UNIS ACG1000 系列应用控制网关

典型配置举例

紫光恒越技术有限公司
www.unisyue.com

资料版本：5W100-20200717

前 言

本配置指导主要介绍了 UNIS ACG1000 系列应用控制网关的常见典型应用及其配置步骤。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

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

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其它运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@unisyue.com

感谢您的反馈，让我们做得更好！

目录

1 简介

本文档介绍设备的 QoS 配置举例，包括通道化的、基于接口、IP 地址、应用和时间的 QoS 配置。在配置 QoS 前，先了解如下几个定义：

- 地址、应用、时间表对象：每一个报文对应的会话或匹配的策略，会携带 IP 地址、应用 ID、时间戳等元素，当上述元素和 QoS 策略中引用的地址、应用和时间表对象全部匹配时，QoS 策略对这些会话上的报文生效。
- 保障带宽：当应用的流速大于或等于流量控制通道配置的保障带宽时，配置的保障带宽值就是该应用的最小带宽，这部分带宽不可以被其它应用抢占。而当应用的流速小于控制通道配置的保障带宽时，空余的带宽可以被其它应用抢占。
- 最大带宽：指定应用被允许达到的最大流速，超过最大带宽部分的流量将被设备的丢弃。
- 线路和通道：线路和接口一一绑定，用来控制接口的上下行流速；流量控制通道分为层级，最多支持 4 级通道，其中第 1 级通道的上一级通道是线路，第 2 级通道的上一级通道是第 1 级通道，以此类推。上一级和下一级之间互为父子节点关系，配置的最后一级通道为叶子节点，每一个叶子节点都会自动创建一个默认通道，默认通道的带宽是通过该级父节点和所有子节点的带宽自动计算出来的。
- 匹配顺序：报文按照从父节点到子节点的顺序进行逐级匹配，直到报文到达无法匹配的一级时，随即匹配该级别的默认通道。
- 通道优先级：当父通道带宽充足，而其子通道中的保障通道尚未用满带宽时，同级的其它子通道可以借用上述通道的空余带宽。借用时，按照优先级高>中>低的顺序严格借用，即当高优先级通道带宽借满时，中优先级通道才可以开始借用，以此类推。当存在多条优先级相同的通道共同借用带宽时，这些通道将平分空余的带宽。
- 通道带宽自适应： 目前配置 QoS 功能的时候支持绝对值输入、采用绝对值输入对用户体验不是非常友好、用户很难判断输入多大的速率是比较合适的、特别是在层级 QoS 中；QoS 保障带宽和最大带宽和父通道还有子通道都有一定的关系、所以这就更加增添了客户配置 QoS 的难度；
  - 为了解决上述情况、增加 QoS 百分比功能、允许客户输入百分比；
  - 其中最大带宽为父通道的最大带宽百分比。
  - 保障带宽为父通道的保障带宽百分比。
  - 当调整父通道带宽线路后，子通道带宽根据初次算的带宽百分比乘以调整后的线路带宽，算出新的带宽值。
  - 为了保证百分比输入的一致性，QoS 百分比只在页面上提供输入接口。
- 带宽自适应算法说明：
  - 初次配置的带宽 百分比是基数不会变。
  - 用带宽/线路值=百分比 A（如果≥8Kb 显示正常的带宽；算出来的带宽＜8kb，带宽置为 8kb，百分比 A 不变（带宽最小 8kb）。
  - 调整线路后，用百分比 A*调整后的线路=带宽值。如果≥8Kb 显示正常的带宽；算出来的带宽＜8kb，带宽置为 8kb，百分比 A 不变（带宽最小 8kb）。
  - web 页面 qos 通道页面编辑后提交。相当于带宽重新下发，需要以 web 页面当前的带宽和线路算百分比。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 QoS 特性。

3 使用限制

QoS 控制流速的粒度范围为 8Kb～40Gb，不可配置超出该范围的流速值。

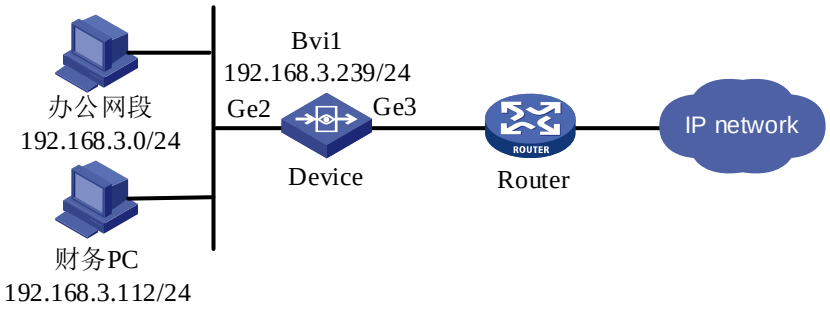
4 配置举例

4.1 组网需求

如图 1 所示，某公司内网办公网段 IP 地址为 192.168.3.0/24，其中预留 IP 地址 192.168.3.112 给财务 PC 使用。使用设备的的 ge2 和 ge3 接口作为透明桥，串接部署在网络中，在设备上启用 QoS 功能。具体应用需求如下：

- 将设备的 ge3 接口的上行流速和下行流速均限制为 8Mbps。
- 针对办公网段用户，限制其上下行流速均为 6Mbps，保障其上下行流速均不小于 4Mbps，该策略生效时间为每周一至每周五的 9:00-18:00。
- 针对办公网段用户的 HTTP 网页浏览和 HTTP 网页图片浏览/下载两个应用，限制其上下行流速均为 5Mbps，保障其上下行流速均不小于 3Mbps，该策略生效时间为每周一至每周五的 9:00-18:00。
- 针对办公网段用户的各种 P2P 软件应用，限制其上下行流速均为 1Mbps，并限制每 IP 的上下行流速均为 500Kbps，该策略生效时间为每周一至每周五的 9:00-18:00。
- 针对财务 PC，不进行 QoS。
- 后续公司将出口带宽升级为 20M 线路，线路下的所有通道带宽根据新的线路带宽自适应调整通道下的带宽。

图1 QoS 通道限速功能配置组网图



4.2 配置思路

- 配置 QoS 时，首先基于接口绑定线路。
- 配置好线路后，基于线路逐级配置基于 IP 地址、应用和时间等其它条件的流量控制通道。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- 在设备的 QoS 配置中，上级通道和下级通道互为父子关系，要求所有子节点的带宽之和必须小于父节点的带宽。在配置前，可以预先对每一层通道需要配置的带宽进行规划。
- 在设备的 QoS 配置中，保障带宽不允许配置为空，保障带宽最小可以设置为 8kbs，如果在流控策略中中没有保障带宽的需求，可直接使用限制通道。
- 设备在透明部署模式下配置 QoS 时，线路中绑定的接口必须是 bvi 接口的成员物理接口，功能才能生效，若在线路中绑定 bvi 接口则 QoS 功能无法生效。
- 设备在三层部署模式下进行 QoS 时，线路中绑定的接口必须是三层接口，功能才能生效。另外，当使用 bvi 接口进行三层转发时，QoS 线路需要绑定在 bvi 接口上才能生效。
- 设备在子接口模式下进行 QoS 时，线路中绑定的接口必须在子接口上做，绑定在子接口的物理口上不生效
- 设备在聚合接口模式下进行 QoS 时，线路中绑定的接口必须在聚合接口上做，绑定在聚合接口的物理口上不生效

4.5 配置步骤

4.5.1 配置设备

1. 配置地址对象和时间表对象

(1) 配置地址对象

如图 2 所示，进入“策略配置>对象管理>地址对象> IPv4 地址对象”，点击<新建>，IP 地址配置为 192.168.3.0/24 创建办公网段地址对象，点击<提交>。按照同样的方法配置财务 PC 地址对象。

