源出导致业务无法访问，启用接口WAN属性后，会自动勾选启用源进源出。

选中“静态IP”，表示通过手工配置方式指定接口IPv4地址或IPv6地址和下一跳地址。

选中“DHCP”，表示接口通过DHCP方式自动获取IPv4地址或IPv6地址和下一跳地址。

高级设置中MTU：显示该网口的MTU信息，可配置MTU，MTU范围：68~1500。

8.1.4. 聚合接口

将多个以太网物理接口捆绑在一起所形成的逻辑接口，可以增加带宽、提供链路可靠性、链路负载分担等优势。新增聚合接口，在网络/接口/聚合接口，点击<新增>，如下图所示。

接口名称：填写聚合接口的编号，只支持填写1-16，即最大支持16个聚合接口。

描述：简单描述该接口的信息。

类型：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，表示该接口工作在三层模式，需要配置 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。

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、主备模式和LCAP模式。

负载均衡-hash:按数据包源目的 IP/MAC 的 hash 值均分。

负载均衡-RR:直接按数据包轮转均分到每个接口。

主备模式：取 eth 数字大的接口为主接口收发包，其余为备接口（如选了 eth2 和 eth1 两个接口，eth2 会作为主接口，eth1 会作为备接口）。

LACP：标准 LACP 协议对接，选择 LACP 选项后，可以支持基于：基于源 IP 和目的 IP 以及源 mac 目的 mac、基于源 IP 和目的 IP 以及源端口目的端口、基于源 mac 目的 mac 三种哈希策略，同时支持主动和被动协商两种模式。

说明：

聚合接口不支持旁路镜像模式。

8.1.5. 本地回环接口

本地回环接口它代表设备的本地虚拟接口，所以默认被看作是永远不会宕掉的接口。

8.1.6. 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。点击<新增>，GRE隧道新增如下图所示。

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，可以选择填写IPv4地址或者IPv6地址。

类型：隧道可以选择IPv4或者IPv6类型。

隧道源端地址：本端出接口实际公网路由源地址。

隧道目的端地址：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IPv4和IPv6 MTU值、报文检验和和发送Keepalive报文的设置。

点击<确定>，完成GRE隧道设置。

8.1.7. 接口联动

接口联动用于AF设备工作在流量负载均衡模式，把负责转发数据的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，则自动宕机，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。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，点击新增，添加接口联动，如下图所示。

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。可选择配置IPv6地址的物理接口。

8.2. 区域

根据网络架构的安全需求，将不同业务或网段划分成不同的安全级别，通过不同安全级别定义不同安全域。定义区域时，根据控制需求来规划，可以将一个接口划分到一个区域，或将几个相同需求的接口划分到同一个区域。区域是本地逻辑的概念，根据转发类型可以分为二层区域、三层区域和虚拟网线区域。

二层区域：只能选择透明接口、旁路镜像口。
三层区域：可以选择所有的路由接口，包括：路由接口、子接口、VLAN 接口。
虚拟网线区域：只能选择虚拟网线接口。

点击<新增>，创建区域，如下图所示。

转发类型：根据部署模式的不同，可以选择二层区域、三层区域和虚拟网线区域。

8.3. 路由

路由配置页面包括静态路由、策略路由、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。

8.3.1. 静态路由

静态路由是需要管理员手工配置的特殊路由。

当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。仔细设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由的缺点在于：当网络发生故障或者拓扑发生变化后，静态路由不会自动改变，必须有管理员的介入。

静态路由能实现设备跨三层访问，静态路由页面如下图所示。

点击<新增>，创建静态路由，可创建单条静态路由和多条静态路由，如下图所示。

新增路由数量：可以创建单条路由和多条路由。创建单条路由则只能创建一条静态路由，创建多条路由，则是通过固定格式刷入多个路由信息。

协议类型：选择IPv4或者IPv6。

启用状态：是否对这条静态路由启用。

目的地址/掩码：需要到达的目标网段和子网掩码。

下一跳IP地址：达到目标网络的下一跳地址，下一跳地址不能填设备本地网口IP。

接口：从设备某个接口转发。

管理距离：可设置静态路由的管理距离，数值越小优先级越高。

度量值：目的地址相同情况下，优先选择度量值越低的转发，即度量值越低，优先级越高。

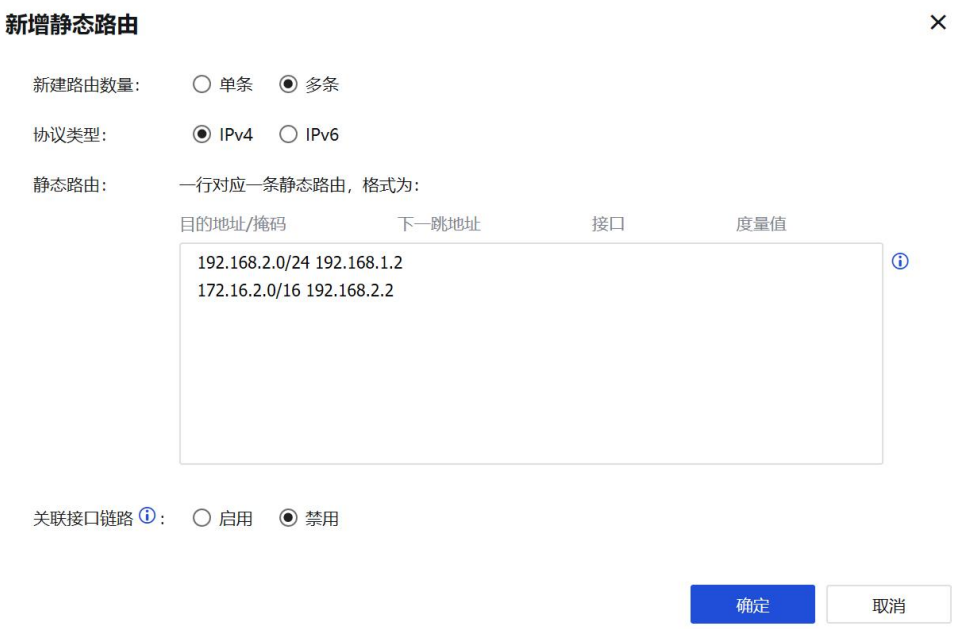
关联接口链路：启用后，当所选接口的链路出现故障(PING或DNS任何一种探测方式探测失败)时，会将此静态路由的状态置为无效，并从对应的路由表中删除。当此路由用作浮动路由时，推荐开启。

路由优先级：显示设备目前路由优先级，点击<修改>可进行优先级调整，如下图所示。

说明：

开启关联接口链路，则需所选接口必须启用链路故障检测功能。

选择创建多条静态路由，根据格式，填写多个IP即可，如下图所示。



8.3.2. 策略路由

策略路由的操作对象是数据包，在路由表已经产生的情况下，不按照先行路由表进行转发，而是根据需要，依照某种策略改变其转发路径的方法。

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。如下图所示。

8.3.2.1. 源地址策略路由

存在多条线路出口情况下，根据源/目IP，端口、协议、应用来定义匹配条件，对于匹配上的流量根据选择指定线路的出口或下一跳，比如多运营商选路场景；点击<新增>，如下图所示。

路由类型：可选择源地址策略路由和多线路负载路由。

协议类型：选择IPv4或者IPv6。

名称：填写对应的名称。

描述：填写该路由的描述信息。

生效时间：制定该条策略生效的时间范围。

添加到：把该条策略放在X之前，匹配顺序从上到下。

数据包：筛选对应的数据包信息进行匹配。

源区域：匹配所属源区域。

源地址：匹配的源网络对象，即筛选的源IP地址。

目的地址：匹配的目的地址，可以调用网络对象、ISP地址、国家/地区。

网络对象：根据实际情况配置的网络对象进行调用。

ISP 地址：根据运营商进行选路，目前支持电信、联通、教育网、移动。

国家/地区：根据国家/地区来进行筛选。

服务：需要匹配的服务对象，如下图所示。

应用：需要匹配的应用，如下图所示。

接口与下一跳：对去往目的IP的流量下一跳走向，可以设置下一跳和出接口。

可靠性检测：可选择不检测和链路故障检测。

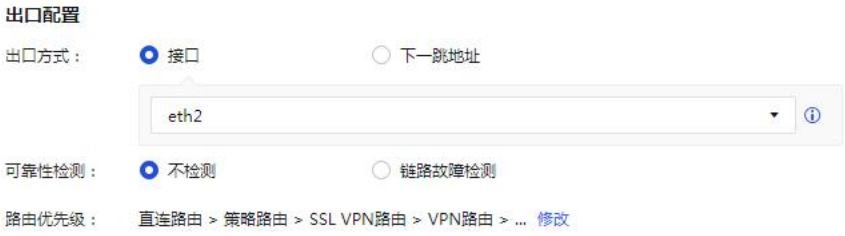
路由优先级：显示设备目前路由优先级，点击<修改>可进行优先级调整。

配置案例

某用户需要访问一个网上银行，地址是100.100.100.100，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eth2接口连接的线路出去。

步骤1.在导航菜单页面中的[网络/路由/策略路由]，点击<新增>，路由类型选择<源地址策略路由>，协议类型选择<IPV4>，基础信息和数据包填写入下图所示。

步骤2.配置出接口为eth2，如下图所示。



步骤3.点击<确定>，完成配置，如下图所示。

8.3.2.2. 多线路负载路由

当某企业存在多条线路出口情况下，根据源/目IP，端口、协议、应用来定义匹配条件，对出接口选择轮询、带宽比例、加权最小流量、优先使用前面的线路策略，进行动态选择线路，实现线路带宽的有效利用和负载均衡。

点击<新增>，选择多链路负载路由，如下图所示。

出接口列表：对该条策略选择多个出接口，然后根据策略进行负载。点击<添加>，增加出接口，如下图所示。

链路状态：当接口配置有链路探测，当PING或DNS任一探测失败时，会认为该线路故障。

出接口选择策略：根据算法对流量进行负载，存在以下4种算法：

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。

配置案例

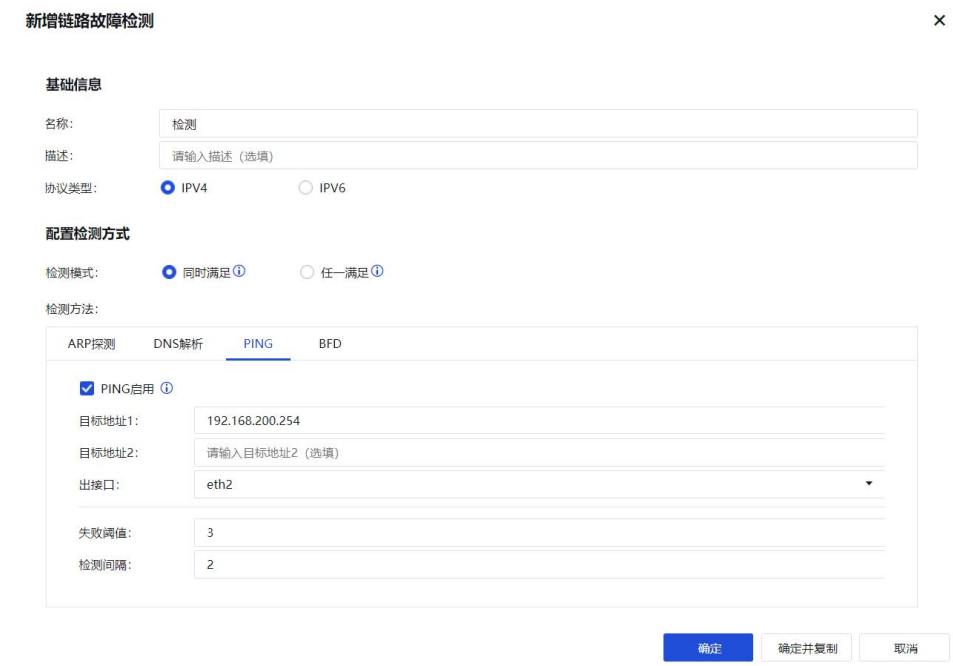
某用户有2条外网线路，分别是2M和10M的电信线路，用户希望实现内网用户访问公网的时候自动选择流量最小的线路。

步骤1.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。

步骤2.配置接口信息，如下图所示。

步骤3.选择负载分担模式，如下图所示。

步骤4.配置对应的接口链路状态检查，当某一条链路故障后，能够进行切换，如下图所示。



步骤5.查看配置情况，如下图所示。

⚠ 注意：

1. 如果要实现多条外网线路的负载，必须开启链路故障检测。
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。

8.3.3. 多播路由

AF本身不转发组播流量，如果需要AF指出转发组播流量，则需要配置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。

源地址：组播数据来源地址。

组播地址：组播数据包目的地址。

源接口：发组播数据主机来源接口。

转发接口：组播流量向下转发的接口（可以选择多个接口）。

8.3.4. OSPF

OSPF(Open Shortest Path First开放式最短路径优先）是一个内部网关协议（IGP），用于在单一自治系统（AS）内决策路由。是对链路状态路由协议的一种实现，隶属内部网关协议（IGP），运作于自治系统内部。OSPF支持负载均衡和基于服务类型的选路，也支持多种路由形式，如特定主机路由和子网路由等。AF设备OSPFv2和OSPFv3动态路由协议。

8.3.4.1. OSPF 列表

步骤1. 新增基础配置。在OSPF列表中点击<新增>，弹出[新增基础配置]页面，如下图。

类型：选择OSPFv2或OSPFv3协议类型。

路由器ID：在OSPF路由中会使用route id来标识路由器的序列号，竞选DR和BDR根据router-id的大小进行。

SPF计算延迟时间：从OSPF收到变化到开始SPF进行计算的延迟时间。

SPF计算间隔时间：OSPF两次计算之间的时间间隔。

域内优先级：配置域内路由类型的管理距离。取值范围1~255，默认值110。

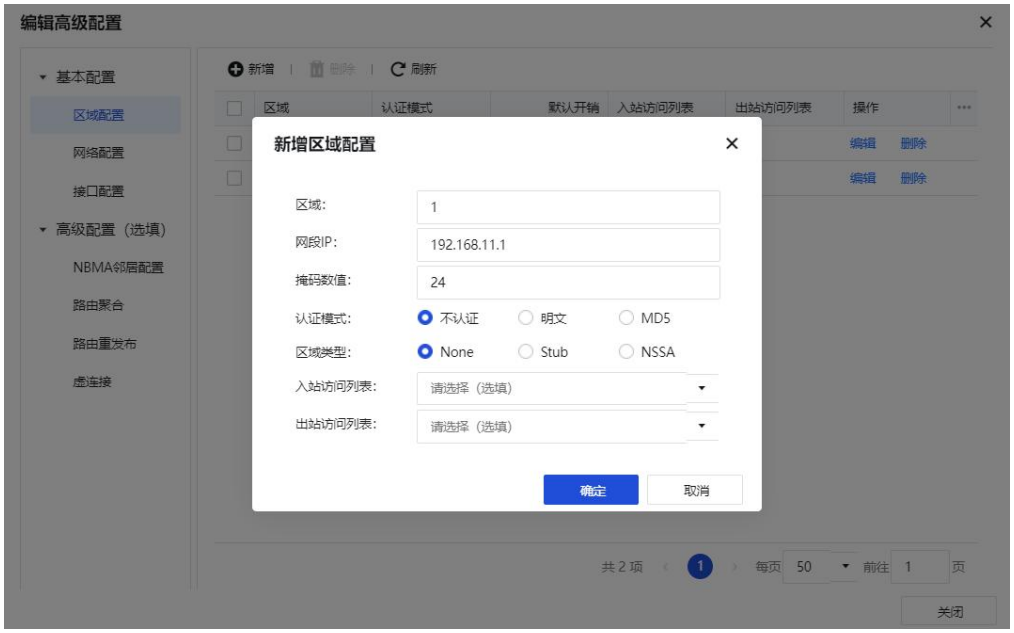
域间优先级：配置域间路由类型的管理距离。取值范围1~255，默认值110。

外部优先级：配置外部路由类型的管理距离。取值范围1~255，默认值110。

路由重发布默认度量值：重发布路由的默认度量值。默认值为20。

BFD功能：全局BFD，开启有加速路由收敛时间，不必等待邻居超时时间。

步骤2. 进行区域配置。完成基础配置，点击<确定并前往高级配置>，进行区域配置，点击<新增>，如下图所示。

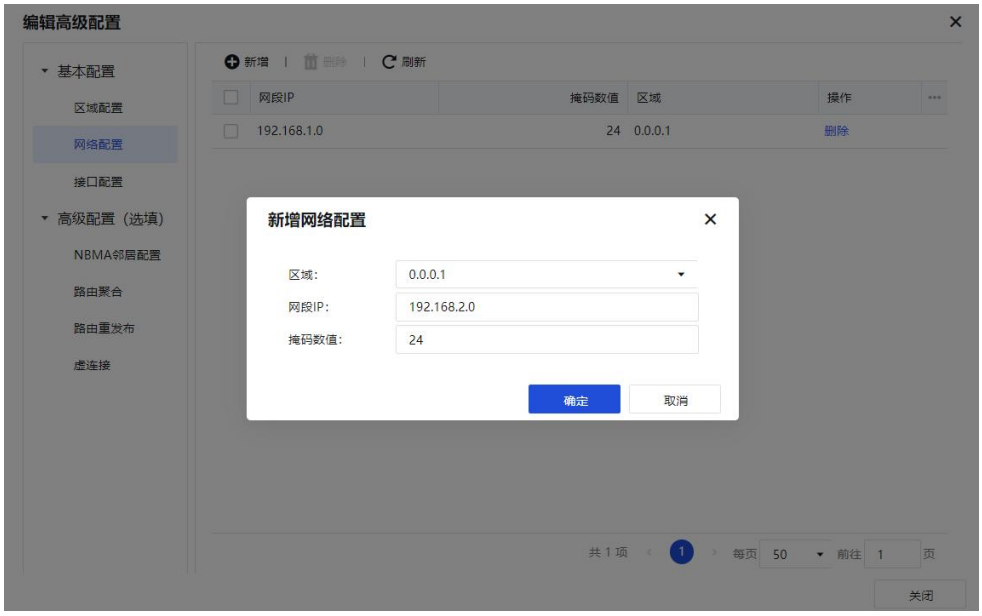


认证模式：包括不认证、明文和MD5三种模式选择。

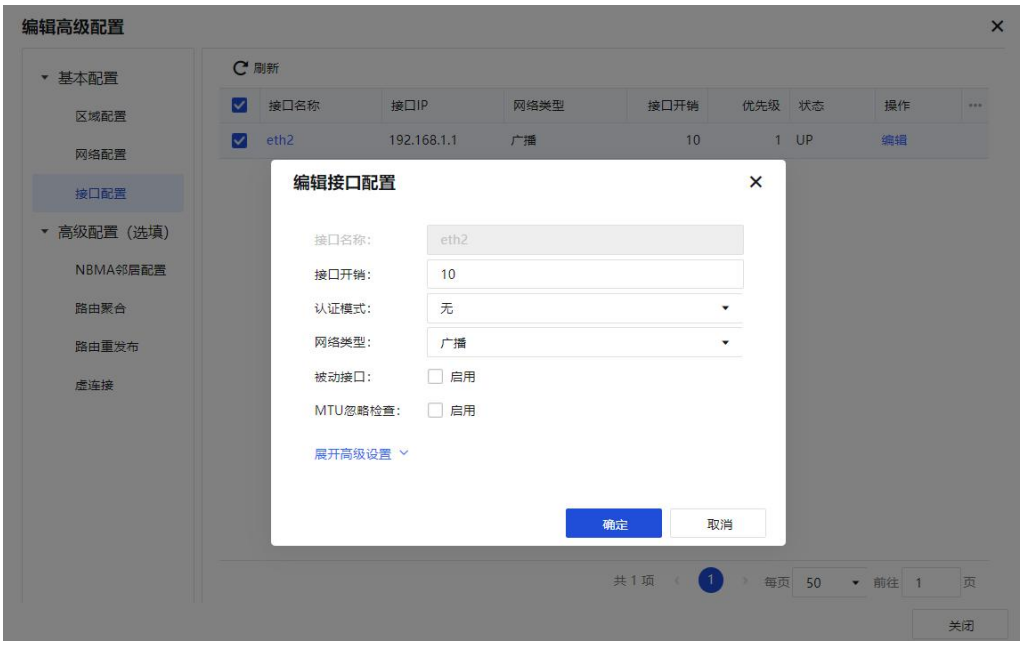
区域类型：包括None、Stub和NSSA三种类型选择。Stub区域的ABR不允许注入Type-5的LSA，在这些区域中路由器的路由表规模以及路由信息传递的数量都会大大减少；NSSA（Not-So-Stubby Area）区域是Stub区域的变形。NSSA区域也不允许Type-5 LSA注入，但可以允许Type-7 LSA注入。当Type7 LSA到达NSSA的ABR时，由ABR将Type-7 LSA转换成Type-5 LSA，传播到其他区域。

入站访问列表、出站访问列表：可在[网络/路由/访问列表]配置后进行选择，进行出入站网段的控制。

步骤3. 进行网络设置。网络设置中需要发布的网段，点击<新增>，选择区域，增加发布的网段及掩码，如下图所示。



步骤4. 配置完网络设置，查看接口配置，显示网络配置中发布的网段对应的接口信息。也可进行编辑，如下图所示。



接口开销：当前接口的链路开销。

认证模式：用户可以配置接口的认证方式。默认情况下，接口没有认证方式。

网络类型：广播、非广播多路访问、点到多点以及点到点四种类型选择。

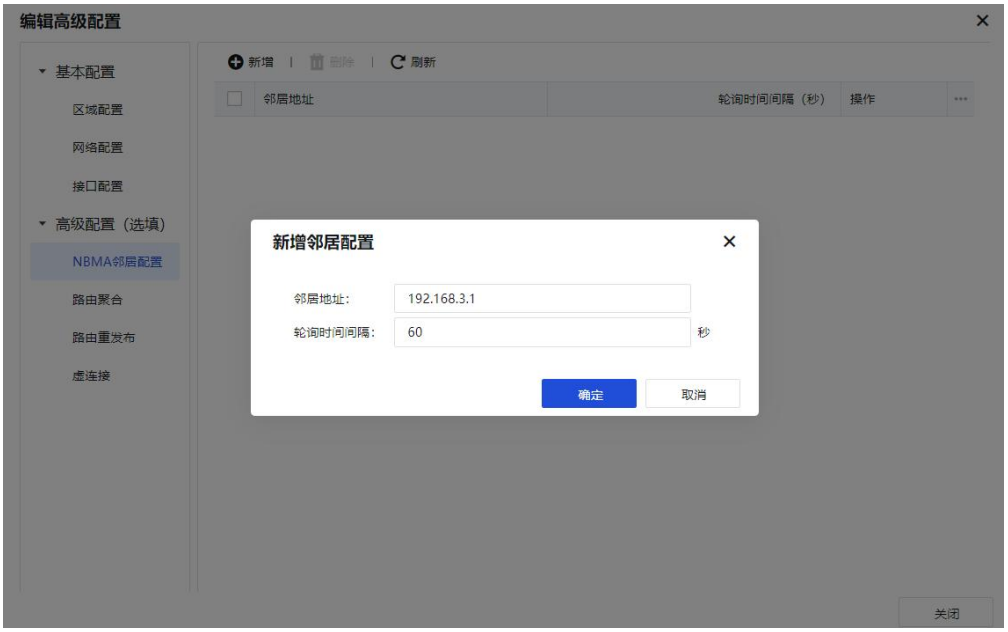
被动接口：用户可以将一些接口设置为只接收更新但是不发送，这种只接口更新的接口就是被动接口。

MTU忽略检查：开启后接口间mtu不一致的情况下，也可建立邻居。

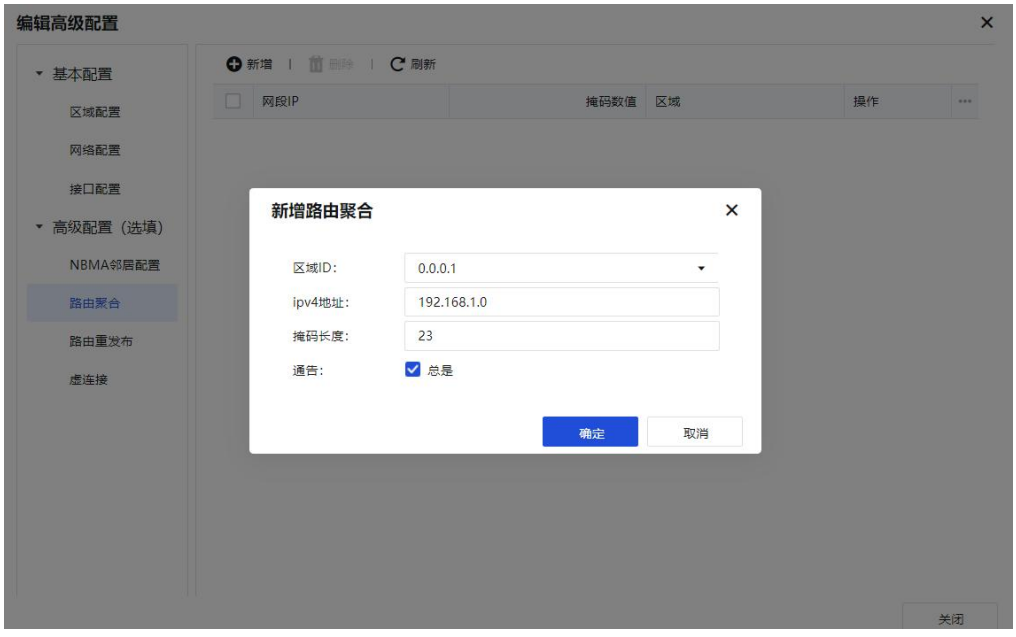
点击<展开高级设置>，可进行DR优先级、传输延迟时间、邻居超时时间、Hello报文间隔和重传时间间隔设置，如下图所示。

步骤5. 进行高级配置(选填，根据实际需要配置)。配置NBMA邻居配置，NBMA网络是指非广播、多点可达网络，比较典型的有ATM和帧中继网络，当接口类型配置为

NBMA网络类型时，接口无法通过广播Hello报文的形式发现相邻路由器，必须通过手工配置相邻路由器linklocal地址的方式来进行探测并建立邻居，后续报文交互以单播的形式进行。点击<新增>，如下图所示。



步骤6. 配置路由聚合。路由聚合是指将具有相同前缀的路由信息通过ABR聚合在一起，只发布一条路由到其他区域。一个区域可以配置多条聚合网段，这样OSPF可以对多个网段进行聚合。点击<新增>，如下图所示。

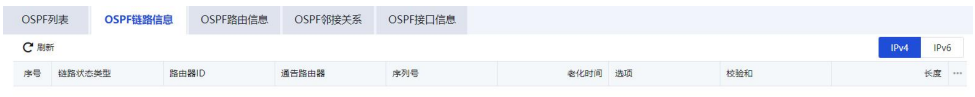


步骤7. 配置路由重发布。OSPF协议允许用户引入其他OSPF进程路由信息以及其他路由协议（直连路由、静态路由、默认路由、BGP、PIR、VPN）的路由信息，并向外发布。用户可以设置被引入路由的度量以及外部路由的类型。点击<新增>，如下图所示。

步骤8. 配置虚连接。虚连接用来连接不连续的骨干区域，使他们能够保持逻辑上的连续性，配置虚拟链路以及定时器参数。点击<新增>，如下图所示。

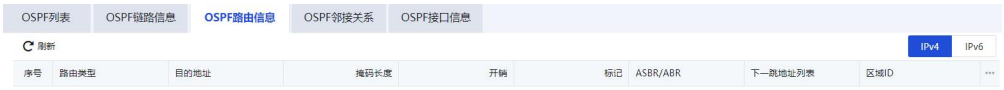
8. 3. 4. 2. OSPF 链路信息

显示 OSFP 的链路状态信息，如下图。



8.3.4.3. OSPF 路由信息

显示网络中的 OSPF 路由信息，如下图所示。



8.3.4.4. OSPF 邻接关系

显示 OSPF 的邻接关系，如下图所示。

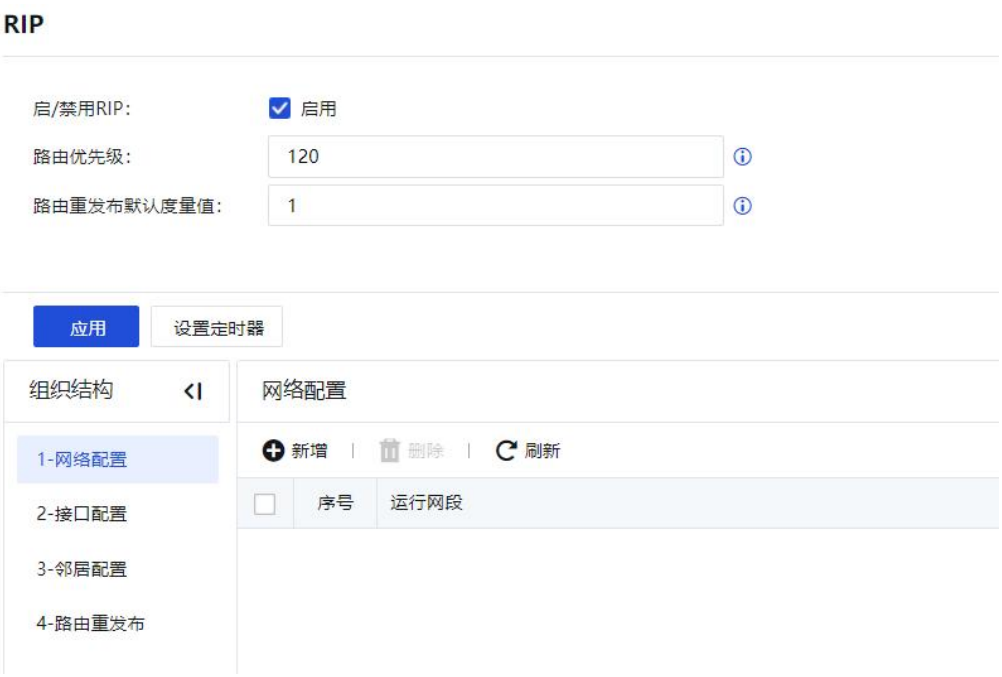
8.3.4.5. OSPF 接口信息

显示 OSPF 的接口信息，如下图所示。

8.3.5. RIP

RIP协议采用距离向量算法，在默认情况下，RIP使用一种非常简单的度量制度：距离就是通往目的站点所需经过的链路数，取值为0~16，数值16表示路径无限长。RIP进程使用UDP的520端口来发送和接收RIP分组。RIP分组每隔30s以广播的形式发送一次，为了防止出现“广播风暴”，其后续的分组将做随机延时后发送。在RIP中，如果一个路由在180s内未被刷新，则相应的距离就被设定成无穷大，并从路由表中删除该表项。

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，路由重发布内容，勾选启用RIP功能，然后点击<应用>后如下图所示。



8.3.5.1. 网络配置

在指定接口上，将其相应的网段设置RIP网段。点击<新增>。

运行网段：设置需要发布的网段地址，填写格式为：IP/掩码。

8.3.5.2. 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网络下新增了网段信息，则自动生成的接口配置如下所示。

点击<接口名称>，出现如下页面。

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。

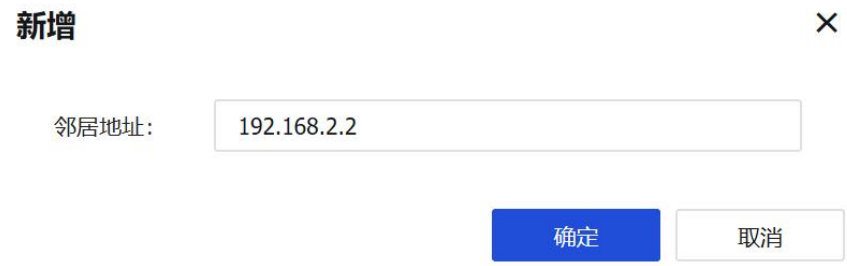
毒性逆转：启用毒性逆转之后，从一个接口收到的路由，会从这个接口泛洪出去，但这条路由的METRIC是无穷大。缺省情况下不启用毒性逆转。

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。

8.3.5.3. 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。



8.3.5.4. 路由重发布

点击路由重发布，出现如下页面。

路由类型：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。

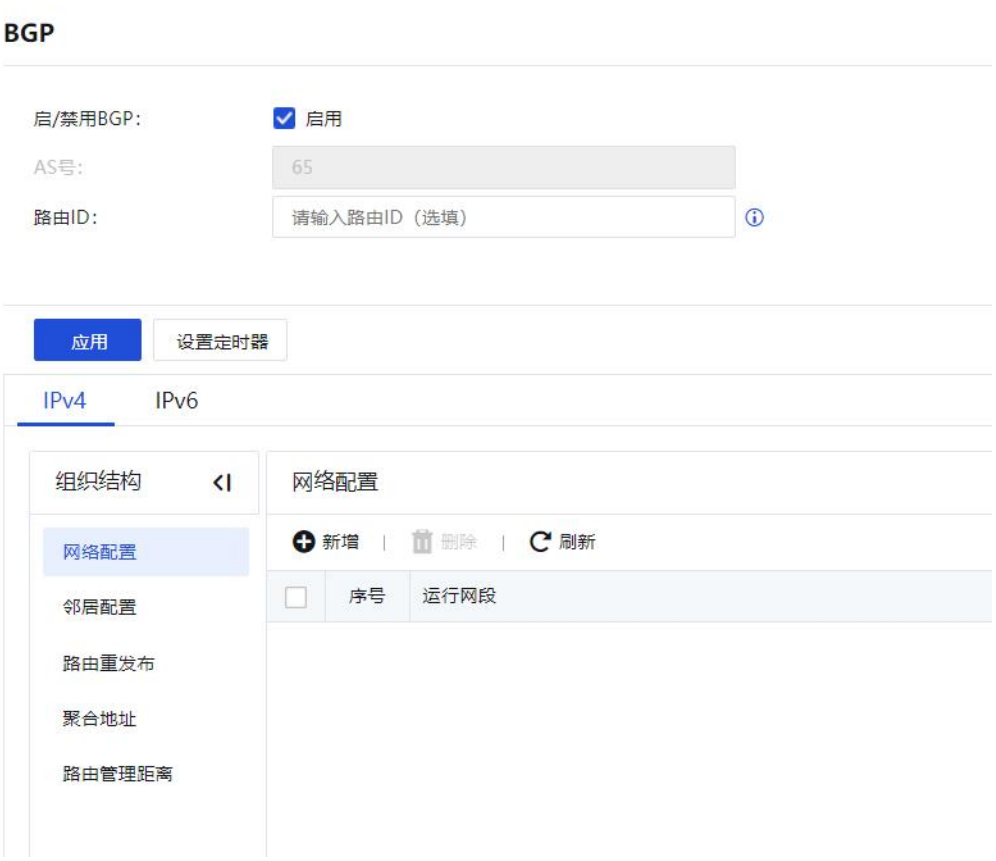
重发布OSPF路由：选择是否需要将直连路由引入RIP路由中作为外部路由信息，并可设置路由引入后的metric 值。默认度量值是20。

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。

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1。

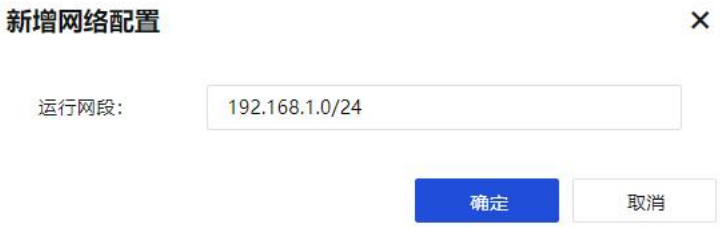
8.3.6. BGP

BGP是一种既可以用于不同AS之间，又可以用于同一AS内部的动态路由协议。当BGP运行于同一AS内部时，被称为IBGP（Internal BGP）；当BGP运行于不同AS之间时，称为EBGP（External BGP）。AS是拥有同一选路策略，属于同一技术管理部门的一组路由器。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，路由重发布等内容。勾选启用BGP，启用BGP功能，填写AS号，然后点击<应用>后如下图所示。



8.3.6.1. 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。

8.3.6.2. 邻居配置

邻居配置是设置BGP的邻居信息，点击<新增>，出现如下页面。

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。

入站路由映射名：为对等体设置基于该路由策略的路由接收过滤策略。

出站路由映射名：为对等体设置基于该路由策略的路由发布过滤策略。

Next-hop-self特性：缺省情况下，路由器向IBGP对等体/对等体组发布路由时，不将自身地址作为下一跳，但有的时候为了保证IBGP邻居能够找到下一跳，可以配置将自身地址作为下一跳。

BFD功能：当本地路由器和BGP对等体之间的链路出现故障时，BFD可以快速检测到该故障，从而加快BGP协议的收敛速度。

8.3.6.3. 路由重发布

点击路由重发布，出现如下页面。

路由类型：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。

⚠ 注意：

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

8.3.6.4. 聚合地址

对网段进行聚合，点击<新增>，创建聚合的地址，如下图所示。

网段：聚合的地址网段。

选项：是否保留原来的AS号。

8.3.6.5. 路由管理距离

路由管理距离用于设置EBGP和IBGP路由管理距离，如下图所示。

8.3.7. 查看路由

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习到的路由，同时当网络不通时，可通过路由查看是否存在相应的有效路由，协助排障，如下图所示。

序号	类型	目的地址	子网掩码/前缀	下一跳地址	度量值	接口	管理距离	状态
1	静态路由	0.0.0.0	0	172.22.7.254	0	eth1	1	有效
2	直连路由	1.1.1.0	24	0.0.0.0	0	veth.0	0	有效
3	本机路由	1.1.1.1	32	0.0.0.0	0	veth.0	0	有效
4	直连路由	1.2.1.0	24	0.0.0.0	0	eth1	0	有效
5	本机路由	1.2.1.1	32	0.0.0.0	0	eth1	0	有效
6	本机路由	127.0.0.1	32	0.0.0.0	0	null0	0	有效
7	本机路由	134.80.72.41	32	0.0.0.0	0	vpntun	0	有效
8	直连路由	172.22.0.0	21	0.0.0.0	0	eth1	0	有效
9	本机路由	172.22.7.111	32	0.0.0.0	0	eth1	0	有效
10	直连路由	192.168.11.0	24	0.0.0.0	0	eth2	0	有效
11	本机路由	192.168.11.1	32	0.0.0.0	0	eth2	0	有效

8.3.8. 路由测试

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。如下图所示。

协议：可选择测试的协议，如TCP、UDP、ICMP或者其他。

协议号：填写对应的协议号，只有选择其他才能够填写。

源地址/源端口：需要测试的源地址和端口。

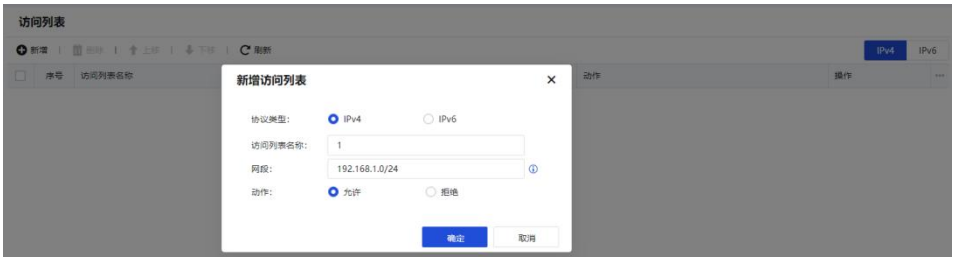
目的地址：到达目的网段的IP，此项为必填项。

目的端口：到达目的IP的端口。

测试完成后，会列出该条路由匹配的详细信息。

8.3.9. 访问列表

限制BGP的路由，可以对这些路由进行允许或者拒绝访问。如下图所示。



协议类型：可选择IPv4和IPv6两种协议类型。

访问列表编号：填写对应的列表编号，只能1-99的数字。

动作：是否允许或者拒绝。

网段：填写对应的网段信息。

8.3.10. 路由映射

默认情况下AF会引入所有的路由信息。用户可以引用路由映射表对引入的路由信息进行过滤。路由映射表主要由路由匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入的路由信息命中了任何路由匹配规则，AF就会执行对应的操作，允许或拒绝引入这些路由信息。

路由映射对BGP的路由进行本地映射，从而可以调整优先级，从而能够自由的控制路由的转发。点击<新增>，创建路由映射，如下图所示。

路由映射名：输入映射的名称。

优先级：输入对应的优先级。

IPv4访问列表编号：填写配置IPv4访问列表的编号。

IPv6访问列表编号：填写配置IPv6访问列表的编号。

AS路径附加：增加对应的AS号。

Origin：修改对应的原始属性，可以修改为Incomplete、EGP、IGP。

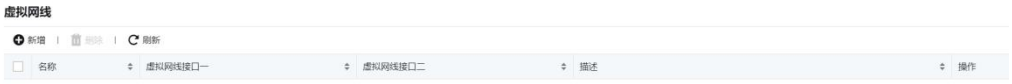
本地优先级：选择本地的优先级。

动作：对该映射是否允许或者拒绝。

8.4. 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。

虚拟网线的配置如下图所示。



点击<新增>，新增虚拟网线，配置如下图所示。

名称：填写虚拟网线的名称。

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或聚合接口。

虚拟网线接口二：选择虚拟接口属性的物理接口或聚合接口。

注意：

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。

8.5. DNS

TCP/IP提供了通过IP地址来连接到设备的功能，但对用户来讲，记住某台设备的IP地址是相当困难的，因此专门设计了一种字符串形式的主机命名机制，这些主机名与IP地址相对应。在IP地址与主机名之间需要有一种转换和查询机制，提供这种机制的系统就是域名系统DNS（Domain Name System）。

8.5.1. DNS 配置

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。如下图所示。

首选DNS服务器：设置AF设备本身访问公网的DNS服务器，AF首先使用该DNS地址进行解析。

备选DNS服务器：设置AF设备本身访问公网的DNS服务器，AF无法解析首选DNS服务器后，则选择备选DNS服务器地址解析。

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。DNS代理使用端口为TCP/53，开启后所有区域都可以访问防火墙上此端口，如防火墙部署在出口，建议在策略>访问控制>本机访问控制中拒绝互联网区域到此端口访问。

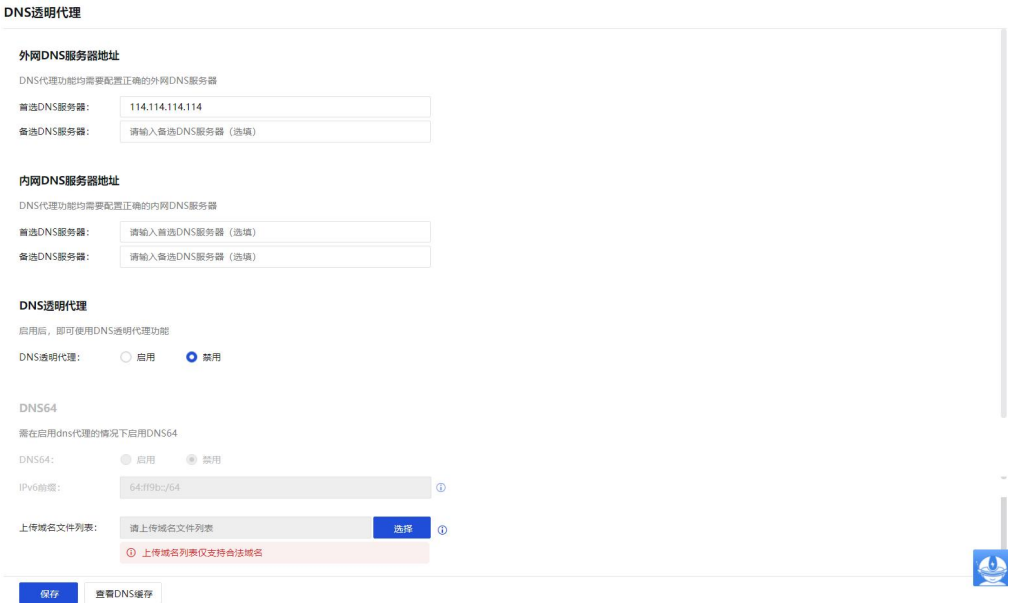
DNS64：需要先启用DNS代理才能使用，DNS64主要是配合NAT64工作，主要是将DNS查询信息中的A记录（IPv4地址）转为AAAA记录（IPv6地址），然后返回AAAA记录给IPv6侧用户。

8.5.2. DNS 透明代理

DNS透明代理就是指中间设备（一般是网关）截获客户端通过设备本身的DNS数据包，由中间设备根据相关设置将请求发送给设备本身配置的DNS服务器进行解析，中间设备收到DNS服务器应答后，再返回给客户端，这个代理过程对于客户端来说是无感知的，是完全透明的。

DNS透明代理页面用于内网用户DNS地址未指向AF设备，但DNS请求经过AF时，AF

进行透明的DNS代理解析设置，如下图所示。



外网DNS服务器地址：设置用于DNS透明代理的外网DNS服务器地址，如114.114.114.114等。此处设置的DNS地址，当开启DNS透明代理后，非上传域名文件列表内上传的域名，一律通过该处设置的外网DNS地址进行代理解析。

内网DNS服务器地址：设置用于DNS透明代理的内网DNS服务器地址，此处设置的DNS地址，当开启DNS透明代理后，只代理上传域名文件列表内上传的域名，一律通过该处设置的内网DNS地址进行代理解析。

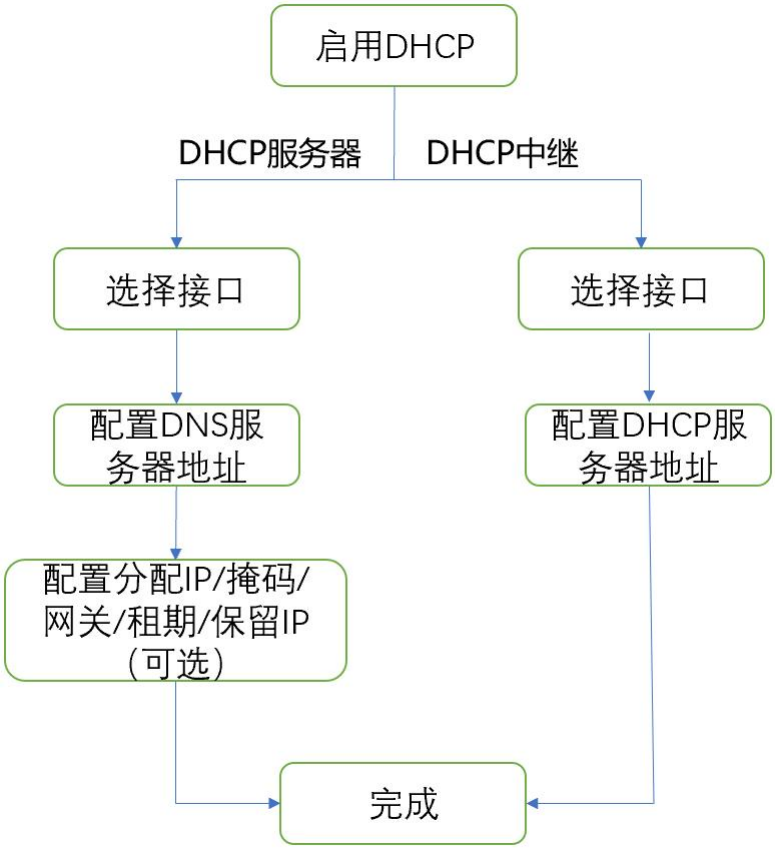
DNS透明代理：设置用于开启/禁用DNS透明代理功能的开关选项。

DNS64：需要先启用DNS透明代理才能使用，DNS64 则主要是配合 NAT64工作，主要是将 DNS查询信息中的 A记录（IPv4地址）合成到 AAAA记录（IPv6地址）中，返回合成的 AAAA记录用户给 IPv6侧用户。

上传域名文件列表：设置用于需要通过内网DNS服务器地址，内配置的内网DNS地址进行解析的域名，常见场景为单位自己的网站域名访问时，直接解析到网站对应的内网IP。

8.6. DHCP

DHCP（动态主机配置协议）是一个局域网的网络协议。指的是由服务器控制一段IP地址范围，客户机登录服务器时就可以自动获得服务器分配的IP地址和子网掩码。而AF部署在用户环境中，充当DHCP服务器，给客户机分配对应的IP地址。



8.6.1. DHCP 服务器

动态主机配置协议DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户IP地址进行动态管理和配置的技术。即使规模较小的网络，通过DHCP也可以使后续增加网络设备变得简单快捷。

DHCP可以提供两种地址分配机制，网络管理员可以根据网络需求为不同的主机选择不同的分配策略。

动态分配机制：通过 DHCP 为主机分配一个有使用期限（这个使用期限通常叫做租期）的 IP 地址。

这种分配机制适用于主机需要临时接入网络或者空闲地址数小于网络主机总数且主机不需要永久连接网络的场景。

静态分配机制：网络管理员通过 DHCP 为指定的主机分配固定的 IP 地址。

相比手工静态配置 IP 地址，通过 DHCP 方式静态分配机制避免人工配置发生错误，方便管理员统一维护管理。

AF充当DHCP服务器，给客户端提供IP地址。点击<新增>，选择协议类型和服务器类型，如下图所示。

网络信息

配置DHCP的网络信息。

接口：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。

可分配IP地址范围：选择分配IP的地址范围，如不填写默认为接口的地址分配。

子网掩码：分配IP的掩码。

DHCP网关：填写DHCP的网关地址，如不填写则接口地址为网关。

DNS服务器：设置分配给客户端的DNS地址。

高级设置

租期：设置DHCP分配IP的租期期限。

首选WINS服务器：配置首选WINS服务器地址。

备选WINS服务器：配置备选WINS服务器地址。

地址绑定

设置需要保留的 IP，即不分配的 IP。点击<新增>，创建保留的 IP 地址。

配置案例

某用户AF设备的内网口eth1下接内网网段，用户要求通过AF自动分配172.16.10.100-172.16.10.199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172.16.10.150的IP地址。

步骤1.新增DHCP服务器，接口列表中选择eth1口进行DHCP配置。配置可分配IP范围和DNS网络参数等，如下图所示。

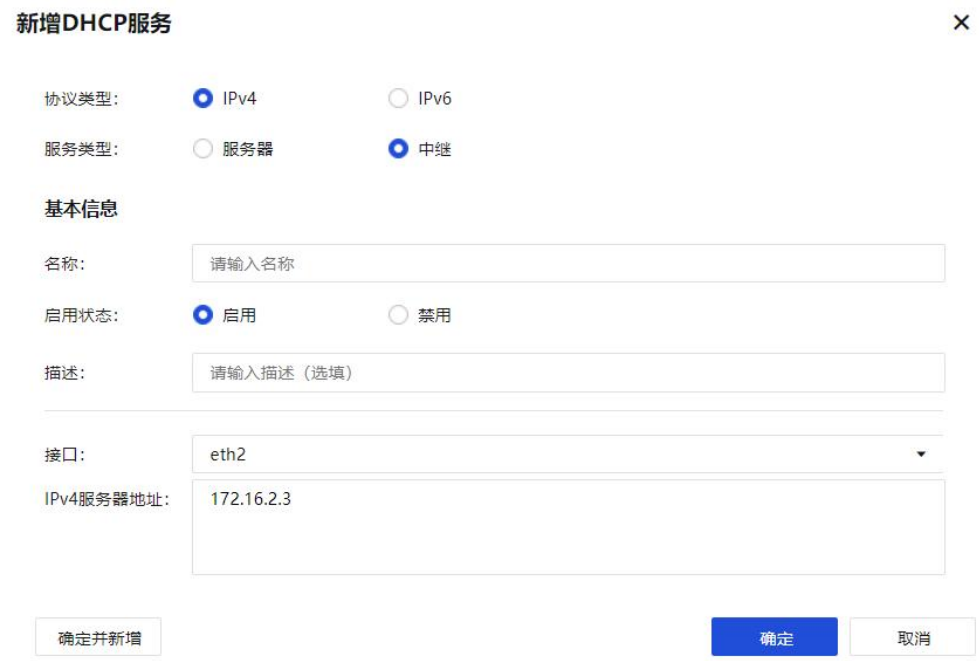
步骤2.（可选）设置租期，即DHCP下发的租期，如下图所示。

步骤3.设置绑定地址，点击<新增>，设置绑定地址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。

步骤4.查看DHCP的运行状态以及DHCP的分配状态。

8.6.2. 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，选择协议类型和中继，如下图所示。



接口：选择哪个接口接收DHCP客户端的请求数据包。

IPv4服务器地址：配置DHCP服务器的地址。

8.7. ARP

ARP全称为地址解析协议。ARP协议是任何以太网设备都必须支持的协议，实现三层IP地址与二层MAC地址之间的动态映射。

ARP（Address Resolution Protocol）用于将IP地址解析为MAC地址。ARP表项可以分为动态和静态两种类型。另外ARP还有扩展应用功能，包括代理ARP、ARP欺骗防御等。

8.7.1. 静态 ARP 表

静态ARP表用于在设备设置静态绑定IP/MAC条目，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。可以点击自动获取MAC地址来自动填写MAC。

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。

8.7.2. ARP 代理

代理ARP也叫路由式代理ARP。当主机上没有配置缺省网关地址（即不知道如何到达本网络的中介系统），它可以发送一个ARP请求（请求目的主机的MAC地址），启动代理ARP功能的设备收到这样的请求后，会使用自己的MAC地址作为该ARP请求的回应，使得处于不同物理网络但网络号相同的内部主机之间可以正常的相互通信。

勾选启用开启ARP代理功能，点击<新增>，创建ARP代理功能，如下图所示。

起始/结束IP：填写需要代理的IP地址。

网络接口：从该接口请求的ARP进行应答。

⚠ 注意：

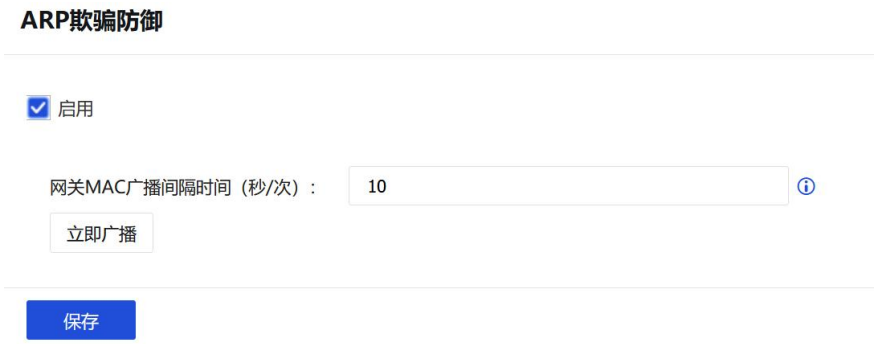
1、指定做 ARP 代理的接口必须是路由口。
2、配置的 IP 网段要与 AF 其他网段不冲突。
3、如果配置错误，会导致相应 IP 的 ARP 冲突，从而引起网络动荡。

8.7.3. 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。设备通过不接收有攻击特征的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。

勾选启用ARP欺骗防御，页面设置如下。



网关MAC广播间隔时间（秒/次）：设置设备广播MAC的间隔时间。

8.8. 高级网络

8.8.1. TCP MSS

TCP MSS（Maxitum 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。

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。

8.8.2. 光口 bypass 设置

AF支持光口bypass功能，需要配合光口bypass交换机一起使用，勾选使用外置光旁路交换机，则启用光口bypass。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。

点击<新增旁路光模块>：选择相应的光模块接口进行配置。

8.8.3. 多次穿越设置

多次穿越设置主要用于，当有数据包多次穿过同一台AF设备时，AF对流经的数据包进行设置，确保安全功能有效且不重复进行检测等。

点击<启用>后，正式启用多次穿越，再点击<新增>，新增一条记录。

数据包源IP：数据包的源IP地址。如一条数据流同时经过AF的eth1和eth2组成的“网桥1”以及eth3和eth4组成的“网桥2”，而当前的安全防护策略配置在“网桥2”的

内/外网区域上，那么此处设置经过“网桥1”数据包的源地址。

数据包目的IP：数据包的目的IP。如一条数据流同时经过AF的eth1和eth2组成的“网桥1”以及eth3和eth4组成的“网桥2”，而当前的安全防护策略配置在“网桥2”的内/外网区域上，那么此处设置经过“网桥1”数据包的目的地址。

数据包入接口：数据包的入接口。如一条数据流同时经过AF的eth1和eth2组成的“网桥1”以及eth3和eth4组成的“网桥2”，而当前的安全防护策略配置在“网桥2”的内/外网区域上，那么此处设置经过“网桥1”数据包的入接口。