图2 配置地址对象

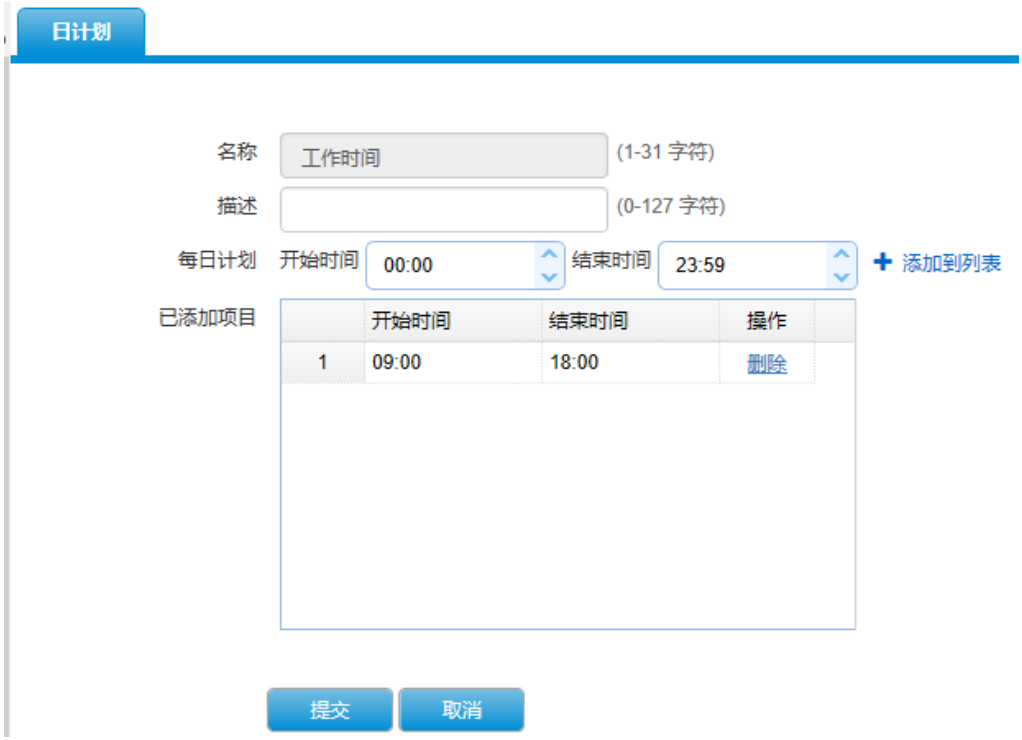
如图 3 所示，创建成功的地址对象配置如下：

图3 地址对象配置成功

(2) 配置时间对象

如图 4 所示，进入“策略配置>对象管理>时间对象>日计划”，点击<新建>，“开始时间”和“结束时间”配置为 9:00 和 18:00，命名为“工作时间”，点击<提交>。

图4 配置日计划时间表对象



如图 5 所示，创建成功的日计划时间表对象配置如下：

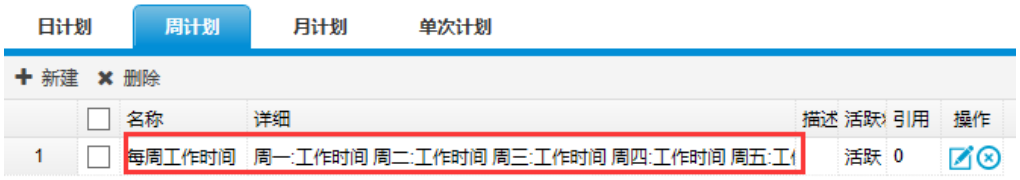
图5 日计划时间表对象配置成功

如图 6 所示，进入“策略配置>对象管理>时间对象>周计划”，点击<新建>，在周一到周五的下拉菜单中选择“工作时间”，命名为“每周工作时间”，点击<提交>。

图6 配置周计划时间表对象

如图 7 所示，创建成功的周计划时间表对象配置如下：

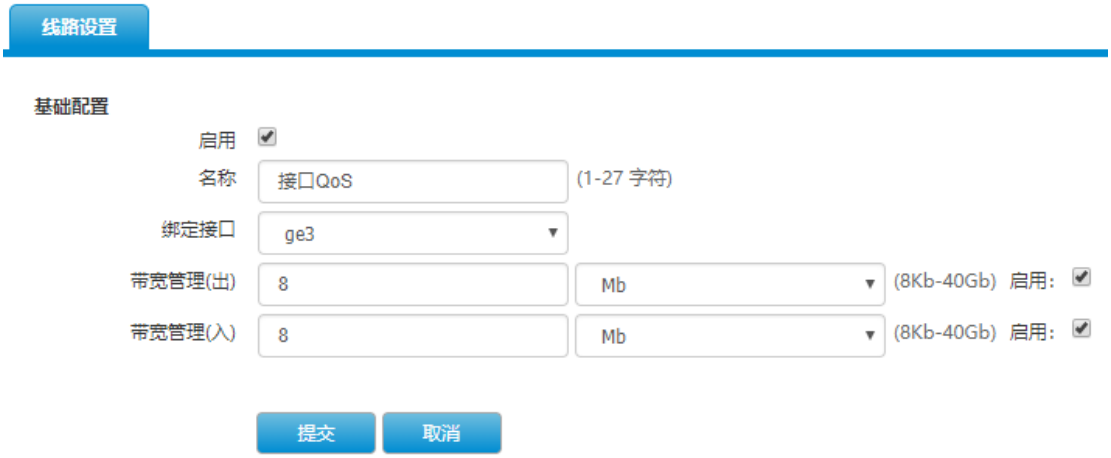
图7 周计划时间表对象配置成功



2. 配置线路

如图 8 所示，进入“策略配置>流量控制策略>流量控制”，点击<新建>，选择<线路>，“绑定接口”配置为 ge3，“带宽管理（出）”和“带宽管理（入）”均配置为 8Mb（这里出和入的方向基于 ge3 接口），命名为“接口 QoS”并点击<提交>。

图8 配置线路



如图 9 所示，创建成功后的线路配置如下：

图9 线路配置成功

3. 配置流量控制通道

(1) 配置办公网段流量控制通道（1 级）

如图 10 所示，进入“策略配置>流量控制策略>流量控制”，使用鼠标单击选中线路“接口 QoS”，再点击<新建>，选择<通道>弹出配置页面。“级别”配置为高，在“带宽设定”中将上下行的最大带宽均配置为 6Mb，上下行保障带宽均配置为 4Mb，“匹配条件”配置为办公网段、“时间”配置为每周工作时间，命名为“办公网段 QoS”并点击<提交>。

图10 配置办公网段流量控制通道

(2) 配置办公网段 HTTP 保障流量控制通道（2 级）

如图 11 所示，进入“策略配置>流量控制策略>流量控制”，使用鼠标单击选中通道办公网段 QoS，再点击<新建>，选择<通道>弹出配置页面。“级别”配置为高，在“带宽设定”中将上下行的最大带宽均配置为 5Mb，上下行保障带宽均配置为 3Mb，在“匹配条件”中的“应用”配置为网络协议/网页图片浏览_下载和网络协议/网页浏览(HTTP)、“时间”配置为每周工作时间，命名为“办公网段 HTTP 保障”并点击<提交>。

图11 配置办公网段 HTTP 保障流量控制通道

(3) 配置办公网段 P2P 限速（限制通道）

如图 12 所示，进入“策略配置>流量控制策略>流量控制”，使用鼠标单击<新建>，选择<限制通道>弹出配置页面。在“带宽设定”中将上下行的最大带宽均配置为 1Mb，每 IP 限速上下行均配置为 500Kb，接口选择 ge3，“匹配条件”中的“应用”配置为 P2P 软件和 P2P 流媒体，“时间”配置为每周工作时间，命名为“办公网段 P2P 限速”并点击<提交>。

图12 配置办公网段 P2P 限速

如图 13 所示，整体配置完成的流量控制通道如下：

图13 整体流量控制通道创建成功

4. 配置 QoS 排除策略

如图 14 所示，进入“策略配置>流量控制策略>排除策略”，点击<新建>，“地址”配置为财务 PC，点击<提交>。

图14 配置 QoS 排除策略

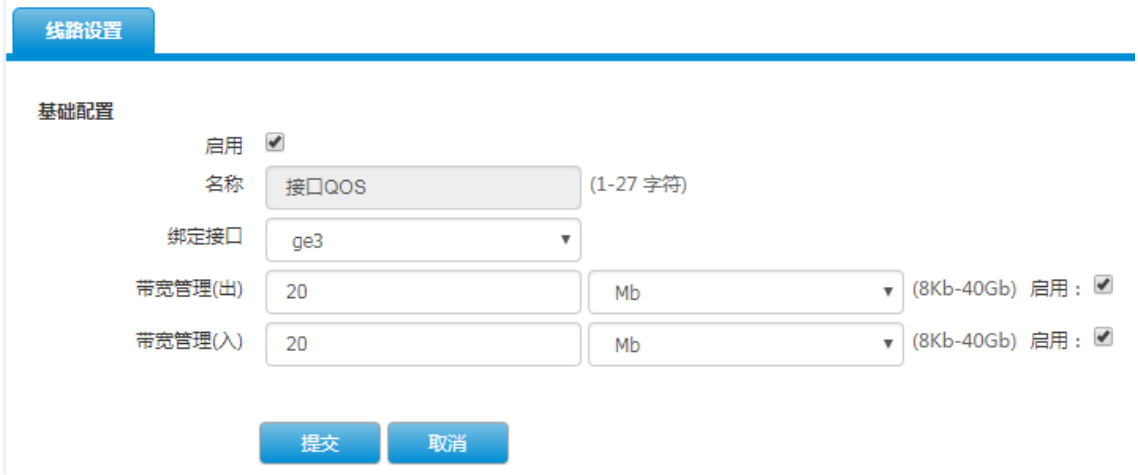
如图 15 所示，创建成功的 QoS 排除策略配置如下：

图15 QoS 排除策略创建成功

5. 调整线路带宽，线路下通道带宽自适应

进入“策略配置>流量控制策略>流量控制”，选中线路，点击<编辑>，修改“带宽管理（出）”和“带宽管理（入）”均配置为 20Mb（这里出和入的方向基于 ge3 接口），并点击<提交>。