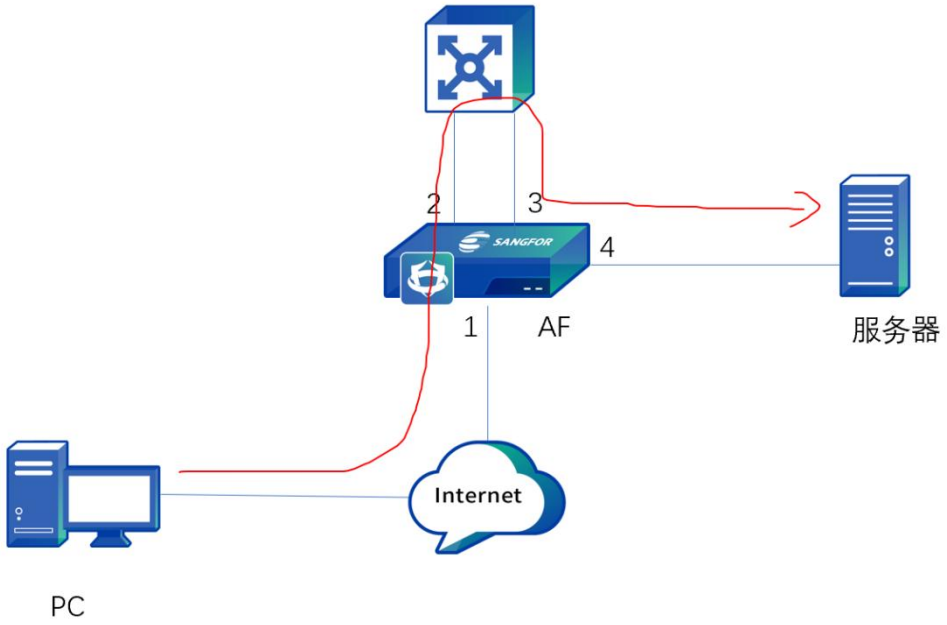
⚠ 注意：

1、配置多次穿越需要来回路径都放行；

2、多次穿越配置后则该流量直接类似 bypass。

案例配置

某公司的环境如下，AF部署在服务器前端，同时起到防护内外网的攻击。AF部署模式为虚拟网，12为一对虚拟线，34为一对虚拟线。当互联网终端PC（100.100.100.1）访问服务器（172.16.10.1）时， 发现无法正常打开页面。经排查为二次穿越防护墙，导致会话异常。因此，需要开启多次穿越来规避该问题。



步骤1. 勾选启用多次穿越按钮，并点击<新增>，从而创建多次穿越。如下图所示。

步骤2. 来回都需要配置多次穿越，配置结果如下图。

步骤3. 互联网终端PC（100.100.100.1）再次访问服务器（172.16.10.1），能够正常打开页面。

8.9. SSL VPN

SSLVPN是解决远程用户访问公司敏感数据最简单最安全的解决技术，通过相对简易的方法实现信息远程连通，任何安装浏览器的设备都可以使用SSLVPN。SSL VPN功能需要通过序列号开启。

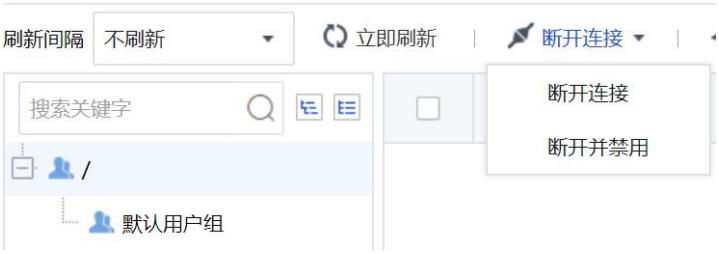
8.9.1. 在线用户

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，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。

8.9.2. 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。

选择单臂模式时，需要选择内网接口，页面如下。

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。

8.9.3. 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。

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。

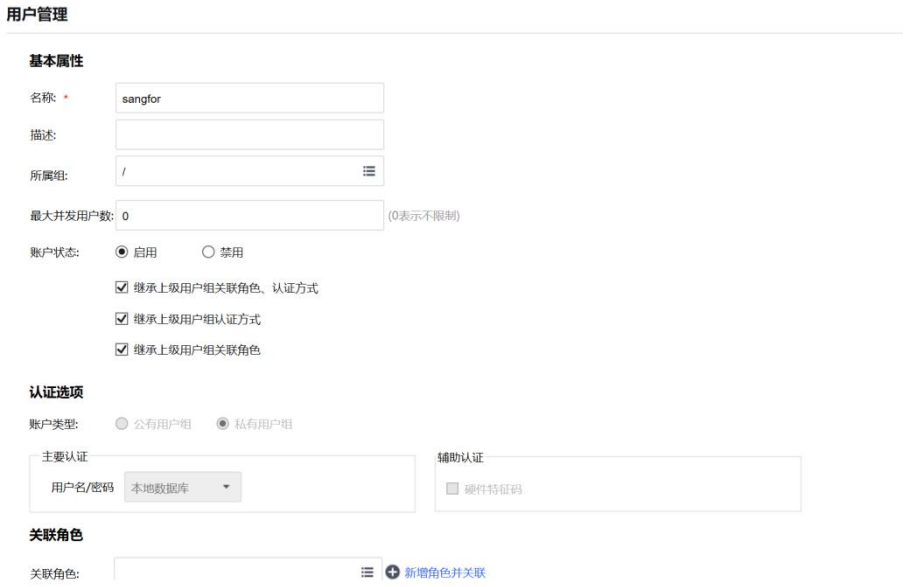
用户组结构树上方的搜索框中可输入目标用户组的关键字，点击放大镜图标进行搜索，搜索到的用户组在用户结构树中会被高亮显示。

表24 用户管理功能说明表

参数	说明
编辑	选中编辑可以直接编辑根目录的基本属性、认证选项和关联角色等，用户的组的修改，如果继承上级用户组关联角色和认证方式。修改根组的时候也会跟着一起修改。
删除	当不需要的组或用户删除，选择需要删除的[组/用户]，勾选<删除>即可。当[认证策略]关联了需要删除的用户组，则此用户组将无法直接删除，需要先把认证策略删掉，才能将该组删除。
导入/导出	可以将组/用户的数据批量导入或者导出设备。 以通过 CSV 的文件导入用户，通过一个 CSV 的文件导入用户，导入用户时可以同时导入显示名、所属组、密码、允许登录的 IP 范围、是否公用账号、自定义属性等。如果导入用户时指定的所属组不存在，也会自动建立用户组。 直接勾选需要导出的组和用户。当某个用户组没有用户时，此用户组不支持单独导出。
移动	可以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并且使用目标组的上网策略。对于普通管理员而言，可能只有管理部分组的权限，在移动组/用户时，无法移动到没有权限管理的用户组。
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。
高级搜索	可以设置查询条件和范围：IP 和 MAC 进行筛选，其他选项可以自己定义来查询。
查看资源	在用户管理选择某一个用户或用户组，点击 » 按钮选择<查看资源>，则会显示所关联的资源

8.9.3.1. 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。如下图所示。



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：可选择启用和禁用用户组。

- 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。
- 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。
- 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。

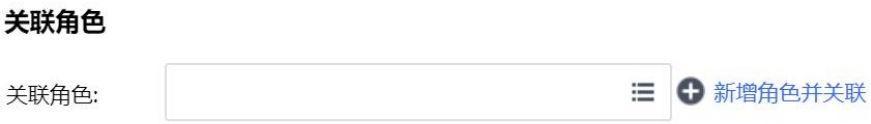
- 公有用户组：指该用户组中的所有用户账号可以供多人同时使用登录 SSL VPN。
- 私有用户组：指该用户组中的所有用户账号仅仅允许一个人使用登录 SSL VPN ，两个人使用时会导致先登录的用户断线。

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：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，具体设置可以参考角色授权章节。



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。

点击 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。

勾选相应的角色，点击<确定>，如下图所示。

再点击<确定>，如下图所示。

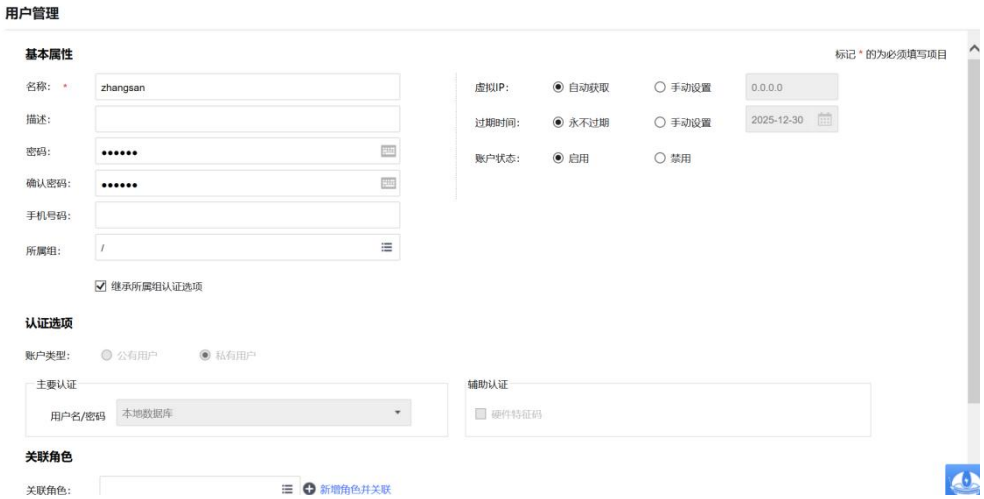
关联角色成功，该用户组关联了两个角色。

点击<保存>，可继续添加角色。

点击<保存>按钮，保存配置。

8.9.3.2. 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。



名称：即SSL VPN用户登录VPN时所使用的账号。

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登录账号的密码。

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。

虚拟IP：可设定该用户在分配L3VPN资源后获取IP地址的方式。

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>。

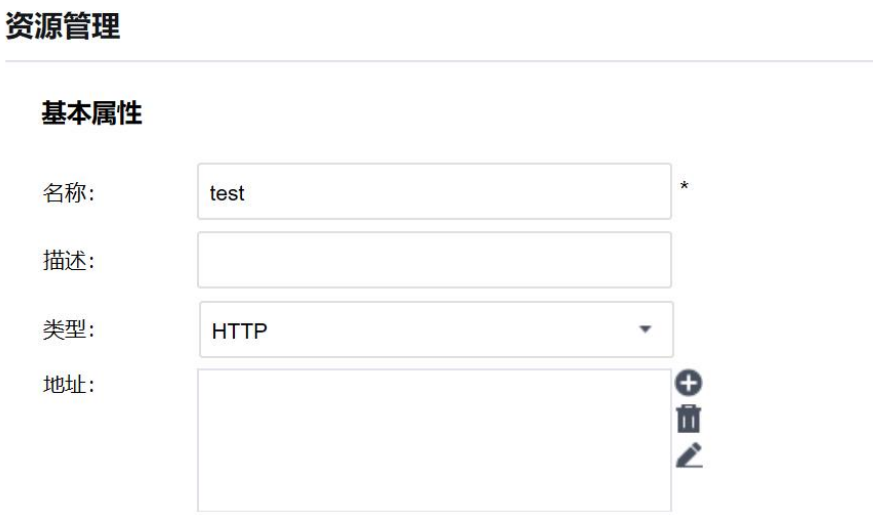
8.9.4. 资源管理

资源管理的主要作用是用户定义SSL VPN内网的可用资源。

8.9.4.1. TCP 应用

TCP应用主要用于定义、配置和管理各种基于TCP协议的SSL VPN内网资源，以适应基于TCP协议的应用程序访问SSL VPN内网资源和内网服务器。

在[资源管理]页面，点击<新增>按钮，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，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，如下图所示。

也可批量添加，选择[批量添加]，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：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”

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，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。

URL访问控制：用来设置允许用户只能访问特定的URL地址，只支持TCP应用的HTTP类型的应用。

⚠ 注意：

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，可能会拦挡 PC 安装插件，可先关闭防火墙或杀毒软件。

2．以“域名”形式填写资源地址时，必须在前面[网络设置/HOSTS]中设置“域名”或“主机名”对应的“IP 地址”，也可以通过[内网域名解析]中设置内网 DNS 服务器解析。

TCP 应用不支持文件共享类的资源。

配置案例

添加一个TCP应用资源服务器是192.168.1.10，使用TCP 80端口的HTTP服务。

步骤5.点击<新增>按钮，选择[TCP应用]，名称自定义为web，类型默认选择HTTP，如下图所示。

步骤6.再点击 ⊕ ，弹出[添加/编辑资源地址]对话框，填写服务器IP 192.168.1.10，端口80，如下图所示。

步骤7.点击<保存>，完成TCP应用资源的添加，如下图所示。

8.9.4.2. 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<新增>按钮， 选择[L3VPN]，弹出[编辑L3VPN资源]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。

如果类型选择为[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，如下图所示。

也可批量添加，选择[批量添加]，如下图所示。

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。

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”

如果不勾选[允许用户可见]选项，则登录SSL VPN后，在“L3VPN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。

URL访问控制：用来设置允许用户只能访问特定的URL地址，只支持L3VPN应用的HTTP类型的应用。

⚠ 注意：

首次使用 L3VPN 时计算机会自动安装虚拟网卡控件，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，可能会拦挡 PC 安装插件，可先关闭防火墙或杀毒软件。

配置案例

添加一个L3VPN资源服务器是192.168.1.10，开放PING服务。

步骤8.点击<新增>按钮，选择[TCP应用]，名称自定义为ping，类型默认选择Other，协议选择ICMP，如下图所示。

步骤9.再点击 ，弹出[添加/编辑资源地址]对话框，填写服务器IP 192.168.1.10，端口80，如下图所示。

步骤10.点击<保存>，完成TCP应用资源的添加，如下图所示。

8.9.4.3. 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<新增>按钮，选择[资源组]，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。

8.9.4.4. 其它操作

其它操作包括导出资源、导入资源、资源排序和资源组排序。 如下图所示。

导出资源

点击<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<确定>按钮，将资源保存在默认生成的rclist.csv文件中。

导入资源

点击<导入资源>将编辑好的资源通过文件导入到[资源管理]中。

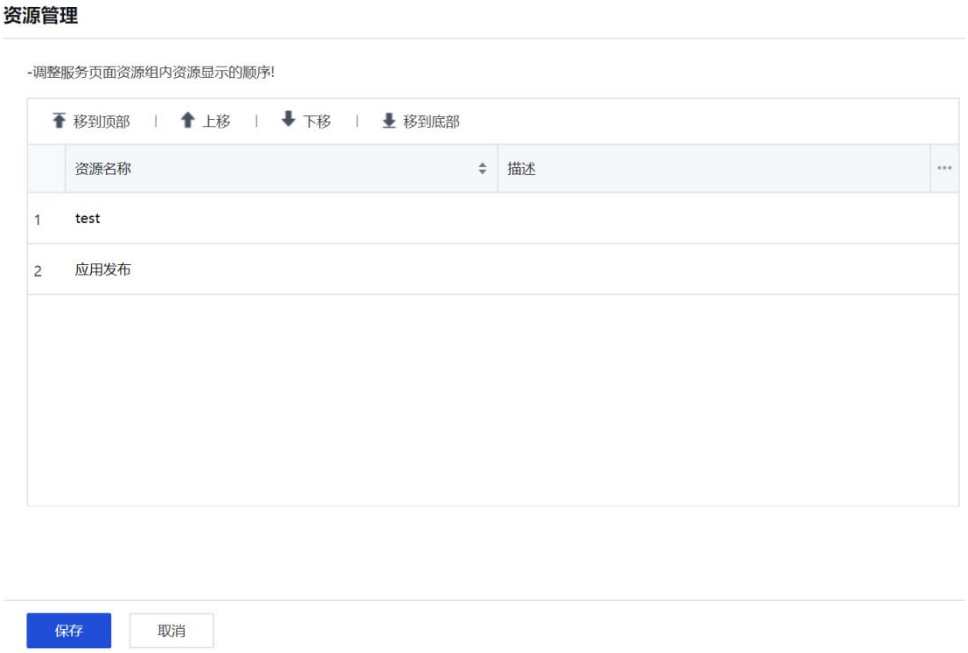
可以通过下载示例文件来编辑资源，将编辑完成的.csv格式的文件导入设备。

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。

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。如下图所示。



资源组排序

[资源组排序]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，通过资源组排序来调整接入SSL VPN后显示的资源组顺序。如下图所示。

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。

⚠ 注意：

移动的时候，只能移动资源，不能移动资源组。

8.9.5. 角色授权

8.9.5.1. 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。

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。

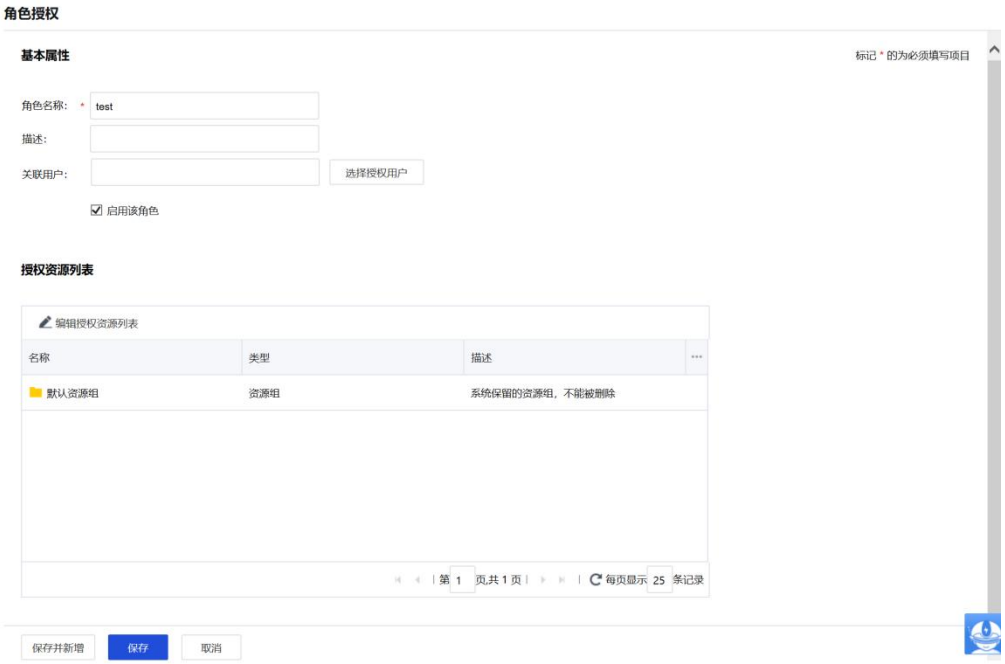
授权给：显示关联了该角色的用户。

点击<编辑>，用来编辑勾选的角色。

点击<删除>，用来删除勾选的角色。

点击选择，可以选择当前页或选择所有页。

在角色管理页面，点击<新增>，选择[新增角色]，弹出[新增角色]编辑页面，如下图。

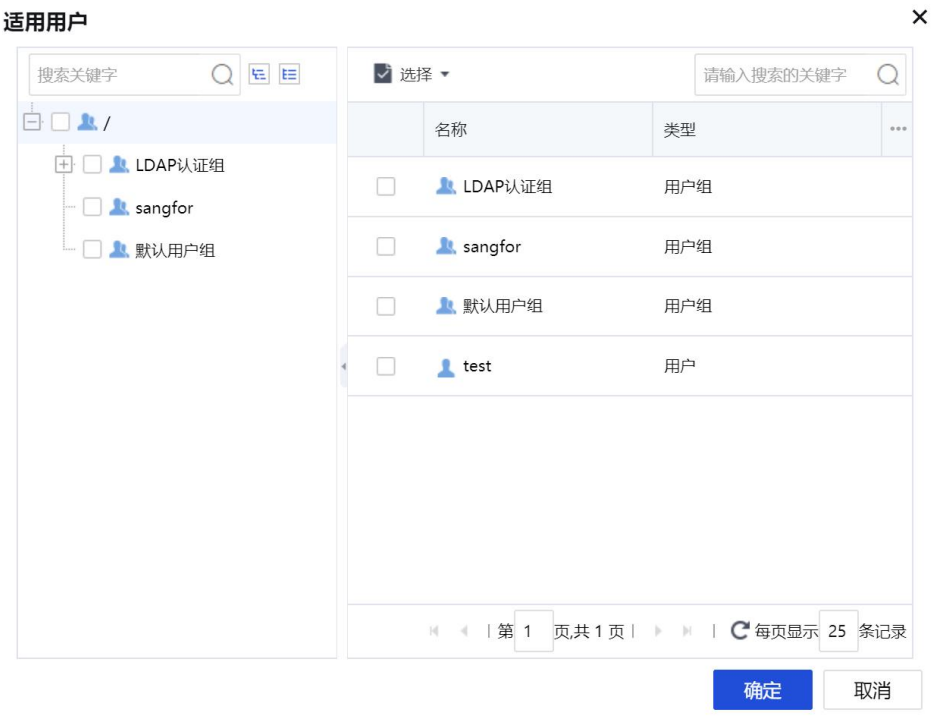


角色名称：该条角色的名称，自定义即可。

描述：可随意填写便于理解和记忆的描述语言。

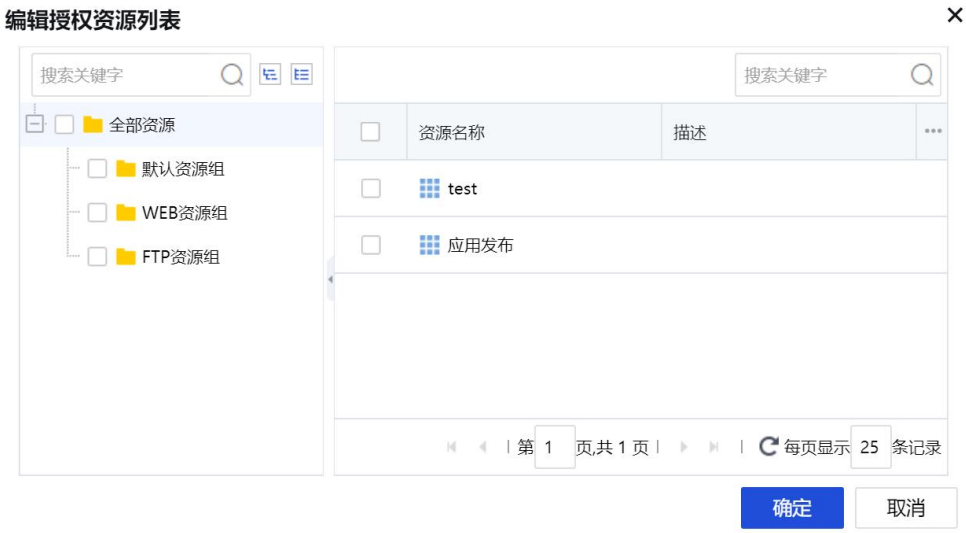
关联用户：选择关联该条角色的用户或者用户组。

点击<选择授权用户>按钮，下面的列表会列出[用户管理]中所定义好的用户/组，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，弹出授权资源列表页面，选择相应的资源。界面如下图所示。



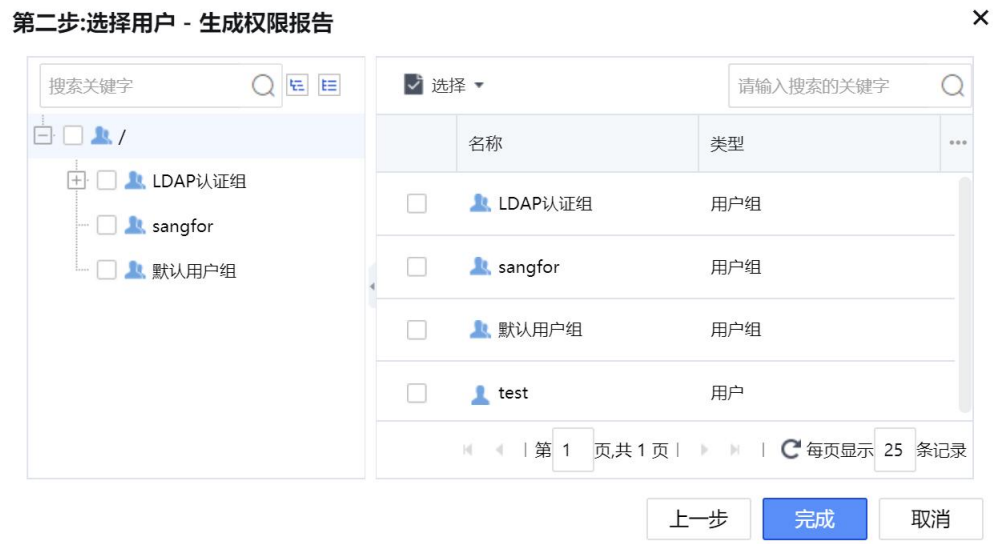
选择<资源>，然后点击<确定>按钮。确定保存。

最后点击<保存>，即完成一条角色配置。

8.9.5.2. 生成权限报告

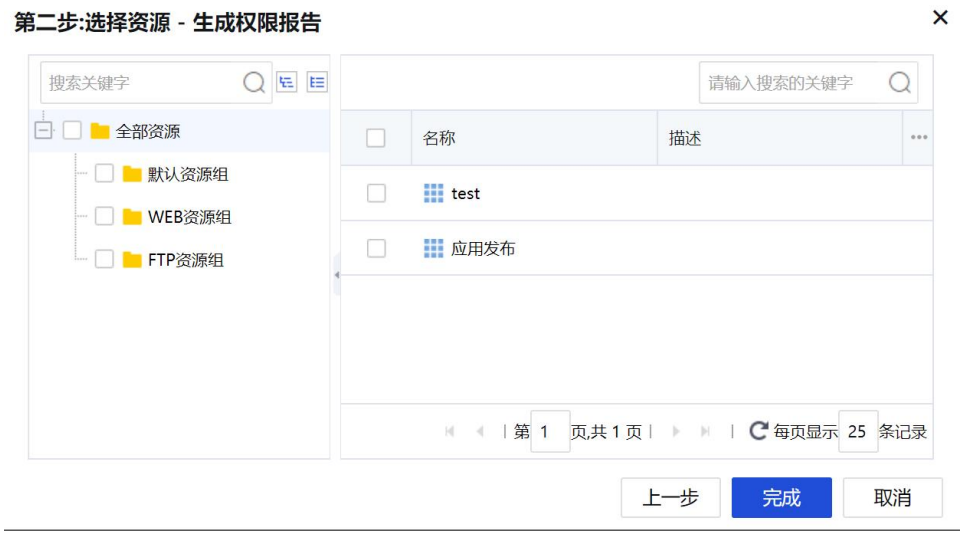
[生成权限报告]用来生成显示用户可访问资源的报表。如下图所示。

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。



选择用户，点击<完成>，生成“.csv”格式的文件。

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。

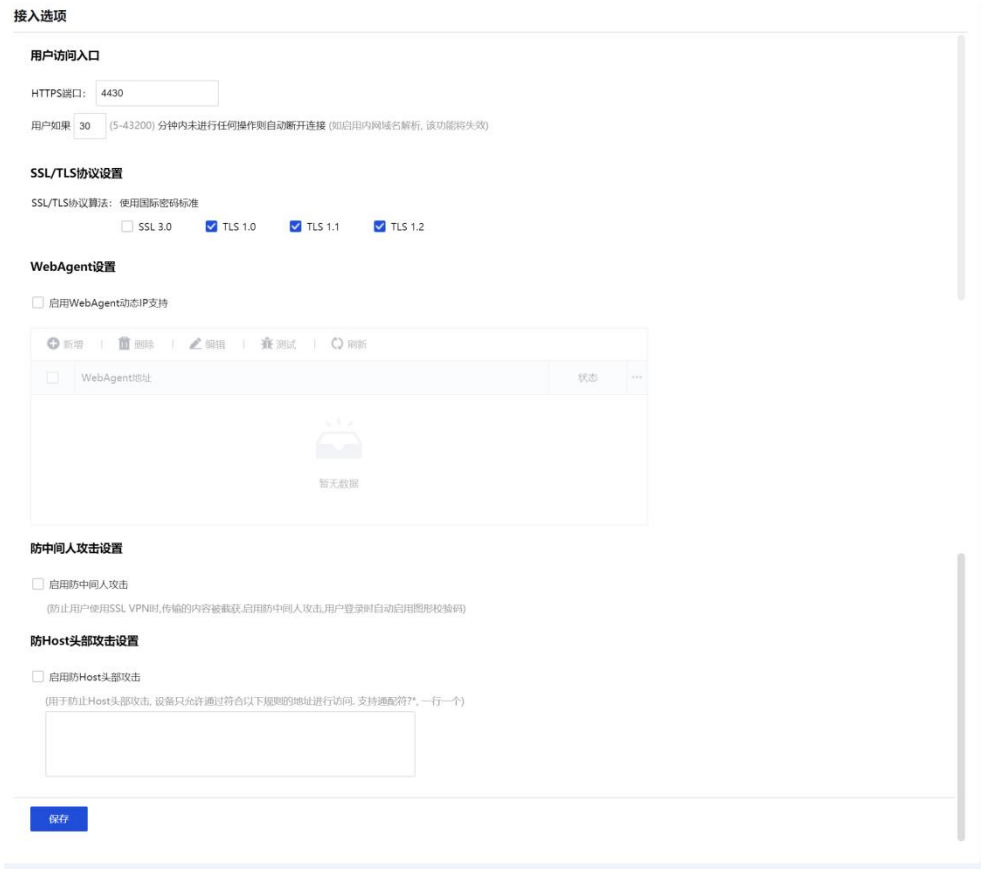


选择资源，点击<完成>，生成“.csv”格式的文件。

8.9.6. 接入选项

[接入选项]用于设置SSL设备的登陆端口，SSL/TLS协议设置，Web Agent设置以及是否启用防中间人攻击等。

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 4430端口。访问SSL登录页面时，需要在主机地址后面添加端口来登录。

SSL\TLS协议设置：该选项设置SSL VPN用于数据加密的加密协议算法标准，包括国际商用密码标准(RSA)和中国国家密码标准(SM2)，默认为国际商用密码标准。

Web Agent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Web Agent动态寻址。

勾选[启用Web Agent动态IP支持]，即启用Web Agent动态寻址功能。可以在这里新增/删除或修改Web Agent。

Web gent地址：用于显示Web Agent地址。

状态：显示当前Web Agent的状态。

点击<新增>即可新增一条Web Agent。点击后如下图。

在弹出的输入框中输入申请到的Web Agent地址，点击<确定>。如下图所示。

勾选相应的web Agent地址，点击<测试>，弹出如下框的提示，证明填写正确。这里需要使用IE浏览器才能测试。

勾选相应的Web Agent地址，点击删除或编辑可以进行<删除>或<编辑>Web Agent地址。

点击刷新，可以刷新Web Agent的当前状态。

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Web Agent寻址。

启用防中间人攻击：用来防止通信的数据被非法用户篡改和窃取。勾选后，用户登录时强制启用图形校验码，并且会强制安装控件。配置界面如下图所示。

防Host头部攻击设置：开启之后用户防止Host头部攻击，设备只允许通过符合规则的地址进行访问。如下图所示。

8.9.7. 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：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。

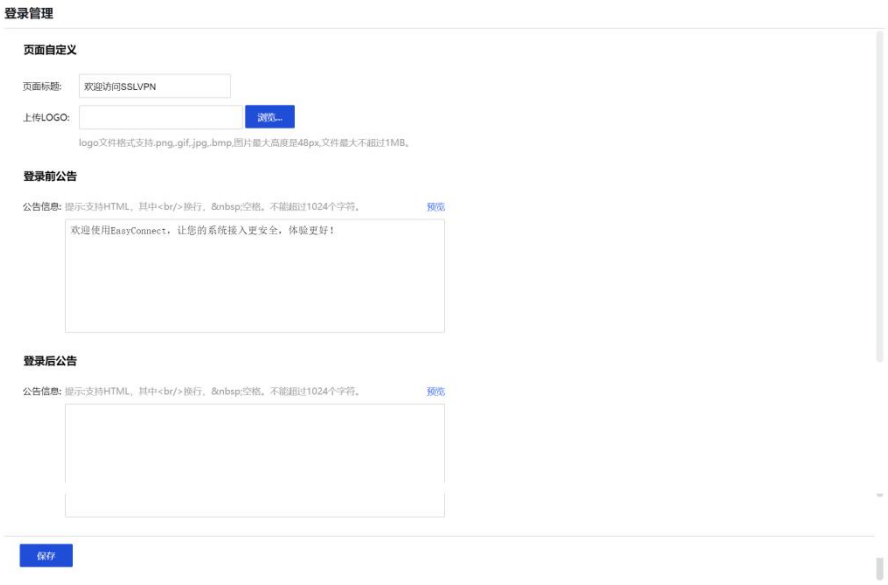
点击<新增>按钮，出现[虚拟IP池]对话框。

⚠ 注意：

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。

8.9.8. 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。

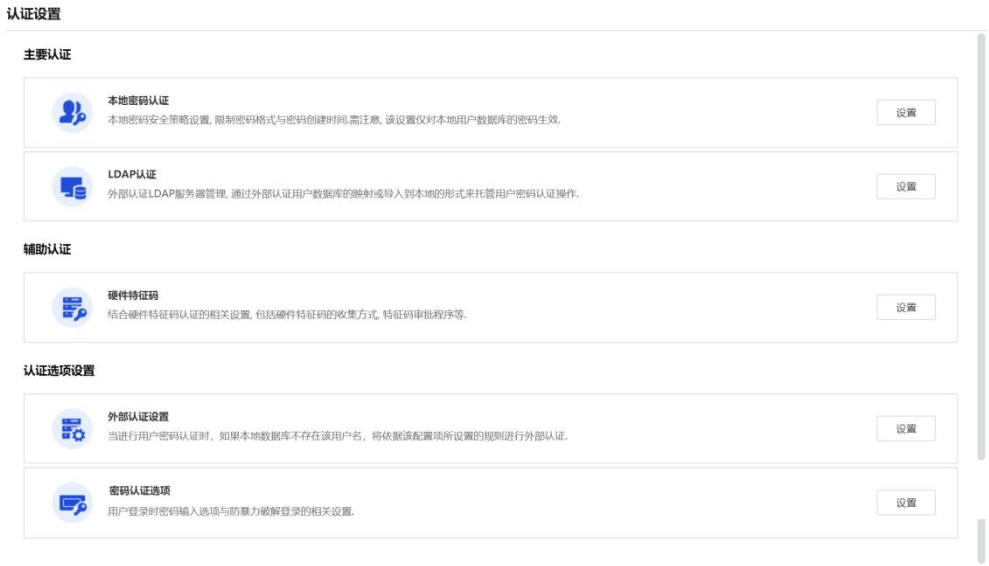
上传LOGO：用来自定义LOGO图片

登录前公告：用来自定义浏览器打开登录页面的提示信息，支持HTML，其中
换行， 空格，不能超过1024个字符。点击预览可以查看编写后的效果。

登录后公告：用来自定义登录SSL VPN后的提示信息，支持HTML，其中
换行，空格，不能超过1024个字符。点击预览可以查看编写后的效果。

8.9.9. 认证设置

[认证设置]包含主要认证、辅助认证、认证选项设置。



8.9.9.1. 主要认证

主要认证方式包括本地密码认证和LDAP认证。

本地密码认证

点击本地密码认证后面的<设置>，界面如下。

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。

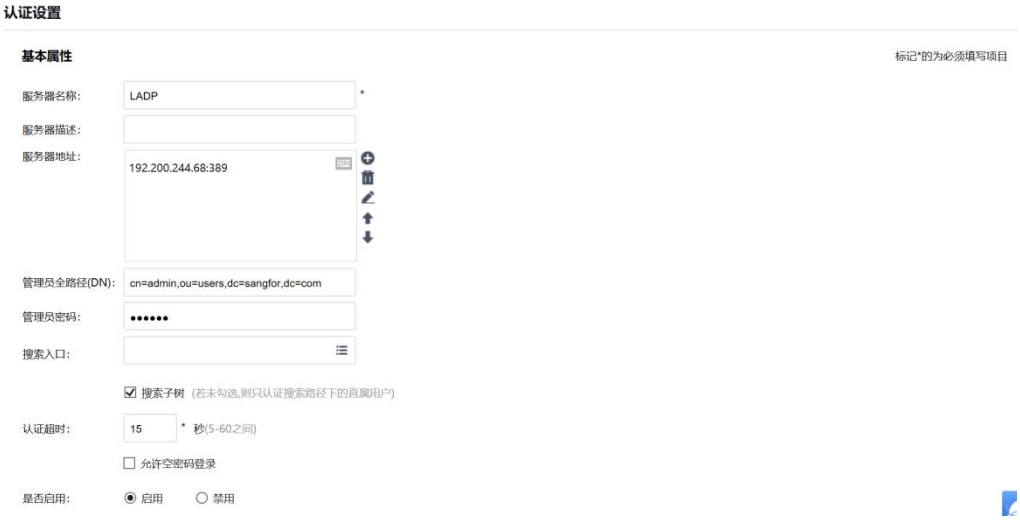
⚠ 注意：

上述策略只对本地密码认证的用户有效。

LDAP认证

点击LDAP认证后面的<设置>，弹出[认证设置]页面。如下图所示。

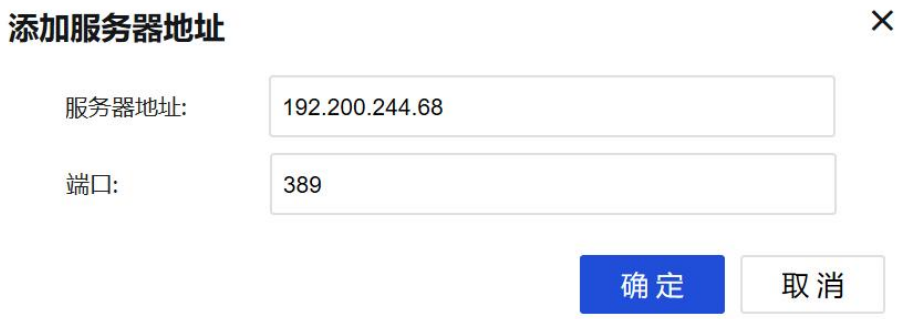
点击<新增>可新增一个LDAP服务器，弹出LDAP外部认证服务器的参数设置界面。配置如下图。



服务器名称和服务器描述：可随便填写便于记忆的文字。

服务器地址：用于设置LDAP服务器的IP地址和所使用的端口，此处可设置多个服务器地址和端口，他们之间是主备关系，第一个服务器为主服务器，其余都为备服务器，当第一个服务器连不上，才尝试连接第二个服务器认证，以此类推。

点击图标 ，出现服务器IP地址和端口的设置页面如下。



管理员全路径（DN）和管理员密码填写LDAP服务器内一个有效的账号和密码，用于读取LDAP结构。所填写的账号一般要以域中DN的形式填写。该账号在LDAP服务器必须有读取用户路径的权限。

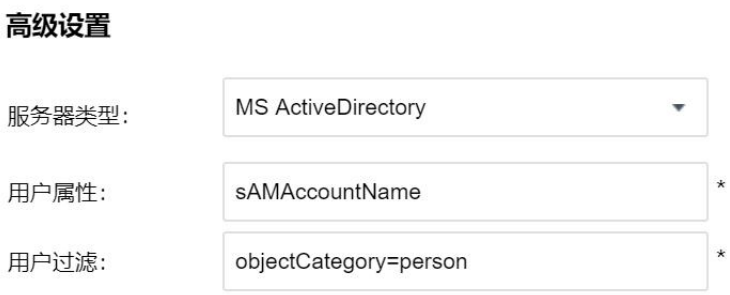
搜索入口：用于选择需要用于认证的LDAP用户账号所在路径。

在所选择用户账号所在路径时，在包含（嵌套）子路径的情况下，若勾选[搜索子树]，该路径下的所有子路径的用户账号都包含进来；若不勾选[搜索子树]，则只包含该路径下的本级用户账号。

认证超时：当连接到服务器但服务器超过这里所设置的时间仍然没有回应，就认为客户端认证失败。

是否启用：用于设置是否启用该LDAP外部认证服务器。

高级设置配置如下图。



高级设置相关配置，请征询LDAP服务器管理员的意见才能进行修改。系统支持普通的LDAP协议和支持微软的MS Active Directory协议。对于MS-AD，用户是以属性sAMAccountName认证属性，以“objectCategory=person”作为过滤用户账号的条件；对于普通LDAP协议，用户是以属性uid为认证属性，以“objectclass=person”作为过滤用户账号的条件。用户也可以自定义其他属性来得到用户名和组名称。

其他属性包含：组映射和用户名密码加密方式。如下图所示。

组映射针对没有导入到本地的LDAP服务器的用户，用于设置将LDAP服务器中的OU和SSL VPN网关本地的用户组绑定起来，那么该OU中的用户登录SSL VPN之后就会拥有本地被绑定用户组的权限。

点击<添加>，出现组映射配置页面如下。

外部OU：填写需要映射的OU在域中的DN。

所属组：选择该OU所要映射的本地用户组。

包含子OU：用于设置是否包含所选OU的子OU。若勾选[包含子OU]，则该OU下的所有子OU的用户账号都包含进来；若不勾选[包含子OU]，则只包含该OU下的本级用户账号。

如果未设置映射，将其自动映射到目标：用于设置当某个OU没有映射到本地用户组的时候，这个OU里边的用户认证通过之后自动匹配为那个用户组的用户。

点击<删除>，可以删除所选的组映射规则。

点击<编辑>，可以编辑所选的组映射规则。

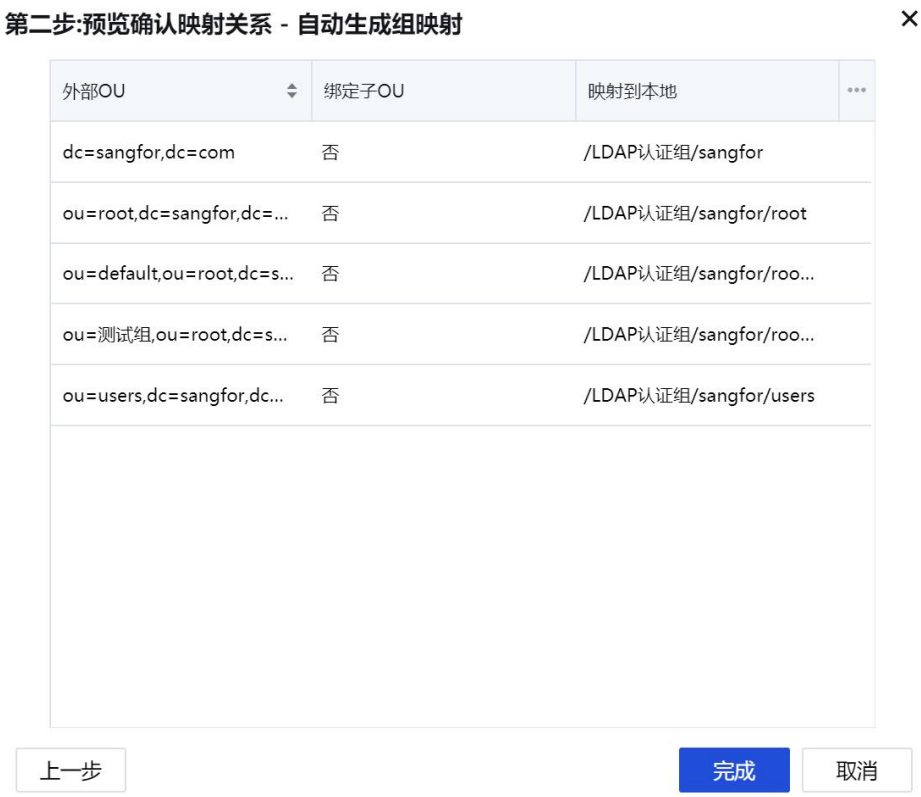
点击<自动生成组映射关系>，出现配置页面如下。

为每个选择的独立的OU生成组映射：用于设置将我们所勾选的所有OU都在本地生成一个用户组并自动映射到该组。并且导入之后组织结构不会变化。

仅对选择的最顶层的OU生成组映射：用于设置只将我们勾选的最上级OU在本地生成一个用户组，该OU及其下级OU都映射到该组。

选择自动映射到本地的起始位置：用于设置最上级OU映射到的本地用户组。

点击<下一步>，出现预览映射关系页面如下图。



点击<完成>，则在[用户管理]中生成用户组并一一映射，如下图所示。

用户名密码加密方式用于将用户的密码将通过加密处理，再转发到LDAP服务器上进行认证。配置页面如下图所示。

启用加密：开启用户密码加密功能。

LDAP加密方式：可选择MD5和SHA1这两种加密方式。

加密字长：可选择32位或者16位。

加密字母大小写：可选择将密码转换成小写或者大写。

8.9.9.2. 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。

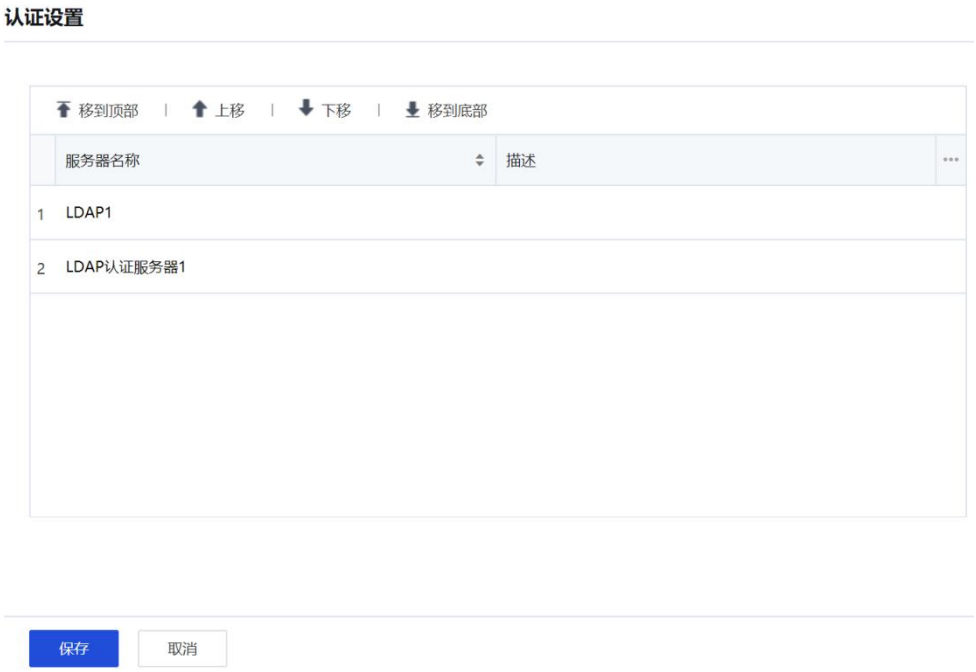
8.9.9.3. 认证选项设置

认证选项设置包含外部认证设置和密码认证选项。如下图所示。

外部认证设置

[外部认证设置]用于设置用户通过外部服务器中的用户名密码认证时，到各个服务器中认证的优先级。

点击<设置>，弹出[外部认证设置]页面，如下图所示。



[外部认证设置]用于对设置好的外部认证服务器进行排序，当创建好外部认证服务器后，必须要将其添加进来，若有多台外部认证服务器，可以选中某台服务器，点击<移到顶部>、<上移>、<下移>、<移到底部>，可对服务器进行相应的排序。

点击<保存>，完成并保存配置。

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]，如下图所示。

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。

点击密码输入框后的小键盘图标，页面如下。

[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，则启用图形校验码或者锁定该IP一段时间。配置如下图所示。

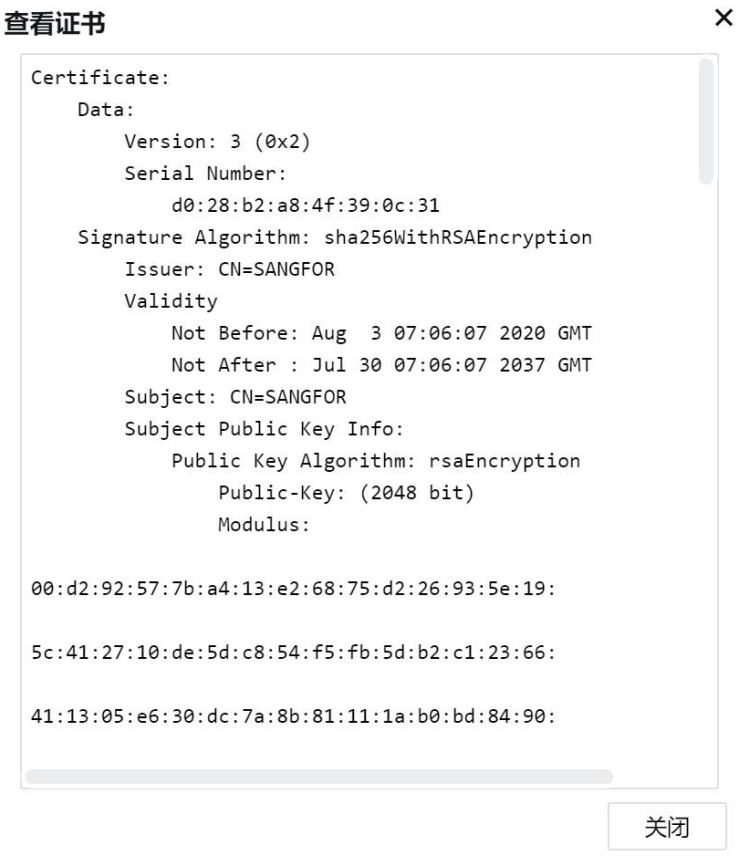
图形验证码选项设置中，输入0表示强制启用，即默认启用图形验证码；输入小于3时，非Windows客户端仍然以3次为标准。

8.9.10. 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<创建证书请求>，即新生成一个证书请求。配置界面如下图所示。

8.9.11. 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。

[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。

[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。

8.9.12. 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。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。

点击<新增>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。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。

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[全部选中]或者[取消选择]。

⚠ 注意：

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。

8.10. Sangfor/IPSecVPN

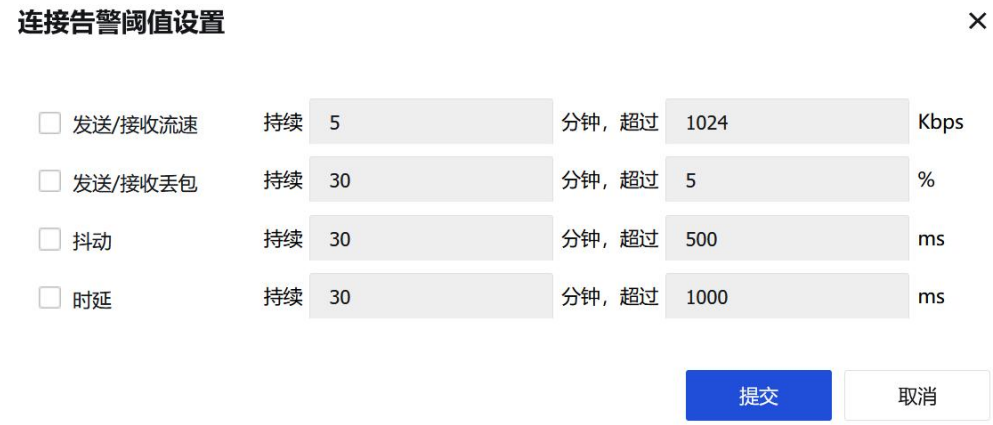
Sangfor/IPSecVPN功能用于和深信服设备或第三方设备建立IPSecVPN连接，在公网上为两个私有网络提供安全通信通道,通过加密通道保证连接的安全。

8.10.1. VPN 运行状态

[VPN运行状态]可以查看当前VPN连接和网络流量信息。如下图。

通过界面可以快速打查看当前VPN对接的设备、对接的IP、VPN接口流量等。

点击<连接告警阈值设置>，可以设备VPN的告警信息，如下图所示。



根据实际情况可以设置发送/接收流速、发送/接收丢包、抖动和时延的告警阈值，从而快速的发现IPsec VPN是否存在异常情况。

说明：

VPN 运行状态，会同时展示当前 IPSec VPN 和 SangforVPN 隧道的连接状态，但显示的隧道连接信息有差异，比如：IPSec VPN 无法看到隧道发送/接受丢包率、时延、抖动、传输类型等参数。

8.10.2. VPN 配置向导

[VPN配置向导]页面提供了选择Sangfor VPN和标准IPSec VPN的配置向导功能，如下图所示。

8.10.2.1. Sangfor VPN 协议

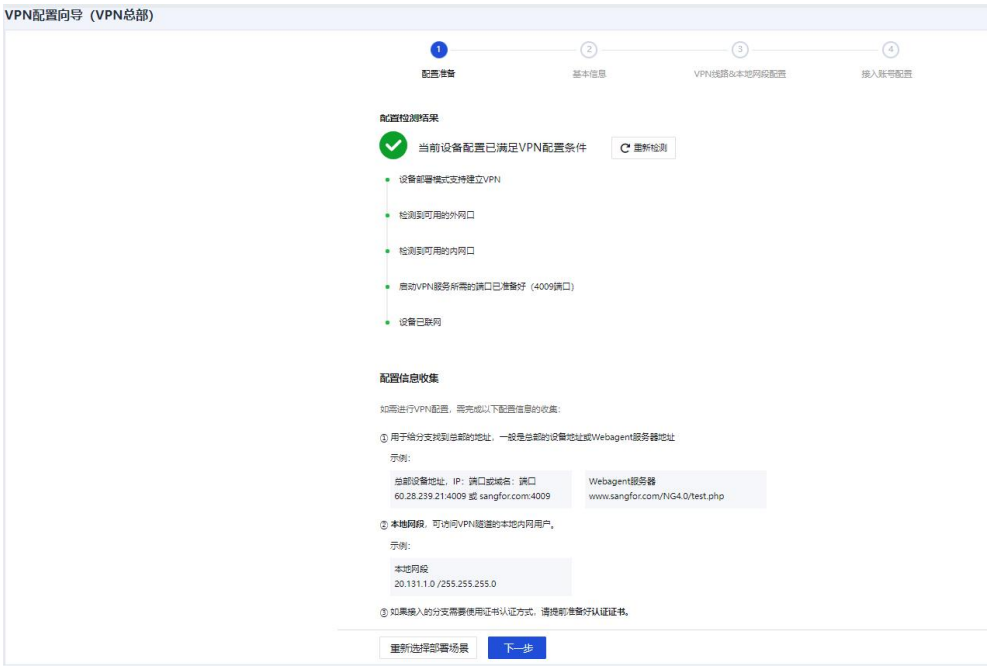
点击<Sangfor VPN协议>，选择当前设备的部署场景：VPN总部、VPN分支。以总部为例，点击<VPN总部>，会自动跳转下一步。

1. 配置准备

配置检测结果：检测当前设备部署模式、可用外网口、可用内网口、VPN 服务端口以及设备联网状态。如果状态发生改变，可点击右侧[重新检测]刷新检测结果。

配置信息收集：显示当前设备配置 VPN 需要的信息，如：总部接入地址、本地网段、采用证书认证的证书等。

确认无误后，点击<下一步>。

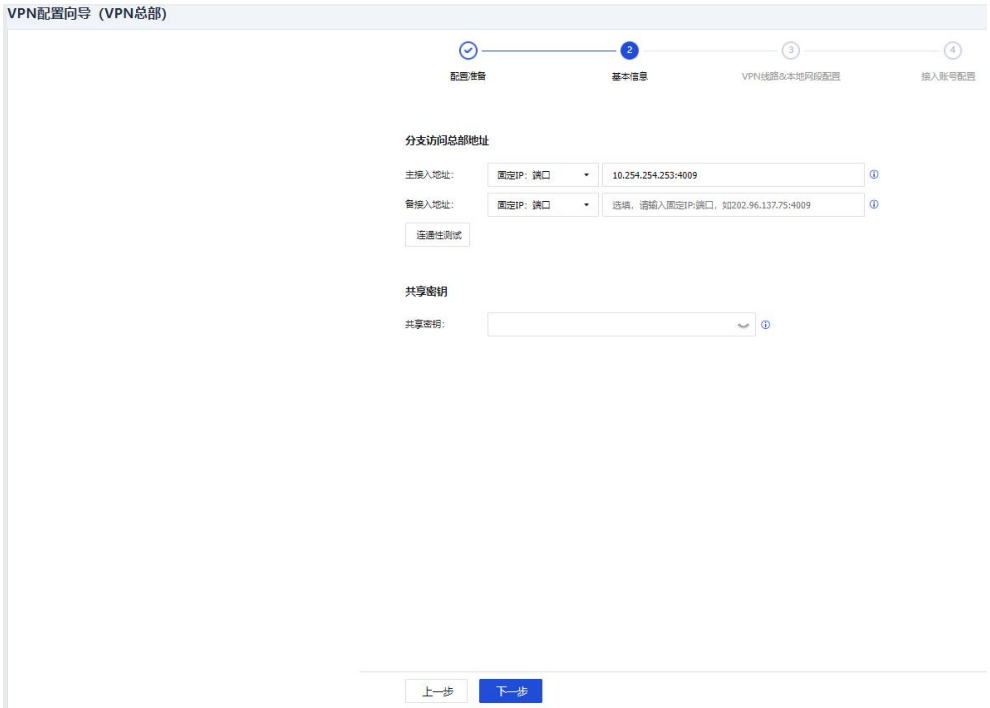


2. 基本信息

分支访问总部地址：填写当前设备作为 VPN 总部提供的 VPN 接入地址，格式为：IP:端口。如果有多个地址，请用#分隔，例如：202.102.2.35#60.25.5.36:4009。