图16 接口 QoS 线路修改 20M



查看调整后的线路下通道带宽如图 17 所示。

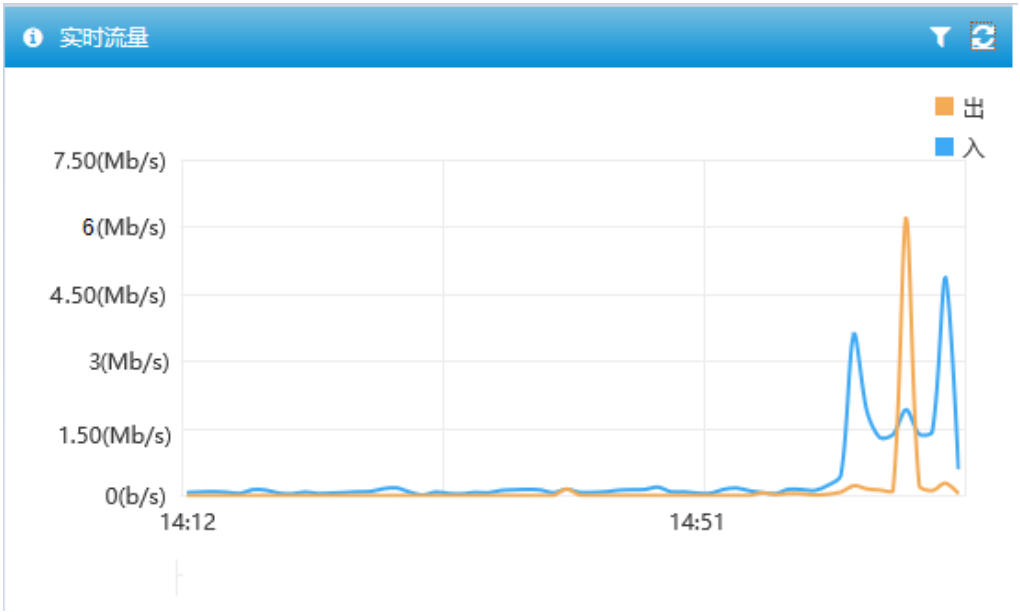
图17 调整后的线路下通道带宽

4.6 验证配置

(1) 验证 ge3 接口流量限制效果

如图 18 所示，观察设备的首页的实时流量统计图，发现上行和下行流速都小于 8Mbps：

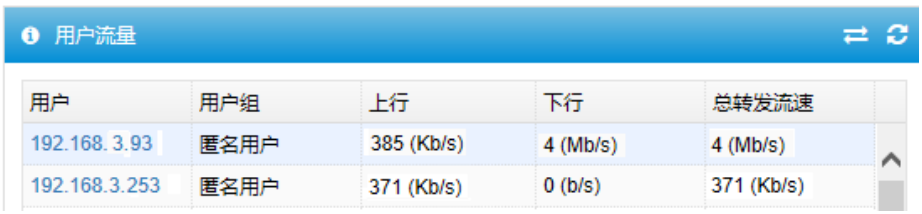
图18 设备的上下行流量统计



(2) 验证办公网段流量限制效果

如图 19 所示，通过观察设备的首页的实时用户流量统计数据，办公网段（IP 地址为 192.168.3.0/24）的用户下行流速无法超过 6Mbps：

图19 办公网段用户流量统计



(3) 验证财务 PC 免流量限制效果

如图 20 所示，使用财务 PC 地址 192.168.3.112 时，则完全不受 QoS 策略的影响，上下行流速可以超出 QoS 限制的 6Mbps。

图20 财务 PC 不受 QoS 限制

4.7 配置文件

```
!
address 办公网段
 ip subnet 192.168.3.0/24
!
address 财务 PC
ip address 192.168.3.112
!
schedule-day 工作时间
 periodic start 09:00 end 18:00
!
schedule-week 每周工作时间
 day monday 工作时间
 day tuesday 工作时间
 day wednesday 工作时间
 day thursday 工作时间
 day friday 工作时间
!
qos-profile white-list any any 财务 PC any any any 2
qos-profile limit-channel 办公网段 P2P 限速
 limit both
 maxbandwidth ingress 1000
 maxbandwidth egress 1000
 perip ingress 500
 perip egress 500
 match interface ge3
 schedule 每周工作时间
 match service any
 match address any
 match user any
 match application P2P_Software
 match application P2P_Media
!
```

```
qos-profile line 接口QOS
 limit both
 maxbandwidth ingress 8000
 maxbandwidth egress 8000
 match interface ge3
!
qos-profile channel 办公网段QOS parent 接口QOS
 bandwidth ingress 4000
 maxbandwidth ingress 6000
 bandwidth egress 4000
 maxbandwidth egress 6000
 priority high
 schedule 每周工作时间
 match service any
 match address 办公网段
 match user any
 match application any
!
qos-profile channel 办公网段HTTP保障 parent 办公网段QOS
 bandwidth ingress 3000
 maxbandwidth ingress 5000
 bandwidth egress 3000
 maxbandwidth egress 5000
 match service any
 match address 办公网段
 match user any
 match application HTTP_PIC_DOWNLOAD
 match application HTTP
!
qos-profile channel def_办公网段QOS parent 办公网段QOS
!
qos-profile channel def_接口QOS parent 接口QOS!
```

目 录

1 简介

本文档介绍设备的 IPv4 控制策略配置举例，IPv4 控制策略包含终端公告提醒、URL 过滤控制，应用过滤控制、终端类型控制，应用过滤控制细分为：应用控制、邮件控制、WEB 关键字、虚拟账号。本文针对部分功能进行详细配置的举例介绍，以引导用户快速了解功能。各功能实现效果简要介绍如下所示。

WEB 关键字实现效果：

- 搜索引擎：

对搜索引擎的搜索内容进行监控，提供告警、拒绝两种处理动作，并支持记录日志。

- HTTP 上传：

对 http 上传的 POST 内容进行监控，提供告警、拒绝两种处理动作，并支持记录日志，如：

web 邮件过滤（发件人、收件人，主题、内容、附件名）；

web 社区论坛（发帖内容、附件上传）；

- 网页内容：

支持所有 http 网页浏览内容过滤，网页内容必须为文本形式，不能为图片中的文字。

虚拟账号控制实现效果：

只支持 QQ 虚拟账号的控制，关键字过滤只支持精确匹配。根据匹配到的动作（黑名单|白名单）进行 QQ 账号控制并产生应用控制日志。

邮件控制实现效果：

邮件控制策略页面包含发件人过滤、收件人过滤、标题及内容过滤、邮件大小以及附件个数过滤。发件人和收件人过滤包括功能开启、策略属性（黑白名单）以及关键字配置。标题及内容支持关键字配置。

终端公告提醒实现效果：

终端公告提醒：当内网终端在访问网页时重定向到公告页面，以达到推送公告的目的，可以设置公告推送频率，支持设备内置公告以及外部公告。

URL 过滤实现效果：

URL 过滤是基于 URL 分类来对用户访问 WEB 站点进行控制，控制动作包含允许和拒绝。这样可以通过对 HTTP 协议的控制为用户提供应用级的安全防护和访问限制。

终端类型控制实现效果：

终端类型定义如下：

any：所有终端类型。

移动终端：基于 Android 或 IOS 系统的智能手机或 Pad。

PC：基于 Windows 操作系统的 PC 或笔记本。

在某此场景下，为了保证办公内网的安全，管理员只允许受控的办公电脑可以正常访问网络，对其通过 wifi 热点接入的移动终端进行控制，以达到管控的目的。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了 IPv4 控制策略功能特性。