共享密钥：可选配置，设置分支接入总部 VPN 的认证密码，如配置则分支必须输入相同密码才能正常建立 VPN。

确认无误后，点击<下一步>。

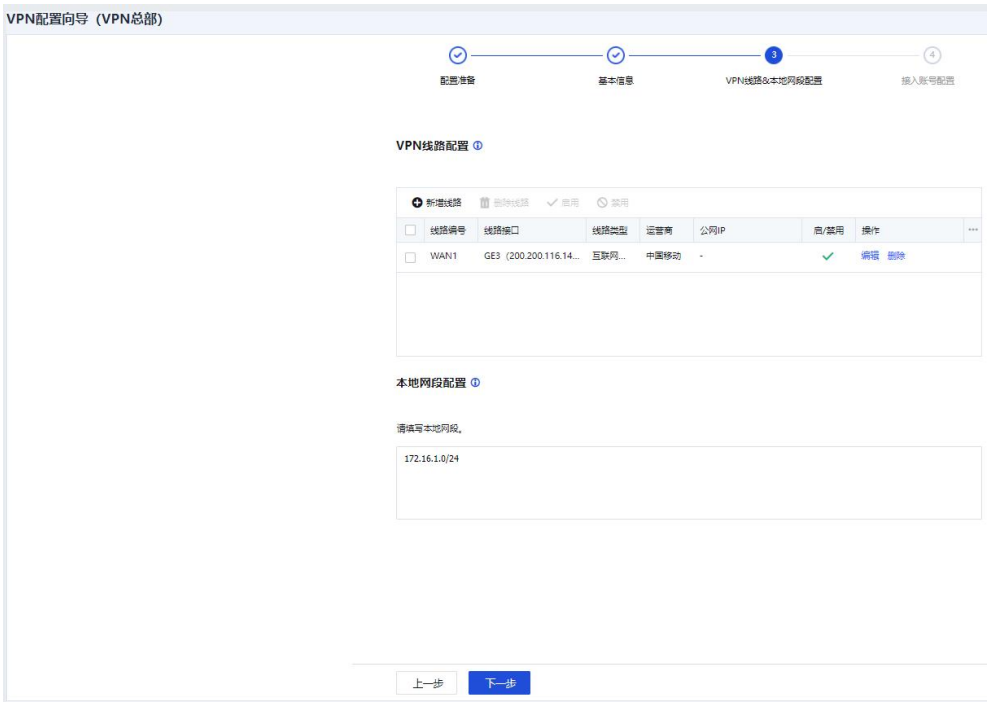


3. VPN线路&本地网段配置

VPN 线路配置：新增用于建立 Sangfor VPN 的 WAN 线路，同时提供[删除线路]、[启用/禁用]线路等功能。

本地网段配置：填写需要通过 Sangfor VPN 访问对端设备内网的本端内网网段。

确认无误后，点击<下一步>。



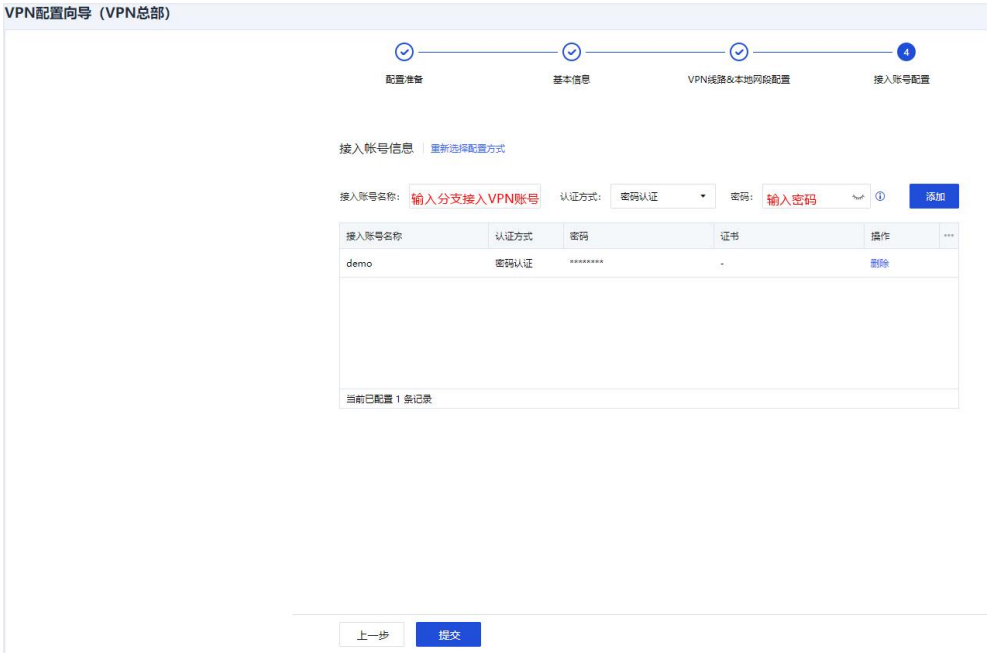
4. 接入账号配置

提供以下两种账号配置方式：

导入配置信息文件：以文件导入形式配置分支设备接入的 VPN 账号密码，支持的文件格式 CSV、TXT。

直接填写配置信息：手动填写分支接入的账号配置信息，此处以手动填写为例，点击<直接填写配置信息>，页面会自动跳转下一步。

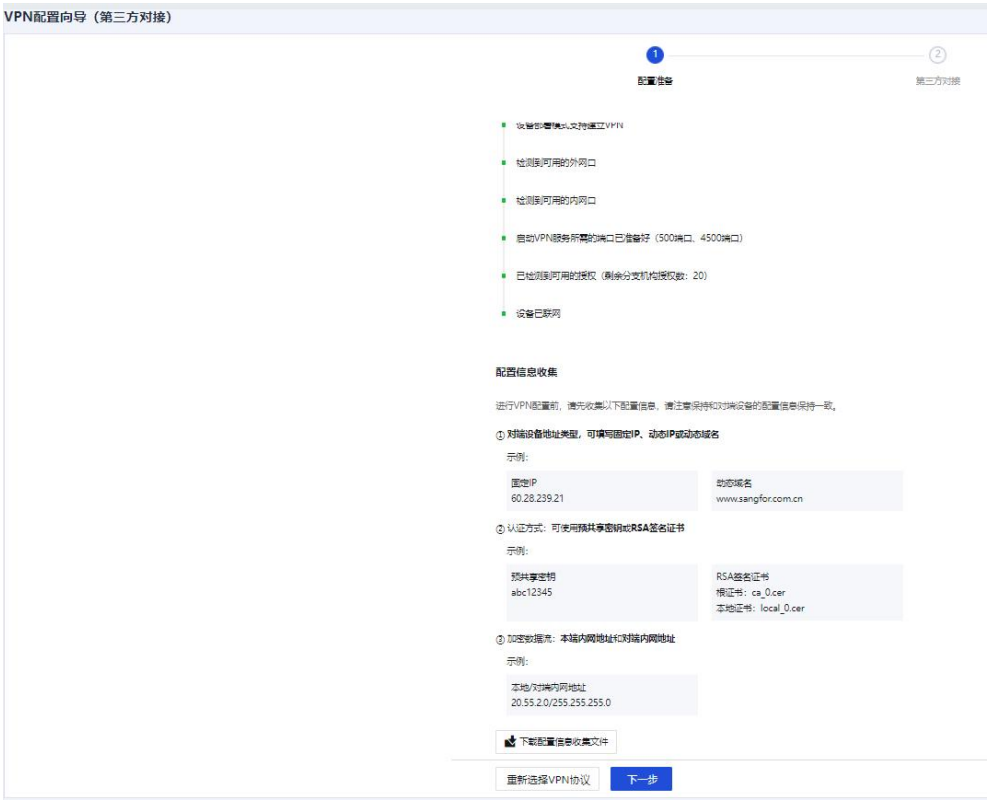
配置分支设备VPN接入的账号名称和认证方式，如果选择密码认证，则需要输入密码。输入完成后，点击<添加>，如下图所示。



5. 最后点击<提交>，Sangfor VPN向导方式配置完成，如下图所示。

8.10.2.2. 标准 IPSec VPN 协议

1. 点击<标准IPSec VPN协议>，自动跳转下一页面，如下图所示。



配置检测结果：检测当前设备部署模式、可用外网口、可用内网口、VPN 服务端口、授权数以及设备联网状态。如果状态发生改变，可点击右侧[重新检测]刷新检测结果。

配置信息收集：显示当前设备配置 VPN 需要的信息，如：对端设备地址和类型、认证方式、需要加密的数据流内网网段等。

下载配置信息收集文件：支持下载配置信息搜集文件模板，点击<下载配置信息收集文件>，下载后的文件格式如下：

需要获取的信息	说明	示例
对端设备地址类型	可填写固定IP、动态域名或动态IP	固定ip:60.28.239.21、动态域名:www.sangfor.com.cn
认证方式	可使用 预共享密钥或RSA签名证书	预共享密钥:123456、RSA签名证书：根证书：ca_0.cer 本地证书：local_0.cer
加密数据流	本端内网地址和对端内网地址	本地/对端内网地址:1.1.1.1/255.255.255.255
阶段二安全提议	协议、加密算法、认证算法以及密钥完美向前保密(pfs)	协议:ESP、加密算法:AES、认证算法:SHA1、密钥完美向前保密:None

确认无误后，点击<下一步>。

2. 第三方对接

设备名称：配置本端 IPSec 设备名称，IPSec 协商不校验此参数，只具有本地意义，自行设置即可。

描述：配置设备的描述信息，可选配置。

启用状态：对当前设备 VPN 启用或者禁用。

[基本配置]各配置项说明：

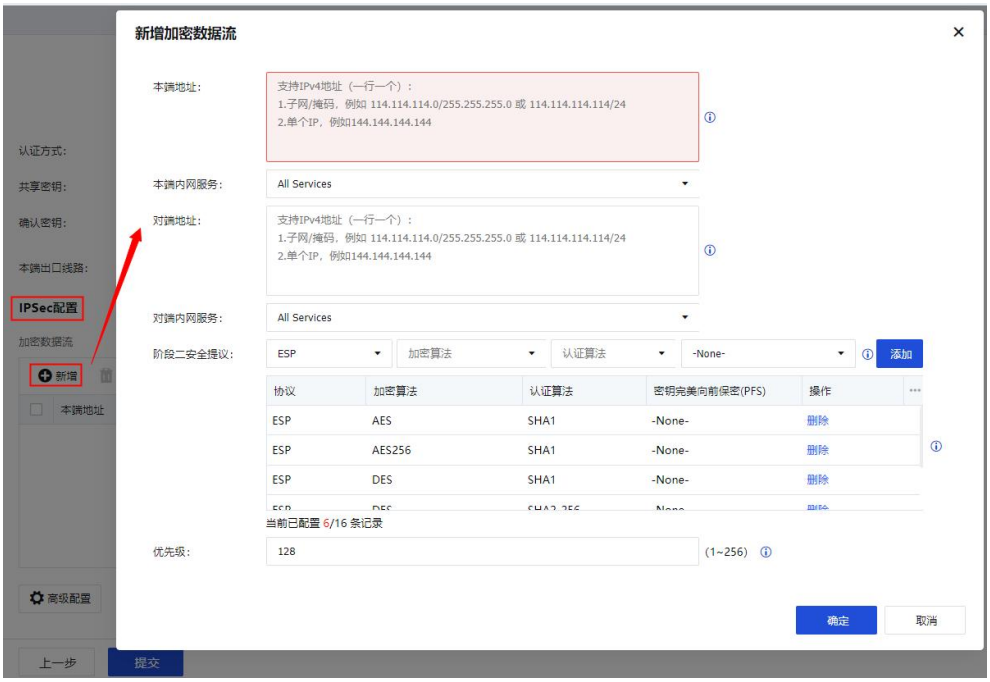
对端设备地址类型：包括固定 IP、动态 IP、动态域名三种，请根据实际情况选择：选择固定 IP，需要填写上对端的 IP 地址；选择动态域名，就填写上对端外网绑定的域名。

认证方式：包括预共享密钥、RSA 签名证书、商密证书三种，按需选择。

共享密钥与确认密钥：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。

本端出口线路：根据实际线路情况选择对应的出口线路。

3. IPSec 配置加密数据流



点击<新增>加密数据流，各配置项说明：

本端地址：设置标准 IPSec VPN 感兴趣流的源 IP 匹配规则，可填写单个 IP 或者 IP 网段。

本端内网服务：设置标准 IPSec VPN 感兴趣流的源内网服务匹配规则，可选择 ALL Services、ALL TCP Services、ALL UDP Services、ALL ICMP Services 这四种服务类型的某一种，请按需选择。

对端地址：设置标准 IPSec VPN 感兴趣流的目的 IP 匹配规则，可填写单个 IP 或者 IP 网段。

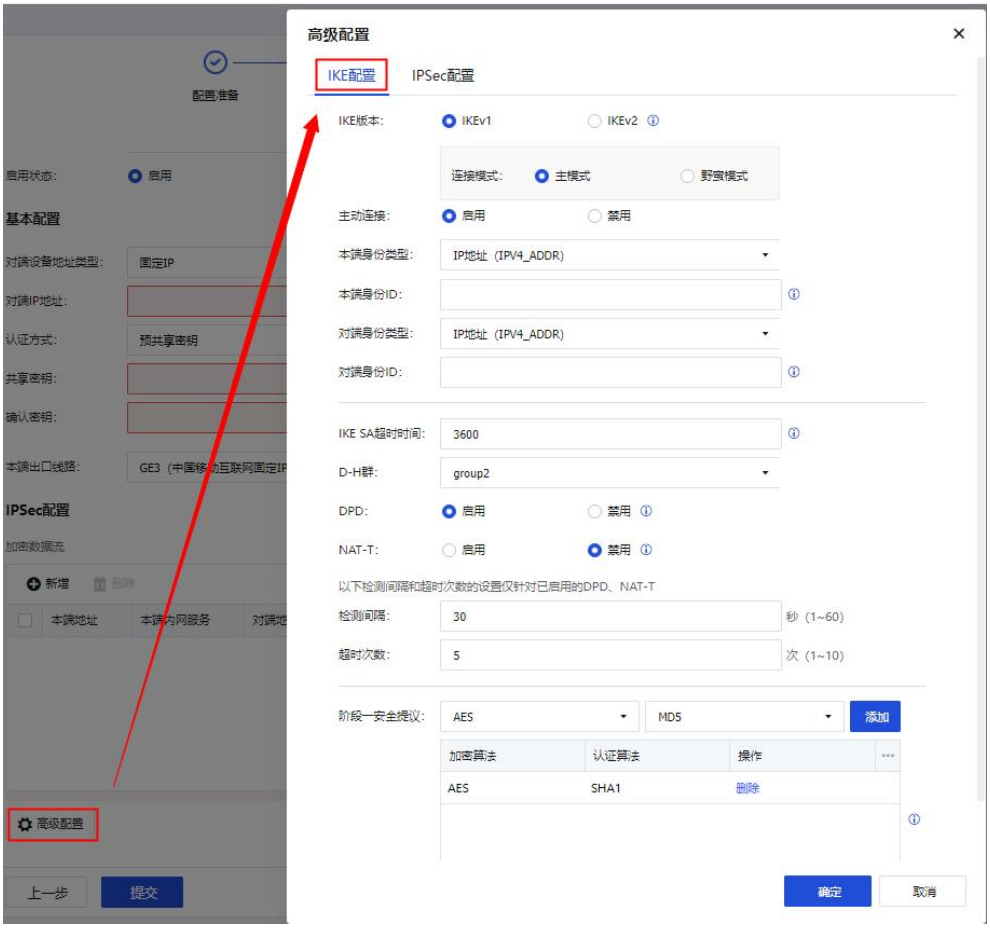
对端内网服务：设置标准 IPSec VPN 感兴趣流的目的内网服务匹配规则，可选择 ALL Services、ALL TCP Services、ALL UDP Services、ALL ICMP Services 这四种服务类型的某一种，请按需选择。

阶段二安全提议：选择阶段二协商时所使用的参数，包括所使用的协议、加密算法、认证算法、是否启用密钥完美向前保密（PFS）；其中数据包封装所使用的协议包括 AH、ESP 协议；数据加密所使用的加密算法包括 DES、3DES、AES、AES192、AES256、SANGFOR_DES、SM1、SM4；选择数据认证的认证算法包含 MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、SM3；PFS 所使用的 DH 组算法。

优先级：设置本端地址和对端地址优先级用于标识路由优先级。

配置完成，点击<确定>即可。

4. 点击<高级配置>，进入 IKE 和 IPSec 配置界面。



[IKE 配置]界面各配置项说明：

IKE 版本：选择 IKEv1 或者 IKEv2 版本，需要和对端保持一致。

连接模式：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定 IP 或者一方固定 IP 一方动态域名方式，并且不支持 NAT 穿透；野蛮模式适用于其中一方为拨号的情况，并且支持 NAT 穿透；根据客户实际需求场景选择主模式或者野蛮模式。

主动连接：用于控制设备是否主动发起建立 VPN 的连接。

本端身份类型：设置本端身份类型，保证对端可以识别到本端设备。该类型包括：IP 地址（IPV4_ADDR）、域名字符串（FQDN）、用户字符串（USER_FQDN）三种类型。

本端身份 ID：按照本端身份类型所选择的类型进行配置。

对端身份类型：设置对端身份类型，保证本端可以识别到对端设备。该类型包括：IP 地址（IPV4_ADDR）、域名字符串（FQDN）、用户字符串（USER_FQDN）三种类型。

对端身份 ID：按照本端身份类型所选择的类型进行配置。

IKE SA 超时时间：标准 IPSEC 协商的第一阶段存活时间，只支持按秒计时方式。

D-H 群：设置 Diffie-Hellman 密钥交换的群类型，包括 1、2、5、14、15、16、17、18 八种，请与对端设备配置保持一致。

DPD：IPSEC 使用 DPD（Dead Peer Detection）功能来检测对端 Peer 是否存活。

NAT-T：NAT-T 在野蛮模式下才会有，主要作用是避免有一方设备处于 NAT 之后导致标准 IPSEC 协商失败。NAT 穿透启用后会增加 UDP 头封装 ESP 报文，当 ESP 报文穿越 NAT 设备时，NAT 设备对该报文的外层 IP 头和增加的 UDP 报头进行地址和端口号转换，转换后的报文到达 IPSec 隧道对端时，与普通 IPSec 处理方式相同。

检测间隔：设置 DPD、NAT-T 的检测间隔。

超时次数：设置 DPD、NAT-T 的检测超时次数，多次检测超时后，设备会认为对端失效而断开连接。

阶段一安全提议：选择阶段一协商时所使用的参数，包括加密算法、认证算法；其中数据加密所使用的加密算法包括 DES、3DES、AES、AES192、AES256、SANGFOR_DES、SM1、SM4；选择数据认证的认证算法包含 MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、SM3。

5. 配置完<IKE配置>之后，点击<IPSec配置>进入IPSec配置界面。

IPSec 配置各项说明如下：

重试次数：设置标准 IPSec VPN 的重试连接次数。

IPSec SA 超时时间：设置 IPSec SA 对应的超时时间。

过期时间：勾选启用或者禁用，来选择标准 IPSec VPN 隧道是否有过期时间。

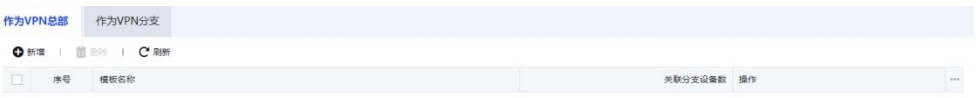
完成 IKE 和 IPSec 配置后，点击<确定>，返回主界面。

6. 主界面配置确认无误后，最后点击<提交>。

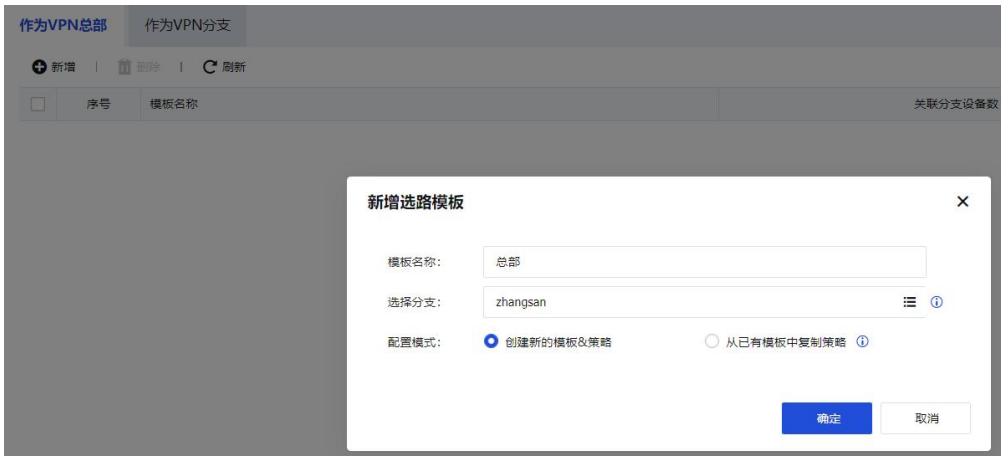
8.10.3. SDWAN 配置

8.10.3.1. SDWAN 选路模板

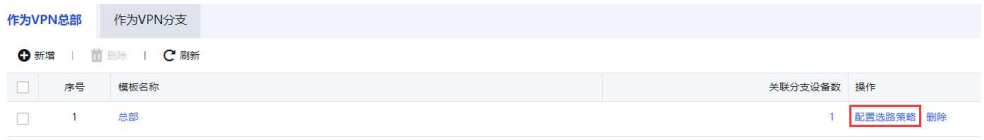
SDWAN选路模板可通过本地端创建也可通过BBC下发到设备端，可创建或查看总部端的选路策略或者查看分支端的选路策略。如下图所示。



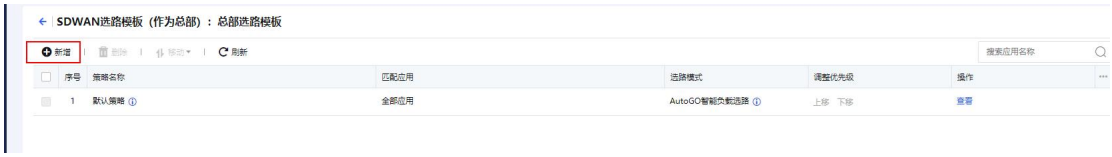
步骤1. 点击<新增>，配置好模板名称并选择好分支并点击<确定>,如下图所示。



步骤1. 创建好模板后，点击该模板后面的<配置选路策略>，如下图所示。



步骤2. 进入[配置选路策略]页面，点击<新增>,如下图所示。



步骤3. 进入[新增策略]页面，应用识别点击<自定义>，默认为智能识别，可通过智能识别算法将应用识别为不同的类型和优先级，并依据应用的服务类型和优先级进行智能选路。这里为了方便演示操作，使用自定义应用进行说明。

步骤4. 点击<应用分类选择框>，并选择要进行SDWAN选路的应用。

步骤5. [指定源/目的IP]项中点击<设置>，指定需要进行SDWAN的网段，默认为所有网段。

步骤6. 选择选路模式，选择AutoGo智能负载选路，选择需要进行选路的线路，默认为所有线路，点击<确定>,完成配置。

说明：

当前线路数以 VPN 线路中配置的线路数为准，对端线路则默认为 4 条，可通过删除功能，保留当前实际存在的 VPN 线路连接。

> ⚠ 注意：
>
> 设备未加入 BBC 的状态下，SDWAN 选路模板和选路策略可以在设备端本地控制台配置；设备加入 BBC 后，则只能由 BBC 端配置和下发，配置方法和本地端一致。

8.10.3.2. SOFAST 优化设置

通过DPI库自动识别应用且划分为交互类、实时类、传输类，智能感知链路质量和匹配链路优化模型，保障在高丢包场景下，依然保障业务流畅访问体验。

点击<启用SOFAST优化>，开启SOFAST优化功能，选择动态自适应或者自定义条件生效模式，如下图。

动态自适应：根据设备内置的应用丢包率启用 SOFAST 优化功能

自定义条件：可自行设置 SOFAST 优化功能生效模式的丢包率阈值

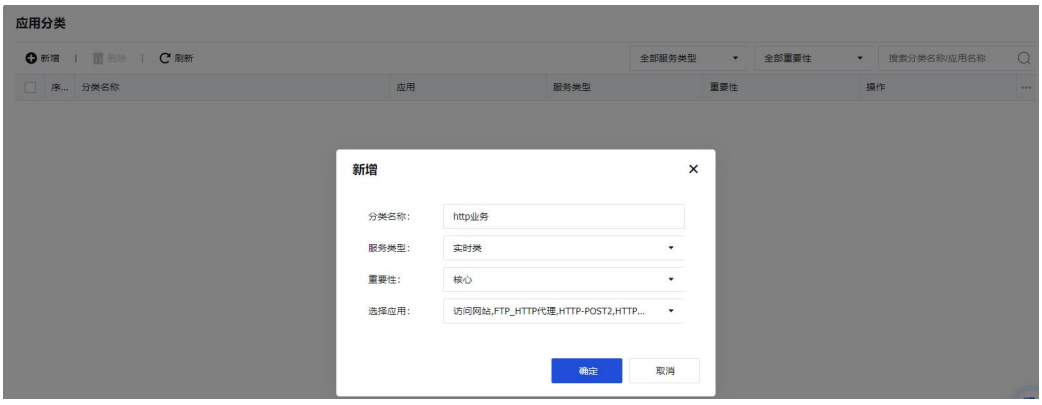
⚠ 注意：

1、SOFAST 优化功能必须结合 SANGFOR VPN 传输模式为 UDP 协议一起使用，并且总部和分支端设备同时开启才生效。

2、启用 SOFAST 优化时，分支和总部端的生效模式可以不一致。

8.10.3.3. 应用分类

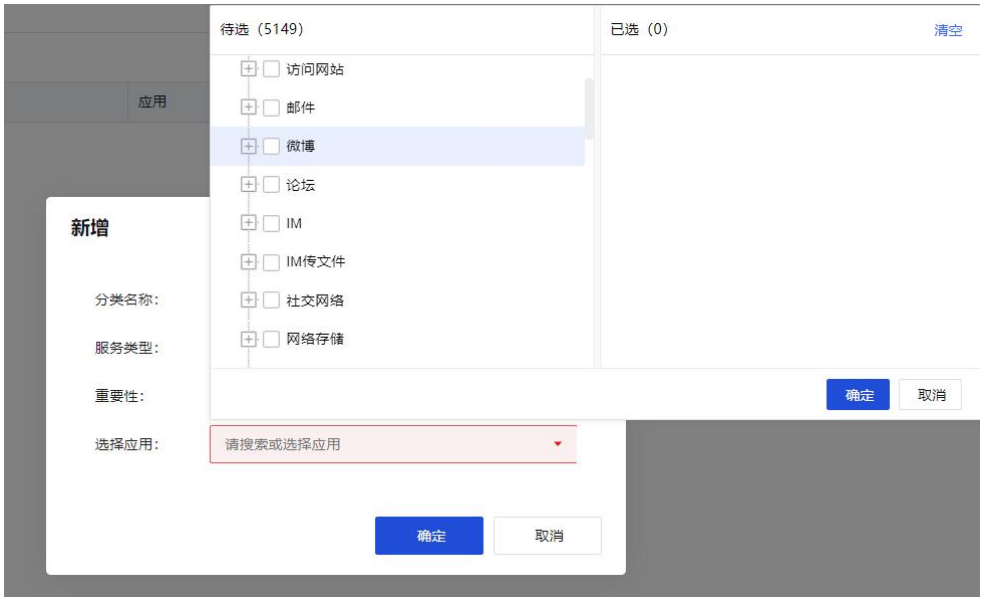
应用分类模块是将已知的应用自定义归类到同一个类别中，方便在SDWAN选路中引用。点击<新增>，如下图所示。



服务类型：包含传输类、交互类和实时类三种类型，方便识别该应用类的类型。

重要性：包含核心、重要、普通和一般四种级别，方便定义该应用类的重要级别。

选择应用：可进行应用识别库中的应用选择。



最后点击<确定>完成配置。

⚠ 注意：

设备加入 BBC 集中管理后，则应用分类只能在 BBC 端的[管理]-[统一管理平台应用]中设置，并下发给 AF 设备。

8.10.4. Sangfor VPN 配置

8.10.4.1. 基本配置

基本设置中包括访问地址&密钥设置、本地网段和高级配置。

访问地址&密钥配置

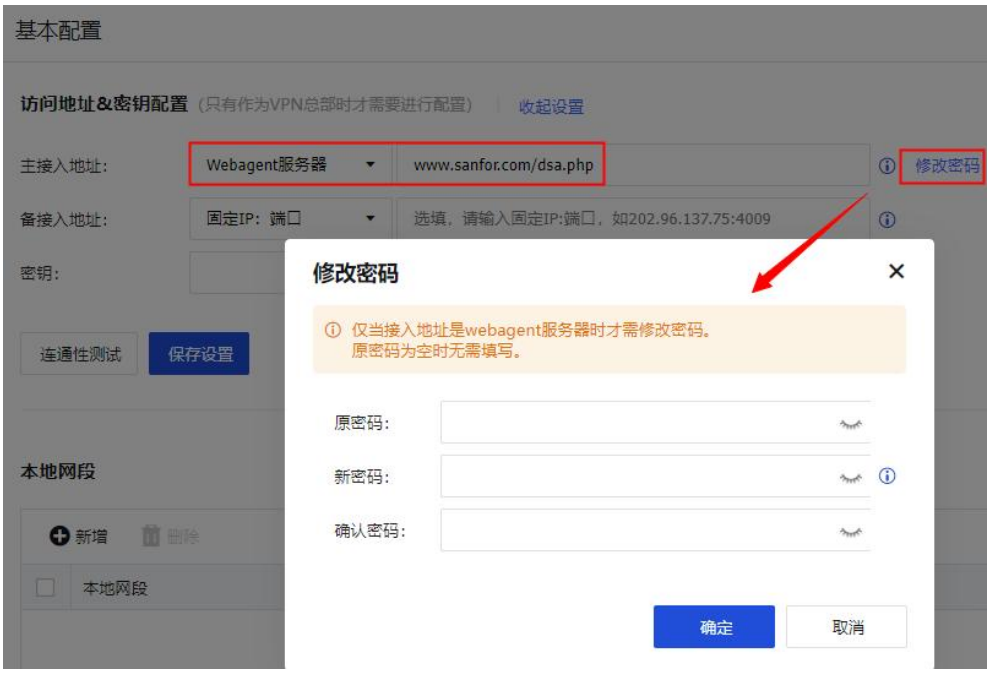
在[访问地址&密钥配置]的页面，配置项说明如下。

主接入地址主要支持的格式有以下三种：

固定 IP：端口（其中固定 IP 支持单 IP 和多 IP，最多支持四个 IP，各 IP 之间以#号分隔，如：202.96.137.75#60.28.239.21:4009），此 IP 为总部网络出口 IP。

动态域名：端口（适用于总部已存在动态域名指向他们出口的公网 IP 的环境。如：www.sangfor.com.cn:4009）。

Webagent 服务器（适用于总部 VPN 设备没有固定公网 IP 的环境，如 ADSL 线路，格式如：www.sangfor.com/NG4.0/test.php、202.96.137.75/test.php）。如果选择 Webagent 服务器方式，可以根据要连接的 webagent 服务器的密码，在此处设置相同的密码，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，Webagent 服务器密码为可选配置。



备接入地址格式和主一致，匹配规则如下：

主接入地址的优先级高于备接入地址，当主接入地址不可用时，备接入地址才生效；分支连接时需要至少与本端配置的主或备webagent匹配上一条。

密钥：可选配置，设置分支接入总部VPN的认证密码，如配置则分支必须输入相同密码才能正常建立VPN。

连通性测试：测试主接入地址的格式是否正确以及TCP端口是否可达。

配置完成后，点击<保存设置>。

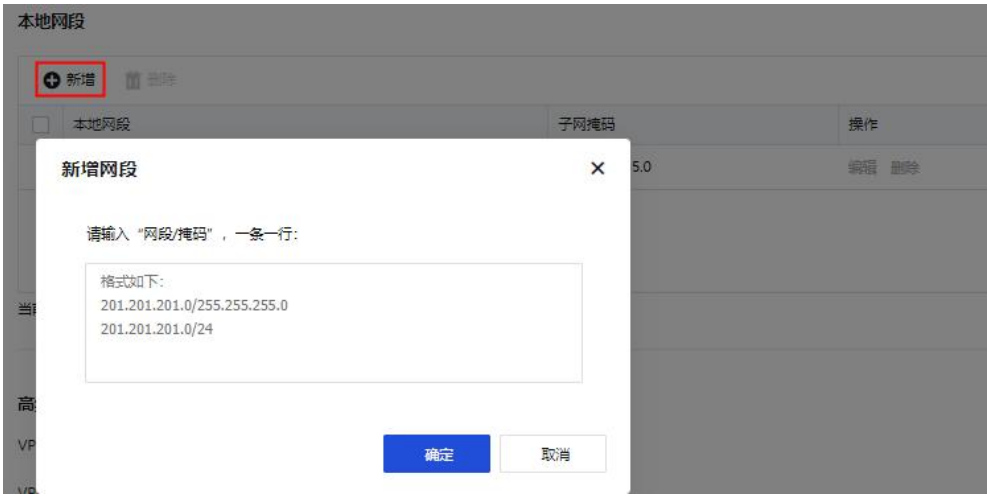
⚠ 注意：

1. 如果设置 Webagent 服务器密码，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。
2. 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。

本地网段

当设备所处内网有三层交换机或者路由器之类设备，划分了多个网段，则需要在这里将除设备[VPN内网接口]所在网段之外的其他多个网段的信息添加进去。

点击<新增>，填入本端其他网段地址即可完成本地子网列表的添加，支持“网段/掩码”的填写格式，页面如下。



添加完成后，点击<确定>即可。

⚠ 注意：

勾选[VPN 内网接口]的接口网段，不需要添加到本地子网列表。只有本地内网有多网段情况，才需要添加其他网段到本地子网列表。

高级设置

高级设置中，包括VPN内网接口、VPN接口、VPN监听端口等配置，页面如下。

各配置项说明：

VPN 内网接口：包括 LAN 口属性的网络接口，用于设置 VPN 网段，即属于 LAN 口口网段范围之内的 IP 地址就认为是 VPN 数据，其他网段 IP 地址都为非 VPN 数据。

⚠ 注意：

[网络]-[接口]中的网口同时没有勾选 WAN 口属性，并且没有配置默认网关的接口，才会显示在 VPN 内网接口选项中，比如：WAN 属性的接口不会显示在 VPN 内网接口中。

VPN 接口：用于设置本端设备的 VPN 接口 IP 地址，可以自动分配或者手动定义 VPN 接口 IP。

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。

MTU：用于设置 VPN 数据的最大 MTU 值，默认为 1500。

MSS：用于设置 UDP 传输模式下 VPN 数据的最大分片。

⚠ 注意：

MTU、MSS 一般情况下请保留默认值，如需设置，请在深信服技术支持工程师的指导下修改。

广播：是否开启广播设置，如果开启广播，则需要填写广播包端口范围。

组播：是否开启组播设置，如果开启组播，可以把从分支 LAN 侧接收到的组播包通过 Sangfor VPN 隧道透传到总部，分支和总部均需要启用。

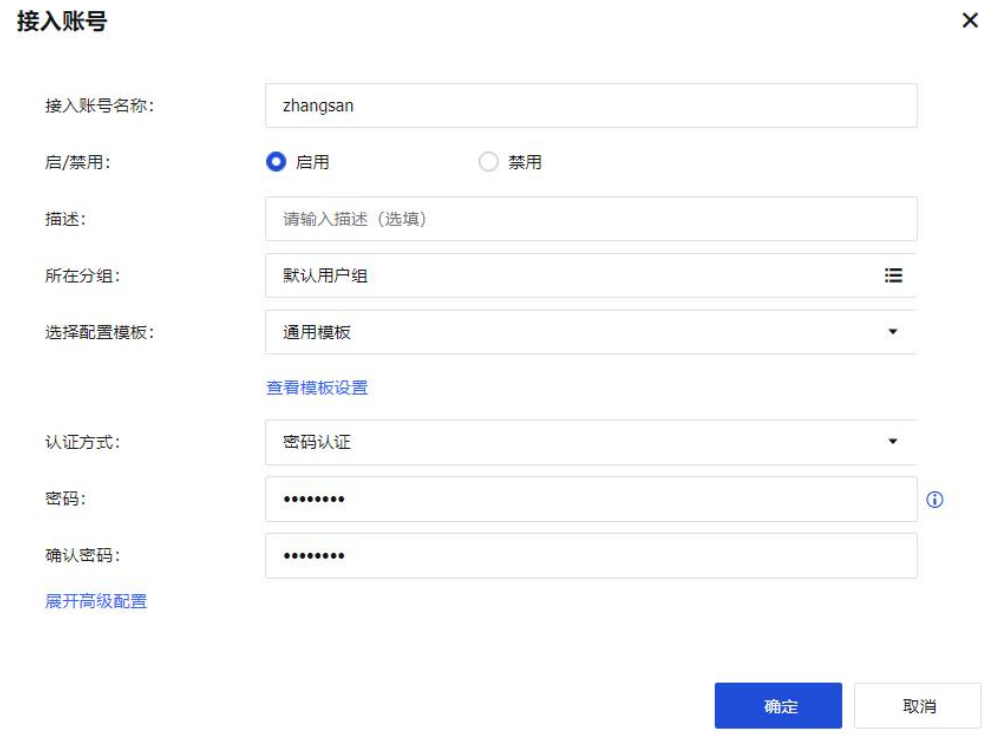
配置完成之后，需点击<保存配置>，配置才可以生效。

8. 10. 4. 2. 接入账号管理

[接入账号管理]用于管理VPN接入账号信息，设置允许接入VPN的用户账号、密码、设置账号使用的配置模板、是否启用硬件捆绑鉴权、隧道内NAT、多线路选路策略等用户策略。

点击[全部]后的 可以新增分组，填写相应的名称，点击<确定>，完成分组的配置，如下图。

接入账号列表中点击<新增>，可以新增VPN接入账号，可依次设置接入账号的名称、描述、所在分组等信息，如下图所示。



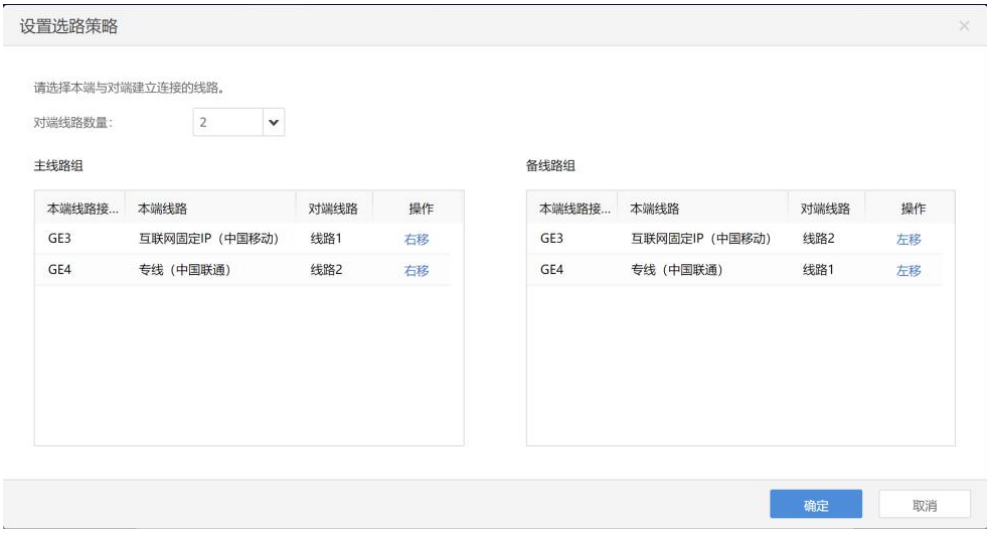
各配置项说明：

选择配置模板：可查看模板设置，也可新增配置模板，以便修改其中的内容，模板中可配置模板名称、加密算法、是否启用多用户登录、用户的内网服务设置、组播服务、Sangfor VPN隧道超时时间等配置。

认证方式：选择用户的认证方式，包括密码认证、证书认证、LDAP认证、Radius认证四种方式。

高级设置：包括用户过期时间、硬件证书捆绑鉴定、隧道内NAT、多线路选路策略等配置。

高级设置/多线路选路策略：当智能选路不匹配时走多线路选路策略，根据实际情况选择建立VPN连接的两端线路数，然后选择主线路数和备线路数，如下图。



配置完成之后，点击<确定>，完成用户相关的配置。

接入账号列表中，可以对接入账号进行删除、启用、禁用、移动到其他分组等操作，页面如下图。

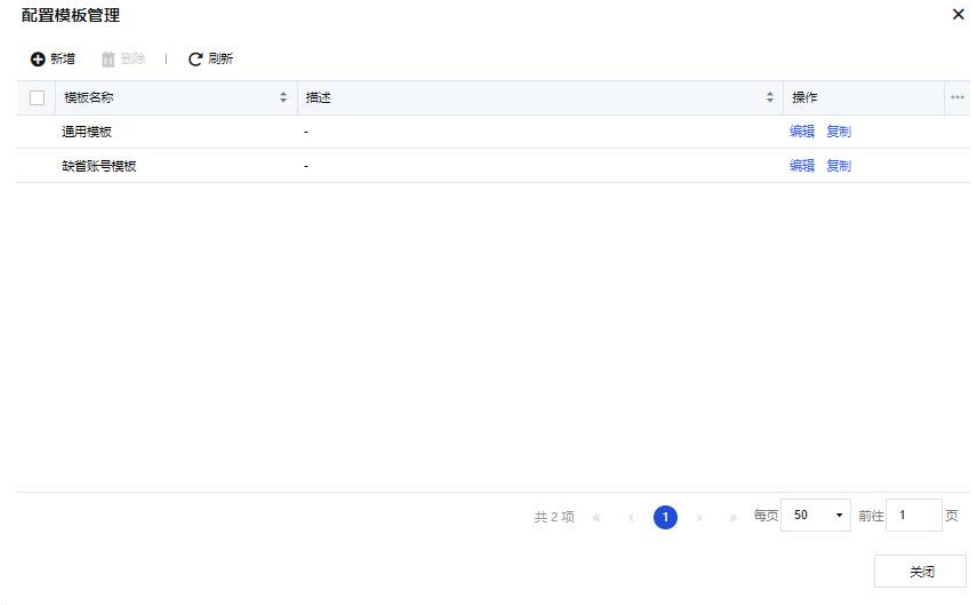
点击<虚拟IP池设置>，创建分支虚拟IP池，分支虚拟IP池中的虚拟IP段提供给分支接入到总部时将分支的原网段替换成虚拟IP池中的一个网段，以解决当两个相同网段的分支同时接入到总部时的内网IP冲突问题。设置时设定虚拟IP的起始IP/子网掩码、网段数、描述，页面如下。

点击<确定>，即可完成虚拟IP池的配置。

点击<更多操作>选择<导入>，可以从本地CSV、TXT文件中导入用户信息，也可以导入第三方服务器认证用户，导入后有相应的提示。

点击<更多操作>选择<导出>，可以从设备上将用户导出到本地进行保存，导出的用户密码为密文导出，页面如下。

点击<更多操作>选择<配置模板管理>，可以管理接入账号配置模板的界面，如下图。



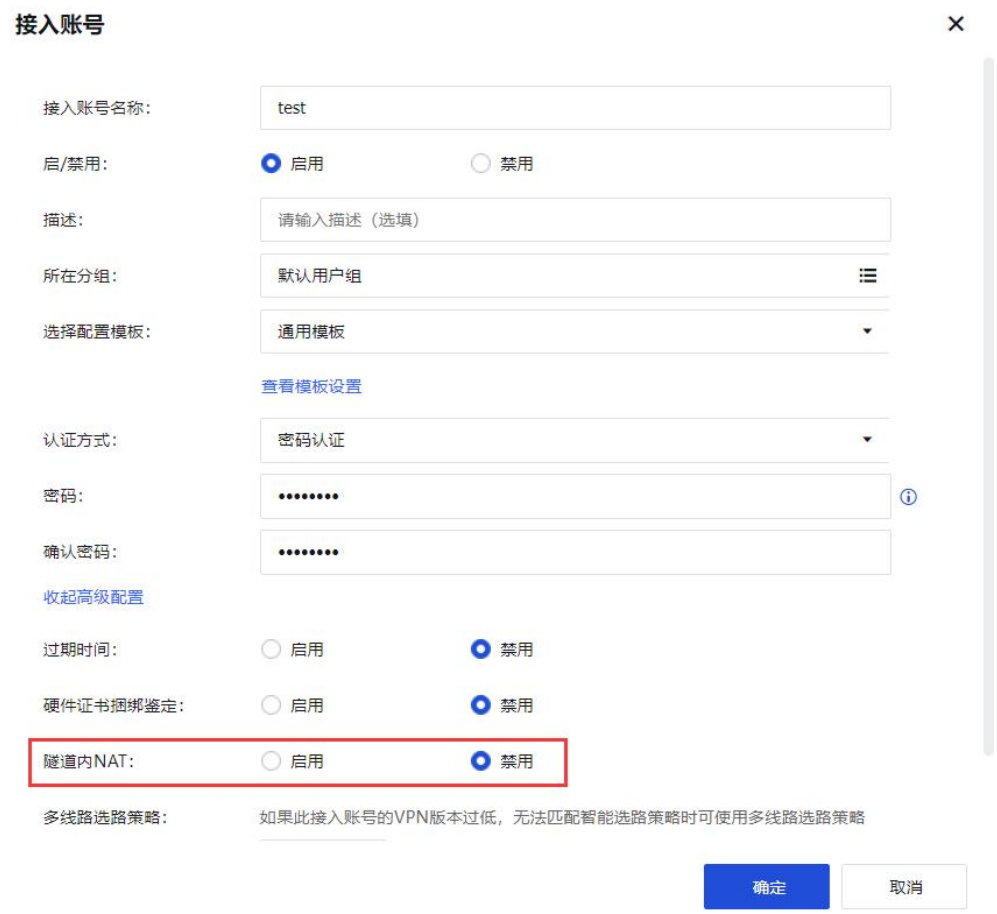
点击<新增>，可以进行配置模板中加密算法，内网服务设置、组播服务等进行配置。

配置完成点击<确定>，即可保存在配置模板列表中。

隧道内NAT

[隧道内NAT]主要用来解决分支之间内网网段冲突问题，通过在总部设备的[接入账号管理/虚拟IP池设置]的配置，如下图。

在新增接入账号中可以看到是否启用隧道内NAT的功能，如下图。



点击<启用>后，选择配置相应的原IP网段，系统支持两种虚拟IP分配方式：自动分配、手动添加，若虚拟IP池分配空了，可以到[接入账号管理/虚拟IP池设置]进行添加。

配置完成后，点击<确定>即可完成配置。

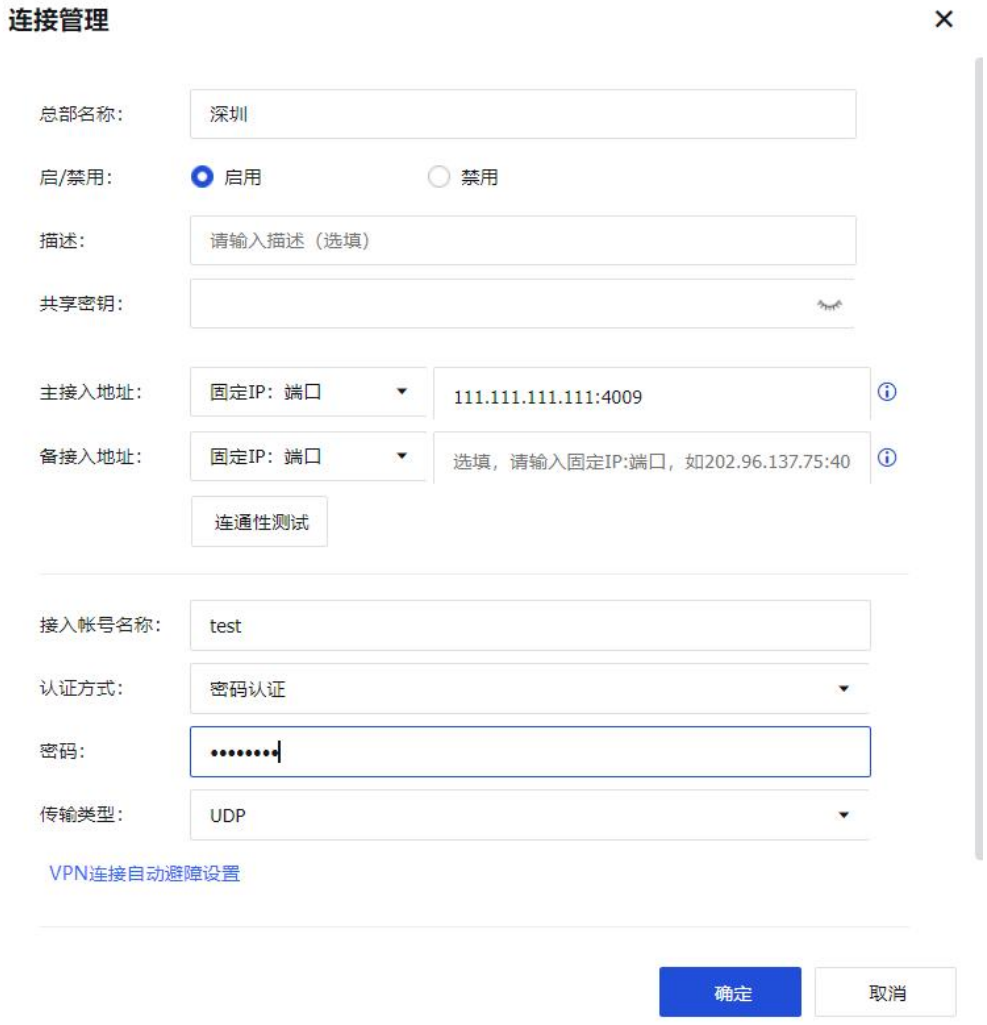
8.10.4.3. 连接管理

为了实现多个网络节点的互联（组成“网状”网络），VPN硬件网关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。页面如下。

⚠ 注意：

连接管理只有设备当分支使用需要连接其他深信服设备时才需要启用，否则本端是 VPN 总部设备，不需要启用连接管理。

点击<新增>，可以添加一个本设备到其他 VPN 总部的连接，页面如下图。



各配置项说明：

总部名称和描述：于标记连接名称，可以自定义填写。

共享密钥、接入账号名称、密码根据总部提供的接入账号信息来填写。

主/备接入地址：用于填写需要连接的总部的对应地址和端口，点击<连通性测试>可以测试地址是否正常联通。

📖 说明：

如果地址是用域名形式，测试成功代表该网页存在，否则网页不存在。如果地址采用固定 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 UDP、UDP + TCP 伪装、UDP + ESP 伪装，用于决定传输 VPN 数据包的封装类型，默认为 UDP 传输模式，当前版本已去除 TCP 的传输类型。

📖 说明：

针对 TCP 的传输类型是在 UDP 的报文中加入 TCP 头部,让数据包从表面上看起来是 TCP 包，从而可以穿透封堵。但是 TCP 穿透并没有真正的 TCP 三次握手，还是有被运营商封堵的概率；针对 ESP 的传输类型是在 UDP 的报文中加入 ESP 头部，让数据包从表面上看起来是 ESP 包，从而可以穿透封堵。这种穿透也有可能被运营商识别从而穿透失败。

VPN连接自动避障设置：用于启用VPN端口定期切换和协议自适应切换，用于缓解运营商端口和协议封堵带来的VPN网络问题，如下图。

启动VPN端口定期切换：从计时器计数到切换时间，VPN会使用新端口先建立起新的VPN连接，此时新老连接共存，当业务切换到新端口建立的VPN连接后再销毁旧的VPN连接。

启用VPN协议自适应切换：在SANGFOR VPN隧道启用协议自适应功能后，该隧道建立VPN连接时会分别通过UDP、FAKE_TCP、FAKE_ESP三种协议建立三条冗余连接，当主连接线路断开或线路劣化大于预设阈值，则主线路会切换为其他两条中质量最好的线路。

点击[展开高级配置]，可以对VPN对端进行权限设置，即指定VPN对端只能访问本端的哪些服务，如下图所示。

设置完以上信息后，勾选[添加]选项即完成内网服务的设置。最后点击<确定>即激活该连接，并保存设置信息。

8. 10. 4. 4. 高级配置

[高级配置]中包括隧道间路由设置、组播服务管理、VPN时间计划设置、RIP设置和生成硬件证书。

隧道间路由设置

AF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。

点击<新增>，可以添加一条隧道间路由，如下图。

选择隧道间路由的应用场景，包含以下五种常用场景：

分支互访：如果分支 A 和总部已经互通，分支 B 和总部也已经互通，此时想打通分支 A 和分支 B，通过隧道间路由实现分支 A 和分支 B 通过总部中转互通。

分支访问级联总部：如果分支 C 与二级总部 B 已经互通，此时分支 C 想访问一级总部 A 时，通过隧道间路由可实现分支 C 访问一级总部 A 通过二级总部中转互通。

总部代理分支上网：分支 B 没有互联网出口，但是分支 B 与总部 A 互通，通过隧道间路由可实现分支 B 的内网用户经过总部 A 的路由中转实现访问互联网。

多总部备份：分支 C 通过总部 A、总部 B 均可访问某业务系统，正常情况下分支 C 通过总部 A 访问业务系统，当与总部 A 连接断开后，分支 C 通过总部 B 访问该业务系统。

自定义隧道间路由：如果以上 4 种不能满足场景需求，可自定义设置隧道间路由。

此处以分支互访为例，点击<下一步>。

各配置项目说明：

源网段：用来设置隧道间路由的源 IP 网络和掩码。

目的网段：用来设置隧道间路由的目的 IP 网络和掩码。

中转路由设置：用来选择隧道间路由条目的 VPN 隧道（例如，A 跟 B 之间建立了 VPN 连接，使用的是用户“A”，现在 A 想通过 B 访问到 C，则对 A 设备而言，VPN 隧道为用户“A”）。

点击<确定>，则启用该隧道间路由条目，配置完成。

注意：

1. 启用通过中转路由分支上网功能时，VPN 远程分支端设备必须部署为网关模式，本端设备网关、单臂部署均可。
2. 新建隧道间路由之前，需先确认在该 VPN 设备的[接入账号管理]中已经建好了用户或者[连接管理]中配置了连接管理，否则将无法创建隧道间路由。
3. 其中[中转路由设置]是指：[接入账号管理]的[配置模板]中未启用多用户登录选项的用户以及连接管理中配置了的用户（不包括二者重名或已禁用的用户）。

组播服务管理

为满足VOIP和视频会议等应用，深信服设备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[接入账号管理]上新增用户，然后在[选择配置模板/添加]新增

配置模板中启用组播服务功能，然后在关联相应的组播服务，页面如下。

VPN时间计划设置

用于定义常用的时间段组合，这些时间组合可以在[接入账号管理/配置模板]模块中使用，以设置VPN内网服务的生/失效时间，该时间以设备上当前系统时间为准，页面如下图。

点击<新增>，出现时间计划配置页面，页面如下。

定义一个名称为“test”的时间段，选取相应的时间段组合，宝蓝色为生效时段，白色为失效时段。点提交完成时间组的定义。

定义完成时间段之后，对[接入账号管理/配置模板]中进行时间限定，如下图。

第三方认证服务器

LDAP服务器设置

深信服设备的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），如下图所示。

设置好LDAP服务器信息后，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，如下图所示。

Radius服务器设置

深信服设备的VPN服务支持使用第三方Radius认证，如需要启用第三方Radius认证，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），如下图所示。

RIP设置

RIP设置用于设置深信服设备通过RIP协议向其它路由设备通告路由信息，以实现内网路由设备RIP路由信息的动态更新，如下图。

配置项说明：

启用路由选择信息协议：整个RIP动态路由更新功能的开关，激活后，深信服设备会向所设置的内网路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对端的路由指向深信服，VPN连接断开后会通告路由设备删除该路由）。

IP地址：用于设置主动向哪个IP（路由设备IP）发布路由更新信息。

更新周期：深信服在路由信息有变化时会触发路由更新信息过程，这时下面设置的RIP更新周期参数失效。

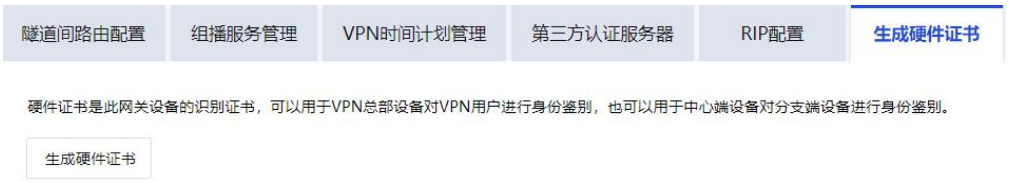
密码验证：用于设置交换RIP协议信息时需要验证的密码，可视具体情况进行设置。

生成硬件证书

基于硬件特性的证书认证系统是深信服公司的发明专利之一。深信服硬件设备也采用

了该技术用于不同VPN节点之间的身份认证。该证书提取了深信服设备部分硬件特征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，页面如下图。

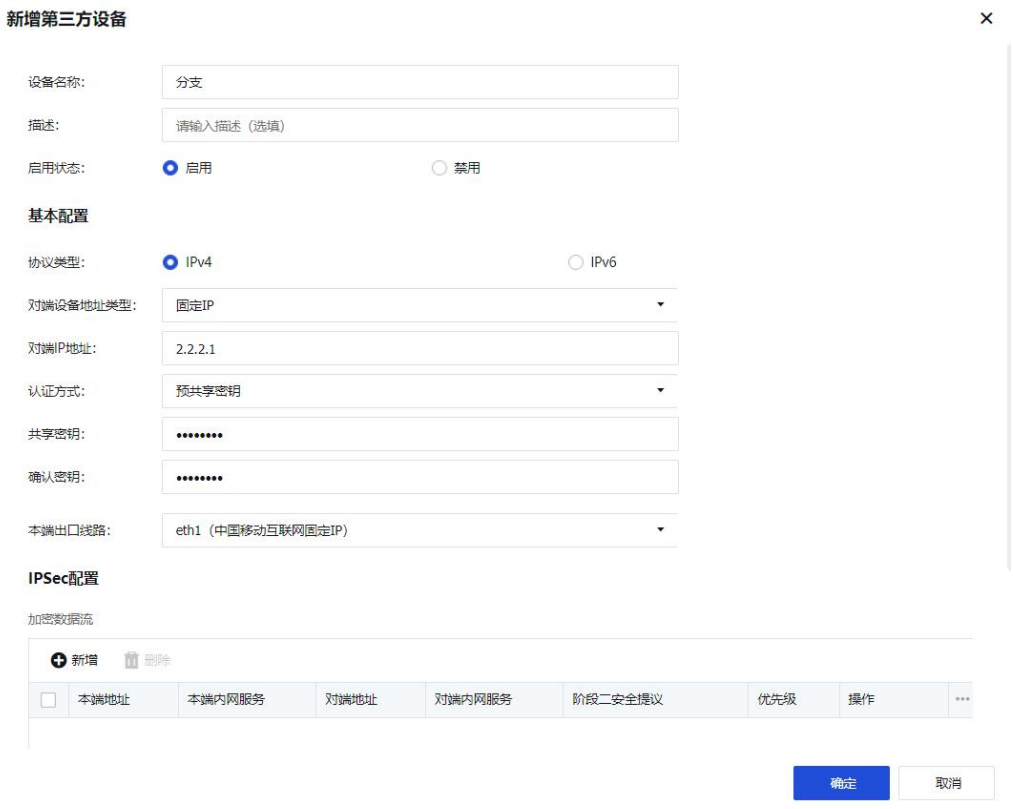


将生成好的证书发给总部管理员，由总部管理员在新建VPN用户账号的时候选择硬件鉴权，将用户和对应的硬件证书进行绑定即可。

8.10.5. IPSec VPN 配置

深信服AF支持与第三方设备之间建立标准IPSec VPN的对接。AF的标准IPSEC遵循的是国际标准的IPSEC VPN协议，只要对端的VPN也是用的是标准的IPSEC协议，那本端设备就支持跟对端进行VPN对接。

点击<新增第三方设备>，可新增标准IPSec VPN连接的配置，如下图。



基础配置界面各配置项目说明：

设备名称：设置隧道名称。

描述：用于标注隧道名称，可自定义填写。

启用状态：启用或者禁用该VPN连接。

协议类型：支持IPv4和IPv6协议。

对端设备地址类型：包括固定IP、动态IP、动态域名三种，请根据实际情况选择：选择固定IP，就填写上对端的IP地址；选择动态域名，就填写上对端外网绑定的域名。

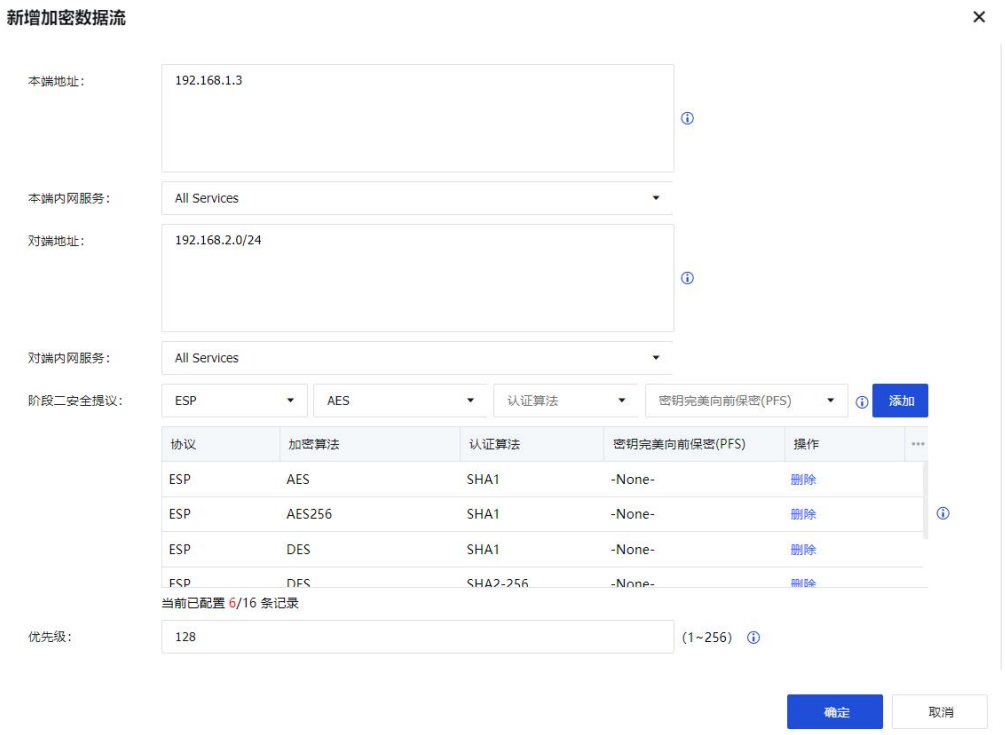
认证方式：包括预共享密钥和RSA签名证书两种，按需选择。

预共享密钥与确认密钥：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。

本端连接线路：根据实际线路情况选择对应的出口线路。

加密数据流：选择设置标准IPSec VPN的感兴趣流以及第二阶段协商的参数。

点击<新增加密数据流>可进行感兴趣流与协商参数的配置，如下图。



各配置项目说明：

本端地址：设置标准IPSec VPN感兴趣流的源IP匹配规则，可填写单个IP或者IP网段。

本端内网服务：设置标准IPSec VPN感兴趣流的源内网服务匹配规则，可选择ALL Services、ALL TCP Services、ALL UDP Services、ALL ICMP Services这四种服务类型的某一种，请按需选择。

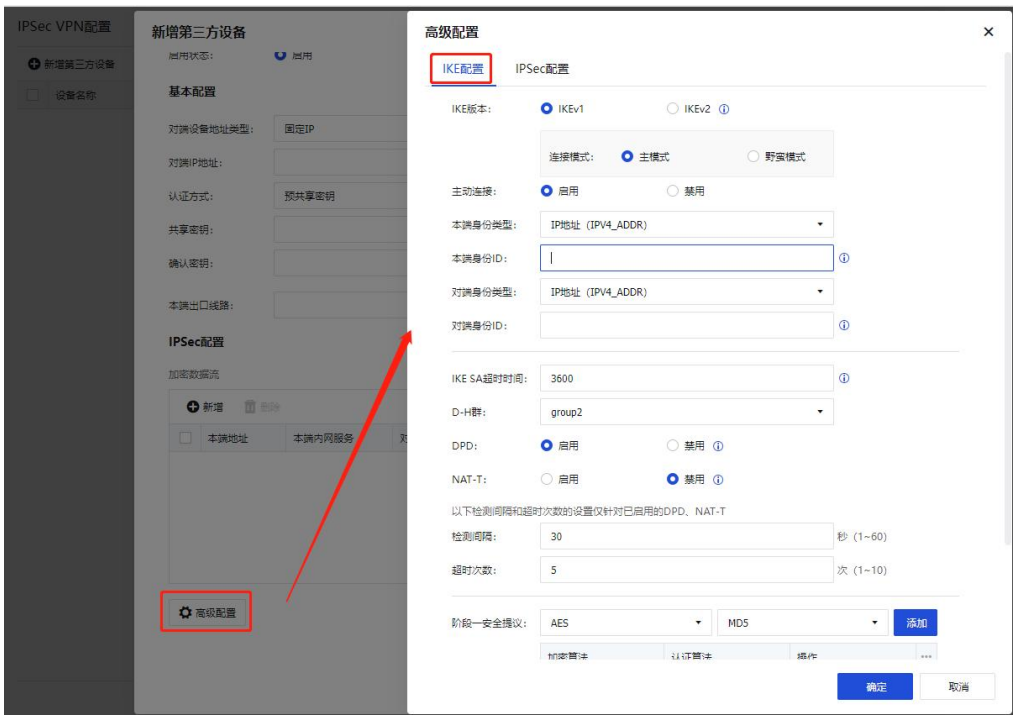
对端地址：设置标准IPSec VPN感兴趣流的目的IP匹配规则，可填写单个IP或者IP网段。

对端内网服务：设置标准IPSec VPN感兴趣流的目的内网服务匹配规则，可选择ALL Services、ALL TCP Services、ALL UDP Services、ALL ICMP Services这四种服务类型的某一种，请按需选择。

阶段二安全提议：选择阶段二协商时所使用的参数，包括所使用的协议、加密算法、认证算法、是否启用密钥完美向前保密（PFS）；其中数据包封装所使用的协议包括AH、ESP协议；数据加密所使用的加密算法包括DES、3DES、AES、AES192、AES256、SANGFOR_DES和SM4；选择数据认证的认证算法包含MD5、SHA1、SHA2-256、SHA2-384、SHA2-512和SM3。

优先级：设置本端地址和对端地址优先级用于标识路由优先级。

点击<高级配置>按钮，进入IKE和IPSec配置界面，如下图所示。



IKE配置界面各配置项说明：

IKE版本：选择IKEv1或者IKEv2版本需要对端保持一致。

连接模式：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定IP或者一方固定IP一方动态域名方式，并且不支持NAT穿透；野蛮模式适用于其中一方为拨号的情况，并且支持NAT穿透；根据客户实际需求场景选择主模式或者野蛮模式。

主动连接：用于控制设备是否主动发起建立VPN的连接。

本端身份类型：设置本端身份类型，保证对端可以识别到本端设备。该类型包括：IP

地址（IPV4_ADDR）、域名字符串（FQDN）、用户字符串（USER_FQDN）三种类型。

本端身份ID：按照本端身份类型所选择的类型进行配置。

对端身份类型：设置对端身份类型，保证本端可以识别到对端设备。该类型包括：IP地址（IPV4_ADDR）、域名字符串（FQDN）、用户字符串（USER_FQDN）三种类型。

对端身份ID：按照本端身份类型所选择的类型进行配置。

IKE SA超时时间：标准IPSEC协商的第一阶段存活时间，只支持按秒计时方式。

D-H群：设置Diffie-Hellman密钥交换的群类型，包括1、2、5、14、15、16、17、18八种，请与对端设备配置保持一致。

DPD：IPSEC使用DPD（Dead Peer Detection）功能来检测对端Peer是否存活。

NAT-T：NAT-T在野蛮模式下才会有，主要作用是避免有一方设备处于NAT之后导致标准IPSEC协商失败，NAT穿透启用后数据会封装成UDP格式传输，而不是ESP封装，这样也可以避免内网没有放通ESP的情况。

检测间隔：设置DPD、NAT-T的检测间隔。

超时次数：设置PDP、NAT-T的检测超时次数，多次检测超时后，设备会认为对端失效而断开连接；

阶段一安全提议：选择阶段一协商时所使用的参数，包括所加密算法、认证算法；其中数据加密所使用的加密算法包括DES、3DES、AES、AES192、AES256、SANGFOR_DES、SANGFOR_NULL；选择数据认证的认证算法包含MD5、SHA1、SHA2-256、SHA2-384、SHA2-512。

配置完[IKE配置]界面中的配置之后，进入到[IPSec配置]界面。

IPSec 配置界面各配置项说明：

重试次数：设置标准IPSec VPN的重试连接次数。

IPSec SA超时时间：设置IPSec SA对应的超时时间。

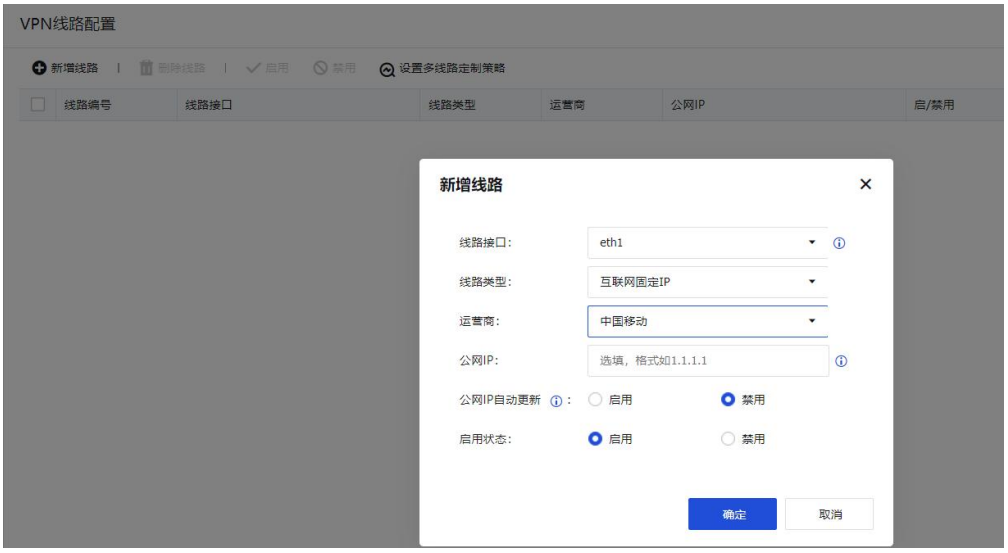
过期时间：勾选启用或者禁用，来选择标准IPSec VPN隧道是否有过期时间。

配置完成之后，点击<确定>即可保存配置。点击<编辑>可对VPN连接中的参数进行修改，点击<查看>显示加密数据流即可查看到对应的加密数据流的匹配规则。

8.10.6. 通用配置

8.10.6.1. VPN 线路配置

设备开启多线路授权的情况下，网络接口处配置了多个WAN接口，可以通过该配置项新增多条VPN线路，点击<新增线路>，对VPN线路进行配置，如下图所示。



各配置项说明：

线路接口：选择相应的WAN口作为线路接口。

线路类型：可以选择设备预先设置好的类型，也可以点击添加进行自定义线路类型名称，页面如下图所示。

运营商：可以选择设备预先设置好的运营商类型，也可以点击添加进行自定义运营商名称，页面如下。

公网IP：填写相应的公网IP。

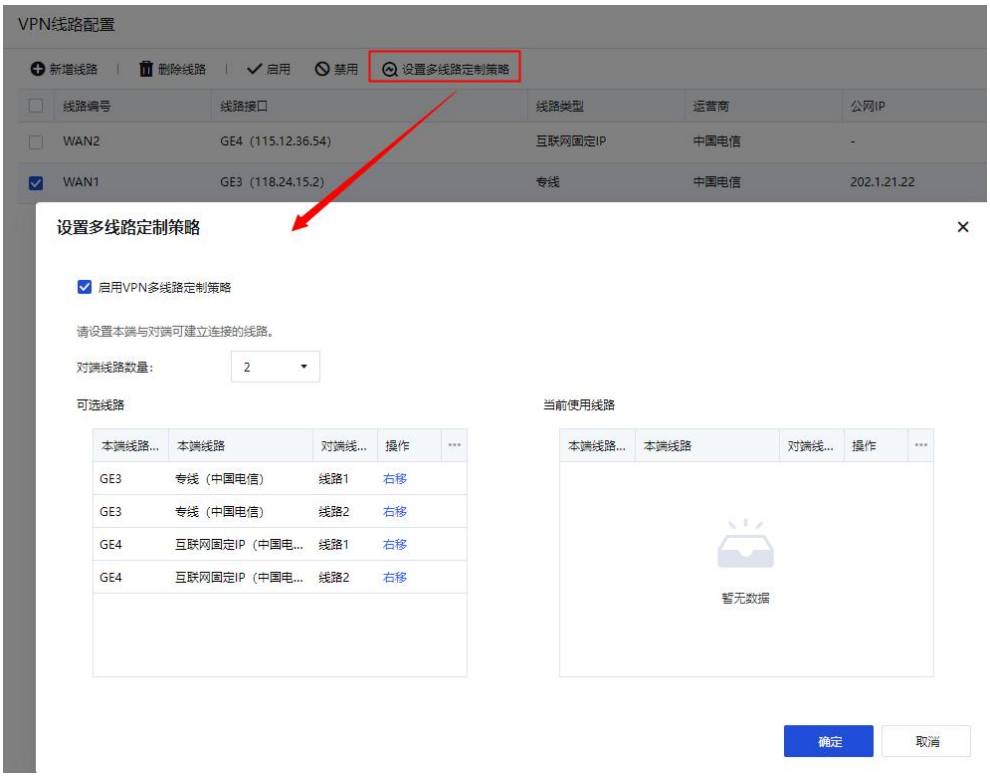
公网IP自动更新：用于拨号场景自动获取出口公网IP的场景，启用后将定期自动更新公网IP。当需要使用手动配置的公网IP时，需点击<禁用>按钮，此时公网IP不会自动变化。

配置完成之后，点击<确定>后，会保留在线路列表中。

多线路定制策略

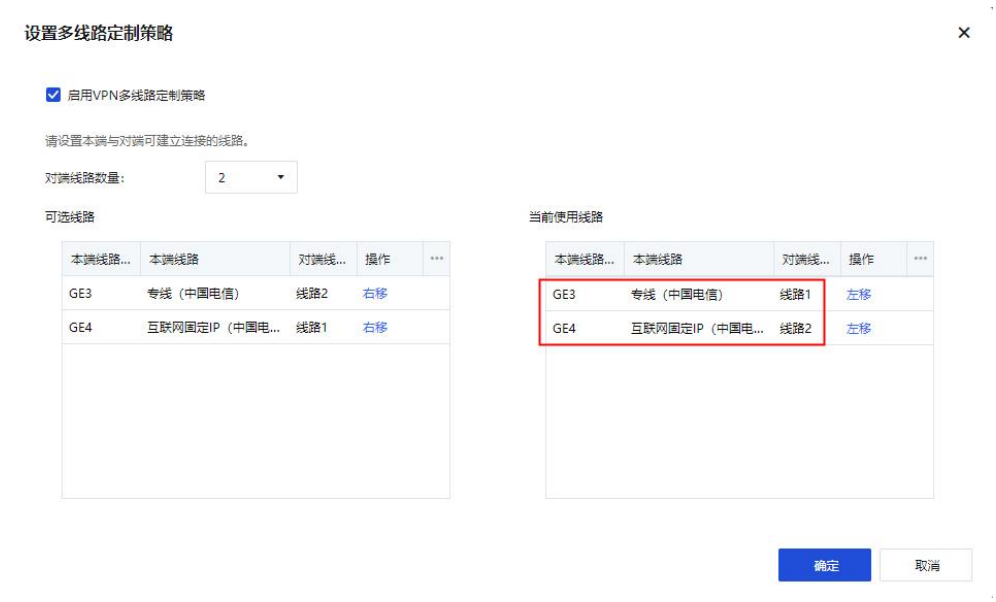
用于设置本端线路与对端指定线路建立SANGFOR VPN连接，未选中的线路不会建立SANGFOR VPN连接。防止跨运营商之间（或者跨线路类型之间）连接SANGFOR VPN连接。例如：总部端线路1为中国电信专线，线路2为中国电信互联网线路；分支端线路1为中国电信专线，线路2为中国电信互联网线路；此时要求总部与分支之间只存在两条SANGFOR VPN连接，分别是总部专线与分支专线之间的SANGFOR VPN连接、总部互联网与分支互联网之间的SANGFOR VPN连接。

点击<设置多线路定制策略>，进入多线路定制策略的配置界面，如下所示。



通过勾选[启用VPN多线路定制策略]启用该功能，根据实际线路情况，选择对端VPN线路数量。

根据案例对端线路数量选择为2，通过[可选线路]中的[操作]来移动相应的VPN线路到[当前使用线路]中，设备通过[当前使用线路]中的VPN线路来建立SANGFOR VPN连接的。本案例中将[可选线路]中的“GE3 专线（中国电信） 线路1”，“GE4 互联网固定IP（中国电信） 线路2”移动到[当前使用线路]。如下图所示：



多线路定制策略配置完成之后，点击<确定>即可。

8.10.6.2. 证书请求

点击<新增请求证书>，如下图所示。

各配置项说明：

名称和主题以及拓展识别信息模块的信息，根据实际情况来进行填写。

密码标准：可以选国际商用密钥标准（RSA）和中国国家商用密码（SM2）。

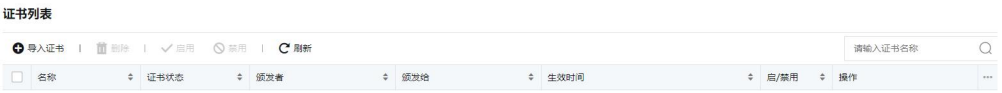
RSA密码长度：可选1024，2048，4096。

摘要算法：可选sha1，sha2。

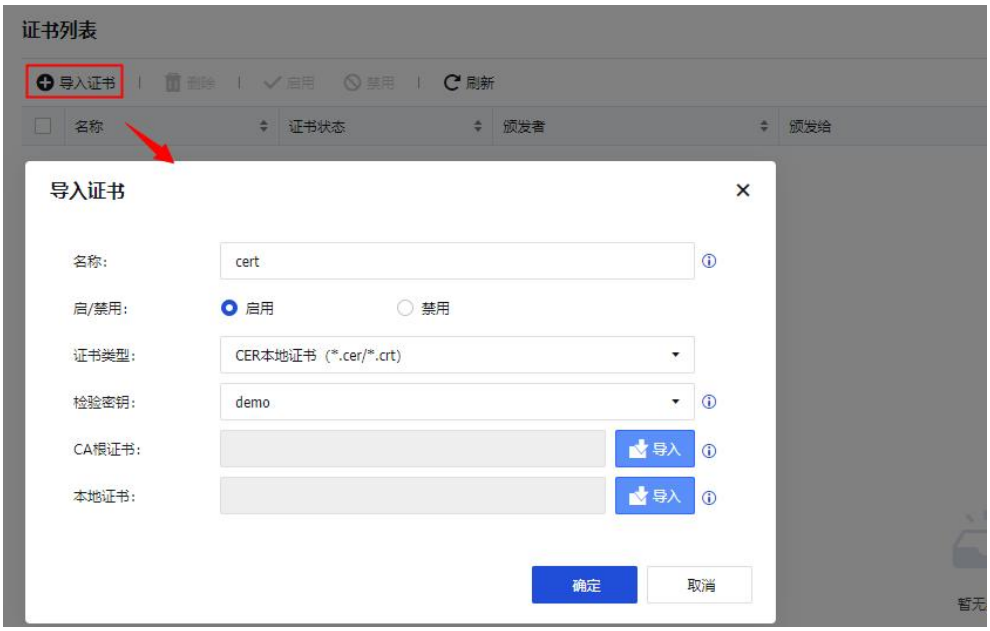
新增申请后，会生成证书申请文件和密钥文件，点击<下载>可将申请文件下载下来。只支持离线证书申请。

8.10.6.3. 证书管理

[证书管理]可以看到证书管理页面，显示如下图。



点击<导入证书>，将离线申请的证书导入证书管理列表，显示如下图。



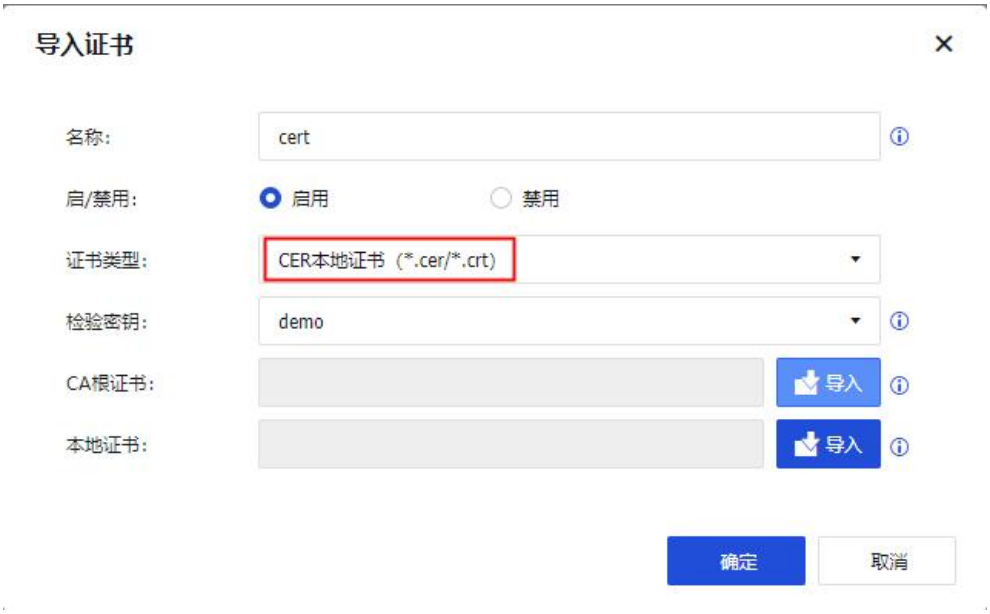
各配置项说明：

名称：可根据实际情况自定义证书名称。

启/禁用：可以启用或禁用该证书。

证书类型：可选择：CER本地证书（*.cer/*.crt）、CER根证书（*.cer/*.crt）、PKCS#12证书（*.pfx/.p12）、PKCS#7证书（*.p7b）。

选择[证书类型]为CER本地证书导入时，校验密钥来自于申请信息列表，即选择即将导入的证书对应的申请信息。显示如下。



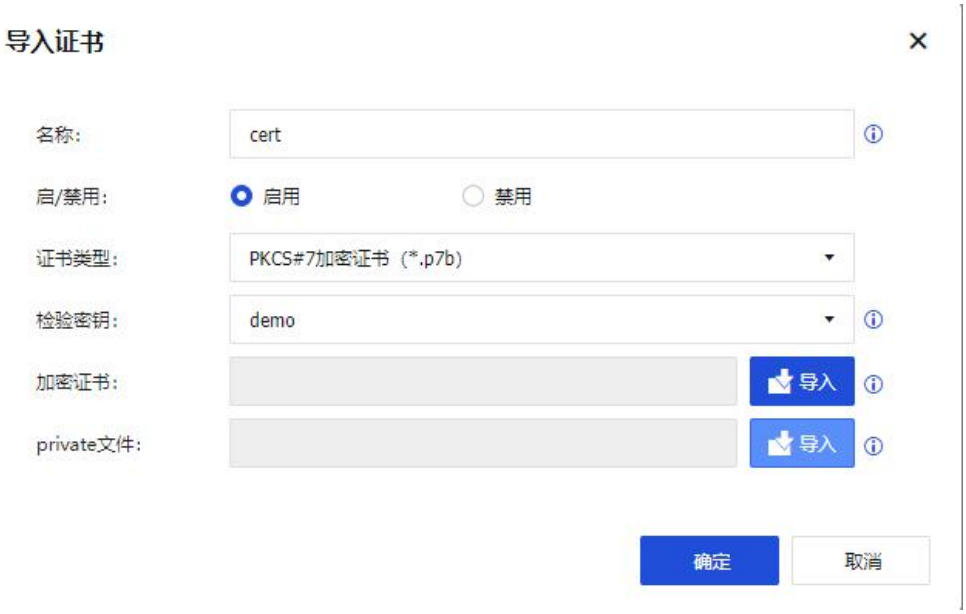
选择[证书类型]为CER根证书导入，显示如下。

选择[证书类型]为PKCS#12证书导入。保护密码为该证书导出/生成时的填写的保护密码，当根证书和保护密码正确时，证书才能导入成功。显示如下。

选择[证书类型]PKCS#7证书导入。校验密钥来自于申请信息列表，即选择即将导入

的证书对应的申请信息。如下图所示。

选择[证书类型]为PKCS#7加密证书导入。校验密钥来自于申请信息列表，即选择即将导入的证书对应的申请信息，同时需要导入加密证书和private文件，如下图所示。



选择[证书类型]为双证书，校验密钥来自于申请信息列表，同时需要导入根CA、一级CA、签名证书、加密证书以及私钥，如下图所示。

证书导入完毕后，可以在证书列表中看到证书信息，可以进行编辑和下载。如下图所示。

📖 说明：

当该证书是根证书时，支持下载 CA 根证。当该证书是非根证时，支持下载 CA 根证或下载 PRCS#12 证书（*.pxf/*.p12）格式证书。

8.10.6.4. VPN 内网服务

SANGFOR系列硬件设备可以为接入的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、某个分支用户只能访问内网的特定计算机和特定服务参数；其次原有老版本智能选路策略也可以根据内网服务中五元组的定义来识别相应的应用，从而为智能选路做应用识别。

通过适当的内网服务设置，对服务进行访问授权和应用识别可以实现VPN隧道内的安全管理，也可以实现智能选路中根据不同的应用做对应的选路策略。页面如下。

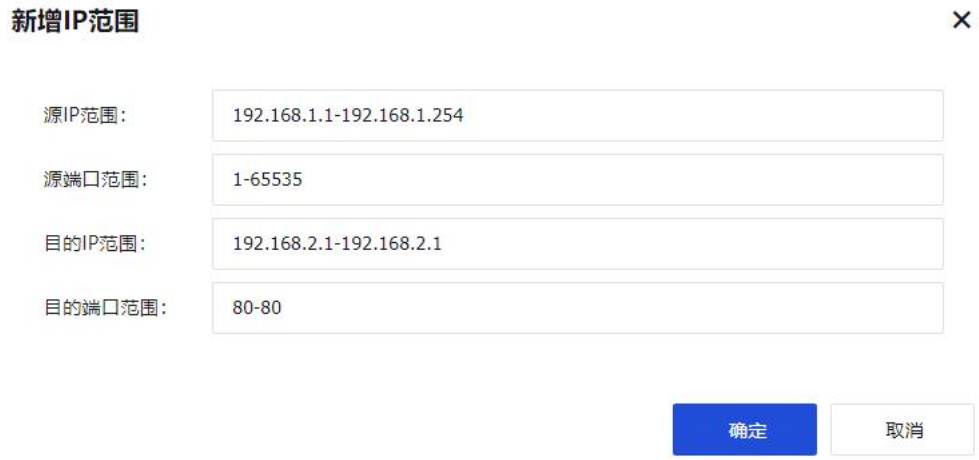
点击<新增>，可以根据协议类型手动添加内网服务，如下图。

各配置项说明：

名称和描述可自定义，方便管理即可。

协议类型：选择定义的内网服务所使用的协议。

选择[TCP]或[UDP]，还可以设置源IP范围、源端口范围、目标IP范围、目标端口范围等，点击新增，如下图。

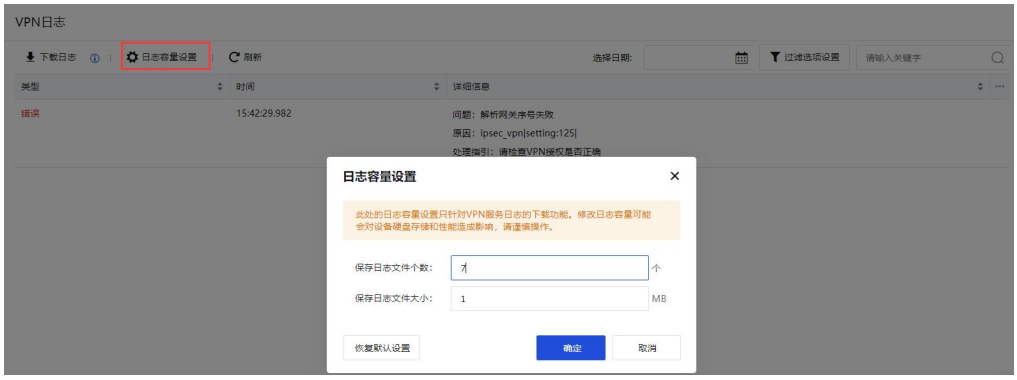


选择[ICMP]，可以设置源IP范围和目标IP范围，如下图。

所有配置完成后，点击<确定>保存配置。

8.10.7. VPN 日志

VPN日志提供了日志的下载功能，并可设置日志的容量：保存日志文件个数、日志文件大小，日志文件大小最大支持10MB。



点击<过滤选项设置>，可设置日志显示的过滤条件：接入账号名称、总部名称、第三方设备名称、对端IP以及日志类型，VPN协商日志需要勾选相应的日志类型才可正常显示在页面中。

点击<下载日志>，下载当前VPN日志，并自动保存到本地，如下图所示。

9. 系统

系统主要用于设置系统功能以及参数方面的设置，包括安全能力更新、通用配置、排障、SNMP、管理员账号、系统维护和高可用性等功能模块。

9.1. 通用配置

通用配置设置包括控制台配置、网络参数、邮件服务器、系统时间、HOSTS、授权管理和隐私设置。

9.1.1. 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、控制超时等配置页面如下所示。

设备名称：可以设置设备的显示名称。

HTTPS端口：用于设置登陆控制台的端口，默认是TCP 443端口。

SSH端口：用于设置通过SSH方式登陆设备的端口，默认是TCP 22345端口。

控制超时(m)：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。

智能客服：设置在控制台界面是否开启智能客户小机器人的选项。

动态验证码：设置在控制台登录时是否开启输入动态验证码的选项。

投屏显示：设置在控制台登录时是否开启投屏显示的选项，开启投屏显示支持后，停留在能自动刷新的页面进行访问时，不会因为控制台超时而退出登录，建议在投影到大屏幕进行监控安全信息状况时开启

使用TLS：用于设置控制台支持的浏览器TLS的选项， TLS协议会影响浏览器是否能够正常打开AF控制台。

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<保存>保存配置生效。

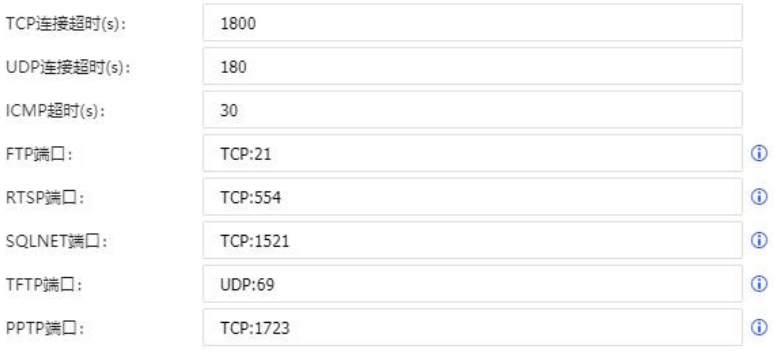
9.1.2. 网络参数

网络参数用于配置全局网络相关参数说明。

网络参数

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。

FTP端口、RTSP端口、SIP端口、SQLNET端口、TFTP端口、PPTP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。



管理口设置

管理口IP：设置后，可改变MANAGE口默认的管理IP。

管理对端IP：设置后，可定义通过管理口接入AF的对端IP地址限制。

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，只允许配置在“管理对端IP”内设置的地址才允许访问。

系统保留IP

VLAN0 IP：设置AF设备对个别页面进行重定向的IP地址。

用户认证IP：设置AF开启用户认证后，重定向认证页面的IP地址。

H.323端口

RAS：设置RAS的端口，默认为标准的UDP:1719端口。

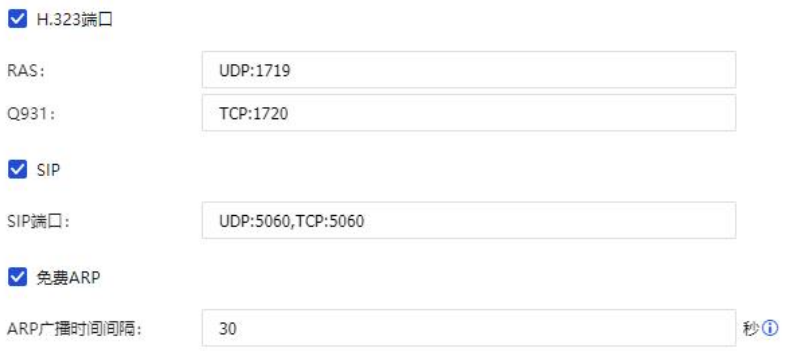
Q931：设置Q931的端口，默认为标准的TCP:1720端口。

SIP端口

SIP端口：设置SIP协议的端口，默认为标准的UDP:5060和TCP:5060端口。

免费ARP

ARP广播时间间隔：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。默认为30s，是为了减少免费ARP过多的问题。



业务/用户安全页面显示设置：设置业务安全和用户安全的显示模式，有缓存模式和实

时模式可供选择。

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。

路由优先级：支持自定义设备内部路由表的优先级，默认优先级如下图所示。

异常包检测：检测包的合法性，防止利用TCP/IP协议逃逸检测。

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。

异常BASE64检测：设定web应用防护是否对不合规范的base64数据进行安全检查。

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。

及时响应网络邻居的MAC地址变化：加快网络邻居MAC地址发生变化时的响应速度，网络邻居的MAC地址可能发生变化时建议开启。

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。

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]。

应用层检测bypass：启用该功能后当业务流量达到设备性能上限优先保证网络正常，放通部分流量不进行安全检测，默认开启。

body严格识别：设定根据body内容来判定数据类型。

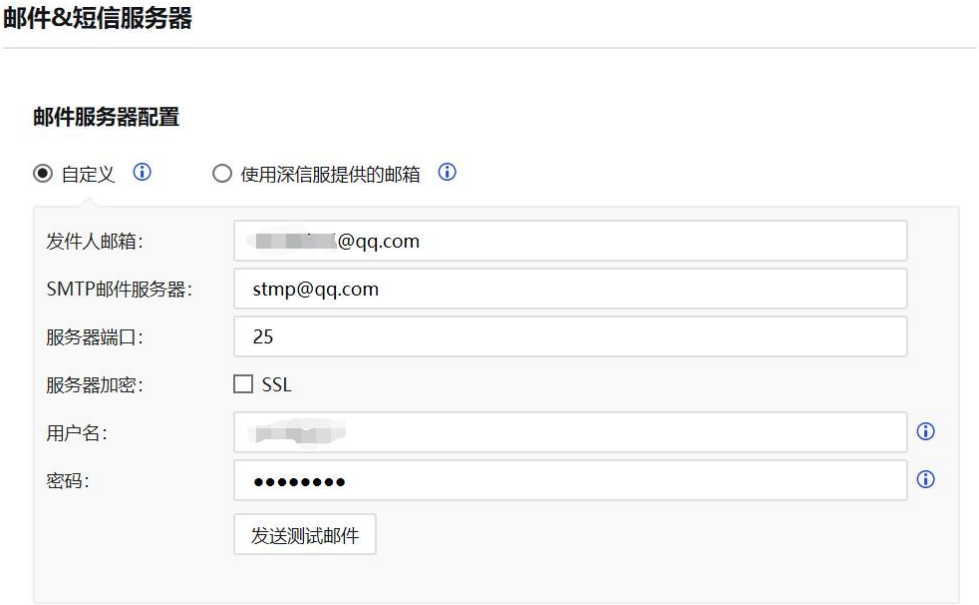
策略路由支持应用：设定是否允许策略路由支持配置应用。

高级配置：勾选后，开启AF相关高级功能，如TCP异常报文检测、异常邮件拦截和TCP会话超时reset。

9.1.3. 邮件&短信服务器

邮件服务器配置

[邮件服务器配置]用于设置设备发送告警邮件的时候使用的SMTP服务器信息也可以使用深信服提供的邮箱。



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。

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。

SMTP邮件服务器身份验证：填写发件人邮箱的用户名和密码。

- 用户名：可填邮箱地址，也可填用户名。
- 密码：如果发件人邮箱已启用第三方客户端授权码，则密码处填写授权码。

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。

点击<测试>，发送测试邮件成功后，可以到测试的邮箱地址查看是否收到测试邮件。

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）。

⚠ 注意：

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。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。

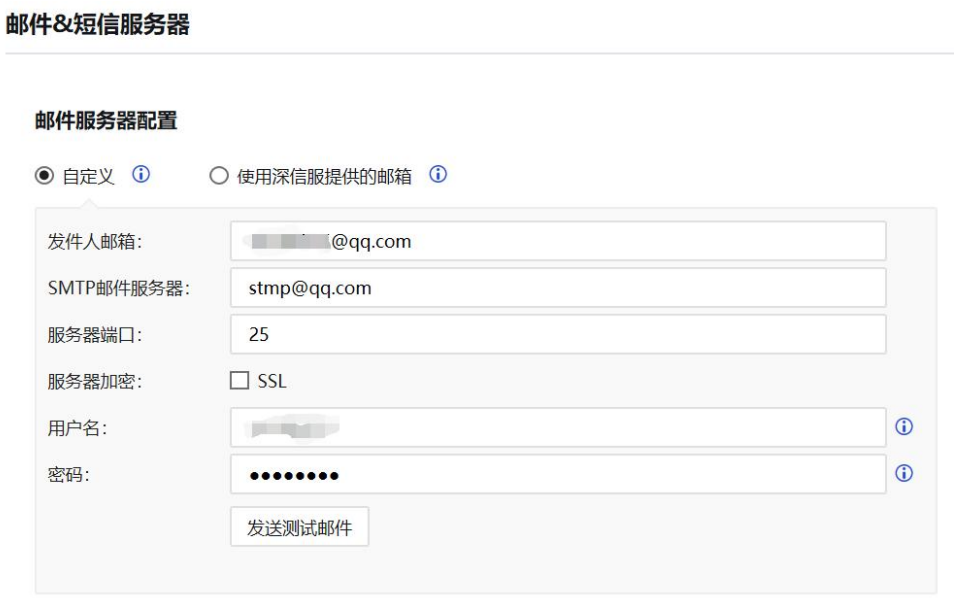
操作步骤

步骤1. 例如配置QQ邮箱服务器，需要在[设置/账号]找到服务器配置方式，确保SMTP已开启。根据需求点击<如何使用 Foxmail 等软件收发邮件？>去获取STMP服务器地址和端口。

步骤1. 点击<生成授权码>，跳转验证码发送页面，使用绑定邮箱的手机号发送短信到指定的号码，手机上发送成功，再点击<我已发送>。

步骤2. 页面弹出生成授权码。

步骤3. 进入[邮件服务器]配置页面。填写刚才配置的邮箱地址、SMTP服务器地址、服务器端口。STMP服务器验证填写的用户名与发件邮箱一致，密码为授权码。



步骤4. 点击<发送测试邮件>，输入能正常接收邮件的邮箱地址进行测试，如下图所示。

步骤5. 发送成功后，发送测试地址的邮箱收到测试邮件，说明配置的发送邮件服务器能正常发送邮件。点击<保存>邮件通知服务器配置完成。测试邮件如下图所示。

短信服务器配置

[短信服务器配置]用于设置设备的短信网关信息，设备产生的告警信息可以通过该短信网关进行发送。

服务商支持Alibaba Cloud、Tencent Cloud和ChuangLan，直接填写具体服务商提供的信息，需要设备能够连接外网。

9.1.4. 系统时间

系统时间用于设定深信服设备的系统时间。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，修改日期和时间会导致web服务器、DHCP

服务器、IPSec VPN服务、SANGFOR VPN服务重启、勒索专项数据清空。

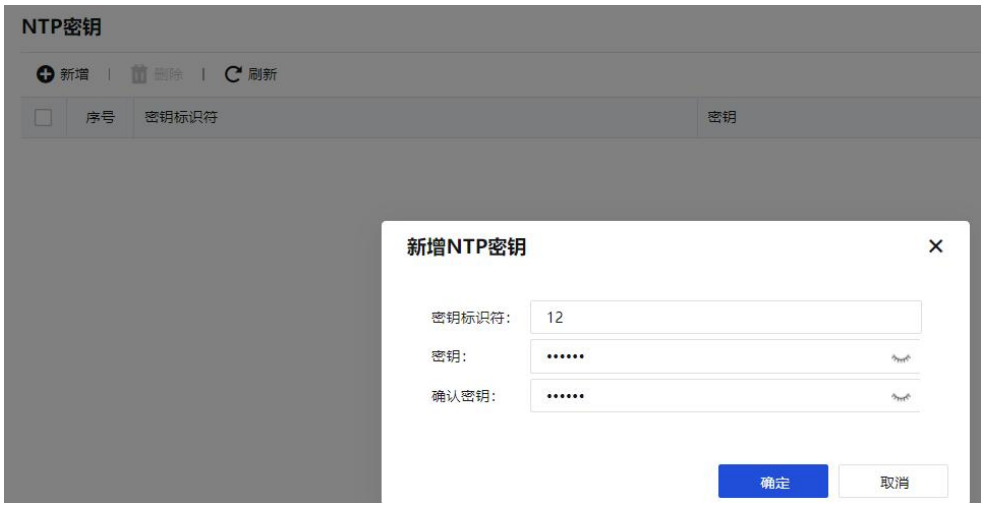
点击<获取本地时间>，则设备的系统时间会和登录控制面板的计算机时间一致。

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]中设置一个或多个时间服务器地址，则设备会自动与此时间服务器的时间进行同步，并支持选择NTP密钥和同步间隔时间。

9.1.5. NTP 密钥

NTP密钥用于设置时间服务器同步的NTP密钥，点击<新增>，如下图所示。



9.1.6. 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。

点击<新增>，新增一条记录。

主机名：设置需要指定的主机名。

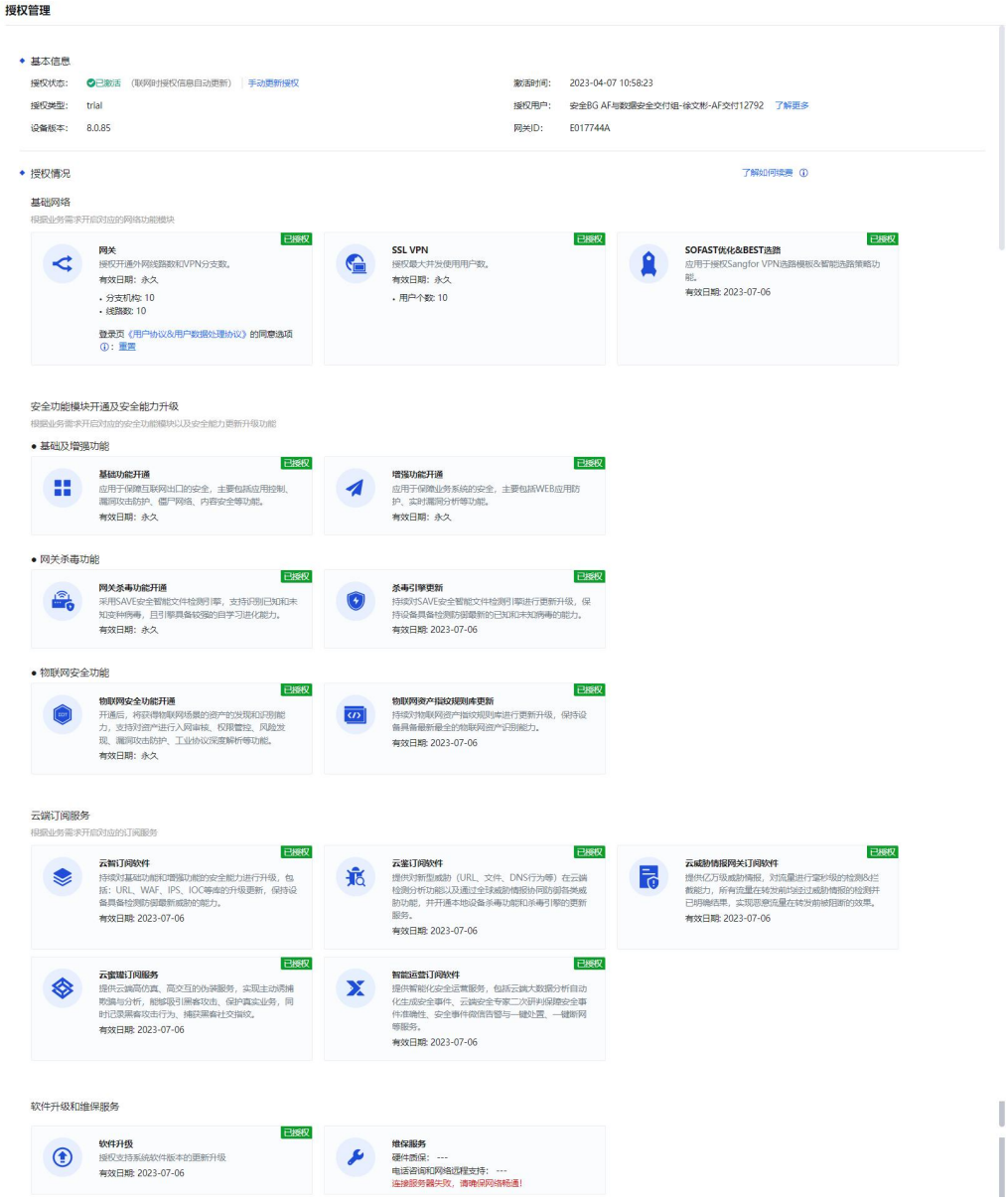
IPv4地址：设置主机名对应的IPv4地址。

IPv6地址：设置主机名对应的IPv6地址.

设置完成后点击<确定>，完成设置。

9.1.7. 授权管理

授权管理包括设备基础信息、基础网络授权、安全功能模块开通及安全能力升级授权、云端订阅服务授权和软件升级和维保服务，如下图所示。



设备基础信息：网关序号是AF设备软件的唯一标识。

基础网络：包括设备的外网线路授权数、标准IPSecVPN对接时分支机构授权数，SSL

功能模块的开通和对应的并发接入授权数以及SOFAST优化&BEST选路功能。

安全功能模块开通及安全能力升级：用于启动设备各安全功能模块，其中基础级包括应用控制、漏洞攻击防护、僵尸网络、内容安全等功能。增强级包括： Web应用防护、实时漏洞分析等功能。网关杀毒包括网关杀毒模块的开通，以及杀毒引擎更新的授权期限。 物联网安全包括 物联网安全功能模块的开通，以及物联网资产指纹规则库更新。

云端订阅服务：与云端联动，实现更新AF的防护能力同时，辅助AF对未知、高级威胁等进行有效检测和抵御。其中云智主要是对AF的各功能模块规则进行更新。云鉴主要是对未知威胁等进行有效检测和拦截。云威胁情报网关订阅软件主要是提供亿万级威胁情报，对流量进行毫秒级的检测&拦截能力；云蜜罐订阅服务提供云端高仿真、高交互的伪装服务，实现主动诱捕欺骗与分析，能够吸引黑客攻击、保护真实业务，同时记录黑客攻击行为、捕获黑客社交指纹；智能运营订阅软件提供智能化安全运营服务，包括云端大数据分析自动化生成安全事件、云端安全专家二次研判保障安全事件准确性、安全事件微信告警与一键处置、一键断网等服务。

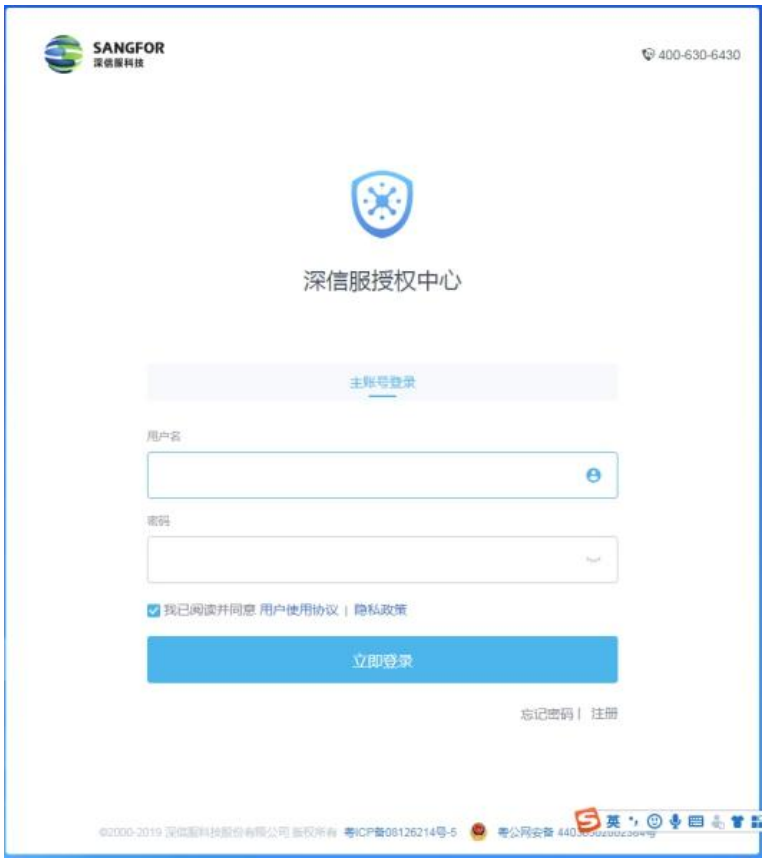
软件升级和维保服务：展示AF目前软件升级的有效限期，在限期内，可对AF进行版本的升级，保持AF在功能上的全面性。

授权激活方法

1、深信服授权中心激活

步骤1.导入设备信息（该步骤在深信服授权中心完成）。

步骤2.打开浏览器，输入深信服授权中心地址：https://license.sangfor.com.cn，输入注册好的账号密码。（若没有账号密码，需注册后方可登录；云图、MSS、SAAS（云眼云盾等）账号可以直接登录）。



步骤3.初始状态下未添加任何设备，点击<现在激活>去添加设备。

步骤4.导入需要激活的设备，可以通过订单号批量添加或通过网关ID添加。（企业名称需与订单系统的名称保持一致）。

步骤5.导入设备成功，可以看到这个账号下绑定的所有深信服设备、激活状态、

授权过期时间等。

步骤6.需要设备“在线激活”，必须在授权中心“启用自动激活设置”。

2、设备激活

该步骤需在设备端完成，激活方式分为在线激活和离线激活。

在线激活

步骤1.在线激活只需配置好网络，将设备联网，输入授权ID和授权即可激活成功。

步骤2.在线激活方式还支持“主动请求激活授权”，当在授权中心完成设备信息导入后，在AF授权管理有一个<激活授权>按钮，点击主动发起请求，激活授权，输入授权ID。（授权ID请拨打销售和400-806-6868获取）。

步骤3.申请成功后会显示使用授权开启的功能、服务和具体功能参数，然后会跳转到设备登录页面。

步骤4.管理员输入账号密码登录设备，再到设备授权管理，查看授权状态显示：已生效。

离线激活

步骤1.进入[授权管理]页面，点击<手动更新授权>，进入[更新授权信息]，可以导出设备硬件信息，也可以直接复制到粘贴板，用于后续生成授权文件。如下图所示。

步骤2. 回到深信服授权中心（https://license.sangfor.com.cn），在列表中找到对应的设备，点击导出授权文件。

步骤3.将刚导出的设备硬件信息导入，点击导出授权文件，即可导出相应的授权文件。

步骤4.回到设备端，点击导入，将刚刚导出的授权文件导入到设备端，即可激活成功。

9.1.8. 带外管理

带外管理可以很好的将客户的业务网络与管理网络进行路由隔离，并配置指定的流量匹配指定的路由进行转发。在此基础上，业务和管理流量相互之间不会产生干扰，攻

击者也无法通过业务网络入侵到管理网络。默认开启，正常情况下不需要设置，如下图所示。

点击具体服务后的<前往配置>会跳转到对应服务的配置界面。

点击具体服务后的<修改网络>，经由网络中有自动、管理区和业务区三个选择，默认是自动。自动是根据系统路由优先级进行选择，管理区是指定走管理口路由，业务区是指定走业务区路由，如下图所示。

9.1.9. 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。

授权云端安全防护及威胁分析：选择“上传所有威胁信息，云智更新安全能力库”后，会上传所有威胁信息包括本地已知威胁和未知威胁文件/HASH/URL/DNS等到云端分析防护，同时授权通过云端更新设备功能模块规则；选择“上传HASH等非文件类型上传未知威胁，云智更新安全能力库”后，会上传HASH/URL/DNS等非文件类型未知威胁等到云端分析防护，同时授权通过云端更新设备功能模块规则 。选择“云智更新安全能力库”后，只通过云端更新设备功能模块规则，不对未知威胁进行云端联动检测。

点击<保存>，完成功能生效。

9.2. 安全能力更新

安全能力升级用于在授权有效期内对设备内置库（云鉴检测威胁情报、SAVE安全智能文件检测模型库、URL库、漏洞特征识别库、应用识别库、Web应用防护库、僵尸网络与病毒防护库、实时漏洞分析识别库、IP地址库和物联网资产指纹规则库）进行升级管理。以下表格是具体规则库说明。

表25 规则库说明表

库名称	说明
云鉴检测威胁情报	云鉴检测威胁情报 5 分钟后会自动更新，不能手动点击立即更新。
SAVE 安全智能文件检测模型库	通过病毒特征识别进行分析学习，不仅能够识别大部分的主流活跃病毒，还能检测出未知的新型病毒。
URL 库	帮助设备识别各类网站，可以对一些 URL 进行管控。
漏洞攻击特征识别库	所有系统漏洞、应用漏洞等攻击特征的集合，提供给漏洞攻击防护模板使用。
应用识别库	根据应用特征识别不同的应用的集合，供应用控制策略等调用。
Web 应用防护库	所有 Web 应用攻击特征的集合，提供给 Web 应用防护模板调用。
实时漏洞分析识别库	对经过 AF 的流量进行分析，从而发现存在的漏洞。
僵尸网络与病毒防护库	僵尸网络、病毒文件的规则集合。
IP 地址库	互联网 IP 地址归属地的集合。
物联网资产指纹规则库	物联网资产指纹特征规则的集合。