3 使用限制及注意事项

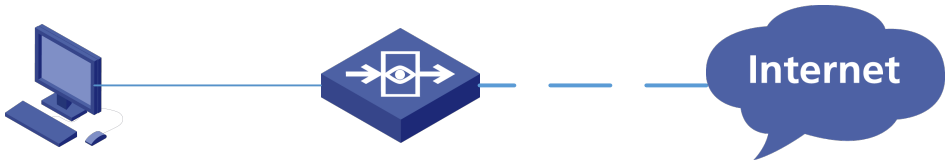
- 配置 WEB 关键字过滤规则之前需要先配置解密策略，由于涉及加密的网站较多，不配置解密无法识别到对应的关键字会导致关键字过滤失败。
- WEB 关键字附件上传过滤不支持压缩文件。
- 关键字过滤同一条流只要检查到第一个符合条件的关键字就会停止匹配。
- 关键字过滤不支持附件内容过滤。
- 关键字过滤字母不区分大小写。
- 网页内容过滤时，有时关键字在网页中的位置比较靠后，此时检测到关键字后，部分网页内容已经加载成功，此时会出现网页部分加载的情况。
- 苹果系统虚拟账户控制不生效，特征加密问题。
- 虚拟账户控制：QQ 账号黑白名单关键字控制，关键字匹配为精确匹配。
- 虚拟账号控制依赖应用特征库，特征库不识别时无法控制。
- 移动端（安卓）测试虚拟账号控制时，需要关闭移动网络。
- 关键字条目规格 512 和 1024 条，每个关键字对象里可以配置 1024 个关键字。
- 旁路模式 qq 阻断不生效。
- 虚拟账户白名单，应用控制不产生日志（只有黑名单阻断后才产生日志）。
- 虚拟账号黑白名单关键字默认显示为“-”。
- 虚拟账号黑名单引用关键字的内容为空，不控制 qq 登录，不引用关键字策略不生效，不阻断。
- 虚拟账号白名单引用关键字的内容为空（匹配不上），阻断 qq 登录，并产生日志。不引用关键字策略不生效，不阻断。
- 配置关键字内容为 qq 号（关键字精确匹配），qq 过滤引用白名单。
- 下联终端使用关键字内的 qq 号码登录，匹配后可以正常登录，不记录控制日志。
- 下联终端使用非关键字内的 qq 号码登录，qq 无法登录，控制日志处应该记录一条日志。
- 配置的虚拟账号阻断，应用控制放行 qq 登录阻断前后会有一条放行的日志--- QQ 登录识别报文和获取账号报文不在同一个报文中，前一个报文识别为 QQ 登录，未获取到 QQ 账号，命中了应用控制策略报放行日志。后一个报文获取到 QQ 账号，命中了虚拟账号策略，报阻断日志，此情况属于正常现象。
- 使用终端公告提醒功能时内网接口管理方式必须开启 http，终端才能正常访问公告页面。

4 WEB 关键字过滤功能配置举例

4.1 组网需求

如图 1 所示，某公司网络管理员针对内网用户上网不允许搜索引擎查找敏感关键字：毒品，不允许外发 WEB 邮件内容包含敏感关键字：内网资产，不允许浏览包含关键字<新闻> 的网页。

图1 WEB 关键字过滤组网



4.2 配置思路

- 在设备上配置各接口地址，如拓扑图所示。
- 生成 CA 根证书。
- 导出 CA 根证书（P12 格式）。
- 将 CA 根证书导入本地证书。
- 创建 https 对象。
- 创建解密策略。
- 创建关键字对象。
- 创建 WEB 关键字过滤策略。
- 在测试终端导入证书。
- 验证配置。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

1. 配置路由接口

如图 2、图 3 所示，在设备上配置各接口地址。点击“网络配置>接口配置>物理接口”，配置接口 IP 地址。

图2 配置 ge0 接口

图3 配置 ge1 接口

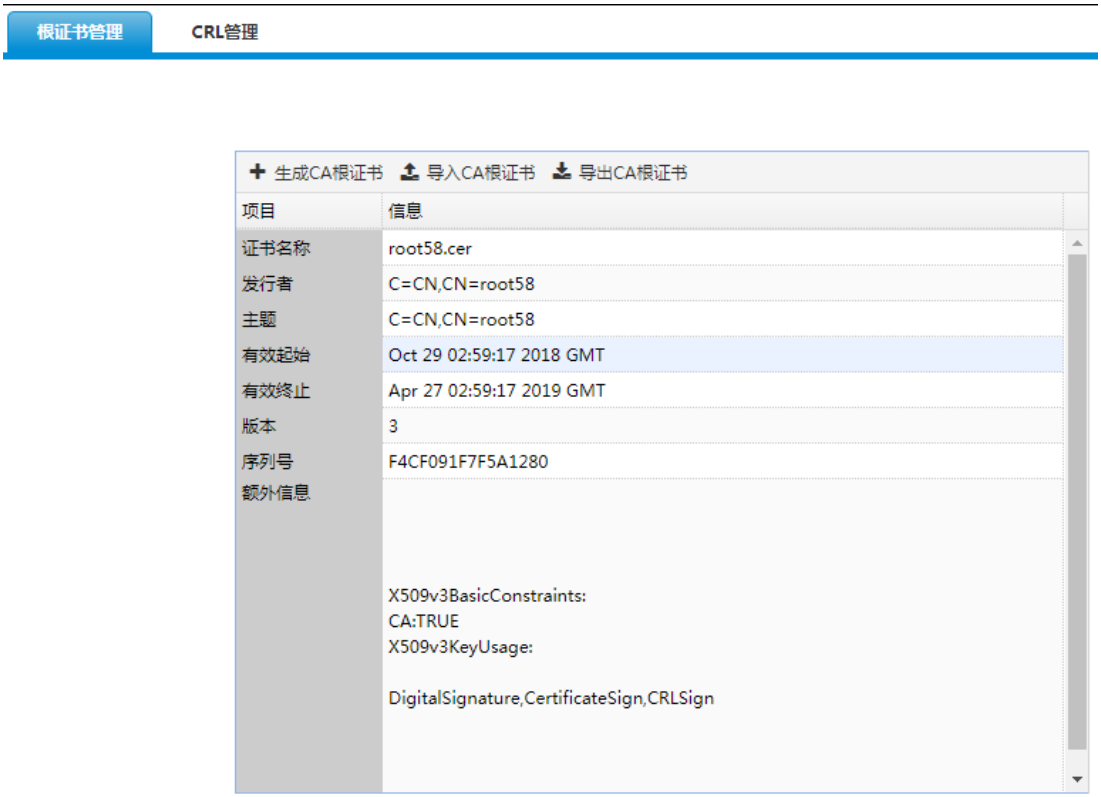
2. 生成 CA 根证书

如图 4 所示，点击“策略配置>对象管理>CA 服务器>根 CA 配置管理”，在根证书管理中点击生成 CA 根证书，配置 CA 信息。

图4 配置 CA 根证书

如图 5 所示，查看已生成的 CA 根证书。

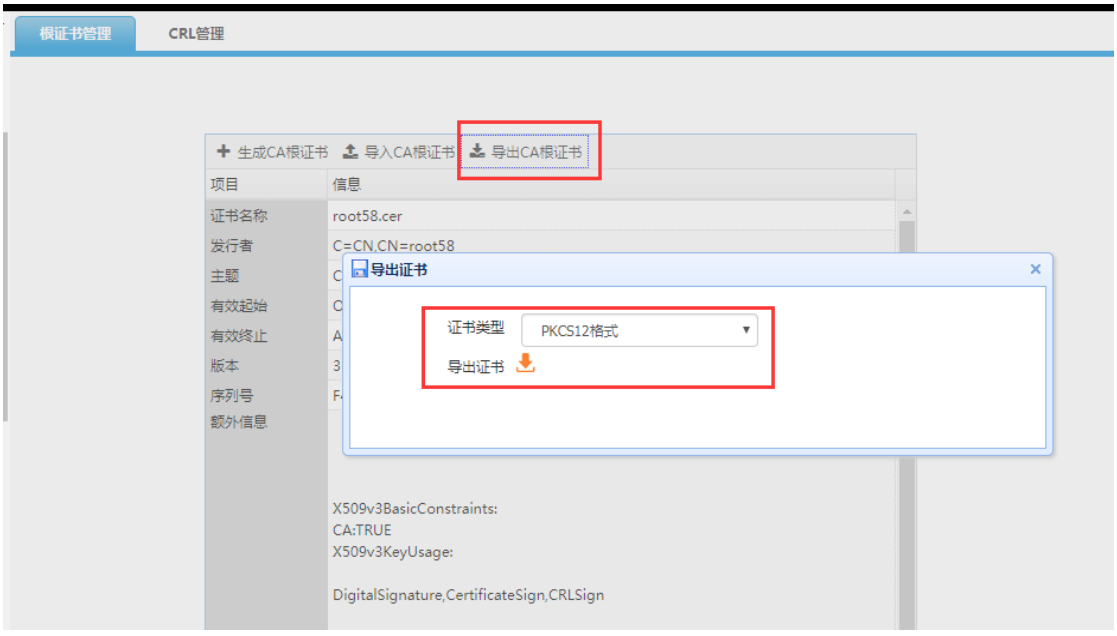
图5 查看已生成的 CA 根证书



3. 导出 CA 根证书

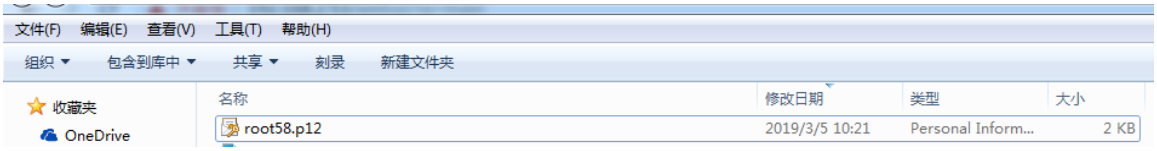
如图 6 所示，点击“策略配置>对象管理>CA 服务器>根 CA 配置管理”，在根证书管理中点击导出 CA 根证书。

图6 导出 CA 根证书



如图 7 所示，查看已导出的 CA 根证书。

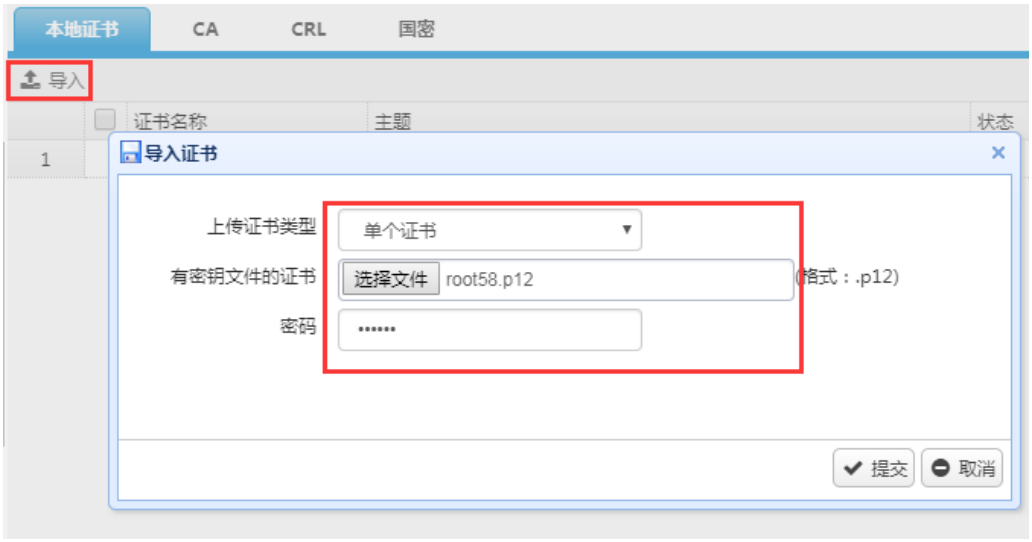
图7 查看导出的 CA 根证书



4. 将 CA 根证书导入本地证书

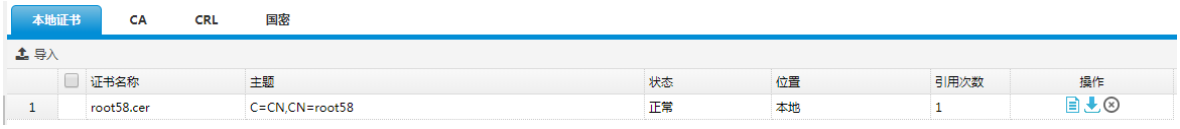
如图 8 所示，在“策略配置>对象管理>本地证书>证书>本地证书”，点击导入，选择之前导出的证书，导入即可，注意密码必须与之前设置的密码一致。

图8 将 CA 根证书导入到本地证书



如图 9 所示，查看导入成功的本地证书。

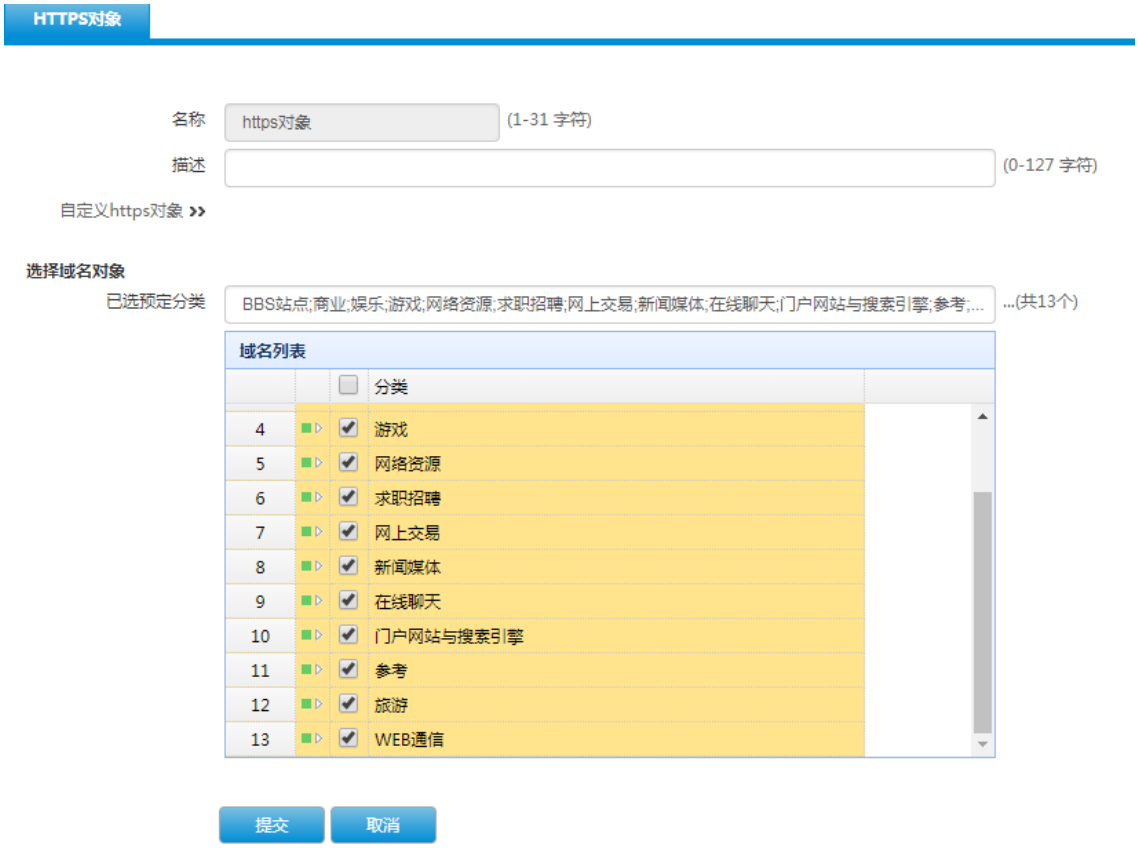
图9 导入成功的本地证书



5. 创建 https 对象

如图 10 所示，点击“策略配置>对象管理>URL 对象>HTTPS 对象”，创建 https 对象。

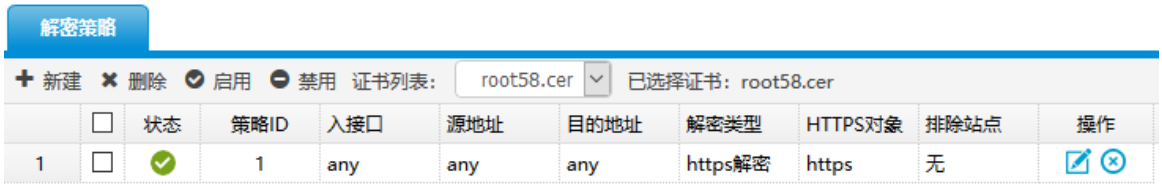
图10 https 对象



6. 创建解密策略

如图 11 所示，由于部分测试网站为 https 加密网站，需要解密后才能识别到关键字，所以需要先创建解密策略，在导航栏中选择“策略配置 > SSL 解密策略”，单击<新建>按钮，配置完成后下发。

图11 解密策略



7. 创建关键字对象

如图 12 所示，创建关键字对象，在导航栏中选择“策略配置>对象管理>关键字对象”，单击<新建>按钮，配置完成后下发。

图12 关键字对象

8. 创建 WEB 关键字过滤策略

如图 13、图 14、图 15 所示，创建 WEB 关键字过滤规则，在导航栏中选择“策略配置 > IPv4 控制策略”，点击<新建>，在弹出页面中依次单击<新建>、<应用过滤>、<WEB 关键字>，分别创建搜索引擎规则、HTTP 上传规则、网页内容规则。

图13 搜索引擎关键字规则

图14 HTTP 上传关键字规则

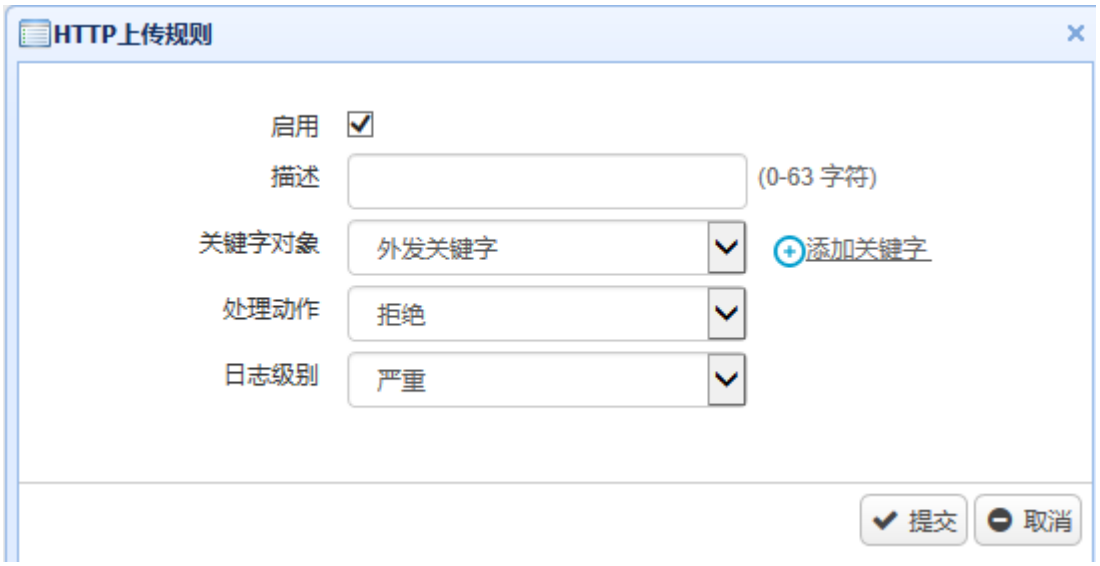


图15 网页内容关键字规则

9. 在测试终端中导入证书

不同终端的导入证书方式不一样，具体方法请参考“解密策略典型配置举例”。

4.5 验证配置

(1) 搜索引擎结果验证

使用百度搜索引擎搜索关键字“毒品”，访问被阻断，无结果回显，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 16、图 17 所示。