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>用于看到内置库版本的实时信息。

规则库升级

在AF设备不能联网的情况下，通过点击<离线升级>可以配置在升级服务有效期内的规则库的手动升级。

在AF已经联网的情况下，点击<立即更新>可 以对已选的有效期内的规则库立即进行在线更新。

情报来源设置

主要用于配置设备使用情报来源以及需要连接的升级服务器，情报来源切换后会重新下载对应的威胁情报库。

点击<情报来源设置>，进入[情报来源设置]页面，情报来源主要有中国区情报库和海外情报库，升级服务器可以实际的外网的线路进行选择，或选择自动选择让设备自动检测可以连接的更新服务器。

代理设置

当网络中有 HTTP 代理服务器时，配置好代理服务器，让设备可以通过代理服务器上网更新内置库，代理设置内置库升级需要设备本身是联网的状态。

点击<代理设置>，进入[代理设置]页面。勾选[启用代理服务器]，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。

URL云查设置

主要用于设置在本地 URL 库查询不到情况下，启用去云端查询 URL 库分类功能。

点击<URL云查设置>，进入[URL云查设置]页面， 默认启用状态。

离线升级配置案例

某企业客户AF部署在内网，AF不能联通外网，为保证AF安全防护能力，现需要对有效期内规则库进行更新。

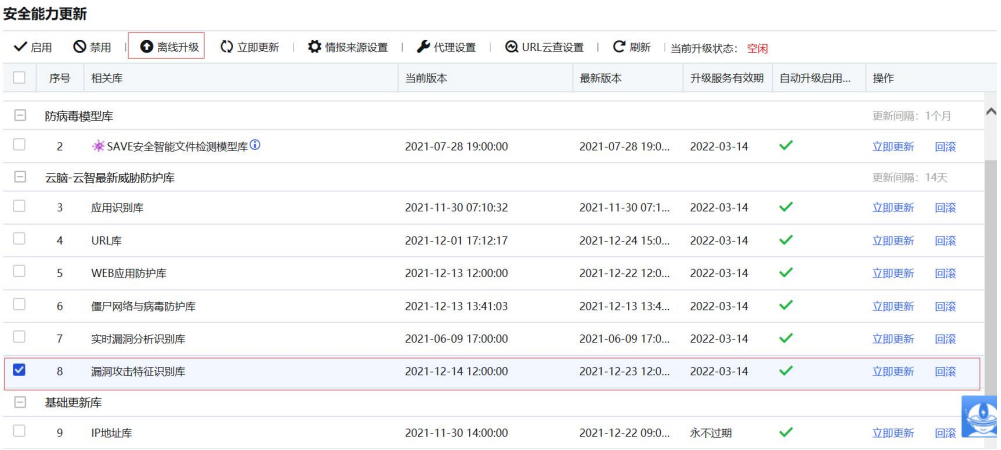
以更新漏洞攻击特征识别库为例，其他有效期规则库也是一样的操作，具体步骤如下。

步骤1.通过如下链接进入深信服社区选择对应AF版本的漏洞特征识别库进行下载，需要注册深信服社区账号。

链接地址：https://bbs.sangfor.com.cn。路径：自助服务›下一代防火墙AF。

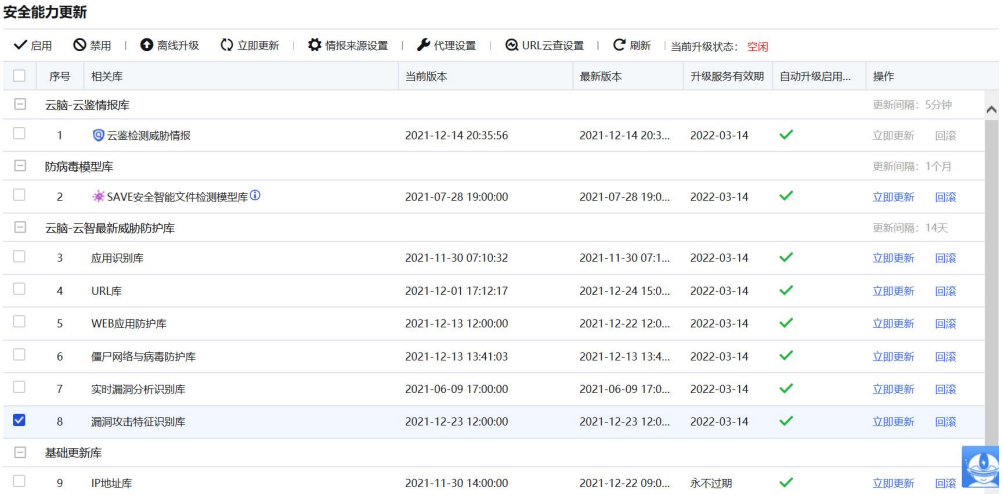
规则类别	更新时间	说明	大小	MD5	下载
漏洞特征识别库	2020-11-10	仅限AF6.8及以上版本使用	18.00MB	64A27D40F08BBBB7BF0FE8A41B22733E	
热点事件预警与处置库(中文)	2020-11-06	8.0.8及以上版本使用	51.02MB	7F073E76875FE9E322838F9E99381A2F	
热点事件预警与处置库(英文)	2020-11-06	8.0.8及以上版本使用	50.22MB	77C426A1441C43212A9613FA17AFC35A	
WEB应用防护库	2020-10-30	仅限AF6.8及以上版本使用	7.32MB	CA63CFF296286343F8C095A17EEC0B3F	
应用识别库（中文）	2020-10-27	仅限AF8.0.14及以上版本使用	1.98MB	D28BD287CDC4E37BCD665BCE29D8D8F3	
应用识别库（英文）	2020-10-27	仅限AF8.0.14及以上版本使用	1.98MB	B0019B43BB0B282D8A8F1E915A88D69C	
URL库(中文)	2020-10-22	8.0.14及以上版本使用	45.58MB	E29B4D480B9E5BB2F69575157CDB7EA1	
URL库(英文)	2020-10-22	8.0.14及以上版本使用	46.00MB	CF964507D13D95658862E86E40538789	
实时漏洞分析识别库	2020-10-10	仅限AF6.8及以上版本使用	3.48MB	B79D86B6574D0D1AF093D00A5A32557E	
僵尸网络与病毒防护库（国内库）	2020-09-02	仅限AF8.0.14及以上版本使用	98.17MB	1A64EEB34DAA4D819EDC3B9686F609A2	
僵尸网络与病毒防护库（海外库）	2020-09-02	仅限AF8.0.14及以上版本使用	97.25MB	9DC31B3FDB7E376413CD9444322CE78B	
热点事件库	2020-08-03	仅支持AF8.0.5及以上版本	1.50MB	60EFC4744DC26C5E4F13C00340FF8700	

步骤2.在[安全能力更新]页面选择漏洞攻击特征识别库后，点击离线升级。如下图所示。



步骤3.进入[手动升级库]页面，点击<手动更新>，选择下载好的漏洞攻击特征识别库。如下图所示。

步骤4.点击<确定>，等待更新完成后，可以查看到漏洞攻击识别库已更新成功。如下图所示。



9.3. 排障

排障功能用于排查定位网络问题，方便管理员进行管理运维。

9.3.1. 故障排查

故障排查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，包括定向数据流分析、全局直通分析和二层调试直通。

9.3.1.1. 定向数据流分析

定向数据流分析针对单独的源IP、目的IP或域名进行分析，获取数据流的匹配详情，便于精准定位问题。建议在个别用户断网或个别服务/应用无法访问时使用，输入源IP地址或目的IP地址/域名进行定向分析，快速定位故障原因。

源IP地址、目的IP地址/域名：填写数据包的源IP和目的IP，二者必须填写一个，也可以全写，便于精确匹配。

协议：设置对符合指定协议类型数据包才输出到分析结果列表中，可选全部、TCP、UDP、ICMP、ICMPv6和其他等协议类型。

数据包定向直通：设置匹配的数据包是否开启策略放通。

数据包状态类型：设置匹配的数据包输出到分析结果列表中的状态是阻断或放行，在排查个别用户无法访问的问题时只选择阻断即可。

点击<开启定向数据流分析>后，会输出数据包的匹配详情到分析结果列表中。如下图所示。

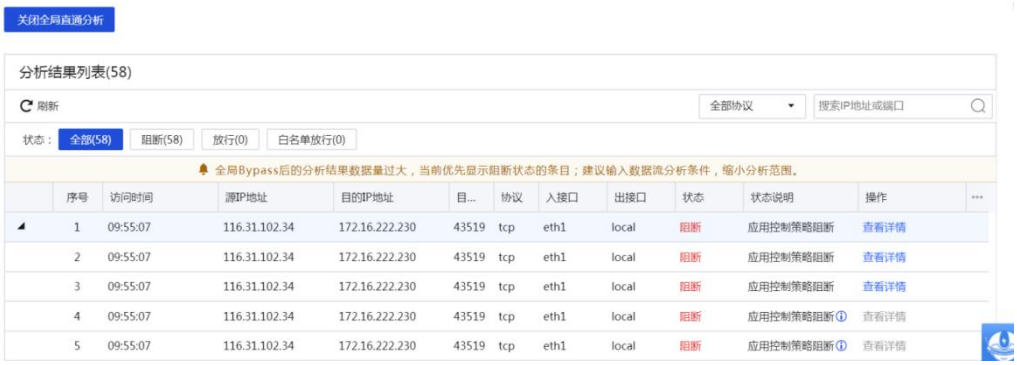
点击<刷新>实时查看数据包匹配的情况。点击<查看详情>可以看到该数据包具体策略匹配的情况。如下图所示。

在故障排查操作完成后，需要点击<关闭定向数据流分析>，使设备针对放通条件的地址策略继续生效，不再放通。

9.3.1.2. 全局直通分析

[全局直通分析]设备所有的策略都进行放通，不再进行防护，建议在无法定向分析的大面积网络中断时（如上架）使用。

点击<开启全局直通分析>后，会输出数据包的匹配详情到分析结果列表中。如下图所示。



点击<刷新>实时查看数据包匹配的情况。点击<查看详情>可以看到该数据包具体策略匹配的情况。如下图所示。

在故障排查操作完成后，需要点击<关闭全局直通分析>，使设备策略继续生效，不再全部放通。

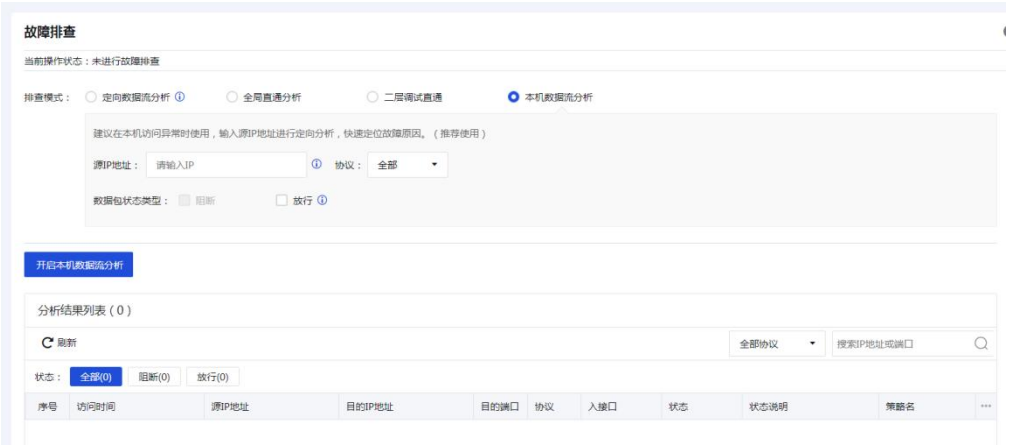
9.3.1.3. 二层调试直通

二层调试直通是在二层网络进行直通，数据包将在二层被Bypass，建议在通过前两种模式排查后仍不能查出故障原因的情况下使用。

在故障排查操作完成后，需要点击<关闭二层调试直通>。

9.3.1.4. 本机数据流分析

本机数据流分析是对于目的地址是本机的流量，单独有一个本机数据流分析模式，专门用于本机的入向流量分析，方便用户或者技术支持人员分析本机流量的阻断情况。具体界面如下图所示。

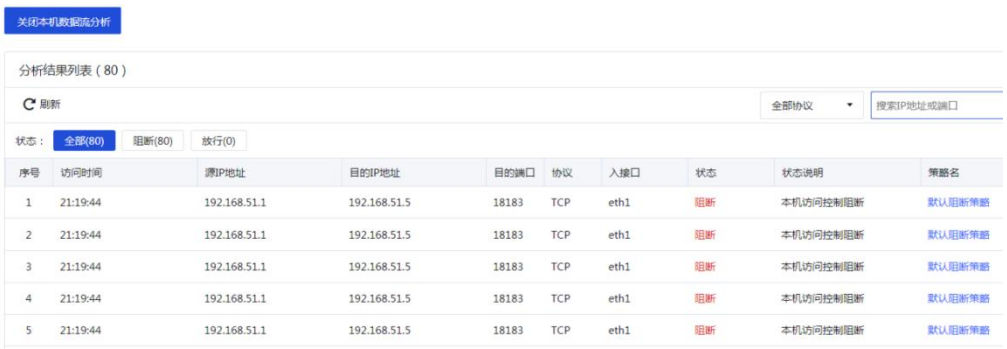


源IP地址：填写本机入向数据包的源IP地址过滤条件，支持单IP地址、IP地址范围、IP地址掩码格式配置方式。

协议：设置符合指定协议类型流量数据包才输出到分析结果列表中，可选全部、TCP、UPD、ICMP、ICMPv6和其他等协议类型。

数据包状态类型：开启放行开关，对于正常通过的报文信息也能进行跟踪记录，该记录一般为单条连接的首包。

点击<开启本机数据流分析>，开启本机数据流分析模式，可以输出本机入向数据包的匹配详情到分析结果列表中，并附上本机访问控制策略名称，点击可以跳转到对应的策略配置页面中，如下图所示。



点击<关闭本机数据流分析>，关闭本机数据流分析模式。

9.3.2. 分析工具

分析工具包括抓包工具和技术支持工具。

9.3.2.1. 抓包工具

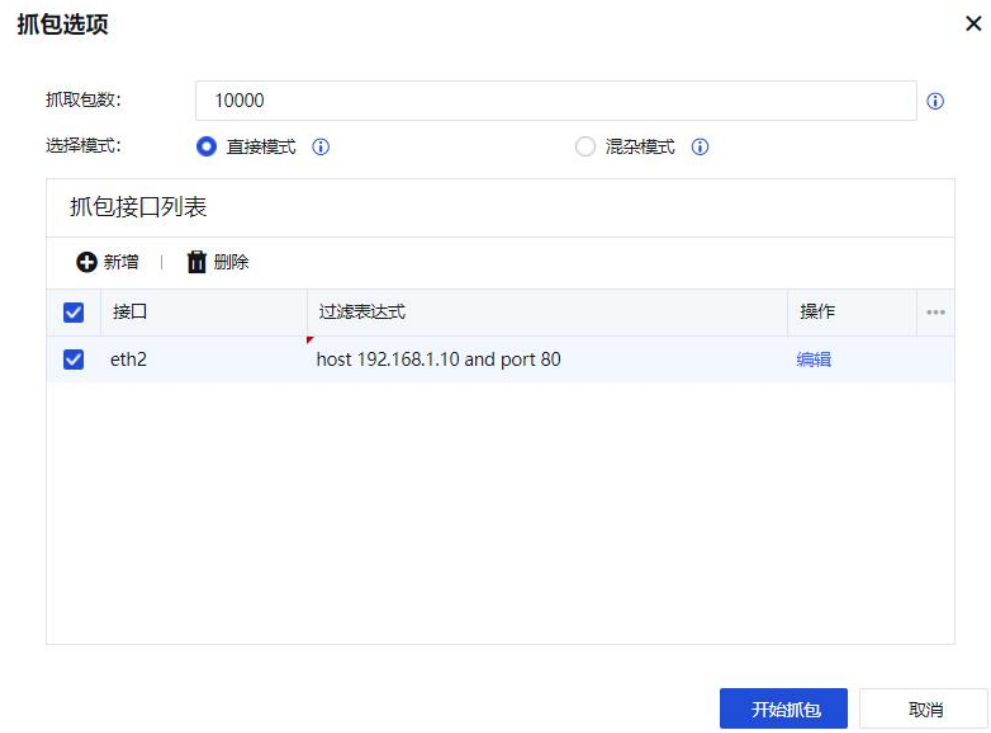
[抓包工具]用于对经过设备的数据包进行抓取，支持物理口、子接口、聚合口、vlan和vpntun等虚拟口抓包，可以同时进行多任务抓包，以便快速定位问题，可以作为排错的辅助工具。有普通抓包和循环抓包可以选择。

普通抓包：抓到对应个数的数据包就会停止。

循环抓包：会抓包24小时后停止，需要配置保存文件的个数和每个文件保存的抓包数。抓包文件数超过设置的文件数时会覆盖掉最前面的文件，最终只保留设置的文件个数，常用于排查偶现的网络问题。

例如抓取内网终端192.168.1.10访问外网80端口的数据包。

步骤1. 点击<新建抓包任务>，网口选择内网接口如eth2，IP地址填写192.168.1.10，端口填写80，如下图所示。

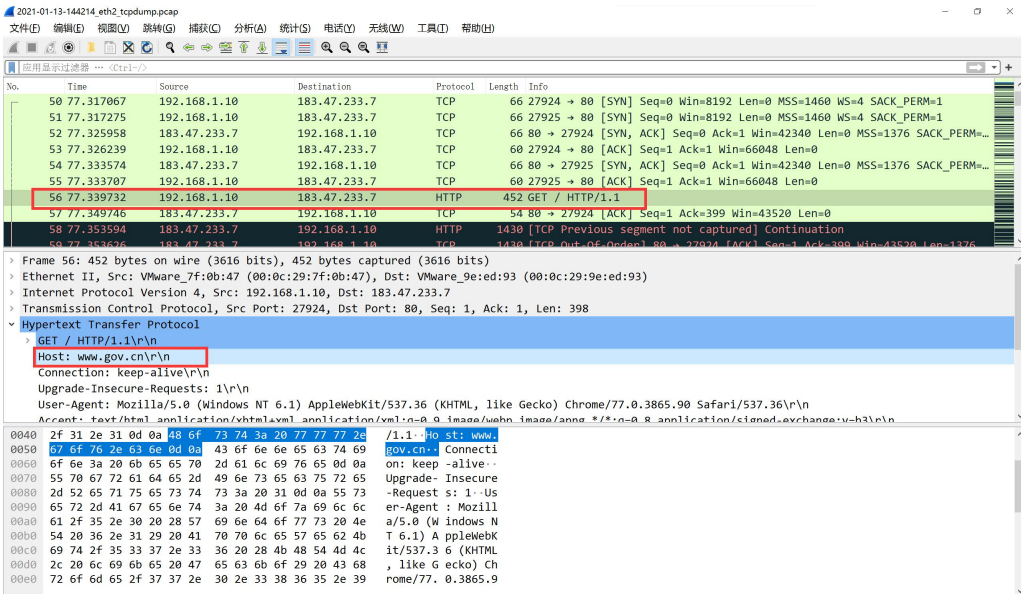


步骤1. 点击<开始抓包>，抓包程序开始运行，界面如下图所示。

步骤2. 在终端192.168.1.10上开始进行http访问，如打开http://www.gov.cn网页。

步骤3. 点击<停止抓包>后，再点击<下载>将数据包下载到本地。如下图所示。

步骤4. 数据包文件可用Sniffer或Ethereal、Wireshark等抓包软件进行查看，查看具体数据包信息。通过分析可以看到终端访问了http://www.gov.cn的网站，如下图所示。



9.3.2.2. 技术支持工具

[技术支持工具]用于技术支持人员对设备进行问题排查、巡检，方便对设备进行维护。

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。

9.3.3. 包回放工具

包回放工具可以高效地还原网络攻击，为网络取证、验证提供了一种有利手段，可自行准备样本包或通过云端获取.pacp样本包，然后导入并进行回放，回放结束可在安全日志中查看回放结果。

配置步骤

步骤1. 选择两个空闲接口建立虚拟网线，不能选择在使用的业务口，接口也需要禁用，以免影响实际业务。


编辑物理接口
基础信息
名称：
eth9
启用状态：
启用
禁用
1. 选择禁用
描述：
请输入描述（选填）
类型：
虚拟网线
2. 选择虚拟网线类型
区域：
poc_B
3. 创建/选择自定义区域xxx_B
接口一：
eth9
接口二：
eth8
4. 选中刚才创建的接口，可以快捷创建一个虚拟网线
基本属性：
WAN口
高级设置
工作模式：
IPv4 MTU：
1500
IPv6 MTU：
1500
巨帧：
开启
MAC地址：
fe:fc:fe:9e:89:74
恢复缺省MAC
确定
取消

步骤2. 新增一条应用控制策略，源区域和目标区域选择虚拟网线接口所在区域，服务为any，应用为全部，动作为允许。

步骤3. 新增一条业务防护策略，源区域和目的区域选择虚拟网线接口所在区域，关联好WEB应用防护、漏洞攻击防护、内容安全以及僵尸网络策略模板，动作为拒绝。

步骤4. 选择导入样本文件，支持pcap或.zip/.gz的压缩包，通用样本可通过点击<云端下载样本包>下载。

步骤5. 导入完成后，左侧会显示导入的样本压缩包。

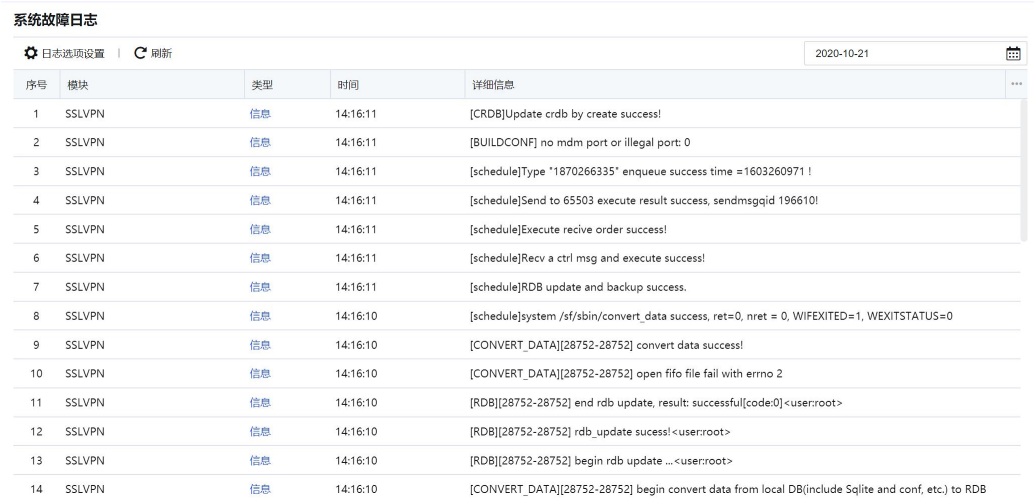
步骤6. 选择需要测试的样本包和虚拟网线，然后点击<立即回放>。

步骤7. 回放结束，显示统计结果。

步骤8. 点击<查看日志>，跳转到安全日志页面可以查看具体的日志信息。

9.3.4. 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，如下图所示。

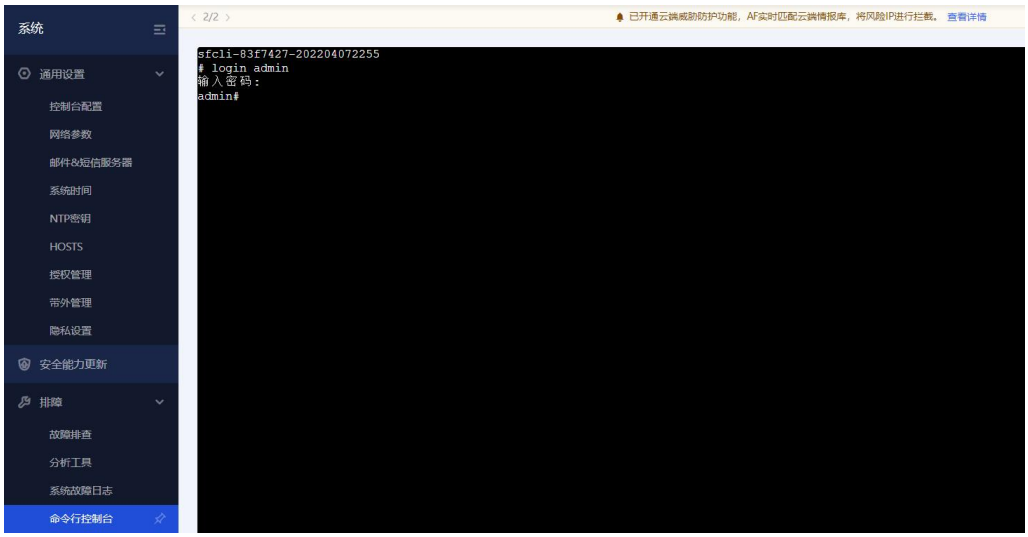


点击<日志选项设置>，出现[日志选项]页面，选择要查看的日志类型，如下图所示。

点击<确定>后，即显示所选日志信息。

9.3.5. 命令行控制台

WEB页面命令行控制台，可在Web页面使用命令行对设备进行配置操作、配置查看等操作，使用方式完全同通过SSH登录命令行，进入后可进行配置、查看等操作（需要在[系统/管理员账号]中开启对应管理员命令行权限），具体命令可参考命令行手册。



9.4. SNMP

SNMP用于支持其他网管设备或软件用SNMP方式来管理和查看深信服设备的相关信息，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。界面如下。

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。支持配置IPv6地址。

团体名：指定SNMP管理主机访问设备时的团体名。

权限：可设置SNMP管理者的权限，可选择“只读”或者“读写”。

点击<确定>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。

用户名称：添加该用户的名称。

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。

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。

加密算法：可选择“DES”或者“AES”加密算法

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，将以选择的机密算法进行加密。

权限：可设置SNMP管理者的权限，可选择“只读”或者“读写”。

点击<确定>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、双机切换、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）。

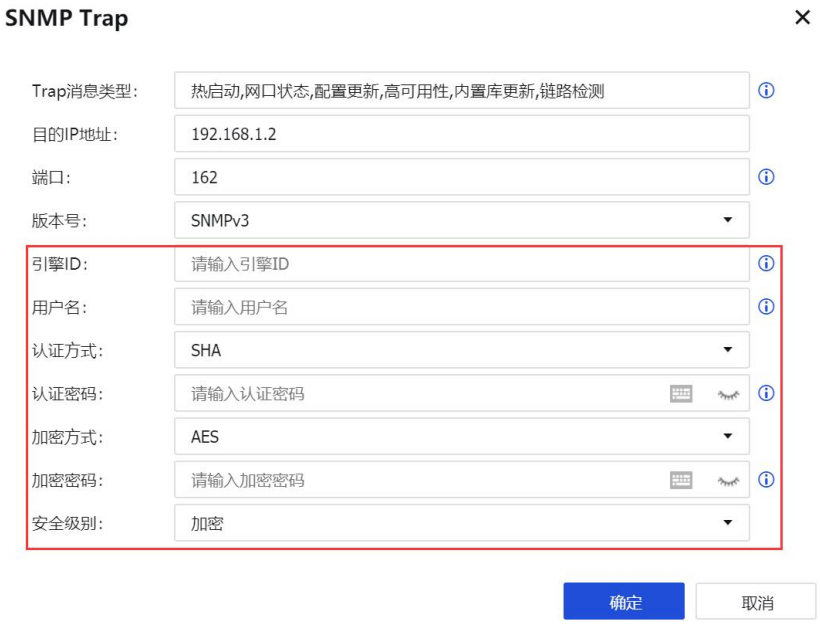
目的IP地址：设置发送SNMP Trap报文的目标主机地址，即SNMP客户端的IP地址，支持ipv4和ipv6地址。

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。

9.5. 管理员账号

管理员账号用来设置能够通过控制台来管理设备的登录用户和管理员角色管理。设备出厂默认的管理员的账号密码为：admin/admin。在导航菜单页面中的[系统管理/系统配置/管理员账户]，进入管理员账户页面，进行新增、编辑、删除、启用和禁用操作。

[管理员账号]用来设置能够通过控制台管理设备的登录用户。

默认已经有四个管理员角色，分别是超级管理员、安全管理员、审计员和系统管理员。

点击<新增>弹出[新增管理员账号]页面。如下图所示。

用户名：设置管理员账户名称。

启用状态：设置管理员账号状态启用或禁用。

描述：设置对该账户的描述。

认证类型：包括本地认证、远程认证和远程/本地认证，角色中去除远程认证用户，选择远程/本地认证时是优先通过已设置的外部服务器进行认证，当服务器无法连接时，通过本地进行认证。

角色：设置管理员账号的角色，共有以下四种角色可以选择其中系统管理员、审计管理员、安全管理员是三权分立账户。

普通管理员：普通管理员账户，可以具有所有模块管理权限。

系统管理员：负责对软件环境日常运行的管理和维护，具有基础网络配置，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相关模块的权限。

审计员：只具有查看监控日志的权限。

登录安全设置：设置管理员账户认证策略和管理方式。

认证策略：设置管理员账户的认证策略，有账号密码和账号密码+USB-KEY两种认证

方式可以选择。

管理方式：设置管理员账户管理设备的方式，共有以下四种管理方式。

Web控制台：允许通过WebUI及网页方式登录管理设备。

Web API：允许第三方平台通过Web API接口方式登录管理设备。

命令行：允许通过SSH方式登录管理设备。

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<密码安全策略>，用于设置控制台管理员密码的安全策略，可设置下次登录是否必须修改密码和密码最长使用天数。注意：只有admin管理员拥有设置此功能权限。

点击<外部认证服务器>，用于有外部服务器进行管理员账号的认证，认证方式有TACACS和RADIUS服务器。如下图所示。

9.6. 虚拟系统

虚拟系统（Virtual System），简称为VSYS(有厂商又称为lsys，逻辑系统)，能够将一台物理防火墙在逻辑上划分成多个虚拟防火墙，每个虚拟防火墙系统都可以被看成是一台完全独立的防火墙设备，可以拥有独立的系统资源，且能够实现防火墙的大部分功能。每个虚拟防火墙系统之间相互独立，不允许直接相互通信。

9.6.1. 虚拟系统介绍

9.6.1.1. 系统划分

AF设备上存在两种类型的虚拟系统：

根系统（Public）

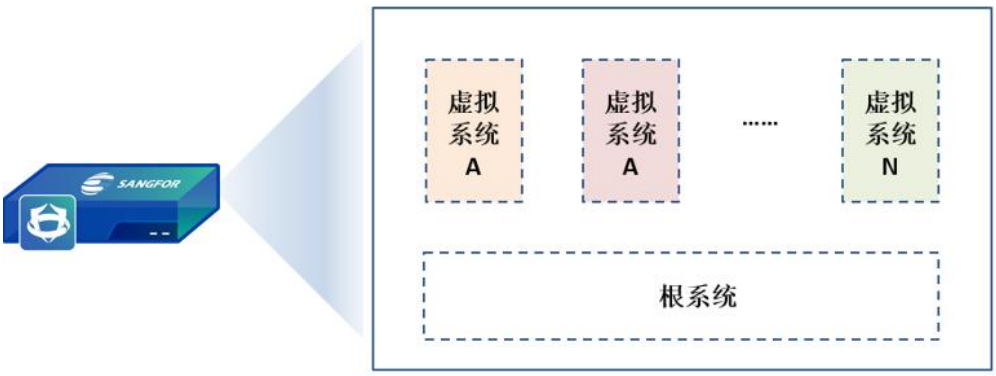
根系统是AF设备上缺省存在的一个特殊的虚拟系统。即使虚拟系统功能未启用，根系统也依然存在。此时，管理员对AF设备进行配置等同于对根系统进行配置。启用虚拟系统功能后，根系统会继承先前AF设备上的配置。

在虚拟系统这个特性中，根系统的作用是管理其他虚拟系统，并为虚拟系统间的通信提供服务。

虚拟系统(VSYS)

虚拟系统是在AF设备上划分出来的、独立运行的逻辑设备。

虚拟系统划分的逻辑结构如下图所示。



为了实现每个虚拟系统的业务都能够做到正确转发、独立管理、相互隔离，AF设备主要实现了几个方面：

资源虚拟化：根系统管理员可以为每个虚拟系统分配固定的系统资源，包括接口、VLAN、策略和会话等，各个虚拟系统自行管理和使用。保证不会因为一个虚拟系统

的业务繁忙而影响其他虚拟系统。

配置虚拟化：每个虚拟系统都拥有独立的虚拟系统管理员和配置界面（CLI/WEB），每个虚拟系统管理员只能管理自己所属的虚拟系统，根系统管理员可以管理所有虚拟系统。使得多个虚拟系统的管理更加清晰简单，所以非常适合大规模的组网环境。

路由虚拟化：每个虚拟系统都拥有各自的路由表，相互独立隔离。，这使得虚拟系统下的局域网即使使用了相同的地址范围，仍然可以正常进行通信。

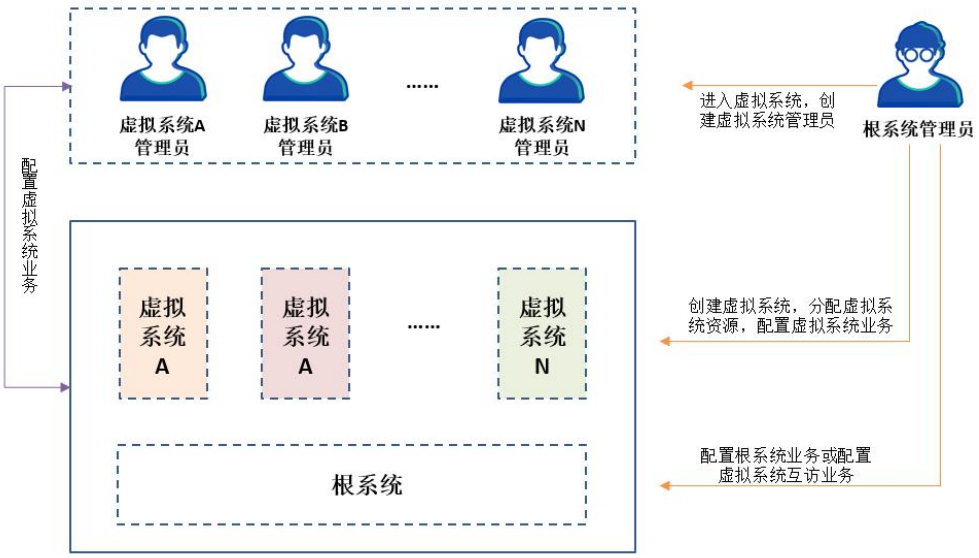
交换虚拟化：每个虚拟系统都拥有各自的MAC转发表、ARP表，相互独立隔离。

日志隔离：每个虚拟系统都拥有各自的日志文件、日志显示界面。

通过以上几个方面，当创建虚拟系统之后，每个虚拟系统的管理员都像在使用一台独占的设备。

9.6.1.2. 管理员划分

根据虚拟系统的类型，管理员分为根系统管理员和虚拟系统管理员。两类管理员的作用范围和功能都不相同，如下图所示。



根系统管理员

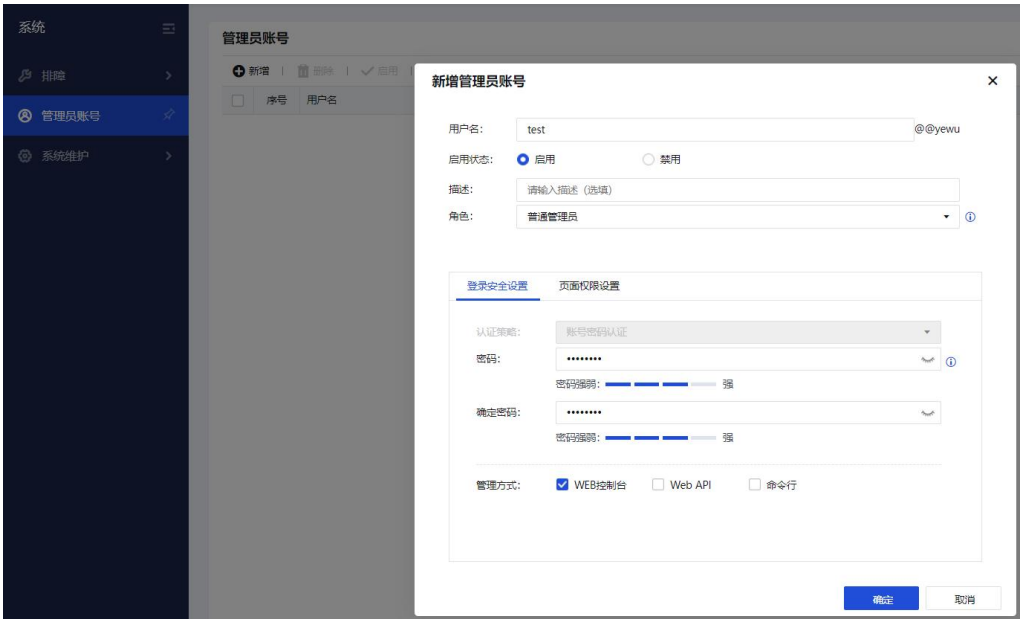
启用虚拟系统功能后，设备上已有的管理员将成为根系统的管理员。管理员的登录方式、管理权限、认证方式等均保持不变。根系统管理员负责管理和维护设备、配置根系统的业务。

只有具有系统管理权限的根系统管理员才可以进行虚拟系统相关的配置，如创建、删除虚拟系统，为虚拟系统分配资源等。

虚拟系统管理员

创建虚拟系统后，根系统管理员可以为虚拟系统创建一个超级管理员和多个其他管理员。虚拟系统管理员的作用范围与根系统管理员有所不同：虚拟系统管理员只能进入其所属的虚拟系统的配置界面，能配置和查看的业务也仅限于该虚拟系统；根系统管理员可以进入所有虚拟系统的配置界面，如有需要，可以配置任何一个虚拟系统的业务。

为了正确识别各个管理员所属的虚拟系统，虚拟系统管理员用户名格式统一为“管理员名@@虚拟系统名”，如下图所示。



9.6.1.3. 资源分配

合理地分配资源可以对单个虚拟系统的资源进行约束，避免因某个虚拟系统占用过多的资源，导致其他虚拟系统无法获取资源、业务无法正常运行的情况。

区域、策略、会话等实现虚拟系统业务的基础资源支持定额分配或手工分配，其中：

定额分配：此类资源直接按照系统规格自动分配固定的资源数（如区域、对象、管理员等），不支持用户手动分配。

手工分配：此类资源支持用户通过命令行或Web界面中的资源类界面手动分配（如会话、策略等）。

此外，其他的资源项则是各个虚拟系统一起共享抢占整机资源，同样不支持用户手动分配。

定额分配和手工分配的资源如下表所示。

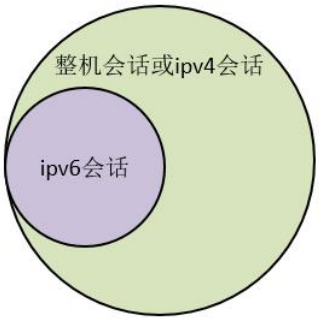
表26 资源分配表

资源名称	分配方式	具体说明
接口	手工分配	1、支持分配给虚拟系统的接口类型包括：三层以太网接口，三层以太网子接口，三层聚合口子接口，虚拟接口； 2、二层接口不支持直接分配给虚拟系统。使用assign vlan命令将VLAN分配给虚拟系统后，二层接口会随VLAN分配给相应的虚拟系统。Trunk类型的二层接口可以随VLAN分配给多个虚拟系统，各个虚拟系统下可配置该接口，例如接口加入安全区域； 3、当存在三层VLAN接口时，使用assign vlan命令将VLAN分配给虚拟系统时，对应的三层VLAN接口会同步分配给虚拟系统。三层VLAN接口也可直接分配给虚拟系统，此时对应的三层VLAN接口会同步分配给虚拟系统； 4、管理口eth0不能分配给虚拟系统。
VLAN	手工分配	对应的三层VLAN接口会同步分配给虚拟系统
IPv4会话	手工分配	
IPv6会话	手工分配	
应用控制策略	手工分配	
NAT44策略	手工分配	
NAT66策略	手工分配	
NAT64策略	手工分配	
本机访问控制	定额分配	默认存在2条，上限32条
网络对象	定额分配	与设备型号相关，50-2048个
服务	定额分配	预定义服务：73个

		自定义服务：512个
时间计划	定额分配	64个
区域	定额分配	30个
静态路由	定额分配	与设备型号相关，512-2048个
策略路由	定额分配	与设备型号相关，256-2048个
管理员	定额分配	根系统容量：30个 虚拟系统：5个，默认不存在管理员

管理员为虚拟系统手工分配资源时，首先需要配置资源类，并在资源类中指定各个资源项的保证值和最大值，然后将资源类与虚拟系统绑定。虚拟系统可以使用的资源数量就受资源类中配置的保证值和最大值控制。

保证值：虚拟系统可使用某项资源的最小数量。这部分资源一旦分配给虚拟系统，就被该虚拟系统独占。



说明：

1、AF 的 ipv4 会话和 ipv6 会话资源是共享的，例如整机会话资源为 N，那么 ipv4 会话资源为 N，ipv6 会话资源为 N/2；
2、当会话剩余资源（使用量+已保证值）>会话的保证值，此时会话的保证值是有效的，否则会话的保证值无法做到真实保留，当会话释放出来，会优先进行保留；
3、策略数的保证值=最大值=至少最多可用数。

最大值：虚拟系统可使用某项资源的最大数量。虚拟系统可使用的资源能否达到最大值视其他虚拟系统对该项资源的使用情况而定。

例如，AF上配置了10个虚拟系统。假定AF会话数的整机规格为500000，虚拟系统A的会话数保证值为10000、最大值为50000。虚拟系统A可建立的会话数一定能达到10000，但能否达到最大值50000，则视其他虚拟系统的会话资源使用情况而定。如果其他9个虚拟系统和根系统当前的会话数总和小于450000，虚拟系统A可建立的会

话数就能达到50000。

如果虚拟系统不绑定资源类，则虚拟系统的资源不受限制，虚拟系统和根系统以及其他未绑定资源类的虚拟系统一起共同抢占整机的剩余资源。如果虚拟系统绑定的资源类对某些资源项未指定最大值和保证值，则虚拟系统的这些资源项不受限制，虚拟系统和根系统以及其他未限定该资源项的虚拟系统一起共同抢占整机的剩余资源。

共享抢占的资源包括：CPU、内存、链路探测、OSPF和各种表项（如ARP表、MAC地址表）等。

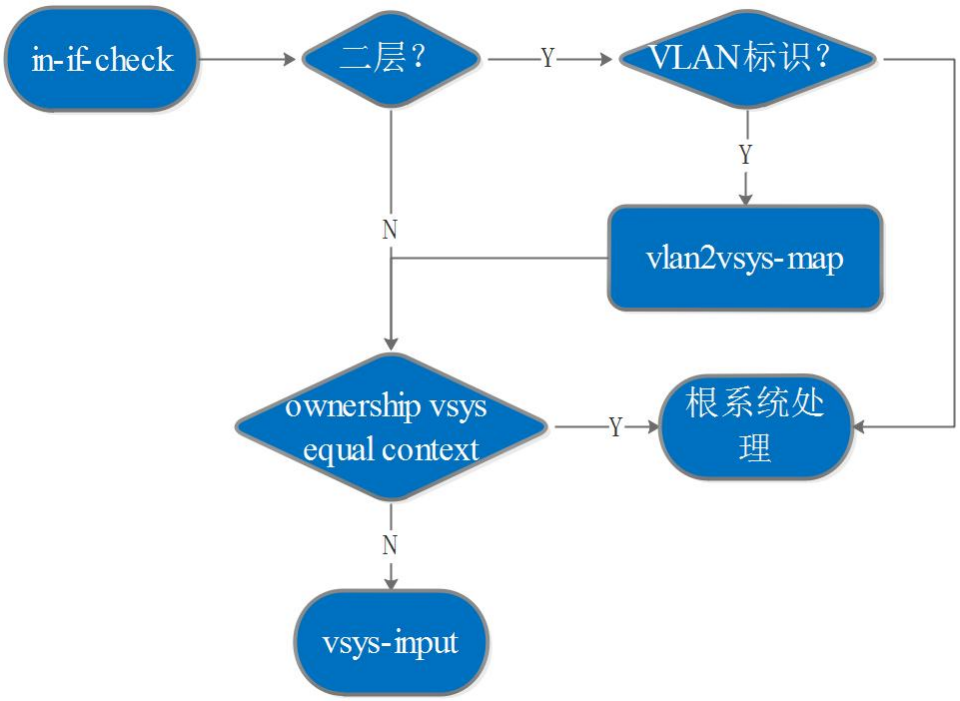
9.6.1.4. 虚拟系统的分流

通过分流能将进入设备的报文送入正确的虚拟系统处理。

AF上未配置虚拟系统时，报文进入AF后直接根据根系统的策略和表项（会话表、MAC地址表、路由表等）对其进行处理。AF上配置了虚拟系统时，每个虚拟系统都相当于一台独立的设备，仅依据虚拟系统内的策略和表项对报文进行处理。因此，报文进入AF后，首先要确定报文与虚拟系统的归属关系，以决定其进入哪个虚拟系统进行处理。我们将确定报文与虚拟系统归属关系的过程称为分流。

AF支持基于接口分流、基于VLAN分流二种分流方式。接口工作在三层时，采用基于接口的分流方式；接口工作在二层时，采用基于VLAN的分流方式。

具体分流过程如下图所示。



三层口分流：

1. 检测接口所属vsys ID和根系统vsys ID是否一致；
2. 如果不一致，则进入接口所属的虚拟系统转发入口处理；如果一致则在根系统继续处理当前数据包。

二层口分流：

1. 检测数据包VLAN ID标识；
2. 如果存在VLAN ID，则匹配VLAN ID到vsys ID的映射表，否则在根系统继续处理当前数据包；
3. 匹配映射表后，检测接口所属vsys ID和根系统vsys ID是否一致；
4. 如果不一致，则进入接口所属的虚拟系统转发入口处理；如果一致则在根系统继续处理当前数据包。

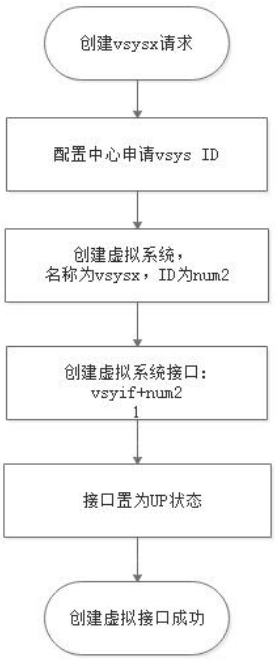
9.6.1.5. 虚拟接口

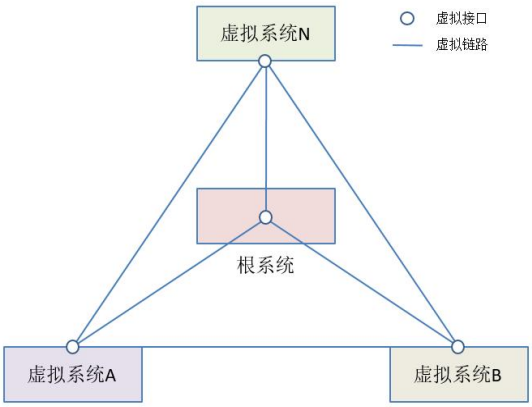
虚拟系统之间通过虚拟接口实现互访。

虚拟接口是创建虚拟系统时系统自动为其创建的一个逻辑接口，作为虚拟系统自身与其他虚拟系统之间通信的接口。虚拟接口的链路层和协议层始终是UP的。在虚拟系统互访场景下，虚拟接口必须配置IP地址并加入安全区域，否则无法正常工作。

虚拟接口名的格式为“vsysif+接口号”，根系统的虚拟接口名为vsysif0，其他虚拟系统的vsysif接口号从1开始，根据系统中接口号占用情况自动分配。

如下图所示，各个虚拟系统以及根系统的虚拟接口之间默认通过一条“虚拟链路”连接。如果将虚拟系统、根系统都视为独立的设备，将虚拟接口视为设备之间通信的接口，通过将虚拟接口加入安全区域并按照配置一般设备间互访的思路配置路由和策略，就能实现虚拟系统和根系统的互访、虚拟系统之间的互访。

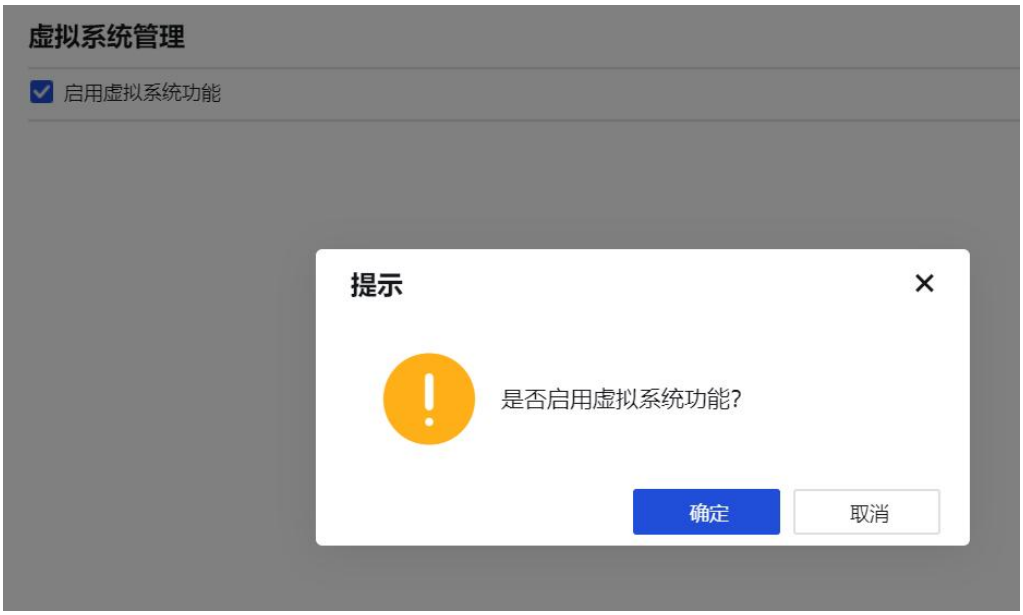




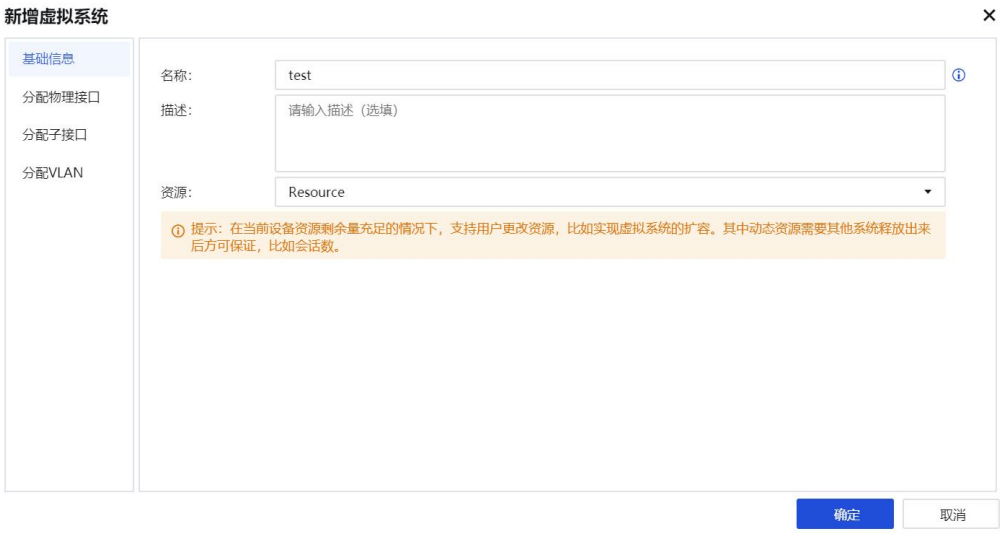
9.6.2. 虚拟系统管理

虚拟系统管理用于启用虚拟系统功能，并在此新增虚拟系统，进行资源池分配，划分物理接口、子接口和VLAN接口。

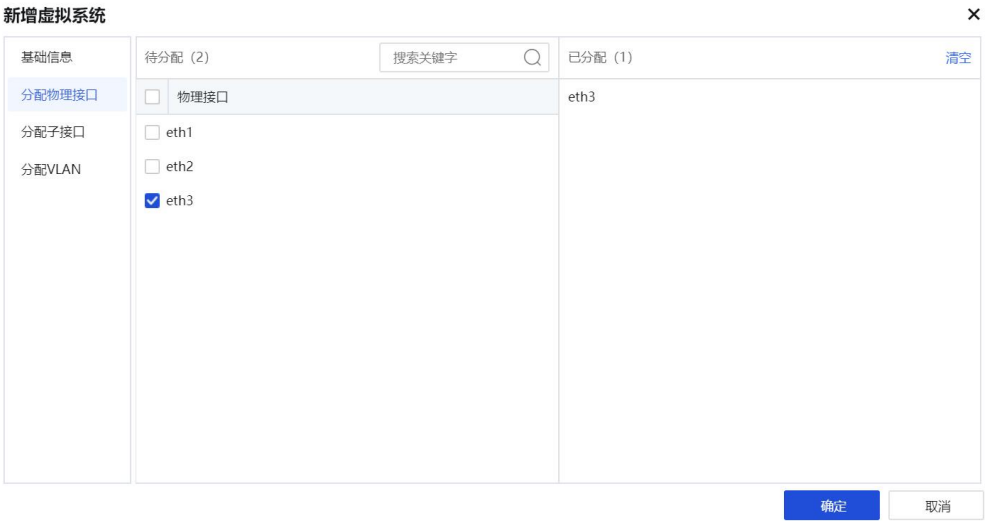
点击<启用虚拟系统>，如下图所示。



启用完成后，点击<新增>，设置虚拟系统名称和资源，资源调用[系统/虚拟系统/资源池]中的设置，如有自定义资源可自行选择，如下图所示。



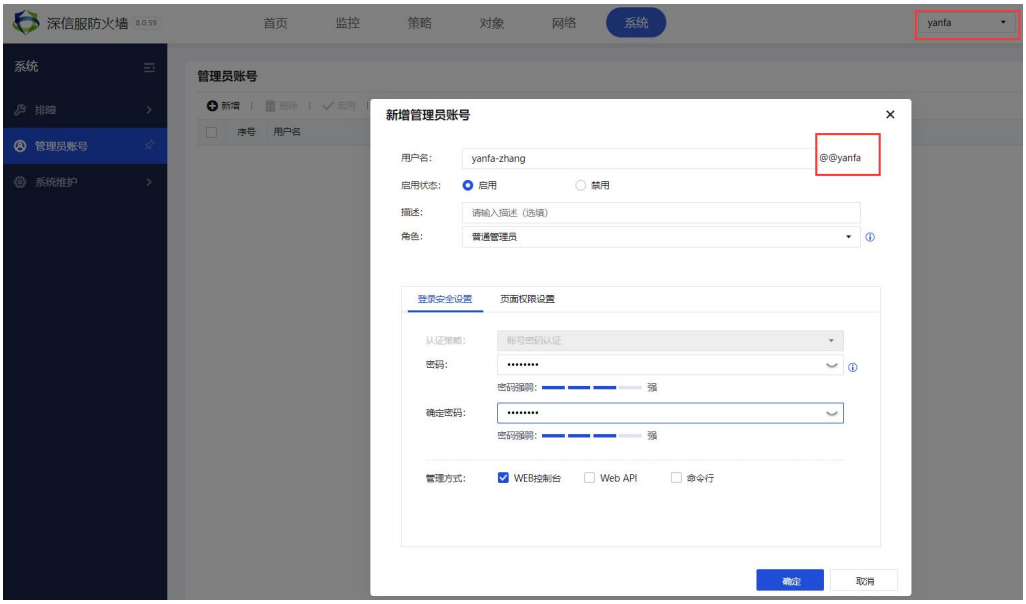
再根据实际情况进行物理接口的分配，如下图所示。



如有需要可再进行分配子接口和分配VLAN操作。

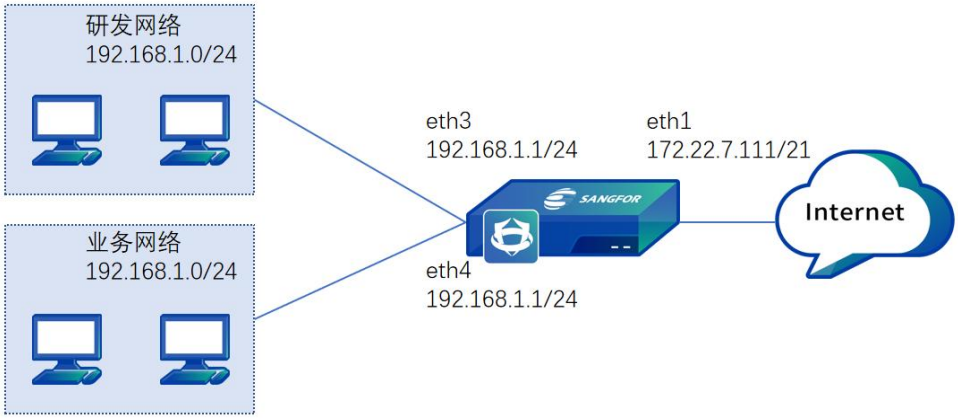
系统创建完成后，根系统管理员可通过页面右上角进行系统的切换，如下图所示。

如需建立虚拟管理员给对应网络运维人员管理，可在对应虚拟系统[系统/管理员账号]中新增管理员，并在对应分配的虚拟系统接口上勾选WEBUI选项即可通过该接口登录管理。