图16 关键字搜索结果

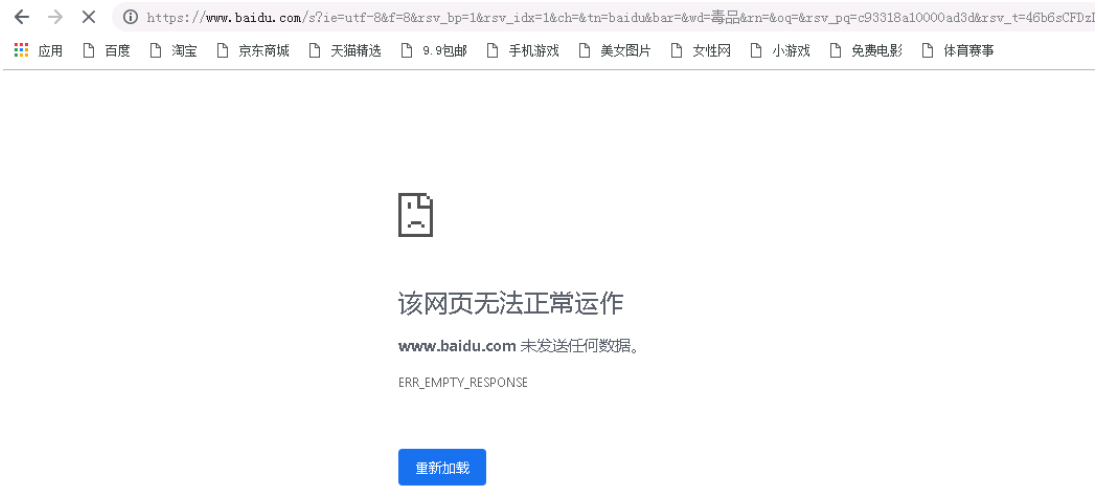
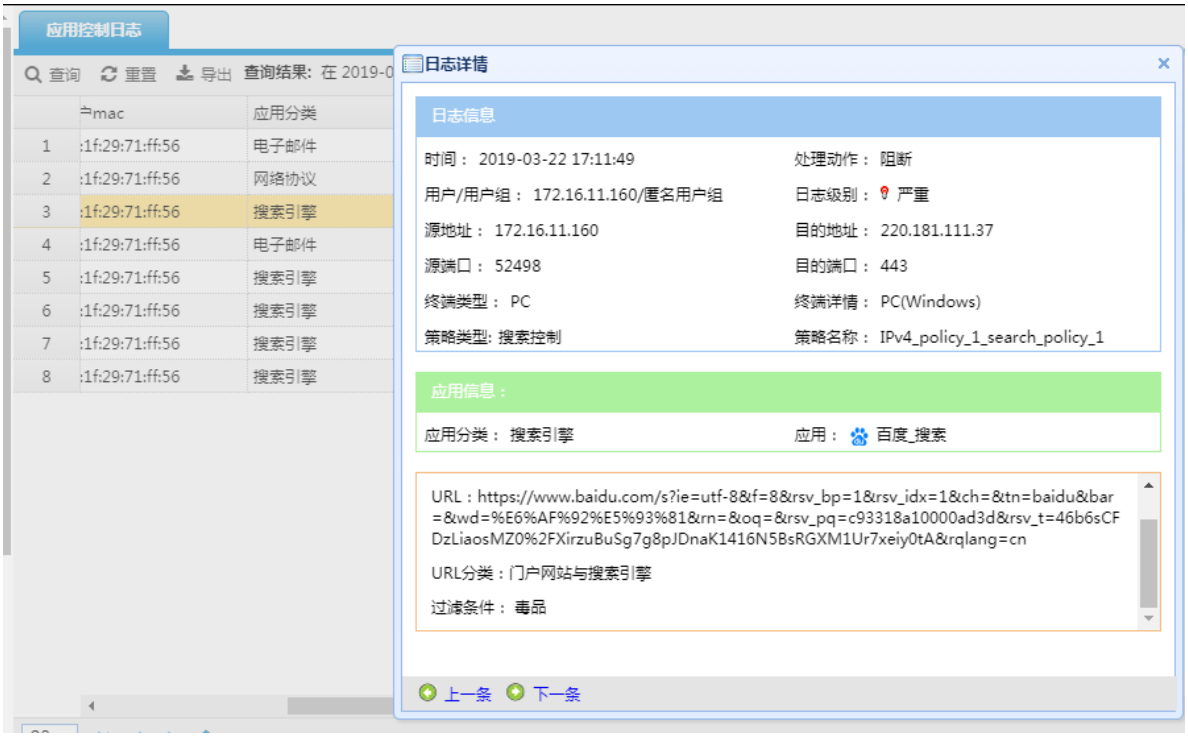


图17 应用控制日志

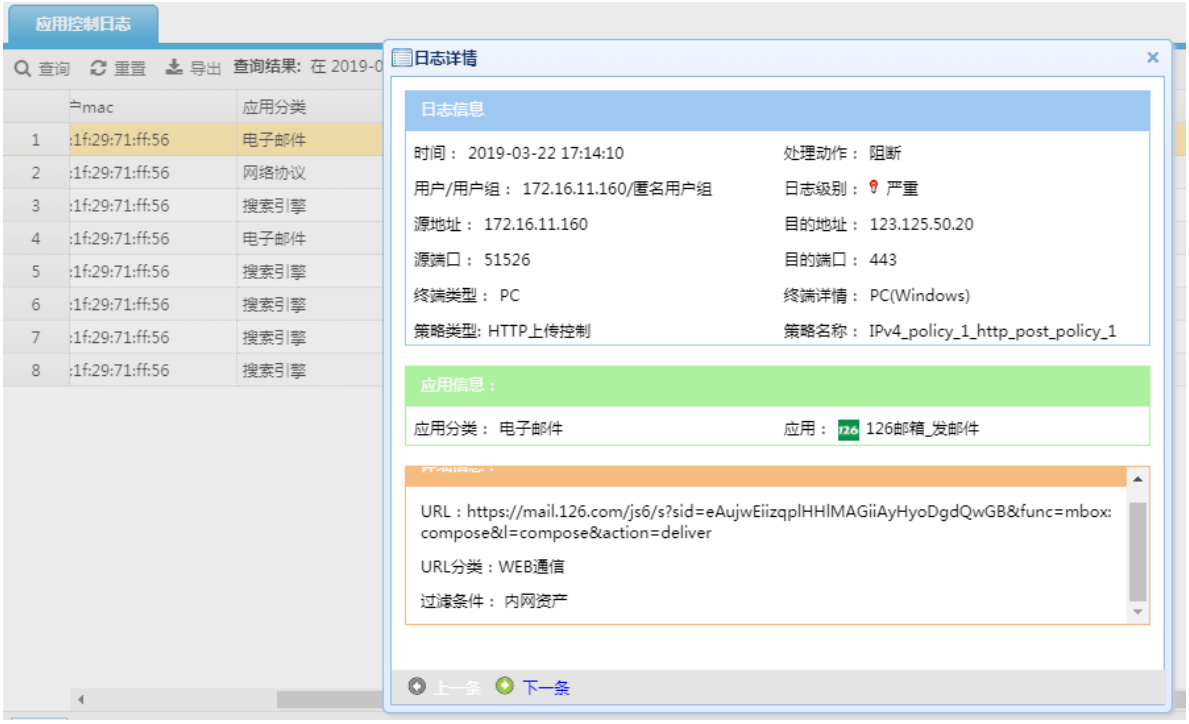


(2) WEB 邮箱结果验证

使用 126 邮箱发送邮件，内容为：内网资产信息请查收，点击发送，邮件无法发送成功，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 18、图 19 所示。