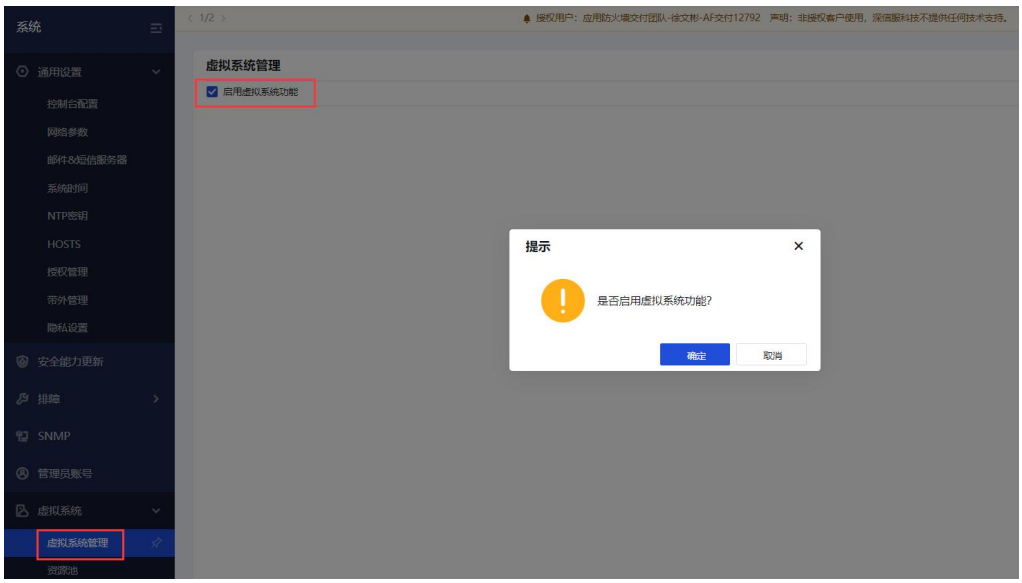


虚拟系统配置案例

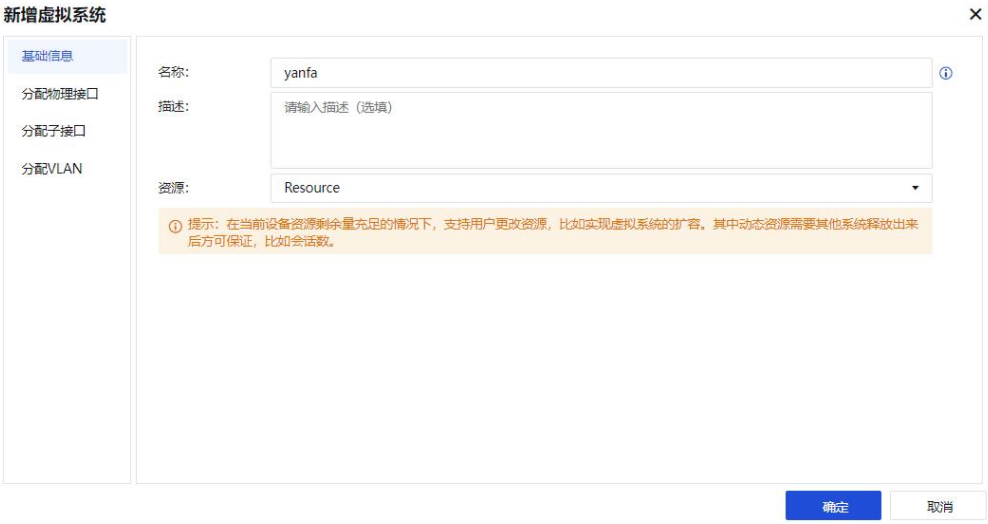
某企业购买了AF做网关部署在集团公司网络出口，有研发网络和业务网络通过该出口访问互联网，两个网络网段都为192.168.1.0/24，需要在AF上虚拟出两个防火墙进行单独管理，两个网络间不需要互访，业务网络可以访问互联网所有应用，研发网络只能访问互联网网页服务，拓扑如下图所示。

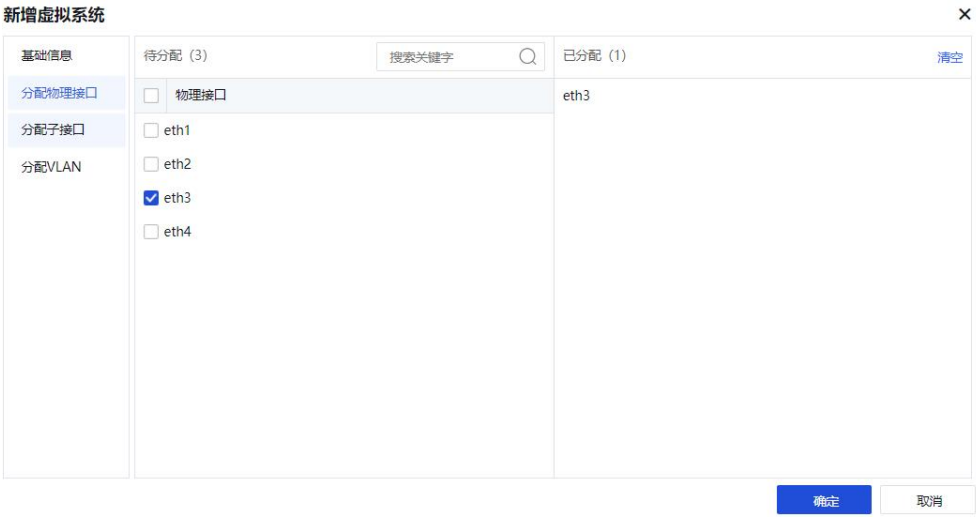


步骤1. 进入[系统/虚拟系统/虚拟系统管理]，启用虚拟系统。



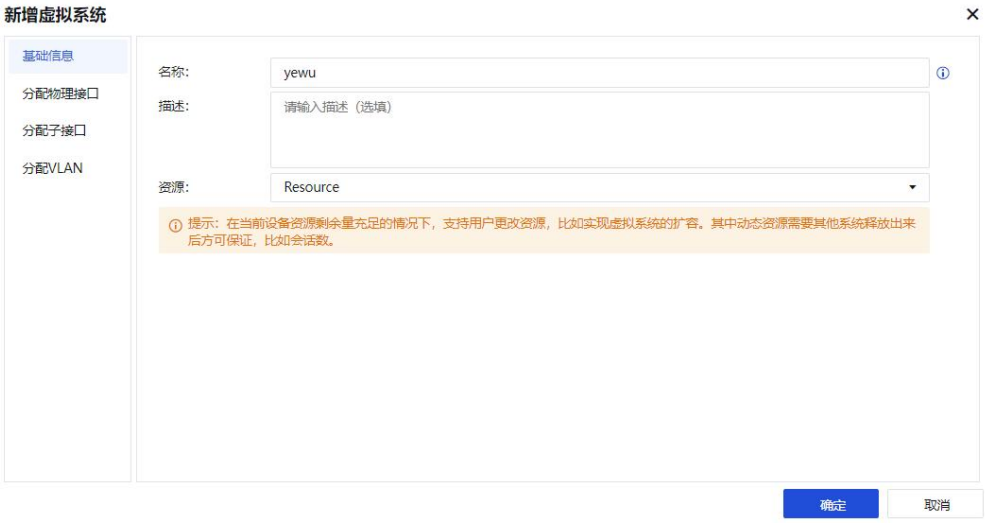
步骤2. 点击<新增>，配置“yanfa”虚拟系统，关联资源（可使用默认资源池“Resource”也可根据实际需要分配资源池），并分配物理接口eth3。

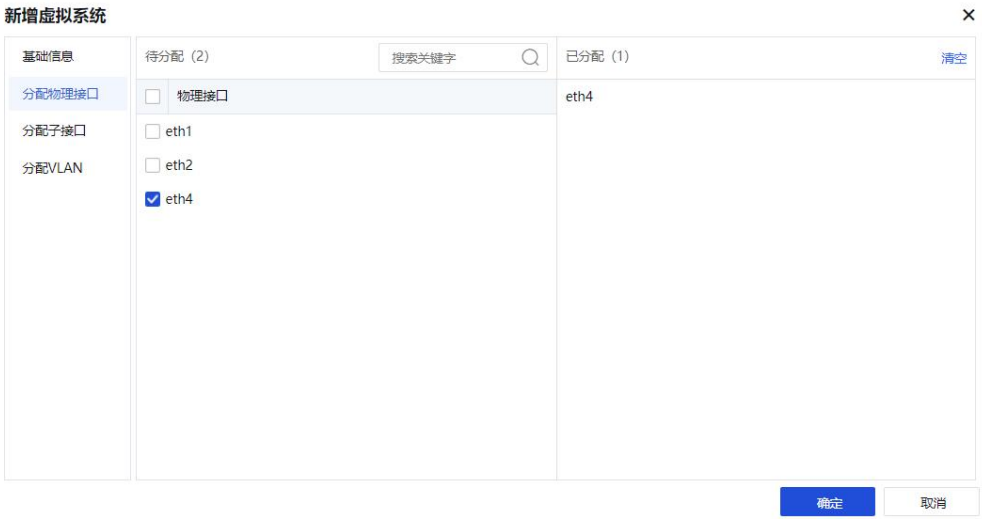




步骤3. 点击<新增>，配置“yewu”虚拟系统，关联资源（可使用默认资源池“Resource”

也可根据客户实际需要分配资源池），并分配物理接口eth4。

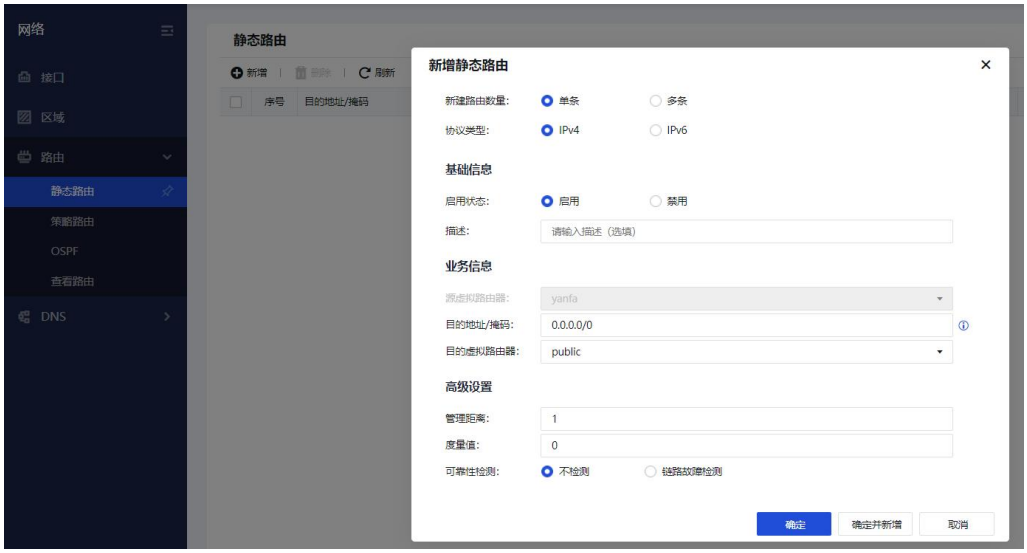




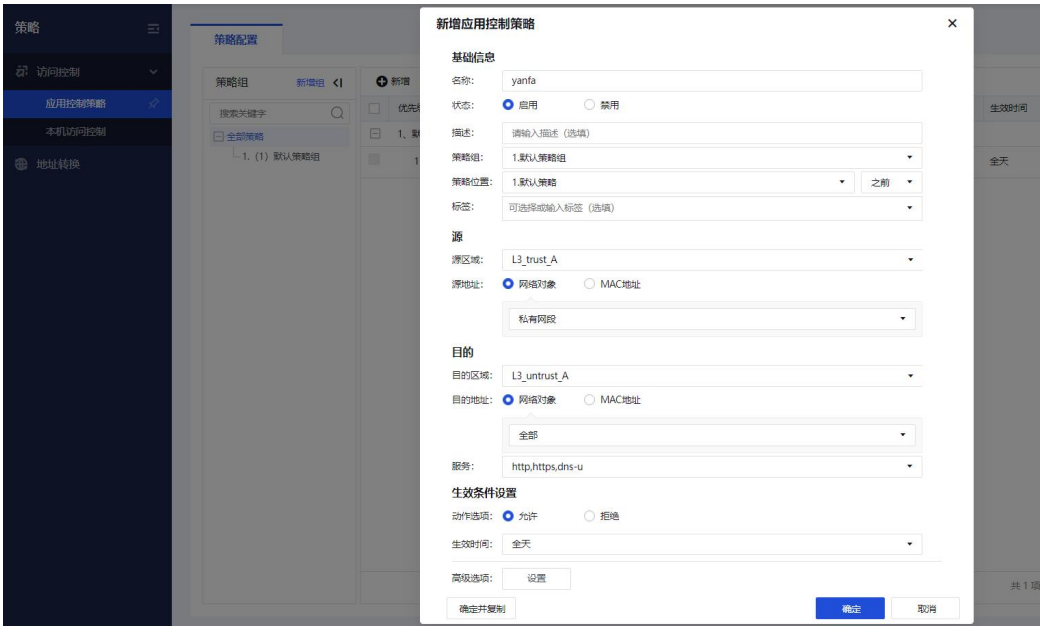
步骤4. 进入“yanfa”虚拟系统[网络/接口/物理接口]配置eth3的区域和IP地址192.168.1.1/24。

步骤5. 在“yanfa”虚拟系统[网络/接口/虚拟接口]配置vsysif1的区域和IP地址172.16.1.1/24。

步骤6. 在“yanfa”虚拟系统[网络/路由/静态路由]配置默认路由指向目的虚拟路由器根系统“public”。

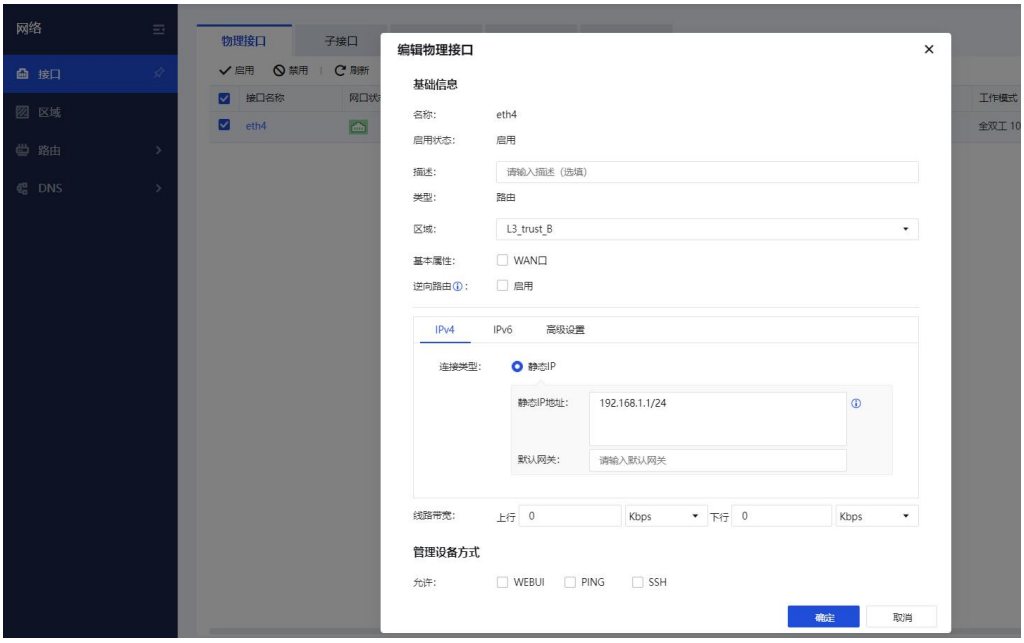


步骤7. 在“yanfa”虚拟系统[策略/访问控制/应用控制策略]新增放通对应区域http、https和dns服务。



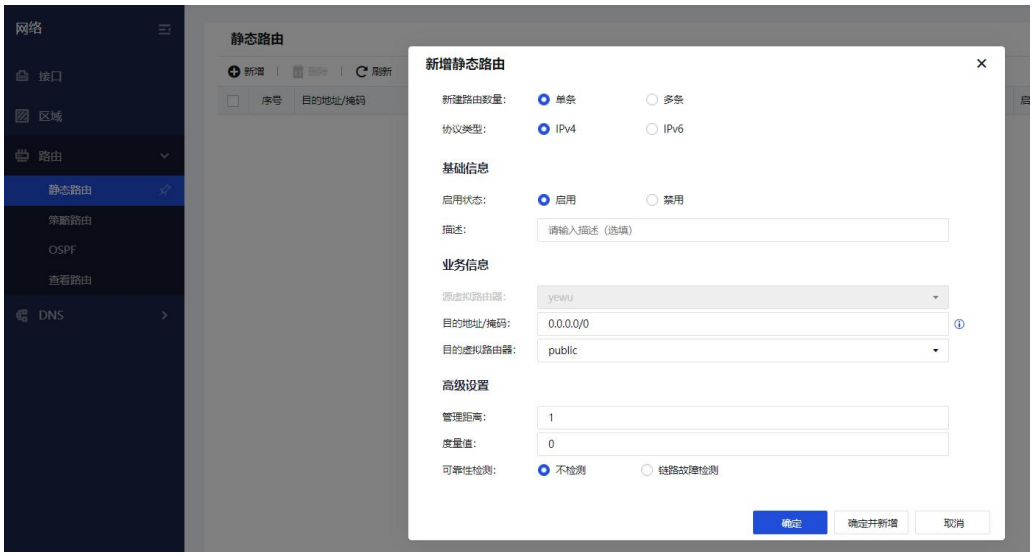
步骤8. 在“yanfa”虚拟系统[策略/地址转换/IPv4地址转换]配置对应区域的源地址转换，源地址转换为出接口地址。

步骤9. 切换到“yewu”虚拟系统[网络/接口/物理接口]配置eth4的区域和IP地址192.168.1.1/24。

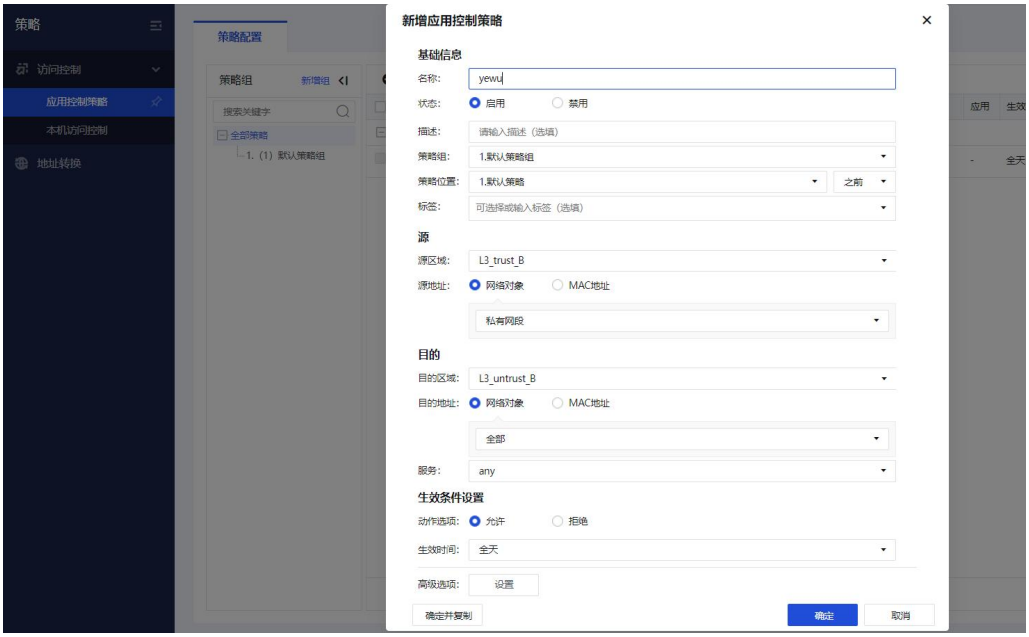


步骤10. 在“yewu”虚拟系统[网络/接口/虚拟接口]配置vsysif2的区域和IP地址172.16.2.1/24。

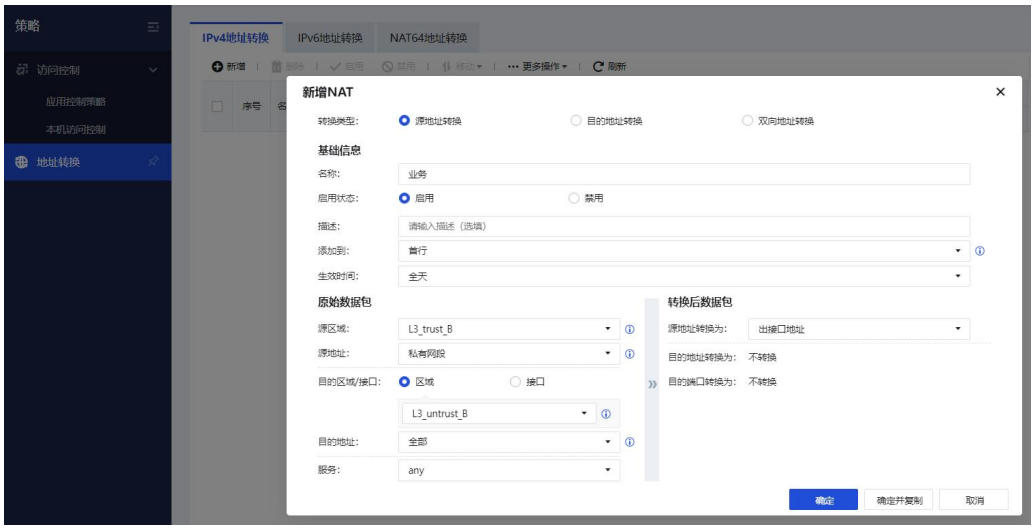
步骤11. 在“yewu”虚拟系统[网络/路由/静态路由]配置默认路由指向目的虚拟路由器根系统“public”。



步骤12. 在“yewu”虚拟系统[策略/访问控制/应用控制策略]新增放通对应区域所有服务。

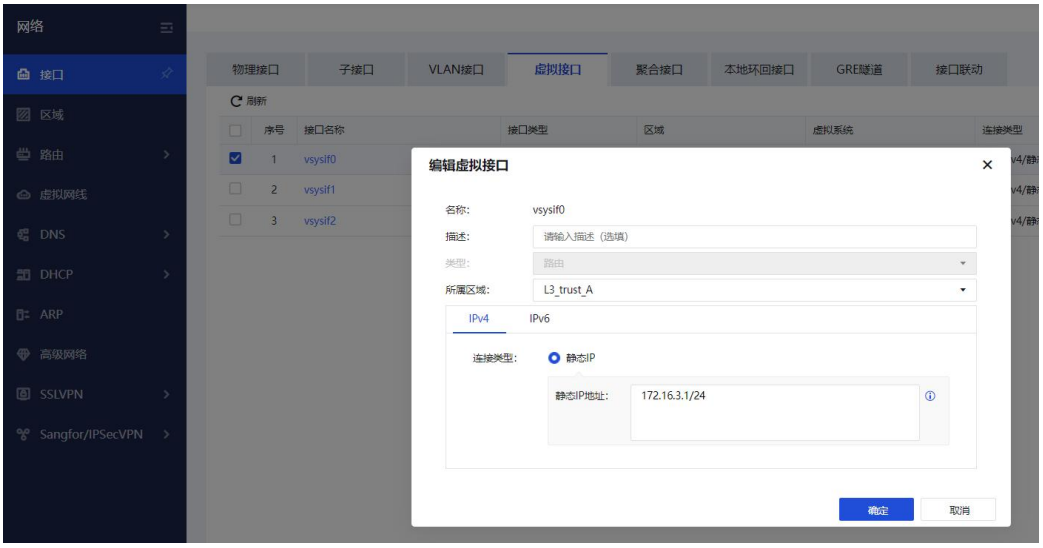


步骤13. 在“yewu”虚拟系统[策略/地址转换/IPv4地址转换]配置源地址转换，源地址转换为出接口地址。



步骤14. 切换到“public”根系统[网络/接口/物理接口]配置eth1的区域和IP地址172.22.7.111/21。

步骤15. 在根系统[网络/接口/虚拟接口]配置vsysif0的区域和IP地址172.16.3.1/24。

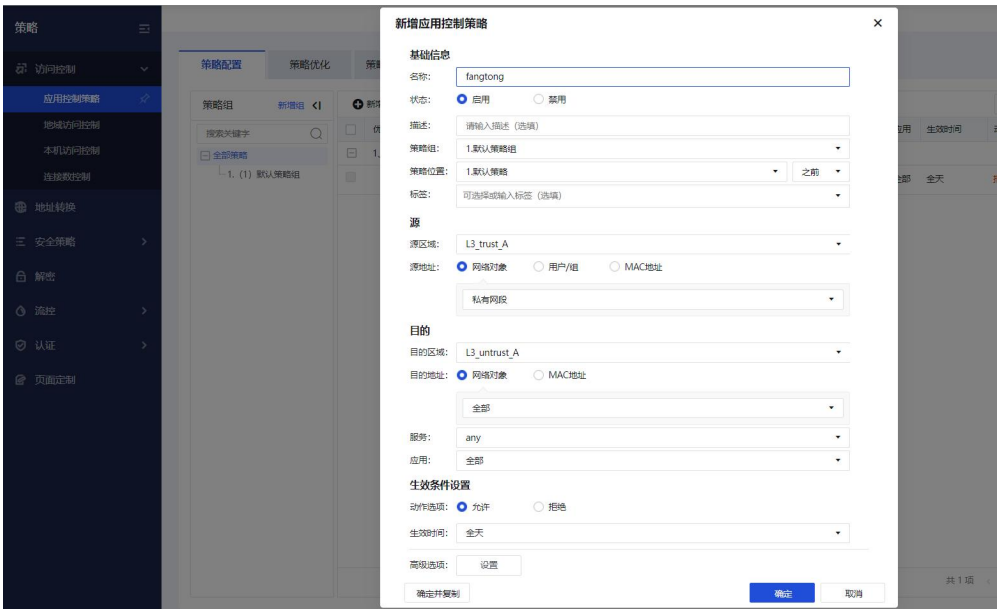


步骤16. 在根系统[网络/路由/静态路由]配置默认路由指向互联网出口下一跳，并配置静态路由分别指向目的虚拟路由器“yanfa”和“yewu”，目的IP是vsys1和vsys2的接口地址。

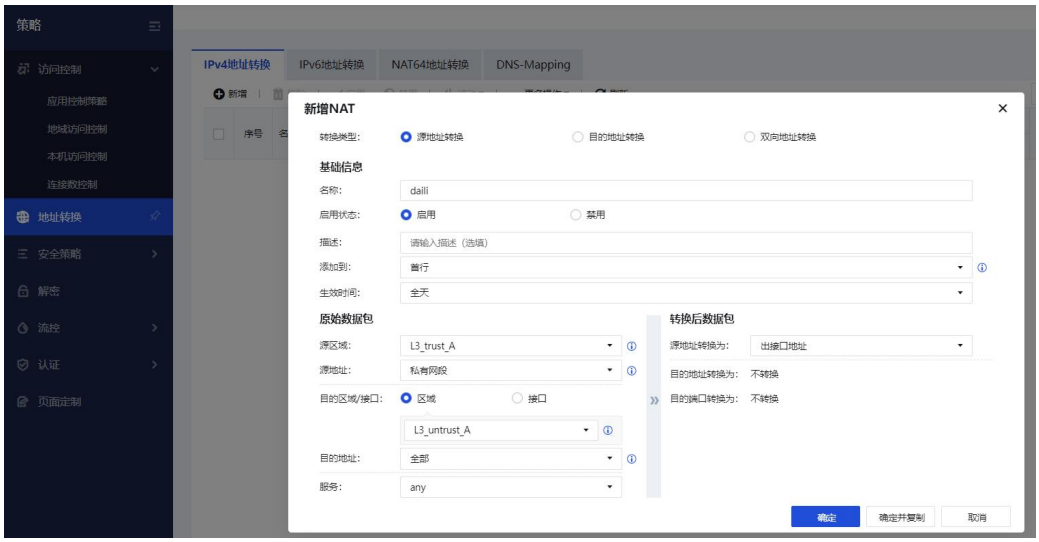

编辑静态路由
协议类型:
IPv4
IPv6
基础信息
启用状态:
启用
禁用
描述:
请输入描述（选填）
业务信息
源虚拟路由器:
public
目的地址/掩码:
0.0.0.0/0
目的虚拟路由器:
public
接口:
自动选择接口
下一跳地址:
172.22.7.254
高级设置
管理距离:
1
度量值:
0
可靠性检测:
不检测
链路故障检测
确定
取消


新增静态路由
新建路由数量:
单条
多条
协议类型:
IPv4
IPv6
基础信息
启用状态:
启用
禁用
描述:
请输入描述（选填）
业务信息
源虚拟路由器:
public
目的地址/掩码:
172.16.1.1/24
目的虚拟路由器:
yanfa
高级设置
管理距离:
1
度量值:
0
可靠性检测:
不检测
链路故障检测
确定
确定并新增
取消

步骤17. 在根系统[策略/访问控制/应用控制策略]新增放通对应区域所有服务。



步骤18. 在根系统[策略/地址转换/IPv4地址转换]配置源地址转换，源地址转换为出接口地址。

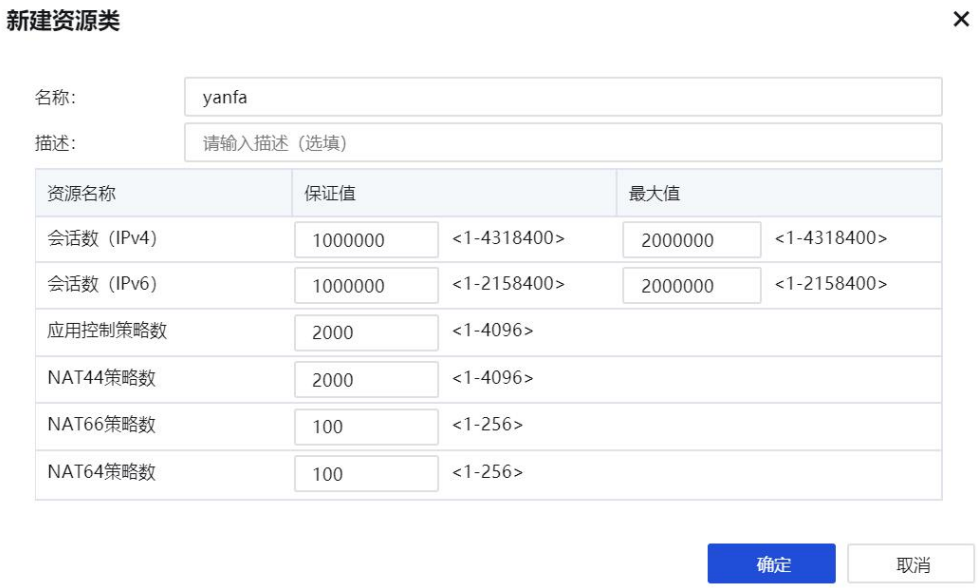


步骤19. 配置完成，研发网络和业务网络终端分别进行上网验证。

9.6.3. 资源池

资源池可以进行手工分配资源的保证值和最大值的设置，供虚拟系统调用该资源池。

点击<新增>，出现如下页面，按照实际需要进行设置。



9.7. 系统维护

系统维护是指为适应系统的环境和其他因素的各种变化、保证系统正常工作而对系统所进行的修改，包括备份与恢复、系统升级、升级日志、重启网关/服务和补丁更新等功能模块。

9.7.1. 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<下载当前配置>，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30天的配置文件，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。

恢复出厂配置：从默认配置中恢复，点击<恢复出厂配置>，可以将设备恢复到出厂状态。

⚠ 注意：

恢复配置或者恢复出厂配置都会导致设备重启，请在恢复之前确认是否可以断网，建议在无业务或者业务低峰时间段操作，避免影响正常业务。

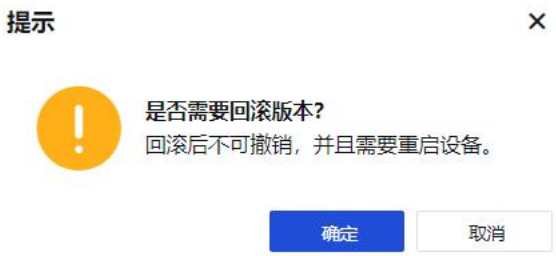
9.7.2. 系统升级

[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。如下图所示。

详细步骤在产品升级指导，有两种操作升级方式，web控制台页面升级和BBC下发升级。

点击[查看升级历史]，可以查看历史的升级记录。如下图所示。

点击[版本回滚]，可以回滚到升级前的版本，会重启设备，同时配置也会恢复到升级前的配置，属于高危操作，只有在升级后版本有问题无法解决时才做此操作。



9.7.3. 升级日志

升级日志主要是展示新版本的亮点功能，能够快速了解新版本新增以及优化的功能，如下图所示。

9.7.4. 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，重启设备和重启全部服务都会断网和影响业务，请谨慎操作。如下图所示。

9.7.5. 补丁更新

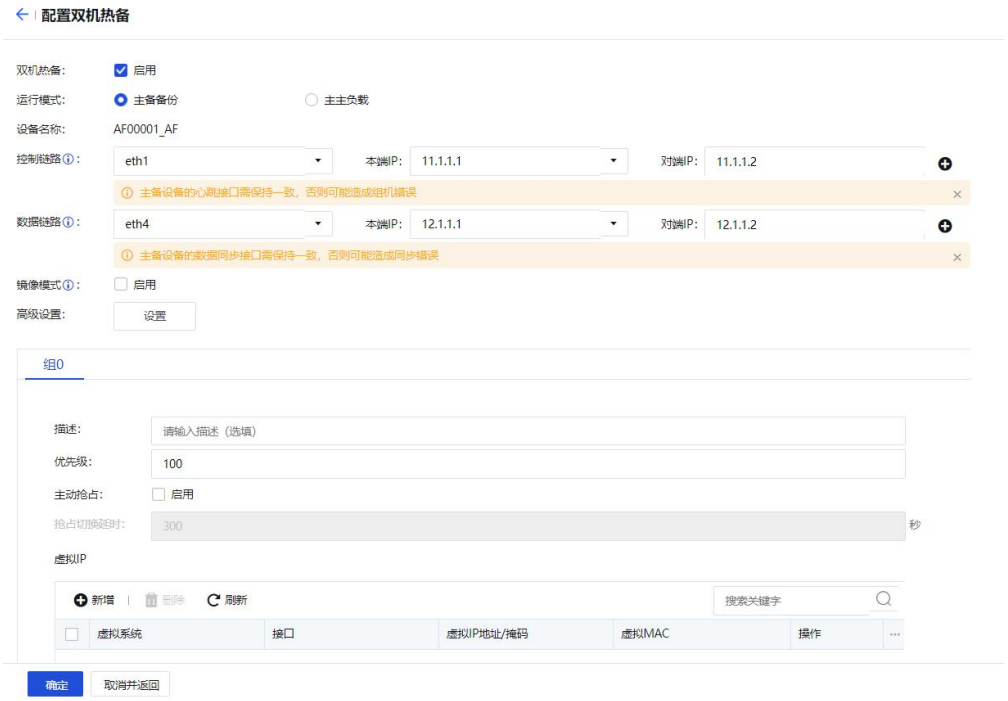
[补丁更新]主要用于获取并更新系统版本的补丁包。详细配置请参考补丁更新指导。

9.8. 高可用性

9.8.1. 基本介绍

高可用性是为了避免单点故障的隐患，采用双机模式是保证业务连续性的一种有效解决方案，能够在很大程度上避免了网络业务的中断，主要是在对网络可靠性较高，业务连续性强的场景中使用。

点击<配置>，界面如下。



双机热备：勾选启用后可以进行双机热备的配置。

运行模式：设置双机的模式，可以选择主备备份和主主负载两种模式。

控制链路：负责传递双机心跳报文，其中包含本端双机配置、本端双机状态等信息。两端使用相同接口配置控制链路后，通过控制链路进行协商主备机，并将主机的配置同步到备机，最终建立双机，支持使用聚合口作为控制链路，主备接口需保持一致。

数据链路：负责同步会话等数据，为选填选项。如果不配置数据链路或者数据链路故障时，控制链路会代替数据链路工作。控制链路故障时，数据链路会承担心跳报文传输。

高级设置：点击<设置>可以进行高级参数的自定义，如下图所示。

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。一定要开启抢占，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。

主动抢占：设置是否开启抢占成为主机。需要与优先级配合使用。

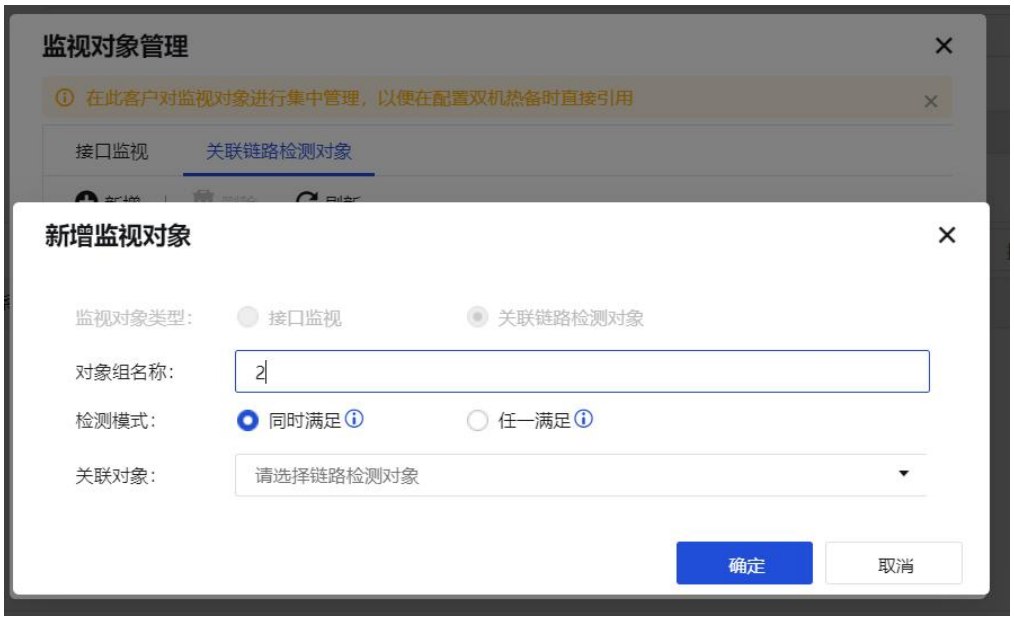
抢占切换延时：设置抢占切换的延时，默认300秒。

虚拟IP：设置各个业务接口作为通信的虚拟IP地址，虚IP会从主机同步到备机，只在主机下发，备机不下发。当主备发生切换时，新主机会下发虚IP，新备机会取消下发虚IP，点击<新增>即可进行配置，如下图所示。

监视对象管理：设置接口监视和关联链路检测对象。点击<管理>进行设置，如下图所示。

接口监视：可进行接口监视的配置，设置需要监控的接口，可设置多个接口组，每个接口组中可设置多个网口，每个接口组可设置所有接口故障时或者任一接口故障时，则判定该组接口故障，进行双机切换，点击<新增>后进行设置，如下图所示。

关联链路检测对象：该设置依赖于[对象/链路对象]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，如果不关联链路检测对象，则双机工作的时候只检测[接口监视]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检测对象，每种链路检测对象可以选择不同的故障判定方式，可设置所有链路检测对象故障时或者任一链路检测对象故障时，则判定该对象组故障，进行双机切换，点击<新增>后进行设置，如下图所示。



监视对象：关联[展开监视对象配置]里设置的监视组，根据对应的条件进行双机的切换。

配置同步

配置同步用于双机进行配置的同步，有主备控状态，主要是控制设备配置同步的方法。如下图所示。

同步对象：用于选择两台设备的同步对象。包括会话表。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。

主备模式：主机永远是主控，备机永远是备控。主备控不可手动切换。

主备镜像模式：主机永远是主控，备机永远是备控。主备控不可手动切换。

路由主主模式：组0为主机的设备是主控，组0为备机的设备是备控。主备控不可手动切换。

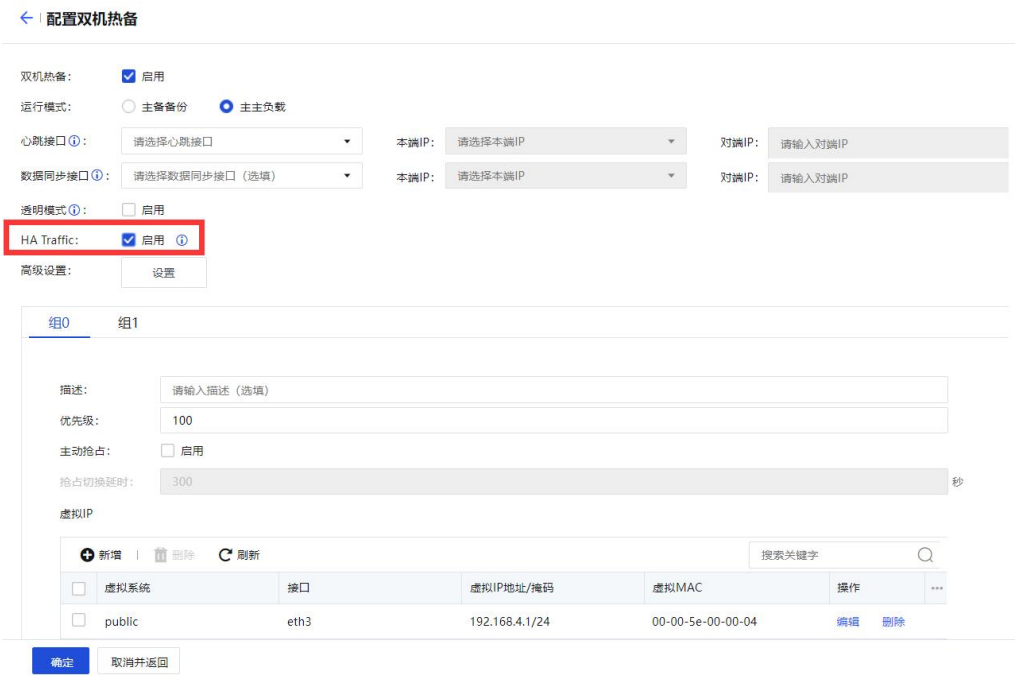
透明主主模式：可以手动随意切换主备控。

⚠ 注意：

1. 主控角色配置会同步给备控角色，备控角色无法修改配置。
2. 主备和双主模式下主、备控角色和组 0 状态一致、双主透明模式下主、备控角色需要手动配置。
3. 只有主主负载透明模式下可以手动切换主、备控。

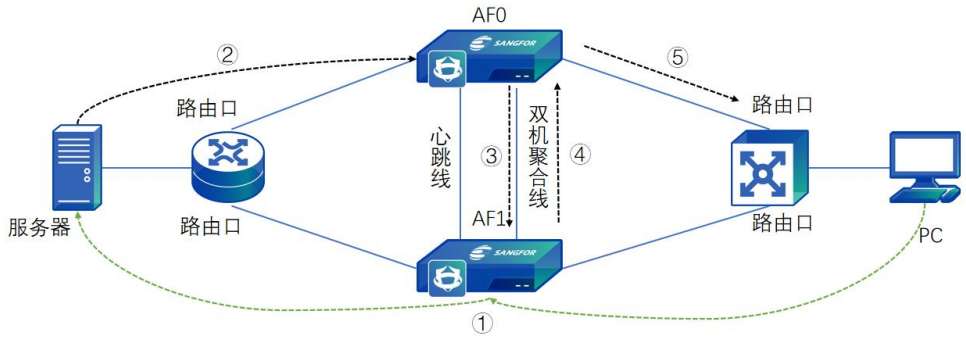
HA Traffic

该功能用于在上下游设备为路由设备，AF做路由双主或者透明双主情况下存在来回流量不一致的场景，需要开启，不存在此场景时无需开启，开启该功能后AF将业务口收到的所有数据包以hash分配方式决定是否通过同步口发送到对端设备进行数据包处理，保证同一条流的所有数据包都能在同一台设备进行安全检测，解决数据非对称转发中出现的网络不通和安全检测失效问题，对端设备安全检测完成后，再将数据包通过同步口发回来，由本端再做数据转发，避免了下游设备路由口因数据包目的MAC地址非本机而丢包，从而导致网络不通。配置如下图所示。



具体工作流程如下：

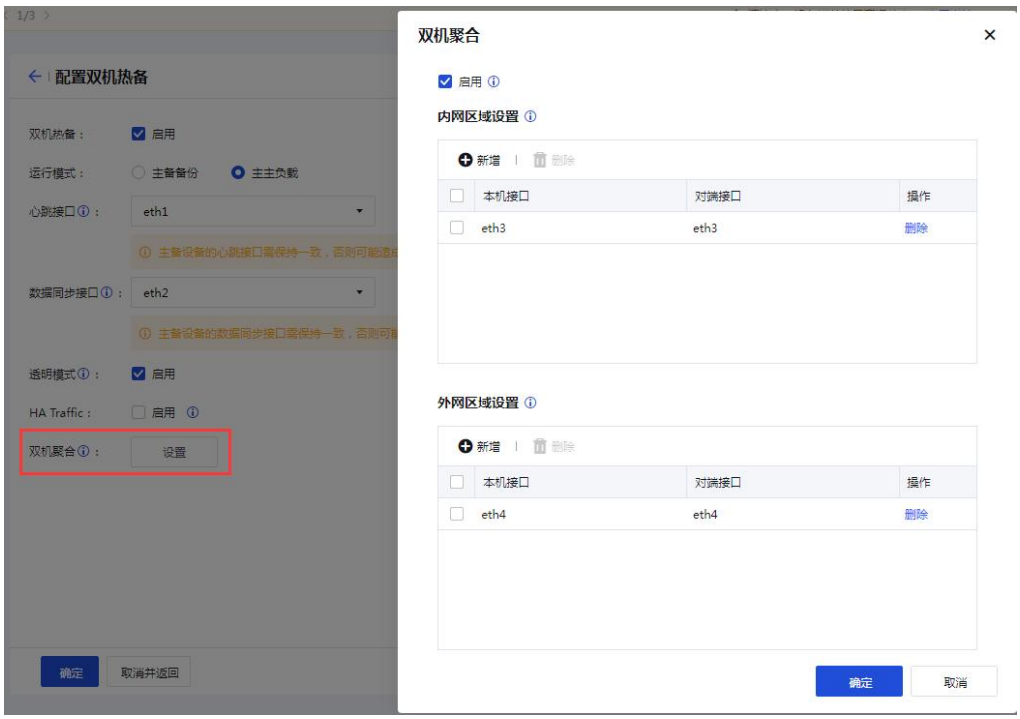
1. PC访问服务器流量经过AF1，AF1经过hash算法计算由AF1进行检测，检测完成继续从AF1转发给服务器；
2. 服务器返回流量到达AF0；
3. AF0经过hash算法计算要由AF1进行检测（同地址计算结果会相同），将数据包通过双机聚合线转发给AF1;
4. AF1收到数据包检测完成后，再通过双机聚合线转发回AF0；
5. AF0将数据包返回给PC。



双机聚合

主要用于AF透明模式主主部署模式下，AF上、下联的设备做了链路聚合并且都为路由口，数据包存在来回路径不一致的场景。如发送的数据经过A防火墙，回来的数据经过B防火墙，导致来回数据包在AF上的连接跟踪不一致而被AF丢包，而双机聚合功能则可以使来回路径不一致数据包经过AF时能够正常转发，开启后，每台AF都会在

后台程序自动生成一个是0或者是1的编号，这个编号界面上看不到，所有经过AF双机聚合配置中内外网区域接口的流量都会是经过算法（即根据源/目的IP地址）计算，看计算结果的值是0还是1，从而将对应数据包转发到对应编号的AF上进行转发（比如根据算法算出来的值是0，则从编号为0的AF转发数据）。配置如下图所示。



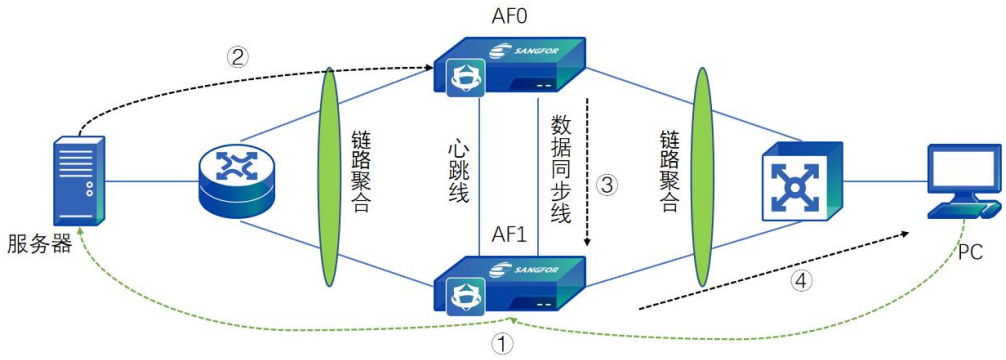
启用：勾选启用双机聚合功能，启用双机聚合条件是：双机热备处于启用状态；双机运行模式是双主透明模式；配置了数据同步口；至少存在两个可选的二层口。

内网区域设置：选择本端和对端下联内网区域的接口。

外网区域设置：选择本端和对端上联外网区域的接口。

具体工作流程如下：

1. PC访问服务器流量经过AF1，AF1经过hash算法计算由AF1进行检测，检测完成继续从AF1转发给服务器；
2. 服务器返回流量到达AF0；
3. AF0经过hash算法计算要由AF1进行检测（同地址计算结果会相同），将数据包通过双机聚合线转发给AF1;
4. AF1收到数据包检测完成后，再通过双机聚合线转发回AF0；
5. AF0将数据包返回给PC。



注意：

1. 主备设备的监控网口必须要设置成一致。
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. 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。
4. 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。
5. 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。

9.8.2. 双机模式

主备模式

主备模式下，只有主机承担业务流量，备机不承担。主机会下发承担业务流量的虚IP，备机不下发。当主机发生故障时，触发主备切换，新主机会下发虚IP，新备机取消下发虚IP，实现双机切换无感知。

在主备模式中，主机作为配置同步角色的主控，在主机中的配置会同步到备机。在备机中无法编辑配置。

主备镜像模式

在主备模式中，只有配置了虚IP的接口会同步到备机，未配置虚IP的接口不会有IP、MAC等的同步。而在主备镜像模式中，AF使用实IP替代虚IP。除带外管理口、控制链路、数据链路外，所有的接口都会同步到备机，两台设备像镜像一样，甚至MAC地址都是一致的。

双主透明模式

双主透明模式是两台设备做透明部署或虚拟网线二层部署模式下，同时处于工作状态，没有组0，组1的概念。

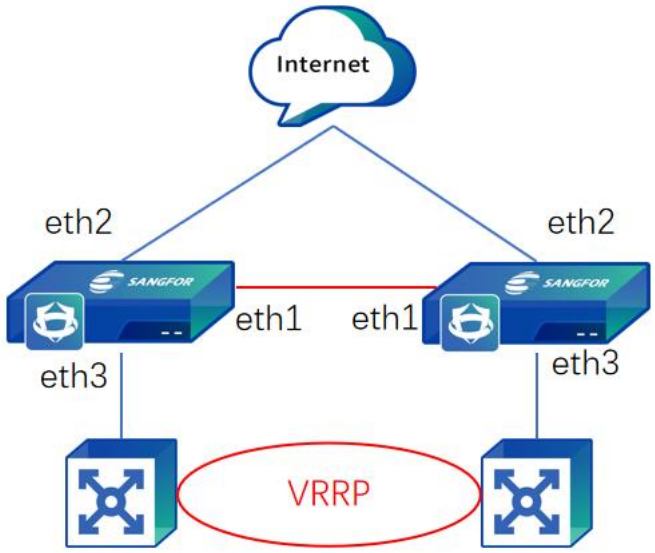
在此模式下，上下游设备如果是聚合口，且存在来回路径不一致数据（非对称流量），则需要开启双机聚合功能，来保障流量的转发，开启此功能后，当流量经过其中一台AF时，AF会通过计算哈希，决定该流量交给哪台AF来处理。同一条流的请求数据和响应数据的哈希值一致，会被同一台AF处理。如果需要交给对端AF处理，则会将流量通过数据链路传递到对端。

9.8.3. 主备部署

主备部署是一台设备处于工作状态，另外一台处于热备状态。两台设备通过心跳口检测对端是否存在并同步配置及会话，当主设备出现问题触发切换条件时，设备会自动把业务切换到备设备，并且通过会话同步等机制，保证业务不断，从而实现业务稳定的运行 。支持路由模式下主备部署和网桥模式下主备部署（网桥模式包括透明模式和虚拟网线模式）。

主备部署配置案例

某企业内部网络是VRRP的环境，现购买了两台AF路由部署进网络中，两台AF需要做双机热备，具体拓扑如下图所示。



前提条件

1. 组建双机条件：软件版本、内存、网口和授权一致。

2. AF设备业务口（内网口、外网口）、心跳口、数据同步口以及IP地址规划好。
3. 主机已配置好透明部署模式以及相关安全策略。
4. 先配置主机信息，再配置备机。

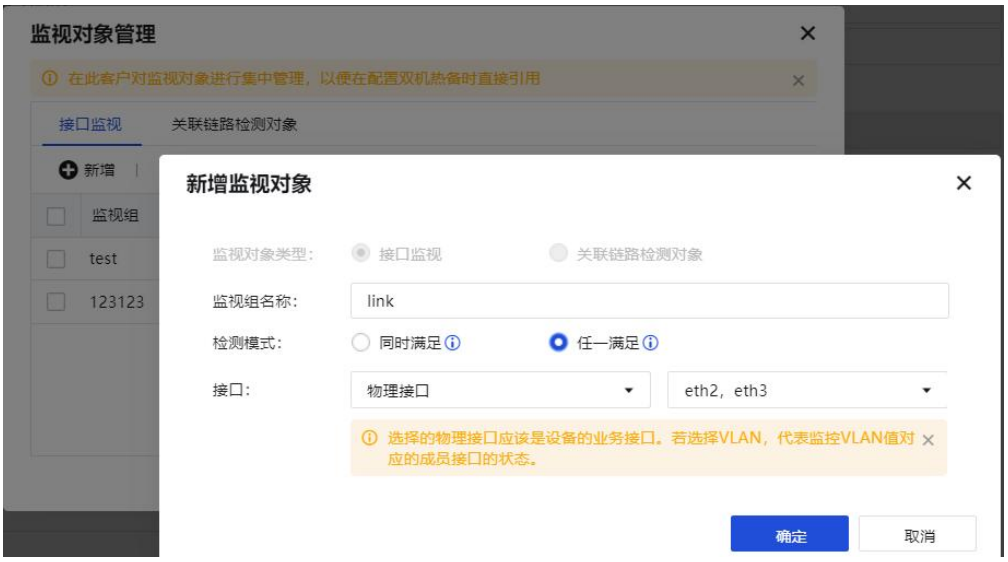
配置步骤

步骤1.主机配置心跳口。在[网络/接口/物理接口]选择eth1口配置IP地址， 本案例中设置为11.1.1.1/24。如下图所示。

步骤2.主机启用双机热备。进入[系统/高可用性/双机热备]页面，点击<配置>勾选启用，选择主备备份模式，控制链路选择eth1，设置对端IP为11.1.1.2（数据链路在主备模式下可不配置）。

步骤3.主机配置优先级和虚拟IP。优先级配置100，在[组0/虚拟IP] 点<新增>，选择接口eth2，配置虚IPv4地址10.2.1.3/24，再选择接口eth3，配置虚IPv4地址10.3.1.3/24，如下图所示。

步骤4.主机设置接口监视。在[监视对象管理/接口监视]点<新增>，检测模式选任一满足，接口选择物理接口，选择eth2、eth3作为需要监视的业务口。



步骤5.主机关联监视对象。监视对象选择前面步骤配置link。如下图所示。

步骤6.点击<确定>完成主机配置。

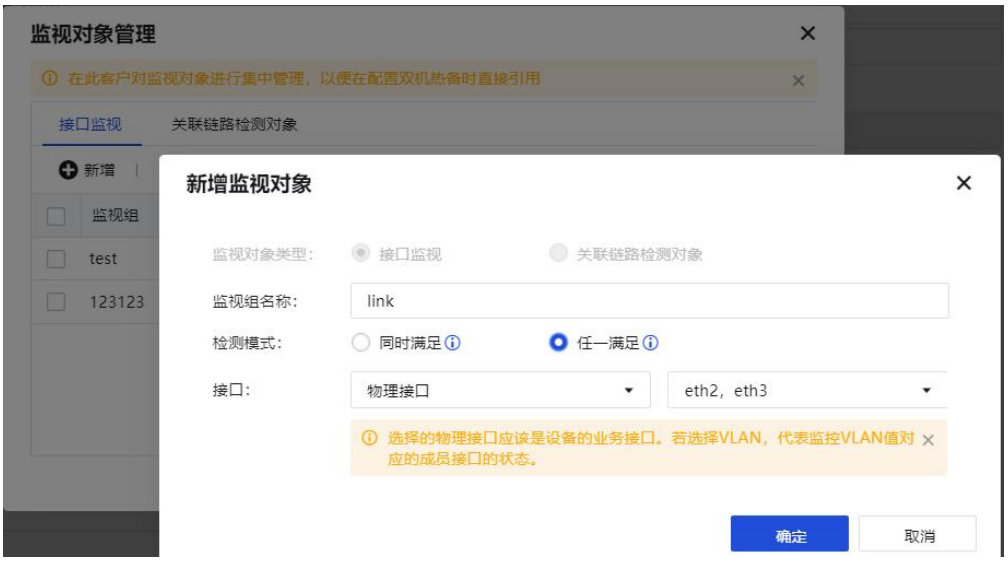
步骤7.备机配置心跳口。在[网络/接口/物理接口]选择eth1口配置IP地址， 本案例中设置为11.1.1.2/24。如下图所示。

步骤8.备机启用双机热备。进入[系统/高可用性/双机热备]页面，点击<配置>勾选启用，选择主备备份模式，控制链路选择eth1，设置对端IP为11.1.1.1（数据链路在主备模式下可不配置）。

步骤9.备机配置优先级和虚拟IP。优先级配置99，在[组0/虚拟IP] 点<新增>，选择接口eth2，配置虚IPv4地址10.2.1.3/24，再选择接口eth3，配置虚IPv4地址

10.3.1.3/24，如下图所示。

步骤10.备机设置接口监视。在[监视对象管理/接口监视]点<新增>，检测模式选任一满足，接口选择物理接口，选择eth2、eth3作为需要监视的业务口。。



步骤11.备机关联监视对象。监视对象选择前面步骤配置link。如下图所示。

步骤12.点击<确定>完成备机配置。

步骤13.主机和备机的主备模式配置完成，先开主机接心跳线以及其他业务线，等主机AF开机完成后再开备机AF接心跳线以及其他业务线。建立双机后在[系统/高可用性/双机热备]选项中可以看到双机状态信息。

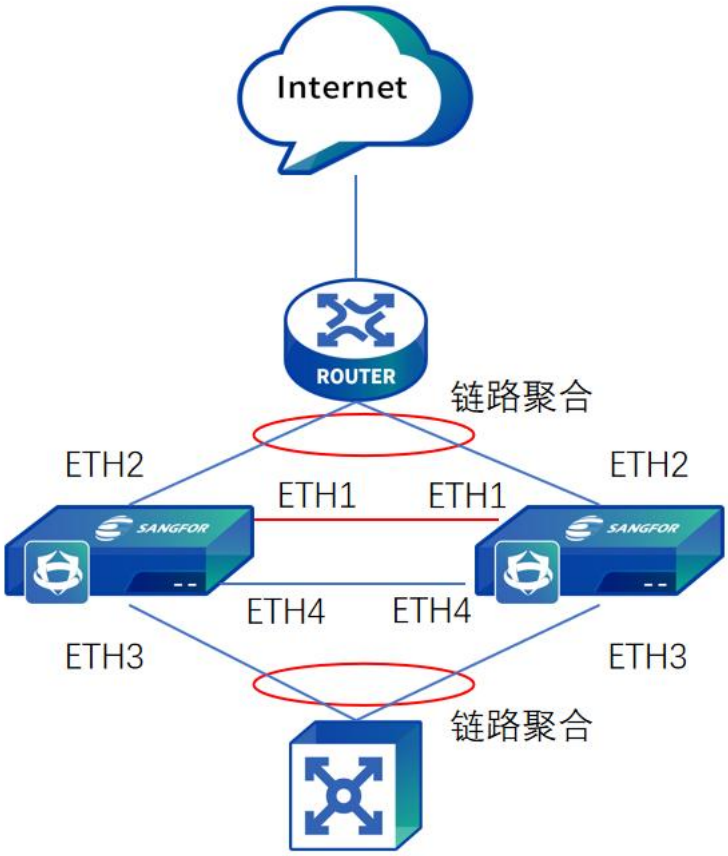
9.8.4. 透明主主部署

透明主主部署是两台AF做网桥部署在网络中，均处于工作状态，根据流量转发到不同

AF的情况，来进行数据处理，通过心跳口同步配置及会话（网桥模式包括透明模式和虚拟网线模式）。

透明主主模式配置案例

某企业内部网络是路由器和核心交换机做链路聚合，现购买了两台AF虚拟网线模式部署进网络中，两台AF需要做网桥主主部署，经过两台AF的流量会存在来回流量路径不一致的问题，需要开启双机聚合功能，具体拓扑如下图所示。



前提条件

1. 组建双机条件：软件版本、内存、网口和授权一致。
2. AF设备业务口（内网口、外网口）、心跳口、数据同步口以及IP地址规划好。
3. 主控已配置好透明部署模式以及相关安全策略。
4. 先配置主控信息，再配置备控。

配置步骤

步骤1.主控配置心跳口。在[网络/接口/物理接口]选择eth1口配置IP地址， 本案例中设置为11.1.1.1/24。如下图所示。

步骤2.主控配置数据同步口。在[网络/接口/物理接口]选择eth4口配置IP地址， 本案例中设置为12.1.1.1/24，并在[高级设置]中开启巨帧，如下图所示。

步骤3.主控配置接口联动。在[网络/接口/接口联动]页面中启用接口LINK状态联动，并点击<新增>，选择接口eth2和接口eth3。如下图所示。

步骤4.主控启用双机热备。进入[系统/高可用性/双机热备]页面，点击<配置>勾选启用，选择主主负载模式，控制链路选择eth1，设置对端IP为11.1.1.2，数据链路选择eth4，设置对端IP为12.1.1.2，并勾选启用透明模式，如下图所示。

步骤5.主控配置双机聚合。在[双机聚合]选项点击<设置>弹出页面中启用双机聚合，内网区域设置新增选择接口eth3，外网区域设置新增选择接口eth2，如下图所示。（双机聚合开启条件满足后需先保存，才可设置）

步骤6.主控设置为主控角色。在[系统/高可用性/配置同步]页面中配合同步角色点<设置>，选择主控角色。如下图所示。

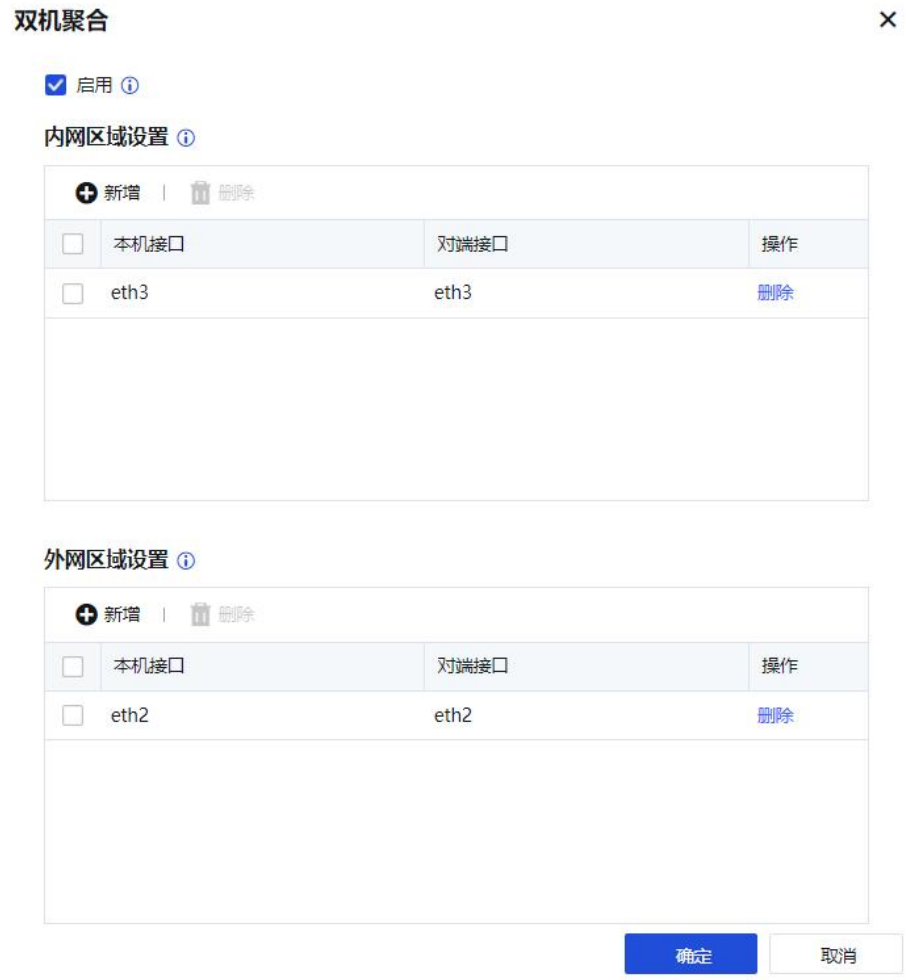
步骤7.点击<确定>完成主控配置。

步骤8.备控配置心跳口。在[网络/接口/物理接口]选择eth1口配置IP地址， 本案例中设置为11.1.1.2/24。如下图所示。

步骤9.备控配置数据同步口。在[网络/接口/物理接口]选择eth4口配置IP地址， 本案例中设置为12.1.1.1/24，并在[高级设置]中开启巨帧，如下图所示。

步骤10.备控启用双机热备。进入[系统/高可用性/双机热备]页面，点击<配置>勾选启用，选择主主负载模式，控制链路选择eth1，设置对端IP为11.1.1.1，数据链路选择eth4，设置对端IP为12.1.1.2，并勾选启用透明模式，如下图所示。

步骤11.备控配置双机聚合。在[双机聚合]选项点击<设置>弹出页面中启用双机聚合，内网区域设置新增选择接口eth3，外网区域设置新增选择接口eth2，如下图所示。



步骤12.备控设置为备控角色。在[系统/高可用性/配置同步]页面中配合同步角色点<设置>，选择主控角色。如下图所示。

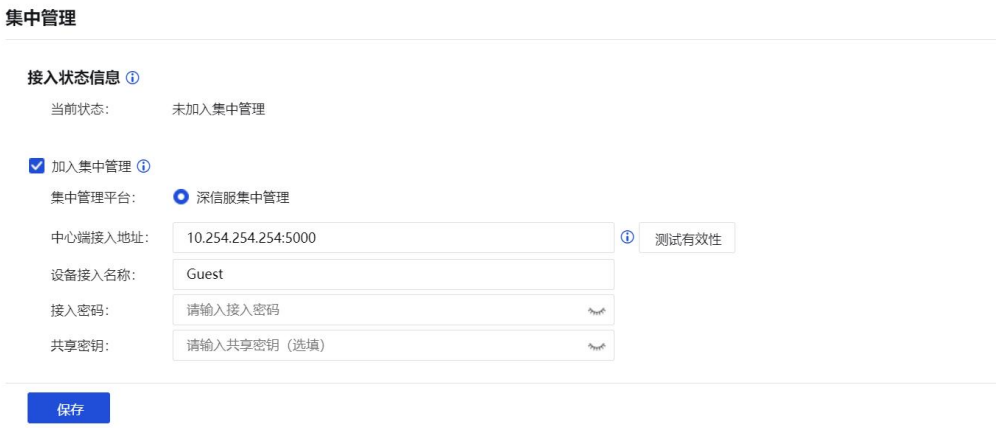
⚠ 注意：

1. 在流量来回路径不一致场景下，使用 AF 做透明双主部署，需要开启双机聚合功能，如果 AF1 和 AF2 上下行学到的下一跳 IP 或 MAC 不相同（也就是上下游是不同的路由口），那么除了开启双机聚合功能外，还需要开启 HA Traffic 功能；
2. 上下游设备做链路聚合，建议是用 LACP 进行聚合，聚合口转发算法要改为源目 IP（默认是源目 mac），否则有概率出现所有流量都是非对称的场景，影响 AF 转发性能。
3. 双机聚合情况下需在对应的数据同步口开启巨帧，因为报文从一台 AF 设备通过控制链路发送到另一台 AF 设备时，需要在原来报文的基础上继续封装二三四层头以及 HA 头和 Zmode 信息，可能大于 MTU 值从而引起报文分片重组，影响性能，开启对应接口处巨帧功能后，就不存在报文分片重组的情况。

9.9. 中台对接管理

9.9.1. 集中管理

集中管理用于设置AF设备是否加入集中管理进行受控，加入后管理员可以对该设备下发策略，并且受控端的权限也能由中心端下发。设备支持加入BBC集中管理平台和MSS安全服务平台。



接入状态信息：当前状态会显示是否加入集中管理平台的情况。

解除集中管理：用于加入集中管理后，输入密码进行解控。该密码由中心端管理员掌控。 （该功能在接入后才会显示）

中心端接入地址：用于设置连接集中管理的设备。该地址由中心端管理员掌控。

点击<测试有效性>，检测 IP 和端口号是否可以通。

接入设备名称：填写接入集中管理中心端的用户名。

接入密码：填写接入集中管理中心端的密码。

共享密钥：输入设备的共享密钥，不是必选项。

AF接入BBC集中管理配置案例

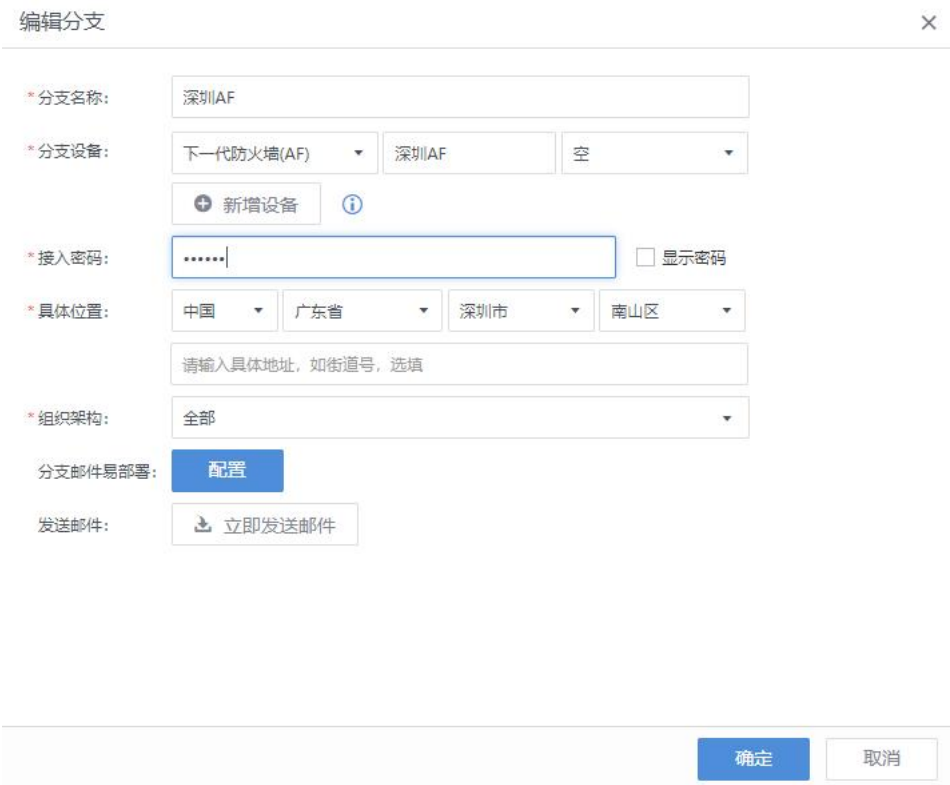
当有需求需要将一台深圳的AF接入BBC设备，让设备进行管控。

配置指导

步骤1.登录BBC系统，进入设备页面进行设置区域名称后点击<确定>。

步骤2.选择刚才创建的区域，点击[新增分支]。

步骤3.设置分支名称、分支设备、接入密码、具体位置、组织架构，点击<确定>。



步骤4.登录AF设备，在[系统/集中管理]页面，勾选加入集中管理，输入中心端接入地址（BBC设备地址）需要加5000端口，设备接入名称输入分支设备中的名称，接入密码输入BBC的接入密码，点击<保存>。

步骤5.AF成功接入BBC集中管理平台，在当前状态显示已加入集中管理平台。

9.9.2. 信服管家

云端信服管家主要是针对设备的运行指标数据进行诊断分析，实时检测告警，协同专家快速消除风险。达到提前预防风险、处置风险，避免客户业务受影响的效果。

此处信服管家页面是在设备无法连接公网时，可通过接入信服管家客户端来传输数据到云端信服管家，如下图所示。

9.9.3. 合规自检

合规自检用于接入深信服合规自检平台，检测终端设备上配置开启情况，以及是否符合合规自检要求，支持云图，云镜等平台的合规自检服务的接入，配置界面如下图。

设备类型：选择要接入的平台设备类型，包括云图、云镜、其他。

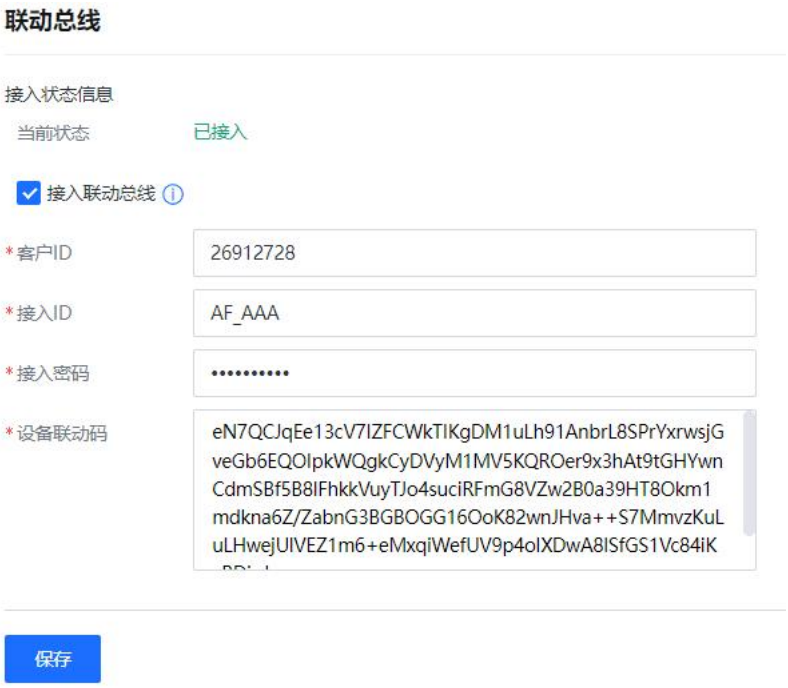
中心端 IP：用于设置连接的合规自检平台 IP 地址，该地址由平台端管理员掌控。

中心端端口：用于设置连接的合规自检平台端口。

当前设备IP：填写当前设备本身连接平台的IP地址。

9.9.4. 联动总线

联动总线主要是可通过输入客户ID等信息接入联动总线，更方便与XDR、EDR等产品进行对接后，同时可满足在集中管理页面接入BBC 集中管理中心的需求。如下图所示。


联动总线
接入状态信息
当前状态
已接入
接入联动总线
*客户ID
26912728
*接入ID
AF_AAA
*接入密码
*设备联动码
eN7QCJqEe13cV7IZFCWkTIKgDM1uLh91AnbrL8SPrYxrwsjG
veGb6EQOIpkWQgkCyDVyM1MV5KQROer9x3hAt9tGHYwn
CdmSBf5B8IFhkkVuyTJo4suciRFmG8VZw2B0a39HT8Okm1
mdkna6Z/ZabnG3BGBOGG16OoK82wnJHva++S7MmvzKuL
uLHwejUlVEZ1m6+eMxqiWefUV9p4oIXDwA8ISfGS1Vc84iK
保存

10. 典型场景案例集

典型场景案例集主要介绍AF在典型网络环境下的配置案例。

10.1. 办公网上网管控场景

办公网上网管控场景主要是将AF部署在网络边界处，对上网数据进行管控，同时对通信中存在的威胁进行防护。

10.1.1. 需求背景

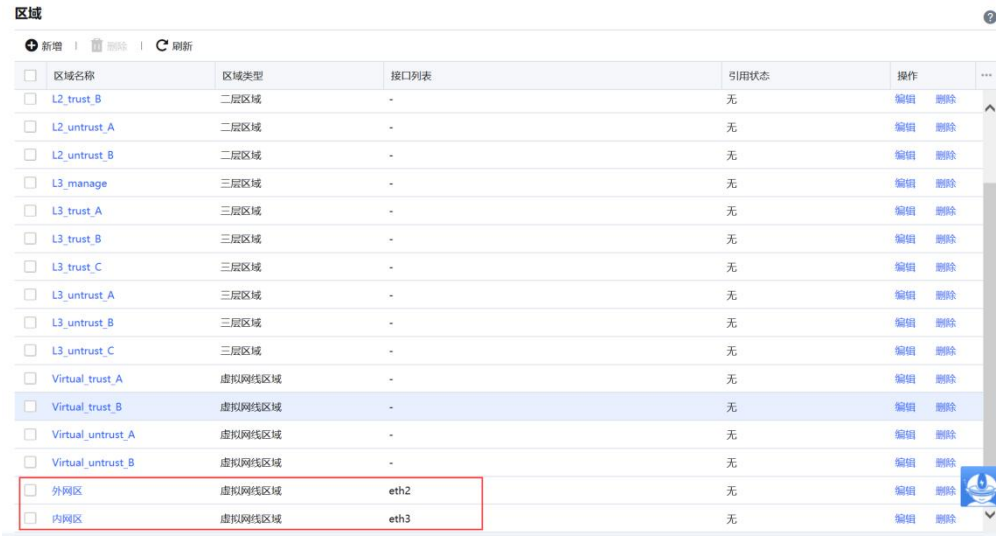
某企业使用AF做透明部署在办公网出口路由器的内网口处，外网带宽是200Mb/s，已经完成了基本网络配置，eth2口接出口路由器，eth3口接内网交换机，内网电脑已经能正常上网，内网网段是192.168.1.0/24。为了不影响网速，管理员希望内网所有的用户都不能使用P2P应用以及相关的下载工具，单个用户的最大流量不能超过3Mb/s，安全方面需要对所有的上网数据进行基本的上网管控和防护，最后管理员自己的电脑192.168.1.3/24不希望有任何的管控。

10.1.2. 需求分析

针对这些需求，需要使用应用控制策略禁止内网电脑的P2P应用以及相关的下载工具，使用流控策略来限制最大用户流量，然后在安全策略里面开启用户防护策略，都使用默认模板即可，管理员电脑不受管控也可以直接添加到白名单。

10.1.3. 配置步骤

步骤1.定义内网口和外网口区域，进入[网络/区域]，新增两个区域，如[内网区]选择eth3，[外网区]选择eth2，如下图所示。



步骤2.配置应用控制策略禁止P2P应用等，进入[策略/访问控制/应用控制策略/策略配置]，新增应用控制策略，策略位置在自定义的放通所有策略前，具体配置如下图所示。

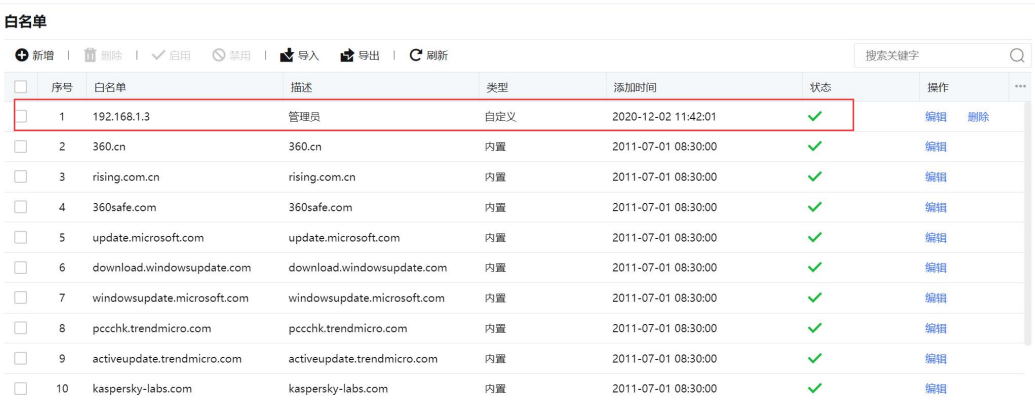
步骤3.配置安全防护策略。进入[策略/安全策略/安全防护策略]新增用户防护策略，进行内网的上网管控和防护，都选择上网管控场景中的默认模板，如下图所示。

步骤4.配置流控策略里的虚拟线路。进入[策略/流控/虚拟线路配置/虚拟线路列表]，选择连接路由器的eth2，并设置实际上网出口带宽，如下图所示。

步骤5.配置流控策略里的虚拟线路规则。进入[策略/流控/虚拟线路配置/虚拟线路规则]新增虚拟线路规则，如下图所示。

步骤6.配置流控策略里的通道配置。进入[策略/流控/通道配置]，勾选[启用流量管理系统]，并新增通道，限制单用户上限为3Mb/s。如下图所示。

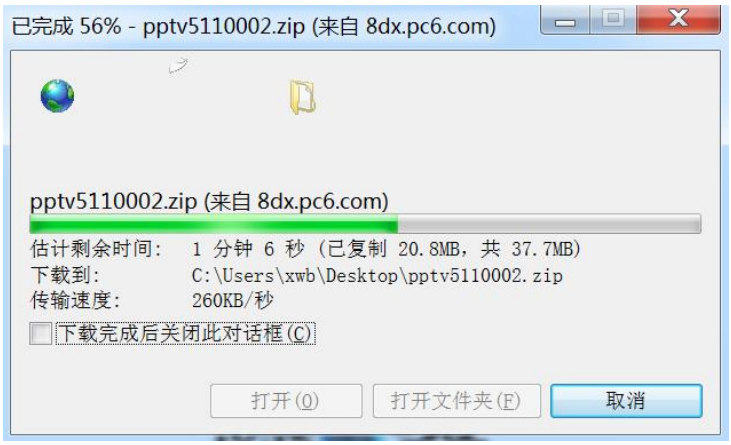
步骤7.配置白名单。进入[安全运营/黑白名单/白名单]，新增白名单，将管理员IP 192.168.1.3加入白名单。如下图所示。



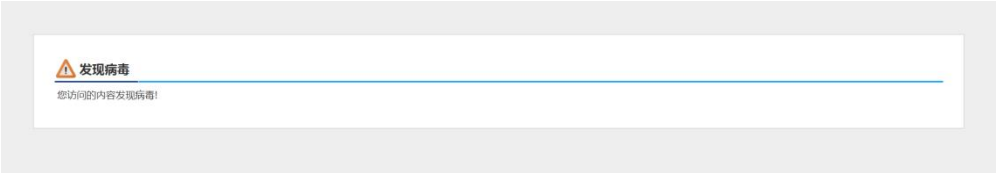
10.1.4. 效果预览

1. 内网电脑使用P2P视频软件看在线视频，发现无法打开在线视频。如下图所示。

2. 单用户流量控制不能超过3Mb/s，下载测试每秒200KB多，换算成Mb没有超过控制上限。如下图所示



3. 访问带有病毒的网站弹出相关提示，并无法打开该网站。如下图所示。



4. 管理员电脑没有任何限制，可以正常使用P2P视频软件等。

10.2. 服务器业务防护场景

服务器对外发布场景主要是内网有服务器提供给公网访问，需要AF部署在服务器区域网络前，对服务器进行安全防护，抵御来自公网的威胁。

10.2.1. 需求背景

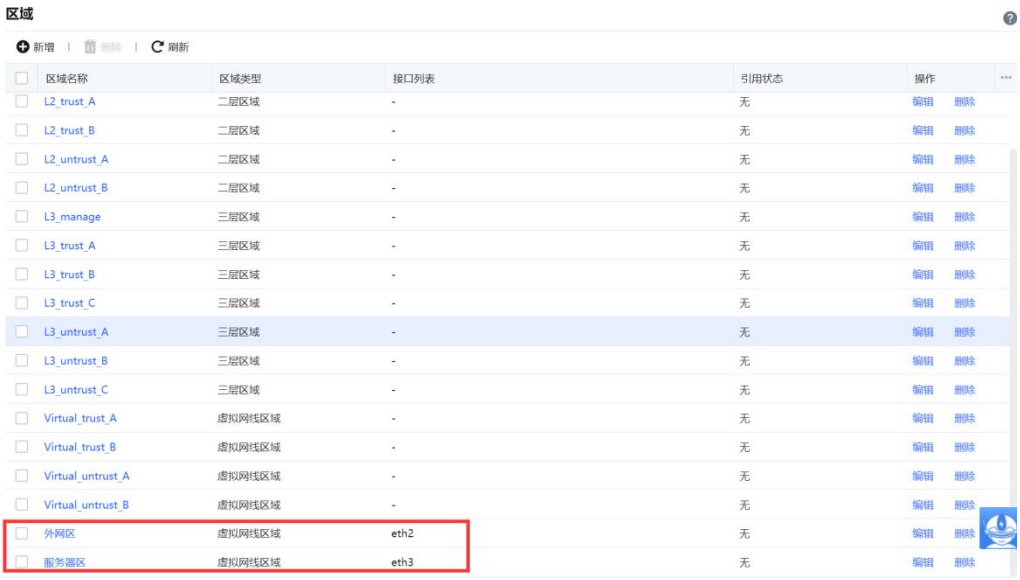
某企业将内网服务器192.168.1.3提供80端口的web服务提供给公网访问。出口路由器已经做好到该服务器80端口的目的地址转换，AF已经虚拟网线部署在服务器区域网络前，eth2口接核心交换机，eth3口接服务器区域交换机，AF虚拟网线模式的基本网络配置已经完成，现需要只允许访问服务器80端口的HTTP应用才能通过AF，并针对服务器进行业务防护，保护服务器不被攻击，同时在访问服务器管理页面 http://192.168.1.3/DVWA/login.php 时需要进行二次认证，最后不允许美国地区IP来访问到服务器。

10.2.2. 需求分析

针对这些需求，需要用应用控制策略来限制访问的服务和应用，用安全防护策略进行业务防护，使用默认模板即可，最后通过地域访问控制来拒绝美国地区IP访问服务器。

10.2.3. 配置步骤

步骤1.定义区域，进入[网络/区域]，新增两个区域，如[服务器区]选择eth3，[外网区]选择eth2，如下图所示。



步骤2.配置应用控制策略，进入[策略/访问控制/应用控制策略/策略配置]，新增应用控制策略，服务选择http，应用选择访问网站，具体配置如下图所示。

步骤3.配置安全防护策略。进入[策略/安全策略/安全防护策略]新增业务防护策略，

都选择业务防护场景中的默认模板，如下图所示。

步骤4.配置地域访问控制。进入[策略/访问控制/地域访问控制]新增拒绝美国地区的访问，如下图所示。

10. 2. 4. 效果预览

1. 公网用户通过网页访问 http://出口路由器IP 可以直接访问内网服务器，如下图所示。

Debian集成测试环境20200224

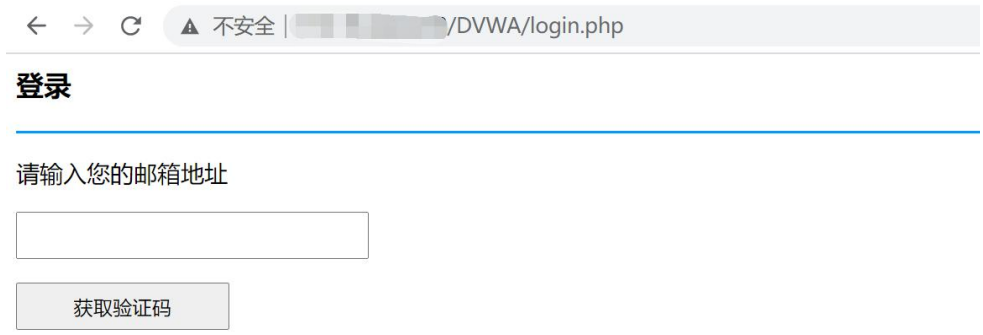
图形界面登陆账号密码	af/sangfor	开启虚拟机后输入此密码进入debian虚拟机
root权限密码	sangfor	进入debian后su命令输入sangfor即可切换root权限，或者ssh root/sangfor
mysql密码	root	root权限下 mysql -uroot -p后输入root即可进入mysql
津城市人社局	admin/123456	此用户名密码为进入admin路径下的后台密码
DVWA登陆密码	admin/admin	DVWA的登陆密码

测试类型	名称及链接	可测试内容
服务器保护		
集成演示网站	津城市人社局	appscan防扫描、sql注入、网页防篡改、敏感信息泄露
OWASP威胁测试网站	DVWA	用户名密码admin/admin，系统命令注入、文件包含、XSS、文件上传、webshell、暴力破解、整站漏洞
整站漏洞测试网站	WordPress	整站漏洞
FTP版本隐藏	使用命令ftp 连虚拟机IP	220 debian.localdomain FTP server (Version6.4/OpenBSD/Linux-ftpd-0.17) ready.
IPS		
双网口网桥回放	工具目录：/root/ips_test1.0/	可测试IPS保护服务器与保护客户端所有类型日志并生成报表
单网口网桥回放	工具目录：/root/ips_test2.0/	可测试IPS保护服务器类型日志并生成报表
单线旁路回放	工具目录：/root/ips_test2.0/	可测试IPS保护服务器与保护客户端所有类型日志并生成报表
病毒防御策略		注意，需关闭waf信息泄露防护，才能直接浏览病毒目录
f-prot病毒	病毒目录：/jcsweb/download/virus/commonvirus/	f-prot与sophos都可查杀
sophos病毒	病毒目录：/jcsweb/download/virus/sophos/	规则库高于2013-04-03的sophos可查杀，文件后缀都改为zip，杀毒配置需添加zip文件类型
测试工具	工具目录：/tools/	注意，需关闭waf信息泄露防护，才能直接浏览工具目录

changlog:
替换原有VI编辑器支持上下左右和退格键
在ips test2.0/中集成cms发布的旁路回放脚本
ipstest1.0和2.0中更新了北研提供的最新IPS测试回放包和描述文件
debian的网口eth1改为开机自动UP默认DHCP模式
将debian系统配置成2C2G

2. 从公网进行攻击测试，攻击不成功，查看[监控/日志/安全日志]有拒绝的信息，如下图所示。

3. 从公网访问服务器管理后台，弹出需要邮箱认证的页面，如下图所示。



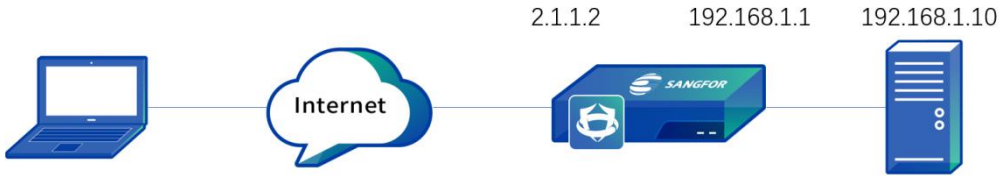
4. 在[策略/访问控制/地域访问控制]中点击<已拒绝的IP列表>查看有访问行为但被拒绝访问的美国IP。

10.3. SSL VPN 接入场景

SSL VPN接入场景主要使用AF的SSL VPN功能，方便移动用户通过SSL VPN的方式安全接入访问内网服务器资源。

10.3.1. 需求背景

某企业总部AF作为网关部署在公网出口，ETH1口接公网，ETH2口接内网，内网有服务器192.168.3.10需要提供80端口的web服务给移动用户访问，同时移动终端还需要能够ping通这个服务器，具体拓扑如下图所示。



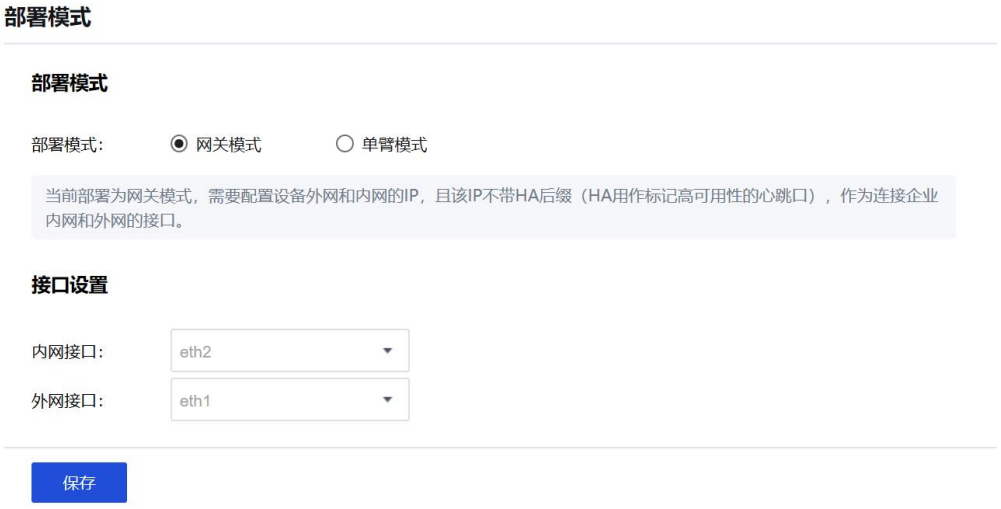
10.3.2. 需求分析

针对这些需求，需要使用AF的SSL VPN功能，建立移动用户的账号密码供移动用户SSL VPN的安全接入，然后建立两个服务器资源供这个移动用户访问。

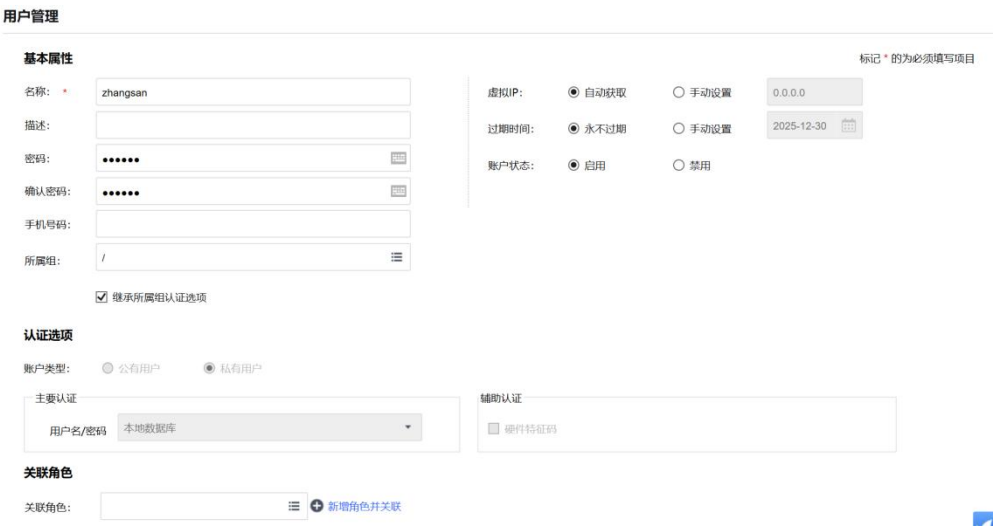
10.3.3. 配置步骤

步骤1.启动SSL VPN服务。进入[网络/SSL VPN]，选择其任意一个页面，点击<启动SSL VPN服务>。如下图所示。

步骤2.设置部署模式。进入[网络/ SSL VPN/部署模式]选择[网关模式]，内网接口选择eth2，外网接口选择eth1。如下图所示。



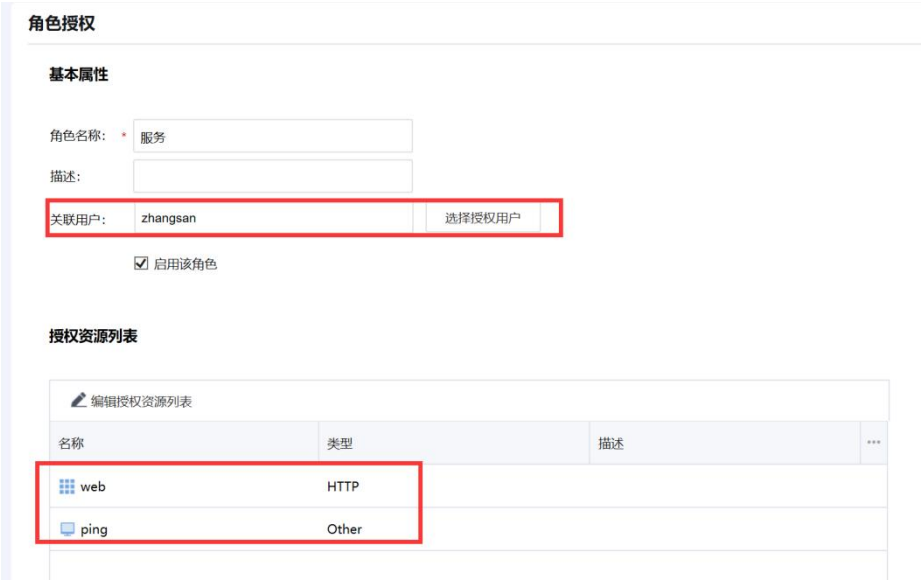
步骤3.配置用户。进入[网络/ SSL VPN /用户管理]新增用户，填写名称和密码。如下图所示。



步骤4.配置TCP应用资源。进入[网络/ SSL VPN /资源管理]新增TCP应用，类型选择HTTP，地址填写服务器IP 192.168.1.10，端口80。如下图所示。

步骤5.配置L3VPN资源。进入[网络/ SSL VPN /资源管理]新增L3VPN，类型选择Other，协议选择ICMP，地址填写服务器IP 192.168.1.10（需要应用控制策略中进行对应的放通）。如下图所示。

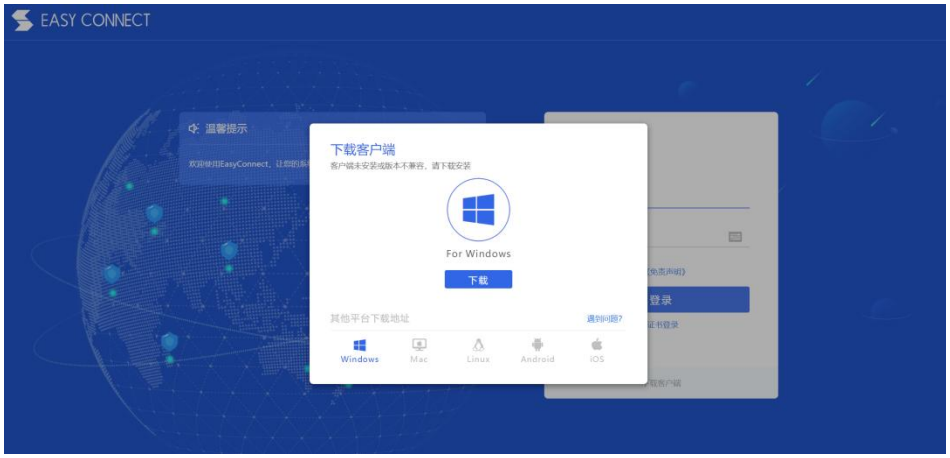
步骤6.配置角色授权。进入[网络/ SSL VPN /资源管理]新建角色，关联用户选择步骤3建立的用户，授权资源列表选择步骤4和步骤5建立的资源。如下图所示。



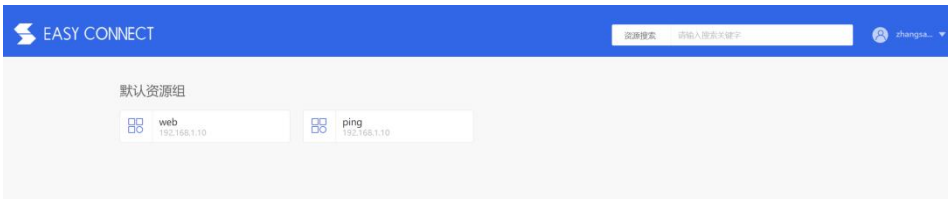
10. 3. 4. 效果预览

1. 移动用户通过网页访问https://2.1.1.2:4430，如是第一次登录深信服SSL VPN，

会提示安装客户端。如下图所示。

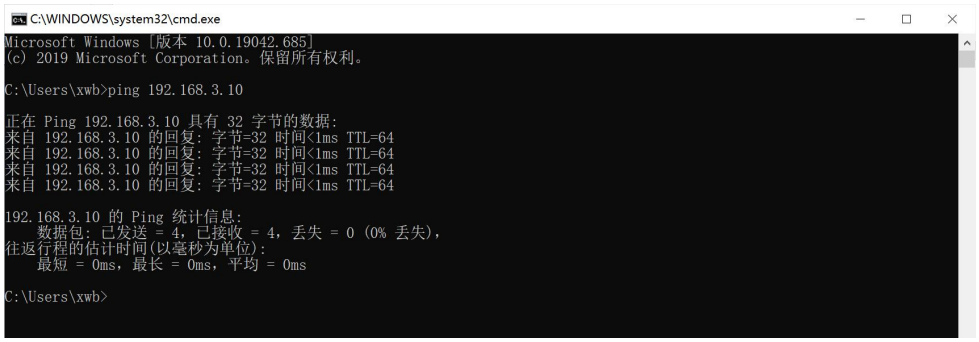


2. 下载安装完成后，打开客户端输入登录地址https://2.1.1.2:4430，再输入用户密码登录，显示资源页面，有授权访问的两个资源。如下图所示。



3. 通过页面直接点击web资源，可以访问到192.168.1.10的web服务。如下图所示。

4. 通过PING测试192.168.1.10能够成功PING通。如下图所示。

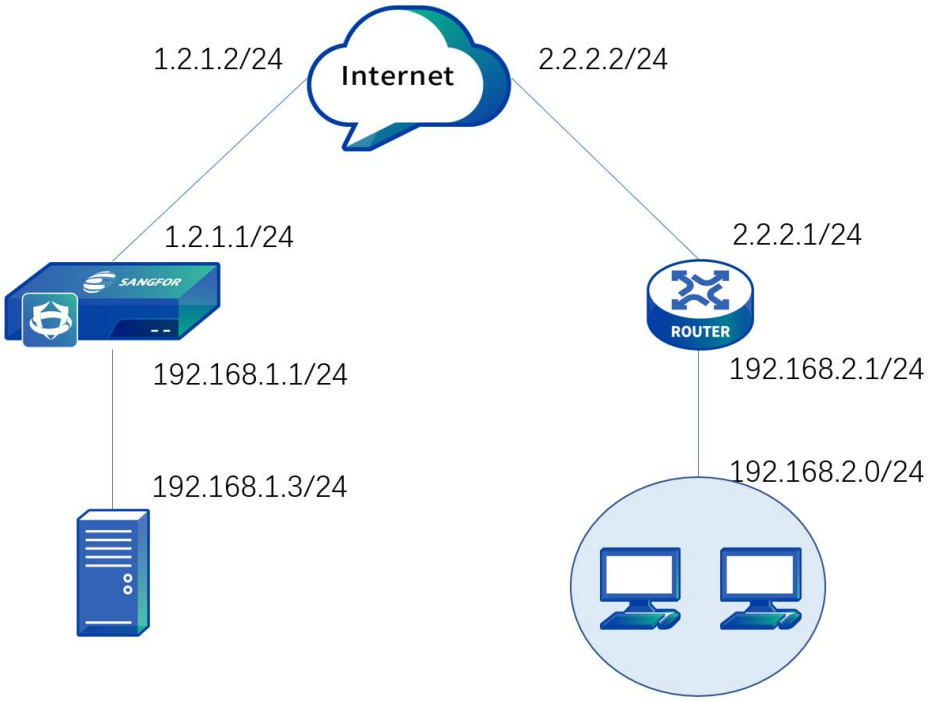


10.4. IPSEC VPN 组网场景

IPSEC VPN组网场景主要应用于通过AF的IPSEC VPN与第三方厂商设备或者深信服设备进行对接，并能够对VPN接口区域过来的流量进行安全防护。

10.4.1. 需求背景

某企业总部AF作为网关部署在公网出口，ETH2口接内网，分部是路由器做出口，总部内网有服务器192.168.1.3需要提供80端口的web服务给分部访问，为了安全考虑，现在需要和分支那边的路由器建立IPSEC VPN连接，同时分部访问总部服务器的时候也需要进行安全防护，以免黑客通过分部终端来攻击服务器，只允许访问服务器的80端口，路由器IPSEV VPN配置已经完成，使用IKE V2，加密算法用的DES，认证算法是MD5。具体拓扑如下图所示。

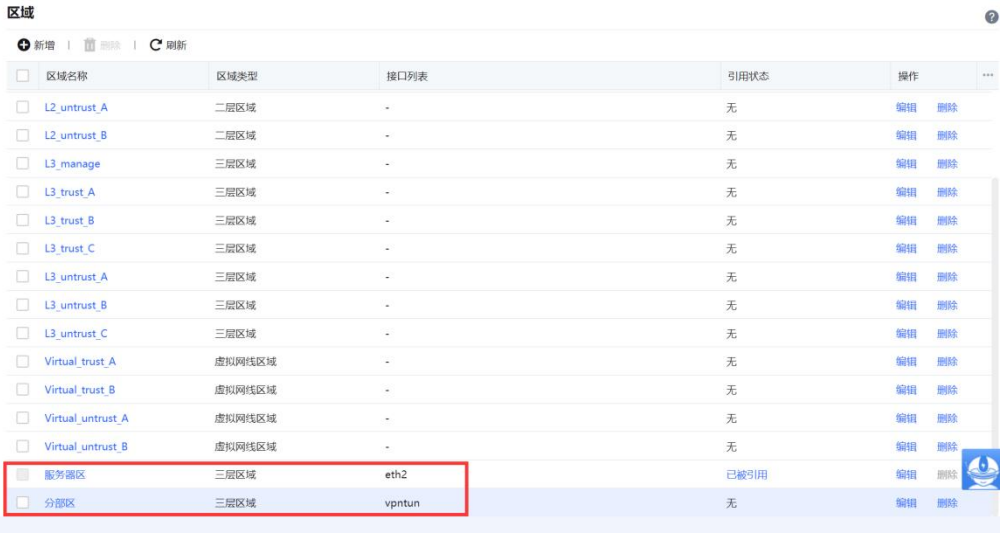


10.4.2. 需求分析

针对这些需求，先和路由器建立IPSEC VPN连接，再用应用控制策略来限制区域访问的服务，用安全防护策略针对vpn区域进行业务防护，使用默认模板即可。

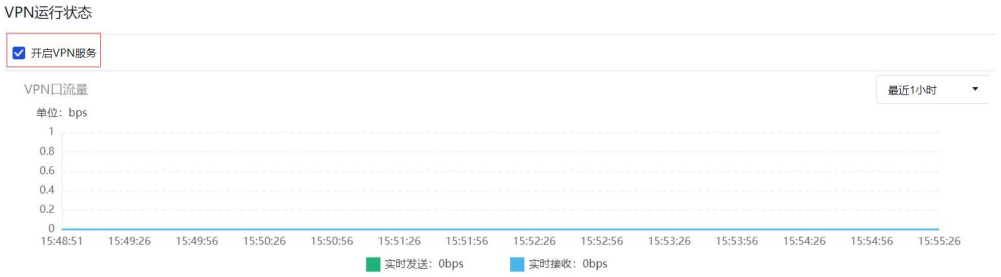
10.4.3. 配置步骤

步骤1.定义区域，进入[网络/区域]，新增两个区域，服务器区选择eth3，分部区选择vpntun接口，如下图所示。



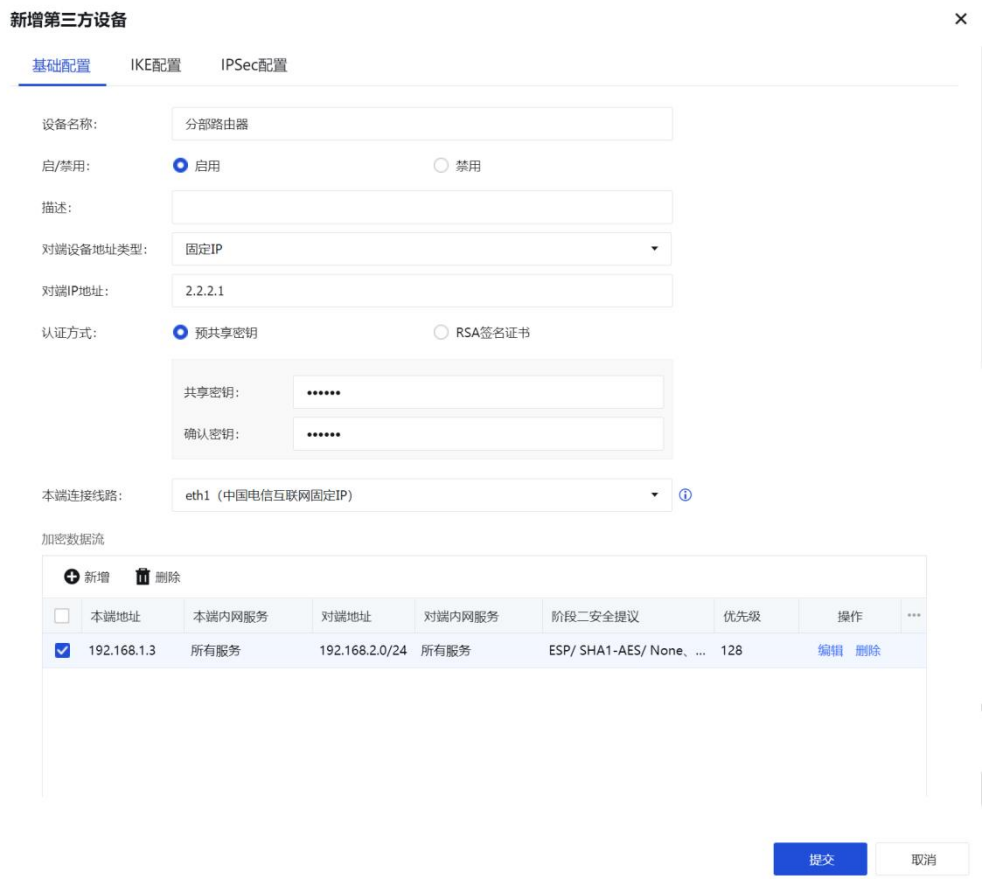
步骤2.启用VPN服务。进入[网络/Sangfor/IPSecVPN/VPN运行状态]勾选[开启

VPN服务]。如下图所示。

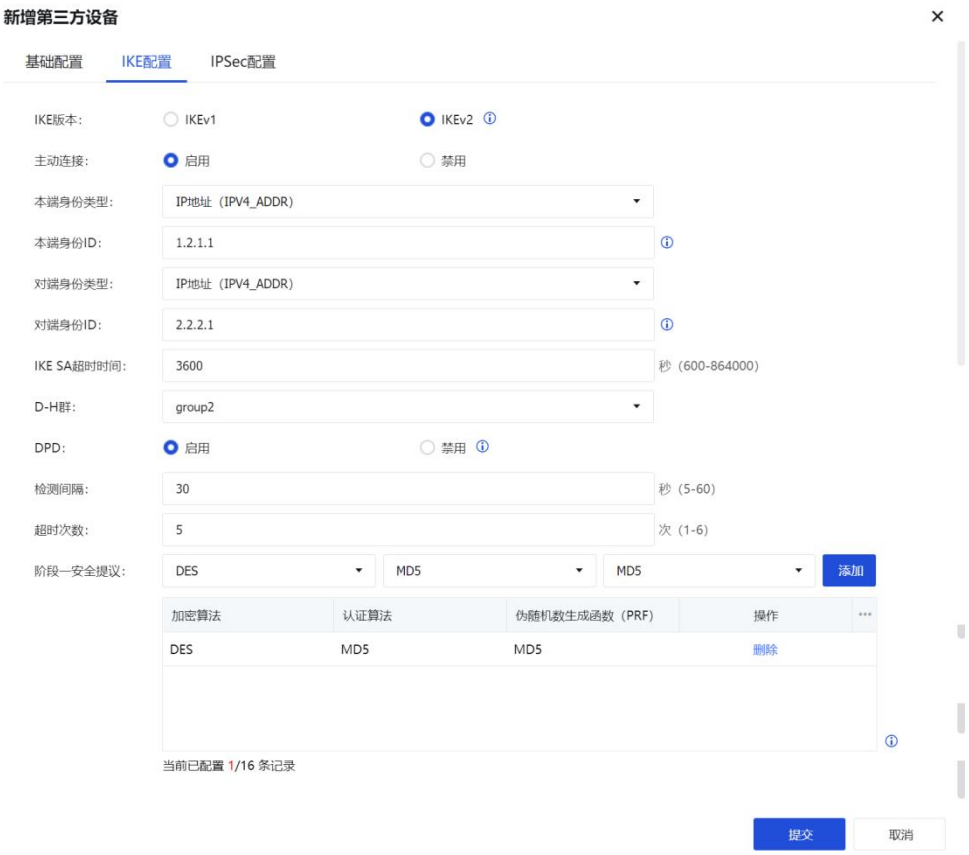


步骤3.配置VPN线路。进入[网络/Sangfor/IPSecVPN/通用配置/VPN线路配置]新增线路，填写公网IP，如下图所示。

步骤4.配置IPSEC VPN。进入[网络/Sangfor/IPSecVPN/IPSev VPN配置]新增第三方设备，进行基础配置，填写对端路由器公网IP地址2.2.2.1和预共享密钥，加密数据流填写本端地址服务器IP 192.168.1.3，对端地址填写分部内网192.168.2.0/24，如下图所示。



步骤5.配置IPSEC VPN。在[网络/Sangfor/IPSecVPN/IPSec VPN配置]进行IKE配置，选择IKEv2，本地身份ID填写1.2.1.1,对端身份ID填写2.2.2.1，加密算法选择DES，认证算法MD5，如下图所示。