图18 邮件发送

图19 应用控制日志

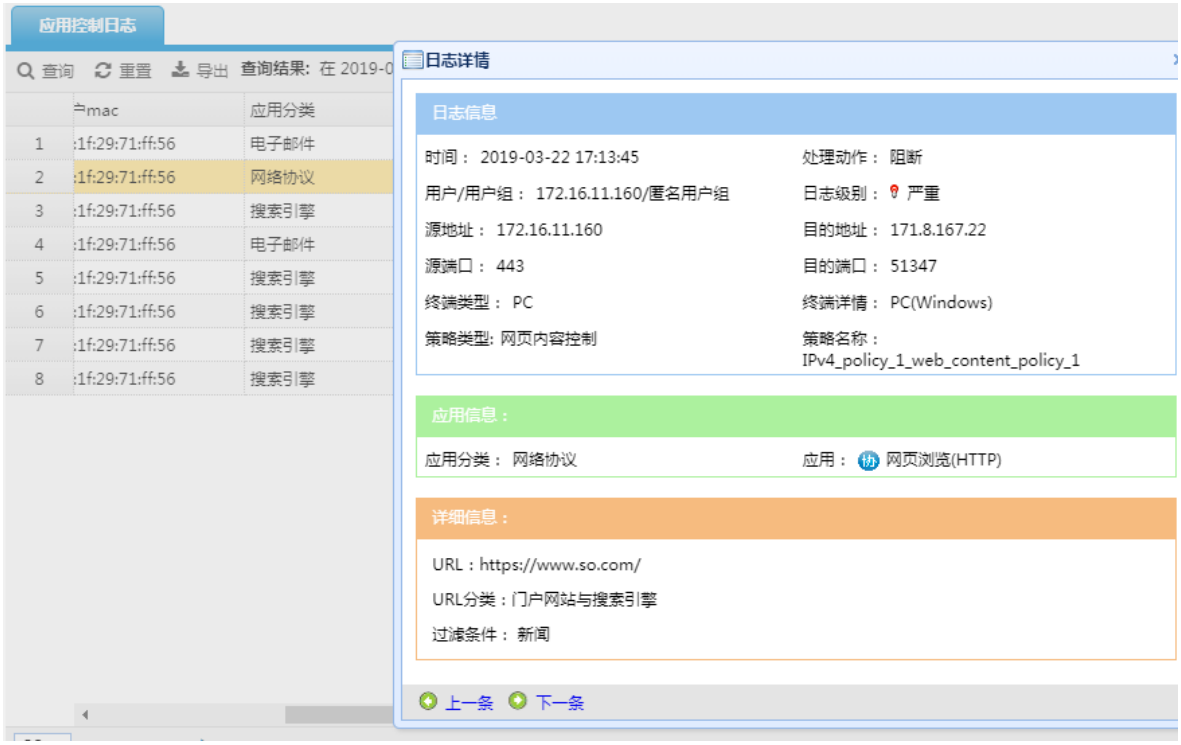


(3) 网页浏览结果验证

使用测试 PC 访问腾讯网站 http://www.qq.com/，同时可以在导航栏“数据中心 > 日志中心 > 控制日志 > 应用控制日志”中产生相应阻断日志，如图 20、图 21 所示。

图20 访问腾讯

图21 应用控制日志



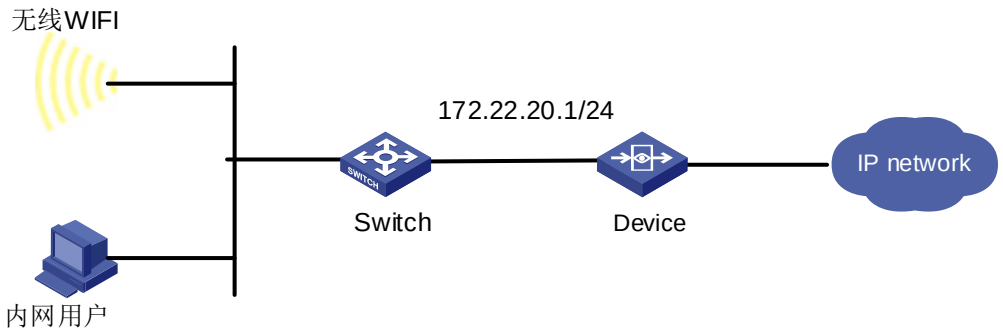
5 虚拟账号过滤功能配置举例

5.1 组网需求

如图 22 所示，公司内网存在内网用户供内部人员使用；无需 wifi 供访客使用，具体需求如下：

- 针对内网用户，公司内部人员只放行特定的 QQ 账户上网，其它 qq 号阻断登录。
- 针对无线 wifi 网络，阻断特定 qq 账户，其它 qq 放行可以上网。

图22 虚拟账户组网图



5.2 配置思路

按照组网图组网

- 新建地址对象
- 配置关键字对象。
- IPv4 控制策略虚拟账户处启用 qq 账户过滤

5.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置设备

1. 配置地址对象

通过菜单“策略配置>对象管理 > 地址对象”，点击<新建>地址对象，配置“内网用户”地址对象和“无线 wifi”地址对象。如图 23、图 24 所示。

图23 添加内网用户地址对象

图24 添加无线 wifi 地址对象

2. 配置关键字对象

通过菜单“策略配置>对象管理 > 关键字对象”，点击<新建>关键字对象，配置“QQ 白名单”关键字对象和“QQ 黑名单”关键字对象，如图 25、图 26 所示。

图25 添加 QQ 白名单对象

图26 添加 QQ 黑名单对象

3. 配置 IPv4 控制策略，虚拟账户配置白名单。

通过菜单“策略配置>IPv4 控制策略”，点击<新建>进入 IPv4 控制策略配置页面，源地址对象选择“内网用户”，虚拟账户启用白名单，如图 27、图 28 所示。

图27 IPv4 控制策略配置内网用户源地址

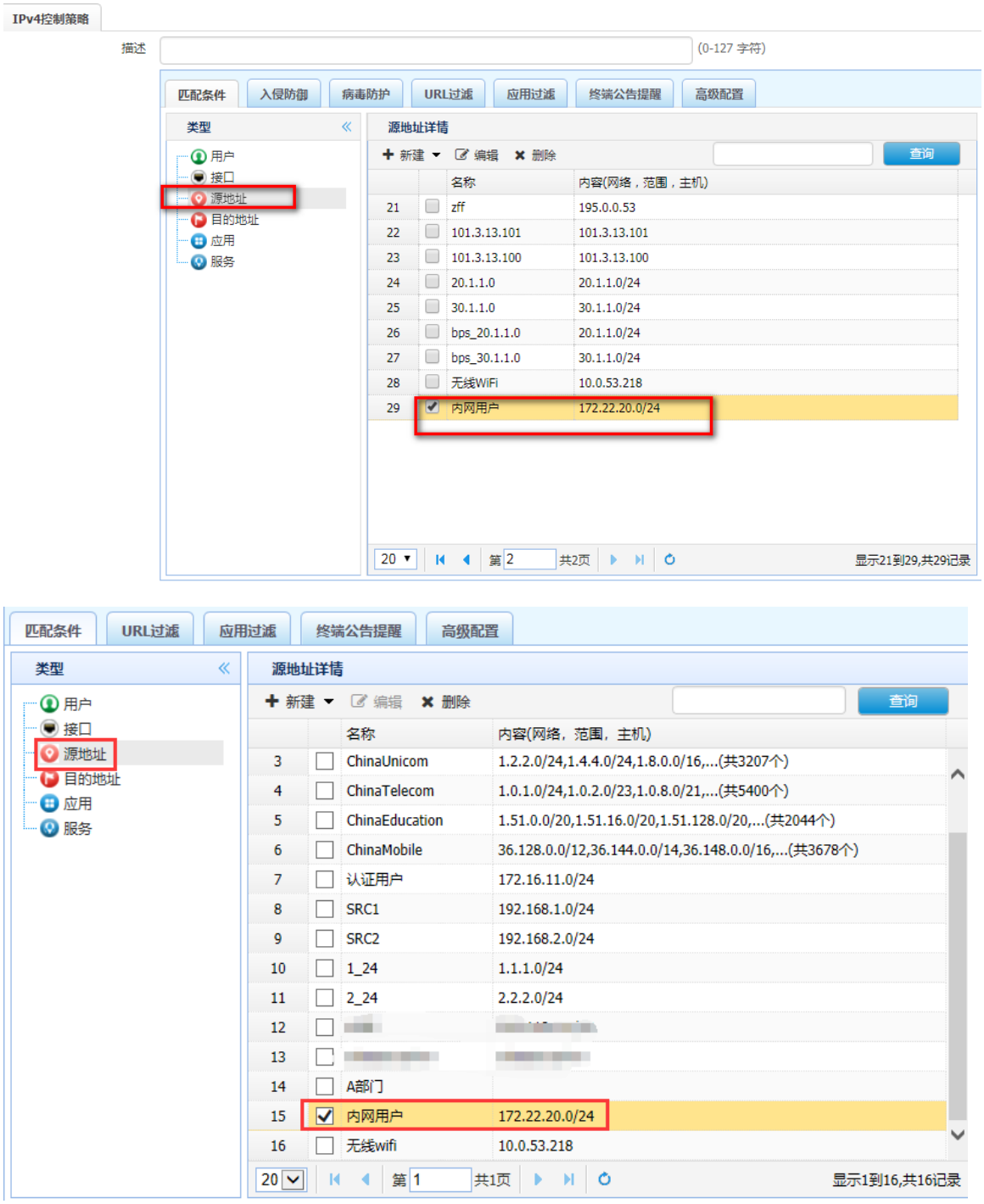
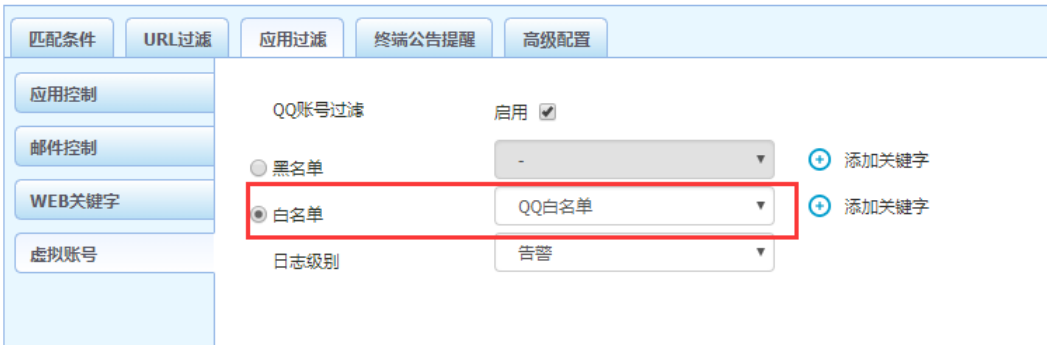