步骤6.配置IPSEC VPN。再进行IPSec配置与对端一致即可，配置完成。如下图所示。

步骤7.配置应用控制策略，进入[策略/访问控制/应用控制策略/策略配置]，新增应用控制策略，源区域选择自定义的[分部区]，目的区域选择自定义的[服务器区]，服务选择http，具体配置如下图所示。

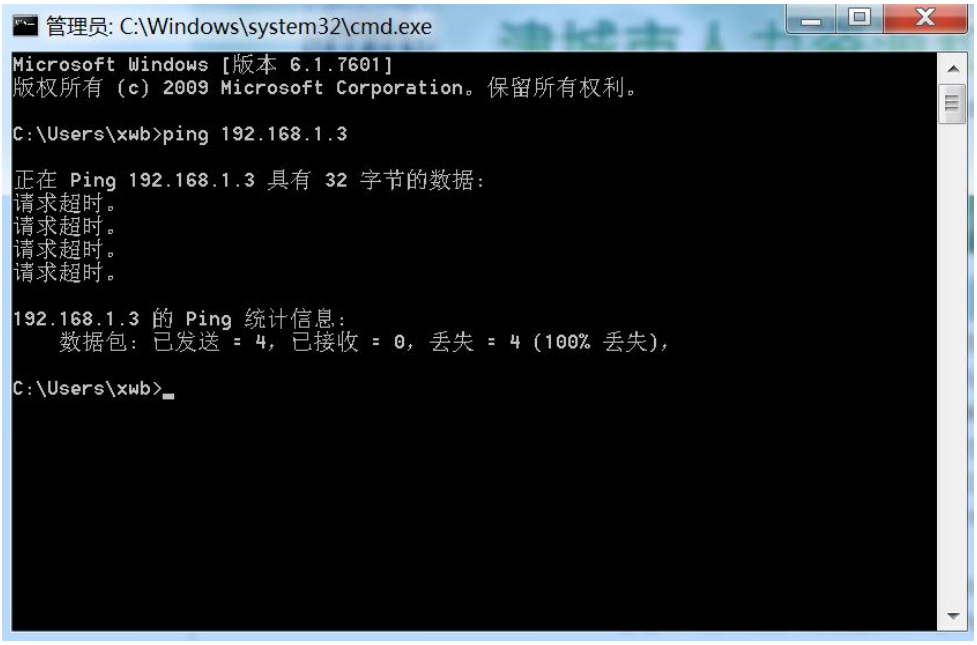
步骤8.配置安全防护策略。进入[策略/安全策略/安全防护策略]新增业务防护策略，都选择业务防护场景中的默认模板，如下图所示。

10. 4. 4. 效果预览

1. IPSEC VPN连接成功，在[网络/IPSecVPN/DLAN运行状态]能够查看到连接状态，如下图所示。

2. 通过分部电脑访问http://192.168.1.3 可以正常打开网页，如下图所示。

3. 通过分部电脑访问无法访问192.168.1.3其他服务，PING测试也不通，如下图所示。

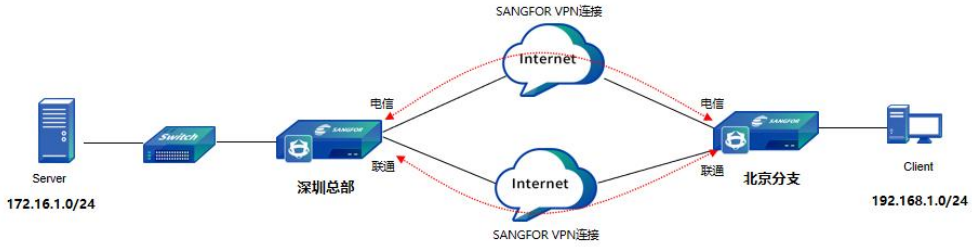


4. 通过分部电脑对192.168.1.3进行SQL注入、网站扫描等web攻击，被安全防护策略拒绝的攻击行为无法攻击成功，查看[监控/日志/安全日志]有拒绝的信息，如下图所示。

10.5. Sangfor VPN 组网场景

10.5.1. 需求背景

某企业总部和分支分别部署AF设备，出口均有两条互联网线路，现需要基于当前互联网线路部署Sangfor VPN，实现分支网段（192.168.1.0/24）和总部业务网段（172.16.1.0/24）的安全互访。



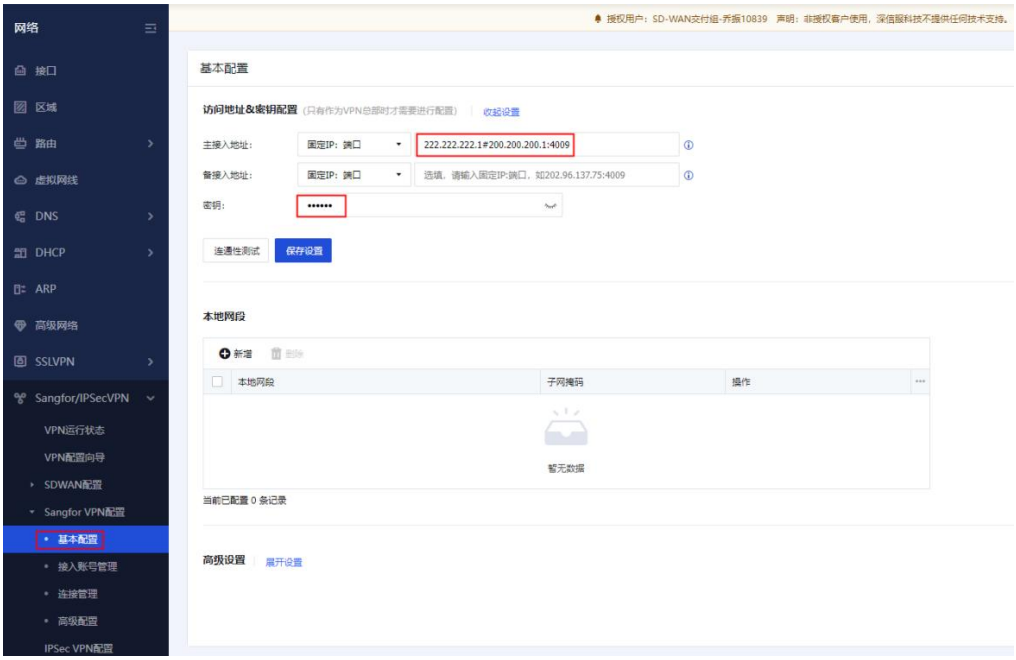
10.5.2. 需求分析

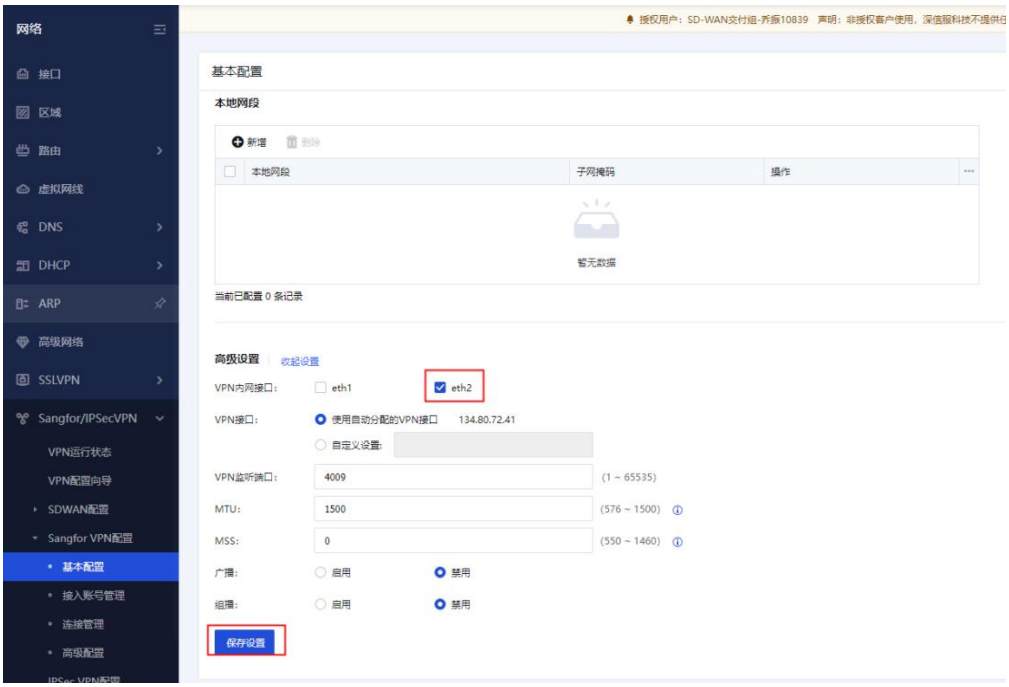
当前总部和分支各有2条运营商互联网线路，基于Sangfor VPN隧道协商机制可以同时创建2*2即4条VPN连接。后续根据业务需求，可基于当前4条VPN连接配置SDWAN智能选路，帮助用户获得最佳的业务访问体验。

10.5.3. 配置步骤

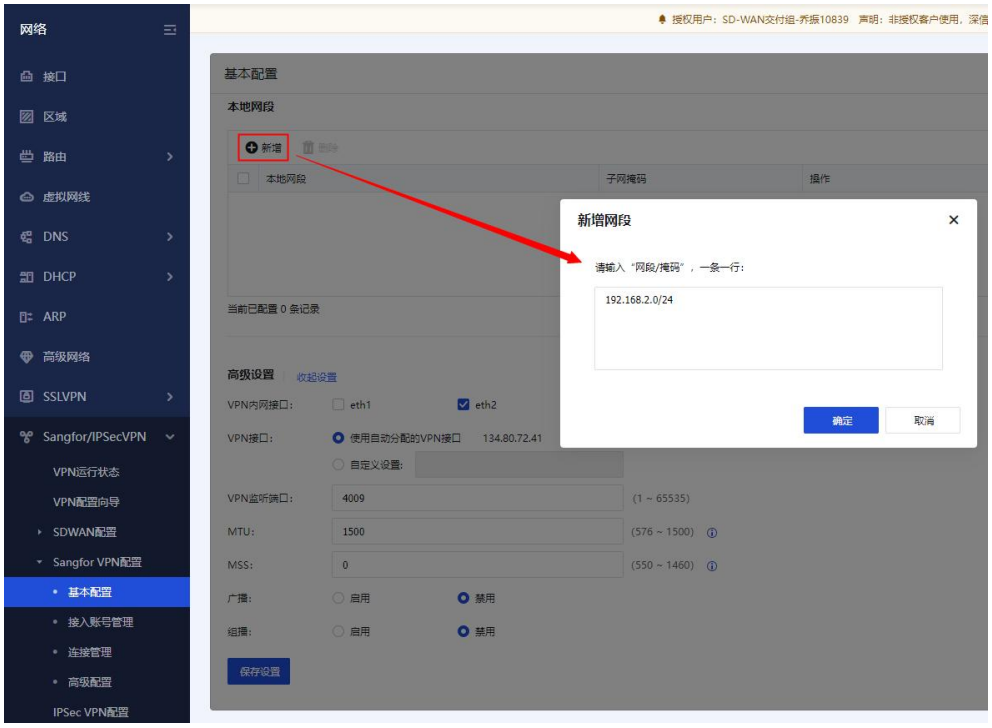
10.5.3.1. 总部端配置

步骤1. 点击[网络]-[Sangfor/IPSecVPN]-[Sangfor VPN配置]-[基本配置]，配置分支访问总部的接入地址和密钥，并且为了保证能正常建立VPN，需要勾选VPN内网接口或者配置本端需要与对端通信的本地子网，用于发布VPN路由。如下图所示。



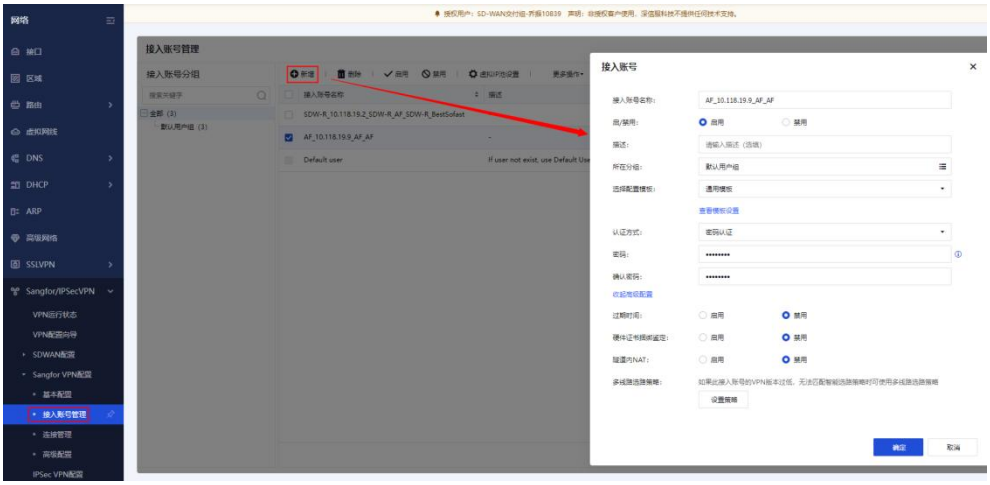


步骤2. 如果内网有其他网段，还需要配置本地子网，用于发布VPN路由实现多个网段互通。如下所示。



步骤3. 点击[网络]-[Sangfor/IPSecVPN]-[Sangfor VPN配置]-[接入账号管理]，点击 全部 (2) 可以新增分组，填写分组名称，完成分组的配置。

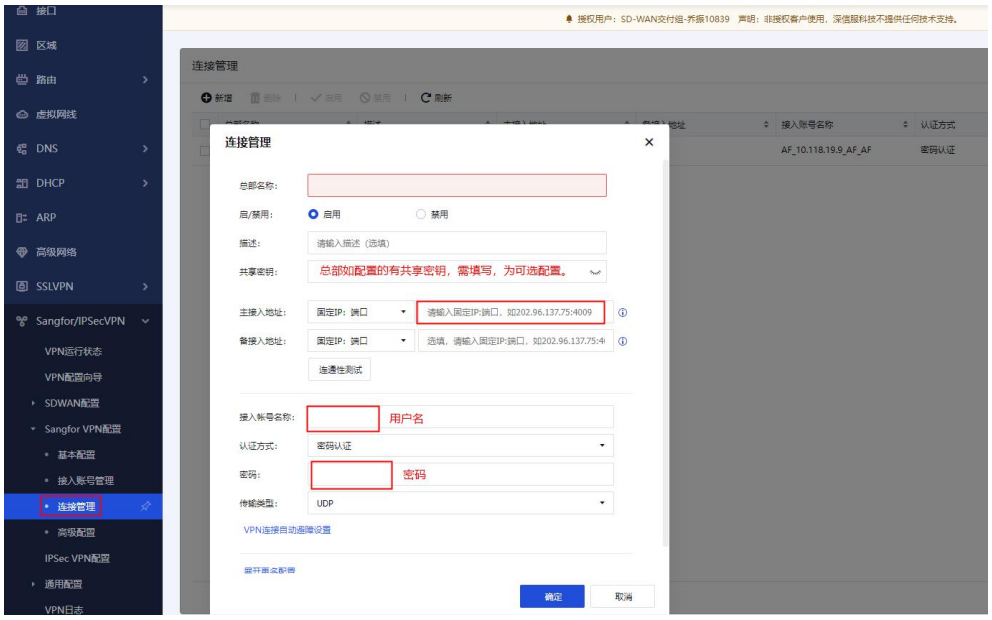
步骤4. 点击[接入账号管理]，配置VPN分支接入账号，用于管理VPN接入账号信息，设置允许接入VPN的用户账号、密码、设置账号使用的配置模板、是否启用硬件捆绑鉴权、隧道内NAT、多线路选路策略等用户策略。如下图所示。



步骤5. 配置完成之后，点击<提交>完成用户相关的配置，再在AF上放通对应的应用控制策略。

10. 5. 3. 2. 分支端配置

步骤1. 点击[网络]-[Sangfor/IPSecVPN]-[Sangfor VPN配置]-[连接管理]，可以添加一个本设备到其他VPN总部的连接，如下图所示。

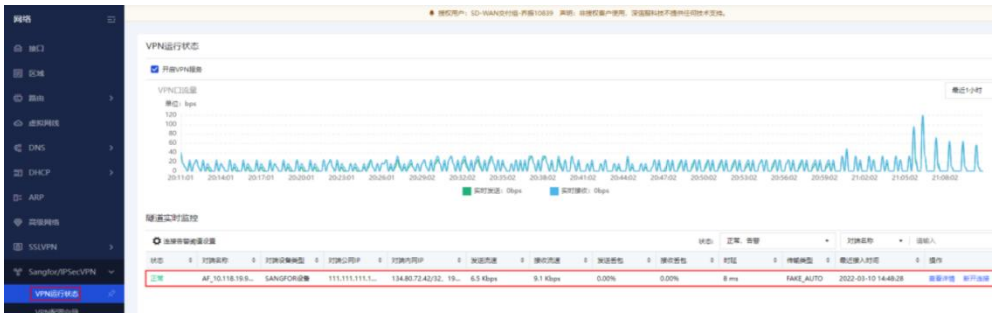


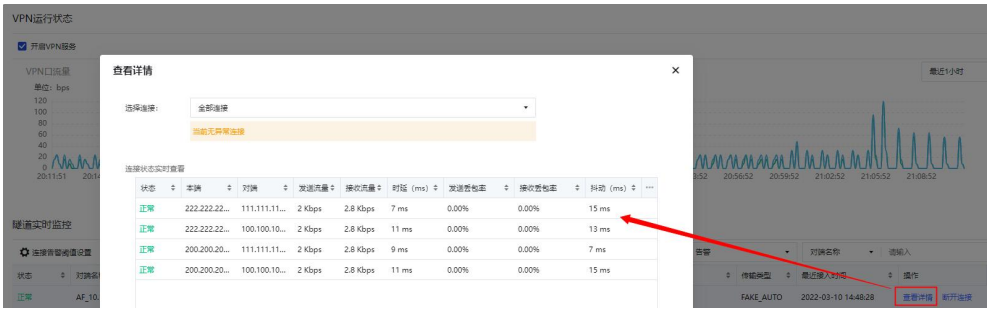
步骤2. VPN连接创建完成。如下图所示。

步骤3. 再在AF上放通对应的应用控制策略。

10.5.4. 效果预览

1. 登录总部AF设备，点击[VPN运行状态]，查看VPN隧道已成功建立。





2. 分别在总部AF和分支AF上配置VPN业务网段互访流量的应用访问控制策略，动作允许。以下图为例。

3. 配置完成后，测试业务网络连通性，如下所示：

11. 运维管理

本章主要讲解产品的运维管理，为管理员例行维护设备以及简单故障排除提供指导。

11.1. 日常巡检

维护事项	维护说明
设备搬移	在移动设备前一定要拔掉所有电源线和外部电缆。
设备上架	1、AF 2U 设备必须安装托盘或导轨。 2、用户并不具备标准机柜情况下，可将设备安装在干净的工作台上。并保证安装工作台足够牢固，足以承担设备及电缆的重量，设备四周留出 10cm 散热空间。 3、不可在设备上放置重物。 4、在机器上架安装过程中，注意同一机柜中其它设备，避免在安装过程中碰掉其他设备的电源，网线接口等
设备耳片安装	设备安装托盘或导轨后，可视情况不安装耳片。其他情况都必须安装耳片。
电源接线	有冗余电源设备必须接通冗余电源。
布线	1、布放走道线缆时，必须绑扎。绑扎后的线缆应互相紧密靠拢，外观平直整齐，线扣间距均匀，松紧适度。布放槽道线缆时，可以不扎绑。 2、信号电缆、尾纤、电源线的布放尽量避开，不要靠得太近，更不能绑扎在一起。线缆在机柜中捆扎后，应平直、捆扎整齐，不得有线缆缠绕、弯曲等现象。 3、尾纤扎绑前检查光纤走线区域附近是否有毛刺、锐边或锐角物体等，如果发现应尽量规避。在机柜外布放时，建议安装光纤保护套管（波纹管）。
标签	线缆必须贴标签注明 1、电源线标签：内容为电缆对端位置信息 ，填写标签所在电缆侧对端设备、控制柜、分线盒或插座的位置信息。 2、信号线标签：标签两面内容分别标识电缆两端所连端口的位置信息。 3、粘贴标签之前先在整版标签纸上填写或打印好标签内容，然后揭下、粘贴在电缆或标识牌线扣上。

11.1.1. 设备硬件状态检查

SANGFOR AF系列硬件设备正常工作时POWER灯常亮，设备的ALARM灯只在设备启动时因系统加载会长亮（大概1～5分钟），正常工作时熄灭。如果在使用过程中此灯亮红灯，且设备无法正常使用请按照如下步骤进行操作：

1.请立即将设备断电关闭，将系统切换到备机；

2.半小时后将设备重启，若重启设备后ALARM灯仍一直长亮不能熄灭，请速与深信服

技术支持工程师取得联系，确认是否设备损坏。

设备另个灯是HA灯，只有双机状态下才可能亮。如果设备以双机热备部署，AF6.8以后版本主机HA灯会常亮，备机HA灯会以规律闪烁标识当前状态。

11.1.2. 接口指示等检查

正常情况下，网口link灯在感知到电信号的时候会呈绿色（百兆链路，如果是千兆链路，该灯会成橙色）且长亮，网口ACT灯在有数据通过的时候会呈橙色且会不停闪烁，如果link或者act灯不闪或者不亮，请按照如下步骤进行操作：

1. 检查该网线是否破损；
2. 检查网口水晶头是否有破损；
3. 检查网卡双工模式是否协商匹配；
4. 上述均没有问题，请及时重启设备切换主备，并及时联系深信服技术支持工程师。

11.1.3. 设备运行检查

通过设备控制台的设备状态，检查CPU、内存、磁盘占用率是否长期居高，如果CPU、内存长期居高，请按照如下步骤进行操作：

注：登陆设备后显示的首页下方就是设备状态。

1. 查看[首页/网络运营/接口吞吐率趋势]，检查当前带宽是否一直处跑满的状态。
2. 查看[首页/网络运营/并发会话或新建会话]，检查是否有突发并发会话或新建会话产生。
3. 开启设备防DOS攻击模块，检查设备是否遭受到了DOS攻击，防DOS攻击日志，可在[监控/日志/安全日志]中查看。
4. 某个进程是否异常 。（需联系深信服技术支持工程师确认）

11.1.4. 设备异常状况检查

检查设备硬件是否有异常（风扇，硬盘是否有异常声响）

如果设备内部有异常声响，这个可能是硬盘或风扇的异常工作导致，请立即断开电源停止设备工作，如有备用机，请立即将系统切换到备用机；并及时联系深信服技术支持工程师以确认故障并返修设备。

11.1.5. 设备配置信息检查

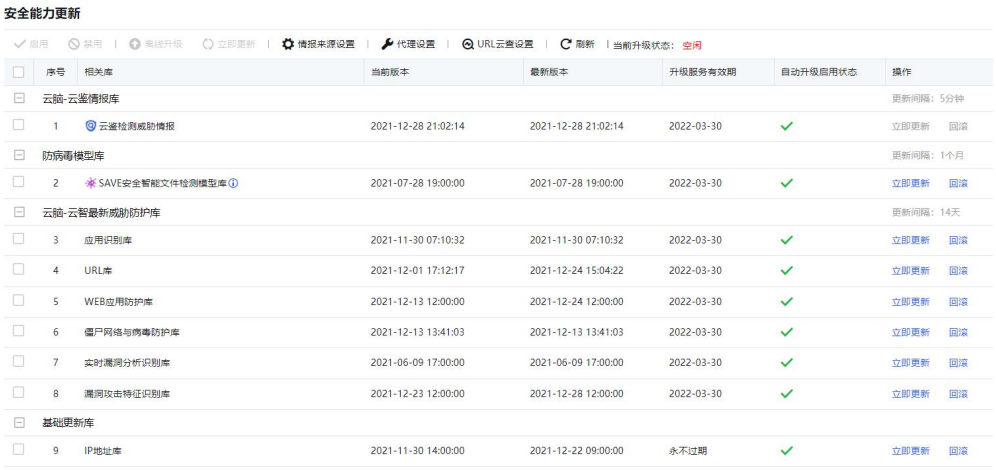
11.1.5.1. 设备配置备份

为了保证网络的稳定运行，建议客户每个月进行一次配置的备份，以防止AF系统意外瘫痪导致系统无法迅速恢复。

方法：登陆AF控制台，点击[系统/系统维护/备份与恢复]，点击<下载当前配置>下载配置并妥善保存即可，如下图所示。

11.1.5.2. 规则库版本检查

为了确保设备能够正常识别最新的网络应用，建议定期检查设备规则库是否更新，如果更新异常，请检查设备自身能否访问外网。



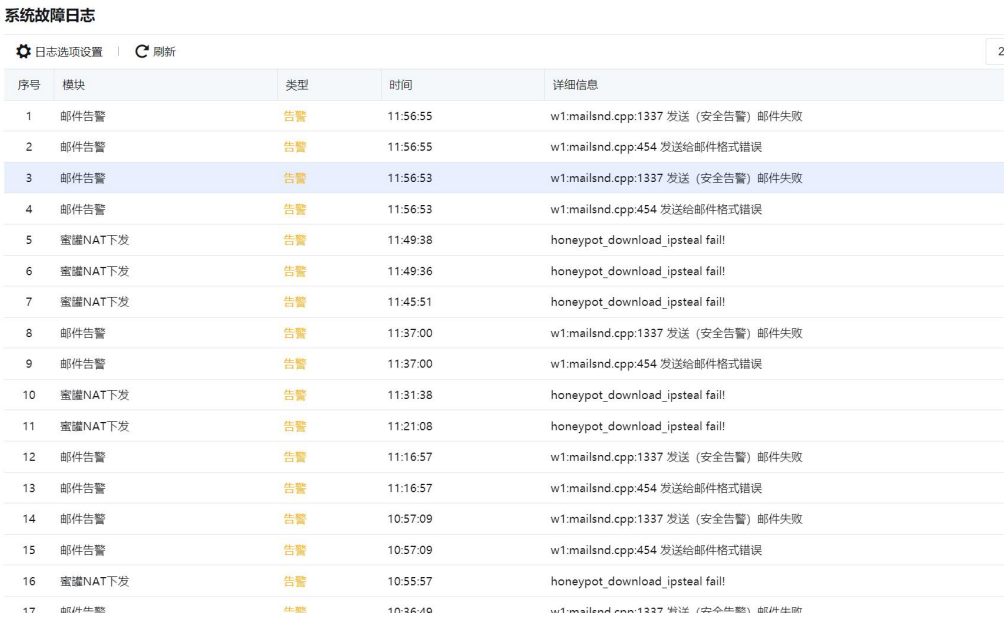
11.1.6. 设备安全检查

11.1.6.1. 控制台账号安全性检查

1. 控制台管理员密码是否为默认的admin或123456之类的简单密码。如果是默认密码或简单密码，请立即修改密码。
2. 控制台管理员密码一个月内有没有修改过，如果控制台管理员密码一个月内都没有修改过，请立即修改并妥善保存密码。
3. 控制台是否有多余账号，如sangfor、test以及公司英文等不必要的简单账号，如果有的话，请删除多余账号，仅保留授权的管理员账号。

11.1.6.2. 设备日志信息检查

通过[系统/排障/系统故障日志]，可以看到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。



系统日志包含信息、告警、错误三个级别，点击<日志选项设置>，可以过滤需要查看的级别以及模块的日志。

如果系统日志中出现大量错误日志和告警日志，请及时联系深信服技术支持工程师，确认是否设备程序运行故障。

11.2. 快捷功能

快捷功能主要介绍控制台页面使用的一些小功能，方便管理员更好的管理。主要包括

菜单搜索、漏洞CVE搜索和快速跳转标签页。

11.2.1. 菜单搜索

菜单搜索用于通过关键字搜索快速找到对应功能菜单。

步骤1. 输入功能菜单的关键字，比如“安全”，会自动出现有该关键的菜单项，如下图所示。

步骤2. 然后选择需要进入的功能菜单，比如[安全防护能力]，就会直接跳转到[安全防护能力]页面，如下图所示。

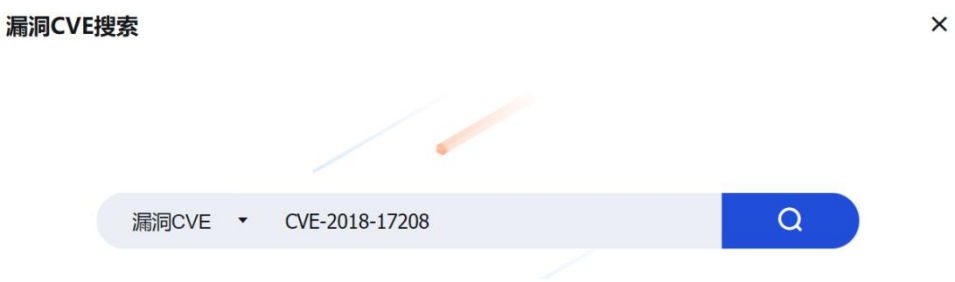
11.2.2. 漏洞 CVE 搜索

漏洞CVE搜索用于搜索AF本地的漏洞规则，查看该漏洞在AF上的防护情况。

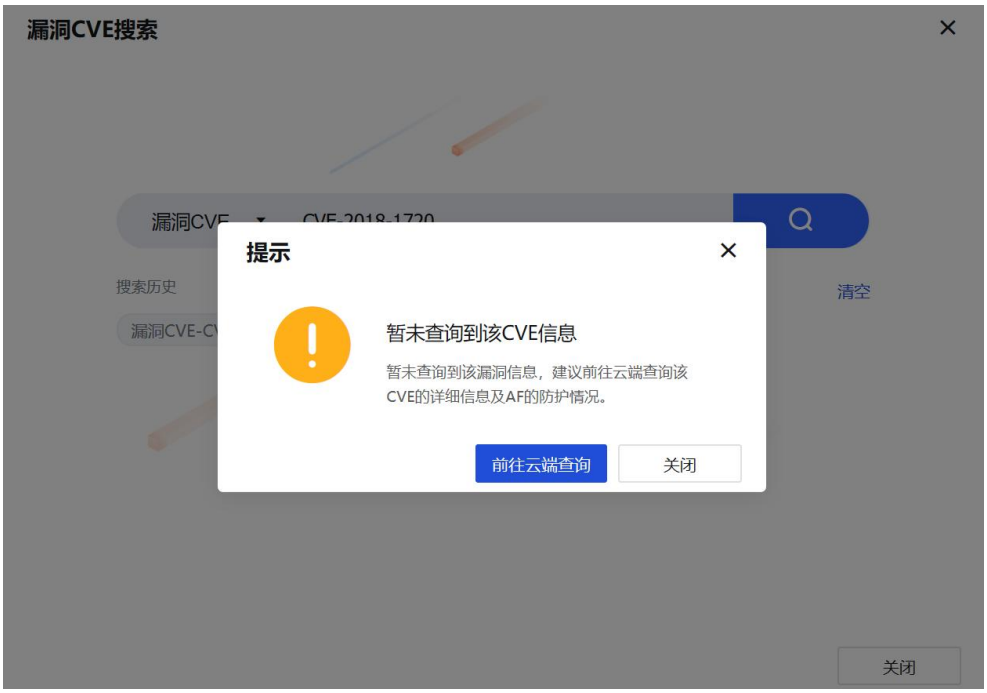
步骤1. 在[首页/快速链接]页面点击<漏洞CVE搜索>，如下图所示。

步骤2. 进入[漏洞CVE搜索]页面，可以通过漏洞名称和漏洞CVE号码查看，如下图所示。

步骤3. 输入查询的信息，如CVE-2018-17208，点击搜索按钮，如下图所示。



步骤4. 如本地规则库没有该规则，则会出现[提示]，并可以点击<前往云端查询>跳转到云端页面进行查询。如下图所示。



步骤5. 如本地规则库有该规则，则进入查询结果页面，如下图所示。

步骤6. 点击<查看详情>进入该漏洞详情页面，查看具体防护情况，并可以点击<查看云端详情>跳转到云端该漏洞规则页面。

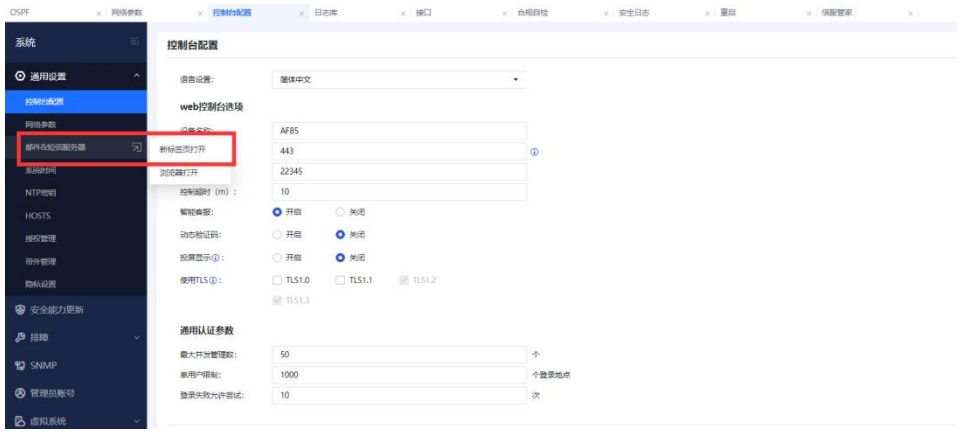
⚠ 注意：

[漏洞 CVE]的搜索方式必须是 CVE 号全匹配，如 CVE-2018-17208，不能通过模糊搜索，而[漏洞名称]的搜索方式可以通过关键字模糊匹配来进行搜索。

11.2.3. 多标签页

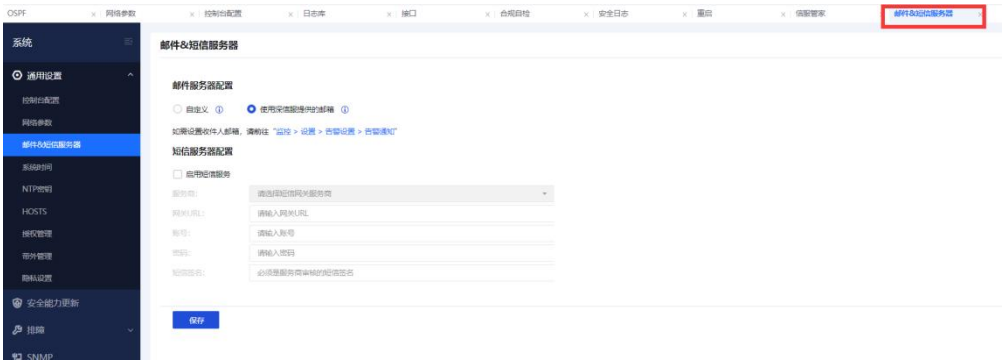
控制台界面可以展示多标签页，方便管理员进行控制台多页面来回切换操作。如下图所示。

步骤1. 在左侧栏用鼠标右键点击需要多开的标签页，如下图所示。



步骤2. 点击<新标签页打开>，即可在上方新增一个标签页，并跳转到新开标签页界

面，如下图所示。



步骤3. 再点击上方其他标签页，可跳转到其他页面进行配置，如下图所示。

11.3. 设备配置和密码恢复

设备配置和密码恢复主要介绍在需要进行相关恢复的具体场景和方法。

11.3.1. U盘重启恢复密码

U盘重启恢复密码主要介绍通过U盘来恢复AF默认管理员admin的默认密码admin。

11.3.1.1. 适用场景

由于admin密码丢失，也没有其它账号可以使用，导致无法登录控制台及后台，但仍然记得设备IP地址。

11.3.1.2. 操作步骤

AF设备支持使用U盘方式恢复密码，恢复方式步骤如下：

1. 在U盘根目录创建一个名为reset-password.txt空文件
2. 插入U盘，重启设备
3. 当设备能够正常登录控制台后，拔出U盘

4. 查看U盘中的结果文件reset-password.log，若恢复成功在该文件中记录恢复后的控制台密码，否则记录的是恢复失败信息

⚠ 注意：

1、这个 txt 文件可以直接在 windows 系统上建立空白 txt 文件，将文件名字改成对应功能要求的文件名即可。
2、txt 文件必须在 U 盘的根目录下。
3、U 盘可以为单分区或多分区。单分区的 U 盘格式必须为 FAT32；多分区 U 盘必须把 txt 文件放在第一个分区，且第一个分区格式必须为 FAT32。
4、以上三个功能不互斥，一次可以同时进行多个操作。

11.3.2. 控制台恢复出厂配置

控制台恢复出厂配置介绍通过控制台页面恢复AF的出厂配置。

11.3.2.1. 适用场景

设备可以正常登陆，希望将设备恢复出厂状态，可直接在设备WEBUI控制台直接恢复。

11.3.2.2. 操作步骤

登陆AF控制台，点击[系统/系统维护/备份与恢复]，点击<恢复出厂设置>或者恢复配置，根据提示操作即可。

⚠ 注意:

恢复出厂配置都会导致设备重启，请在恢复之前确认是否可以断网，建议在无业务或者业务低峰时间段操作，避免影响正常业务。

11.4. 补丁更新指导

11.4.1. 深信服补丁获取方式

深信服针对不同的场景提供了五种补丁获取方式：

1. 设备能与在线补丁服务器联通时：自动获取补丁；
2. 设备通过代理服务器访问外网时，配置代理服务器获取补丁包；
3. 设备无法访问外网时，通深信服OLU内网补丁服务器获取补丁包；
4. 设备不能与在线补丁服务器联通，但是访问设备控制平台的PC可以上网时：通过PC浏览器访问深信服在线补丁服务器获取补丁；
5. 设备不能与在线服务器联通，且本机PC无法上网时：可使用手机扫描二维码方式获取离线补丁。

11.4.2. 检查环节

确认设备联网情况，分为以下五种：

1. 设备正常联网，可以直接访问深信服在线补丁服务器；
2. 设备无法直接访问网络，但能使用代理上网获得规则库更新；
3. 设备离线但能使用“OLU内网补丁服务器”获得补丁更新
4. 设备离线但访问设备的PC可以联网，且不支持使用“OLU内网补丁服务器”；
5. 设备以及访问设备的PC均完全离线，且不支持使用“OLU内网补丁服务器”。

确认升级服务器设置，用户可以通过以下三种方式设置升级服务器：

1. 手动输入服务器地址：手动输入OLU内网补丁服务器地址，则可以从OLU内网补丁服务器中获取补丁更新。(OLU内网补丁服务器只支持补丁更新，暂不支持规则库更新)；
2. 自动选择服务器地址：设备会在深信服支持的在线升级服务器中轮寻，自动选择一个最优的服务器获取更新信息；
3. 选择特定的服务器地址：指定从特定的在线补丁服务器上获取更新信息。

11.4.3. 场景介绍及配置

场景介绍及配置主要介绍设备在各个场景下如何进行补丁的更新。

11.4.3.1. 设备能联网且开启补丁自动更新

设备能联网且开启补丁自动更新，那么无需用户操作，用户可查看已经更新的补丁。

管理员进入[系统/系统维护/补丁更新]补丁更新页面，查看更新的补丁。

11.4.3.2. 设备能联网且未开启补丁自动更新

设备能联网且未开启补丁自动更新，那么设备可以自动获取更新补丁，但是需要用户操作，才能安装补丁。

1. 管理员进入[系统/系统维护/补丁更新]补丁更新页面，查看补丁更新列表；
2. 点击<一键安装>，执行补丁安装。
3. 查看补丁是否成功安装。

⚠ 注意:

建议用户自动[补丁自动更新]功能，涉及到重启设备或者其他特殊场景的补丁更新时会提醒客户，需要手动确认后才会执行此类补丁的更新。

11.4.3.3. 设备通过代理服务器获得补丁更新

若设备不能联网，但是内网有可以代理上网的服务器，那么可以通过设置代理服务器，使设备通过用户内

在配置完代理服务器后，且设备通过代理服务器能正常访问外网后，设备获取补丁包的方式则和场景一、

1. 进入[系统/系统维护/补丁更新]点击<更新设置>，如下图所示。

2. 勾选[启用代理服务器]，填写代理服务器的IP地址、端口。如果连接代理服务器需要用户名和密码，则勾选[验证用户]输入代理服务器需要验证的用户名和密码（此部分的信息由客户提供）。

11.4.3.4. 设备不能联网但访问设备的 PC 可以上网

设备不能与在线补丁服务器联通，但访问设备控制台的PC可以上网时：通过PC浏览器从深信服在线补丁服务器上获取补丁。

1. 管理员通过首页提醒，或者补丁更新页获取更新的补丁检测。（用户登录设备的控制台后都会有提示）。
2. 通过补丁更新页获取补丁：点击[补丁更新]界面的<获取补丁包方式>按钮。

3. 管理员下载补丁到本地，再通过<手动上传安装>将下载的补丁上传到设备安装。

11.4.3.5. 设备不能联网且 PC 不能联网

设备不能与在线服务器联通，且访问设备的PC无法上网时，可使用手机扫描二维码方式获取离线补丁。

1. 用户可以在登录首页或者补丁更新页，点击<获取离线补丁包>，用手机扫描弹出窗口里的二维码，复制链接下载补丁更新。

2. 用户可以将下载的补丁传到PC后，进入补丁更新页，在手动安装，并查看补丁安装成功的情况。

11.4.4. 注意事项

1. 如果不能联网，尽可能的帮助用户在内网搭建OLU服务器。
2. 如果用户仍不同意，告诉用户可以浏览器代理或扫描二维码的方式获取补丁。
3. 升级配置结束后，需要扫描二维码自动上报设备信息。
4. 需要重启设备的补丁包不会通过自动更新下发，只能手动更新。
5. 需要重启服务的补丁包会弹提示让客户确认。

11.5. 常见问题排查

常见问题排查主要介绍AF运维中遇到的部分常见问题的现象以及处理流程，方便管理员根据情况快速进行处理。

11.5.1. 无法登陆 AF 控制台

1. 检查设备面板上红色alarm灯是否常亮。
2. 是否能够正常ping通设备内网口。
3. 从内网是否能telnet通设备443、51111端口。
4. Tracert设备内网口地址，看数据包是否能够到达AF设备内网口。
5. 尝试用一台电脑通过网线接到MANAGE口(默认eth0口)，将电脑的IP配成10.251.251.0/24网段，测试访问MANAGE口的默认IP 10.251.251.251是否能通。
6. 换浏览器重复5步骤。
7. 如经过上述步骤仍无法登陆设备，请速联系深信服技术支持工程师。

11.5.2. 业务系统访问异常

1. 检查业务系统本身是否正常。
2. 检查AF应用控制策略是否放行数据。
3. 将AF开直通再测试是否可以正常访问网络应用。
4. 深信服AF设备提供在设备出现异常情况下一键软bypass功能。

具体操作：

在[系统/排障/故障排查]点击<开启全局直通分析>功能，此操作将使设备所有具备拦截功能的模块失效，并打出本应被拦截但是当前状态下放通的数据信息。

5. 如经过上述步骤应用依然无法正常使用，请速联系深信服技术支持工程师

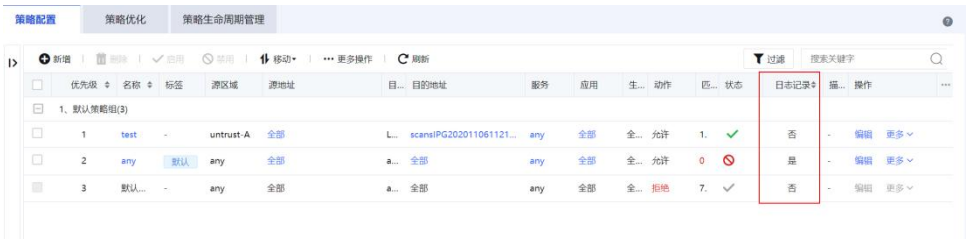
11.5.3. 设备 IO 异常

当经过设备的流量变大的时候，设备的性能就明显下降，登入控制台比较卡顿，或者直接登录控制台失败，更有严重的时候出现设备的假死状态，上网变慢，甚至断网。

排除了dos/ddos攻击等攻击导致的设备异常之外，还有一种容易忽略的问题：

AF开启应用控制策略中的日志记录或者是流量审计记录，磁盘频繁的读写，导致IO和cpu飙高，甚至导致磁盘损坏。这类日志是强烈不建议在内置数据中心中记录的，建议使用外置数据中心或者是syslog 服务器记录。

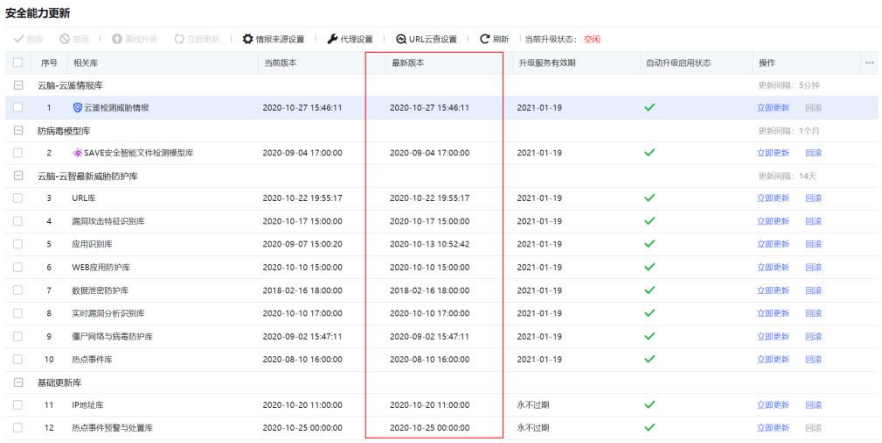
应用控制如下图：（日志显示为是，代表记录日志）



流量审计日志如下图（一般不要开启，如需开启推荐使用syslog或者安全感知系统来记录，不推荐在防火墙记录）：

11.5.4. 规则库无法更新

1. 检查[系统/系统更新/库升级]中，相应规则库升级服务有效期是否最新。



2. 如果设备本身不能上网，又要更新规则库如何处理，官网上下载离线规则库升级，如果官网还没有联系400或者当地驻外技术服务人员上门更新规则库。

11.6. 突发事件应急处理

11.6.1. 重要业务系统异常或断网

1. 针对该业务系统，开启定向数据流分析，看业务系统是否恢复正常，如果恢复，则通过查看拦截日志，找到拒绝数据的模块，修改策略。关闭定向数据流分析，测试业务访问是否恢复正常，如果仍然未恢复，则再开启定向数据流分析，根据拦截日志修改策略，直到故障修复。
2. 从内网PC上ping下AF设备，测试PC能否正常访问AF，如果能正常访问AF，尝试使用命令行工具从AF上分别ping一下网关和外网，确认外网是否正常。
3. 开启全局直通分析，看用户上网是否恢复，如果恢复，则通过查看拦截日志，找到拒绝数据的模块，修改策略。关闭全局直通分析，测试上网是否恢复正常，如果未恢复，则再开启全局直通分析，根据拦截日志修改策略，直到故障修复。
4. 设备网桥部署，确认设备桥接接口是否为bypass口，设备接口面板一般有标注bypass接口，如果未标注则默认eth0和eth2口是一对bypass接口，如果使用bypass接口为网桥接口，可尝试关闭设备测试。
5. 可以关闭设备看业务是否恢复，如果设备界限不是一堆bypass口，可以将上下联节可接入一对bypass口看业务是否恢复，或者直接跳开防火墙。
6. 上述操作依然无法排除故障，可尝试跳过设备做进一步验证。
7. 如果跳过设备业务系统恢复正常，请联系深信服技术支持检查设备是否异常。
8. 如依然无法排除故障，请检查其他网络设备配置是否异常。

11.6.2. 设备硬件故障

Alarm灯不亮，设备无法通电

1. 跳开设备恢复网络。
2. 先确定设备有几个开关，部分设备只有一个硬开关，其他设备分为一个硬开关一个软开关（弹性开关）
3. 如果只有一个硬开关的设备，打开开关，如果设备无法通电，Alarm灯不亮，更换排插和电源线，依旧无法通电，请联系深信服技术支持返修。
4. 如果设备有两个开关，则先打开硬开关，再按下软开关（弹性开关）方能正常开机。如果按上述方式操作后并且更换电源插座和电源线之后，设备仍不通电，请联系深信服技术支持返修。

Alarm长亮，无法登录设备

1. 跳开设备恢复网络。

2. 关机30分钟后，再开机并等待2小时，如两小时内设备正常启动，说明设备之前进入自检状态，如两小时后alarm等依旧长亮，请联系深信服技术支持返修。

网口故障

1. 更换一根网线，检查接口能否正常工作。
2. 尝试修改故障接口的速率和双工模式，确认是否网口兼容性问题。
3. 在[网络/接口/物理接口]点击对应接口，进入[高级设置]分别尝试各种速率和双工模式，检查接口能否正常工作。

4. 将故障接口接交换机其他接口或其他网络设备，检查接口能否正常工作。
5. 将设备跳开网络，联系深信服技术支持确定硬件故障并返修。

12. 产品升级指导

产品升级指导主要介绍设备系统升级的具体方法以及升级前后的检查。

12.1. 产品升级步骤

1. 内网升级场景，升级前需提前准备好升级包，确保升级包的完整性。
2. 在[深信服社区/自助服务/软件下载/下一代防火墙AF]获取升级包下载链接，下载并保存到电脑本地。
3. 使用MD5校验工具校验升级包的MD5，保障升级包的完整性。
4. 在线升级场景，升级前需保障待升级设备和服务端网络畅通。

12.2. 产品升级前检查

升级前需要确认本版本是否支持直接升级到目标版本，升级是否影响老功能特性，升级后是否需要重启，升级时间估算，用户配置、日志、数据是否平滑升级、升级限定条件。请先登录深信服社区，访问如下链接查找目标版本升级文档确认升级细节：https://bbs.sangfor.com.cn/plugin.php?id=service:download&action=view&fid=100000003677756#/100000011367652/all/undefined

12.3. web 系统升级指导

web系统升级方法用于升级要求方法简明，设备本身可以访问公网或者云端服务器已放置升级包等升级场景使用，这种升级方式升级过程更加直观，升级过程更透明，无需额外工具配合。

12.3.1. web 系统升级步骤

web系统升级分为在线升级和离线升级两种方法。

在线升级，进入设备web控制台[系统/系统更新/系统升级]路径后，设备会自行联网检查，服务器端是否有高于当前设备软件版本的升级包，如果有，提示可以在线升级；如果没有，提示“已是最新版本！”

离线升级，进入设备web控制台[系统/系统维护/系统升级]路径后，点击<离线升级此设备>按钮，上传本地升级包，并按照提示操作，完成升级。

12.3.2. web 系统升级操作方法

步骤1.进入[系统/系统维护/系统升级]页面，如下图所示。

步骤2.点击<离线升级此设备>，进入到[准备升级包]页面，如下图所示。

步骤3.点击<上传升级包>，选择下载好的版本升级包进行上传，如下图所示。

⚠ 注意：

上传升级包过程中不能关闭该页面，否则需要重新进入页面再执行升级操作。

步骤4.升级包上传完成后，点击<下一步>完成配置的备份即可开始升级，升级完成后，手动[重启设备]。完成重启后，登录设备控制台，检查设备升级后状态。

12.4. BBC 下发升级任务指导

BBC下发升级任务方法用于AF设备加入BBC做集中管控升级场景使用，这种升级方式适用于多分支AF设备批量完成升级任务。

12.4.1. BBC 下发升级任务步骤

1. 登录BBC控制台，[管理/设备升级/分支设备升级]。
2. 新增升级计划，完成升级计划配置。
3. 在计划升级时间，BBC自动对分支AF设备下发升级任务。

12.4.2. BBC 下发升级任务操作方法

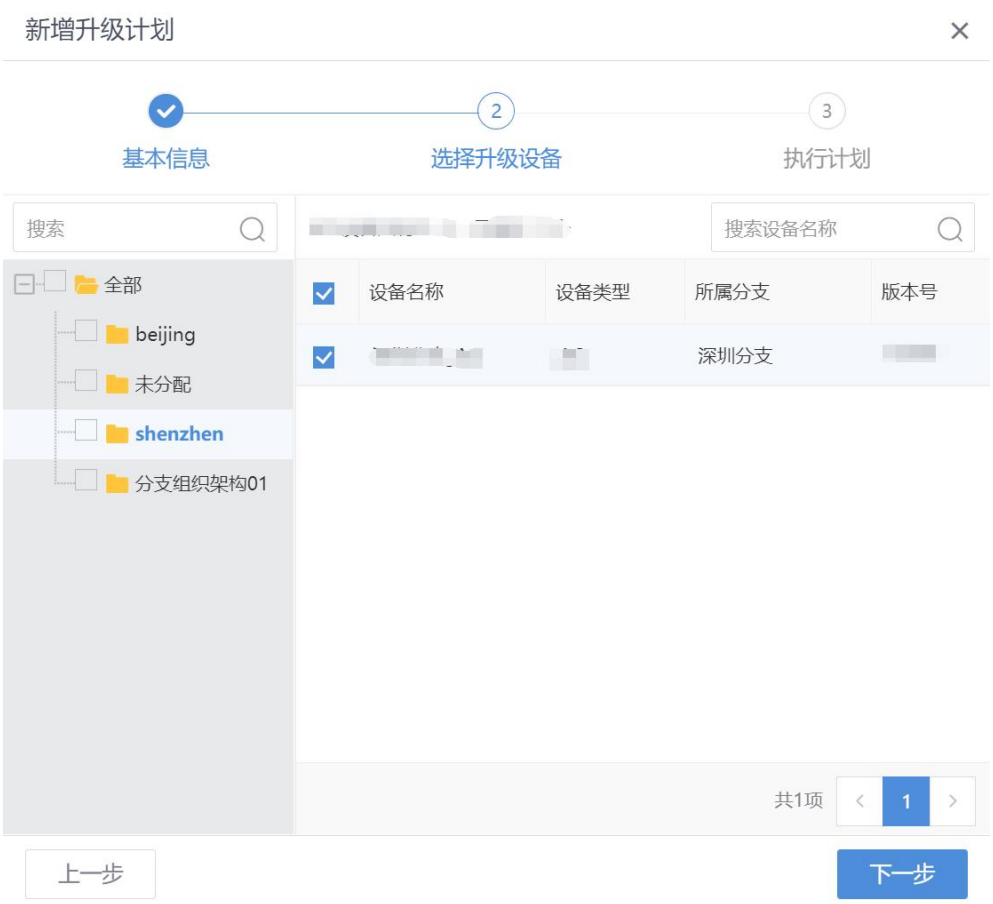
步骤1.管理员登录BBC设备控制台，在[管理/设备升级/分支版本设备]页面，点击<新增升级计划>完成配置基本信息。

⚠ 注意：

1．如果 BBC 设备本地未上传过升级包，可以点击<新增升级包>加载需升级版本的软件升级包。

2．分支设备获取升级包方式，可以通过与 BBC 通讯获取升级包或在 BBC 设备勾选“优先从公网服务器下载升级包”两种方式。

步骤2.点击<下一步>，选择升级设备，定义批量升级范围。



步骤3.点击<下一步>，配置执行计划。

步骤4.到了升级计划时间后，会触发执行升级任务。

12.5. 产品升级后检查

网络连通性检查：

序号	检查项	检查要求
1	终端上网是否正常	设备上线，不影响终端的正常上网需求
2	服务器主动访问外部特定地址是否正常	设备上线，不影响用户要求的服务器主动访问外部特定地址
3	服务器对外发布的业务是否访问正常	设备上线，不影响服务器对外发布业务的正常使用
4	双机按 POC 手册要求切换是否正常（有双机环境）	确保按 POC 手册给出的切换方案，各切换结果满足预期要求
5	管理员是否可通过管理地址访问到 AF	确保 AF 可以远程打开控制台，同时界面操作正常
6	设备自身是否可以正常访问互联网	设备需要连接互联网，用来更新规则库和补丁包

设备健康检查：

序号	检查项	检查要求
1	设备 CPU 使用率是否正常	正常情况，CPU 平均使用率应 70%以下
2	设备内存使用率是否正常	正常情况，内存平均使用率应 70%以下
3	系统日志是否有错误或告警日志	正常情况系统日志应无错误日志，异常情况请联系厂商处理
5	是否已关闭外网远程维护	基于安全考虑，要求实施完成后，外网远程维护建议关闭的
6	检查是否有备份设备配置	实施完成后，应该备份设备配置，本地存档
7	规则库是否升级到最新	基于应用识别准确度考虑，要求实施完成后，保证当前规则库更新到最新
8	数据中心配置符合《网络安全法》规定留存相关的网络日志不少于六个月要求	实施完成后，如果使用防火墙期望保留天数需大于等于 180 天；如果使用外置 syslog 期望保留天数需大于等于 180 天

13. 缩略语

缩略语	英文全称	中文全称
SNMP	Simple Network Management Protocol	简单网络管理协议
RADIUS	Remote Authentication Dial In User Service	远程用户拨号认证服务
DNS	Domain Name System	域名系统（服务）协议
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
ARP	Address Resolution Protocol	地址解析协议
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
VLAN	Virtual Local Area Network	虚拟局域网
NAT	Network Address Translation	网络地址转换
NetBIOS	Network Basic Input/Output System	网上基本输入输出系统
BBC	Branch Bussiness Cente	深信服集中管理平台 BBC
IM	Instant Messaging	通讯软件
EDR	Endpoint Detection and Response	终端检查响应平台
AD	Active Directory	活动目录
VPN	Virtual Private Network	虚拟专用网络