图28 IPv4 控制策略配置虚拟账户白名单控制



4. 配置 IPv4 控制策略，虚拟账户配置黑名单。

通过菜单“策略配置 >策略配置 > IPv4 控制策略”，点击<新建>进入 IPv4 控制策略配置页面，源地址对象选择 “无线 wifi”，虚拟账户启用黑名单，如图 29、图 30 所示。

图29 IPv4 控制策略配置无线 wifi 源地址

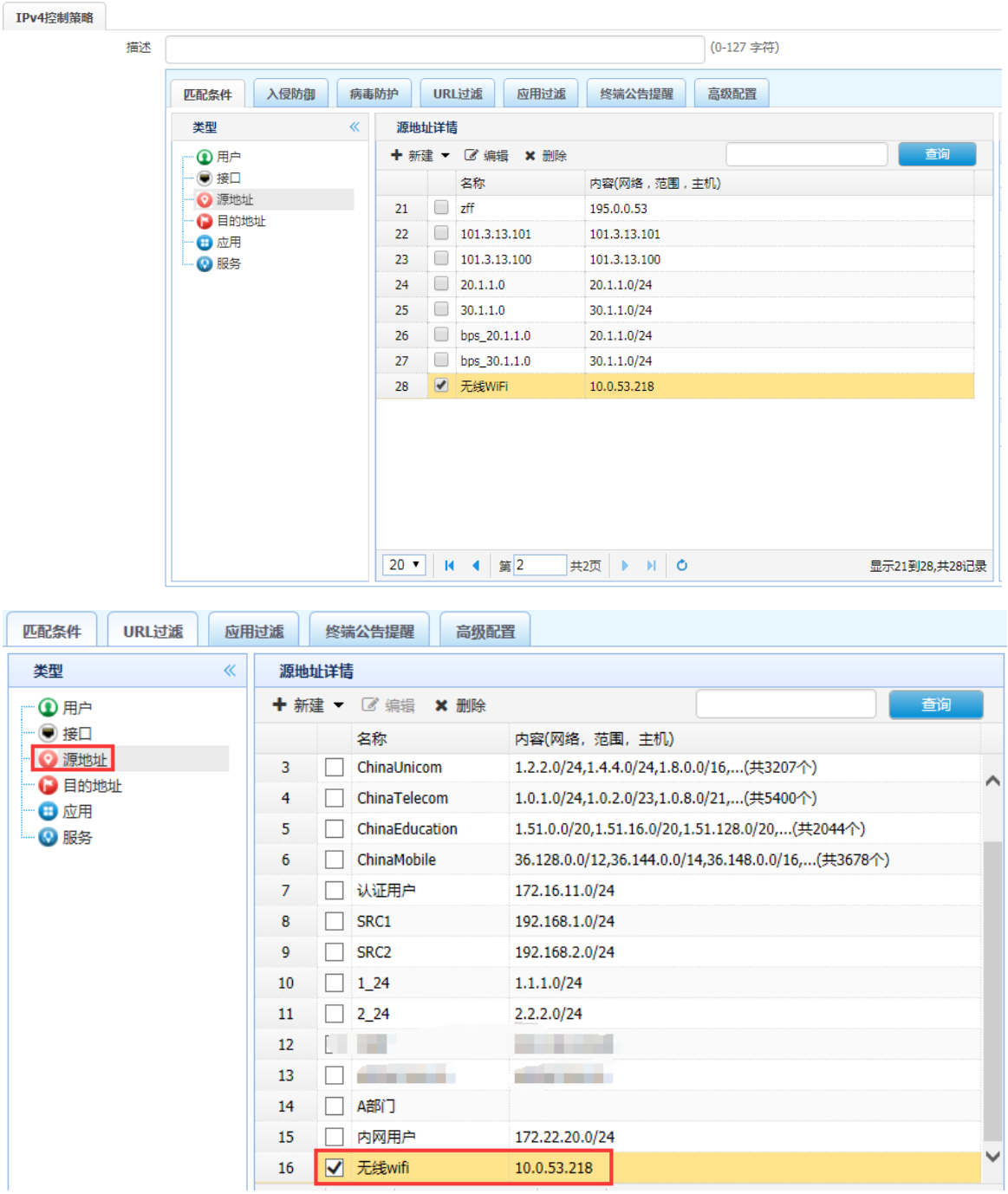


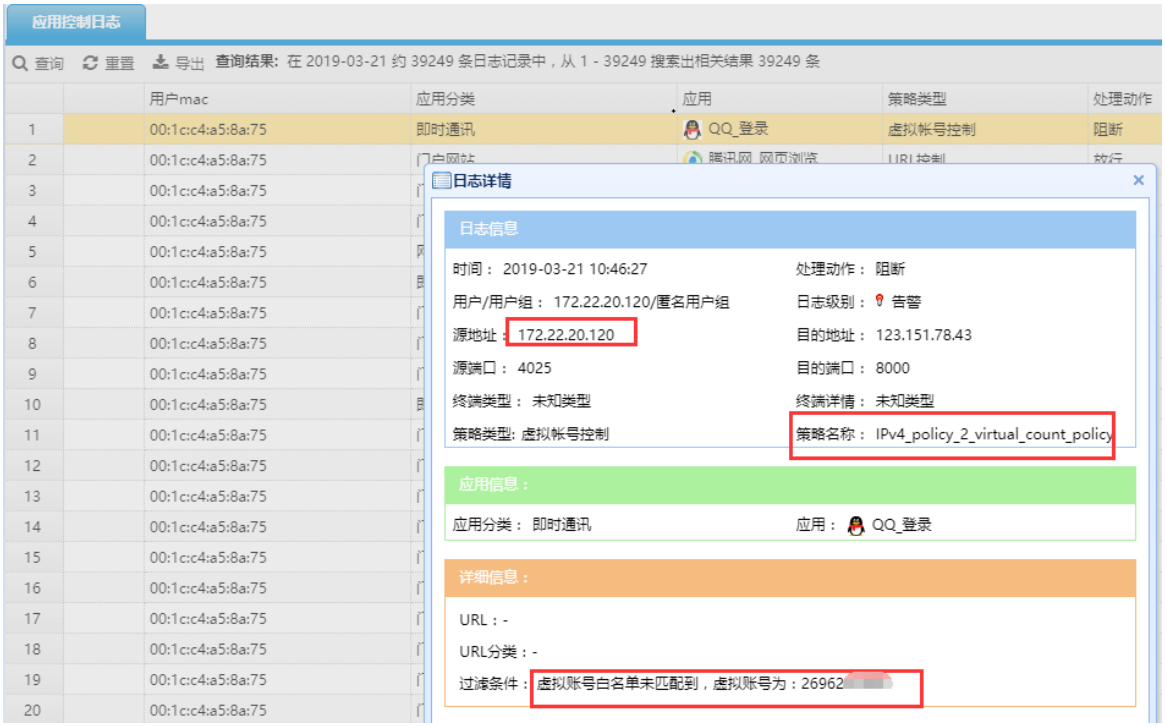
图30 IPv4 控制策略配置虚拟账户黑名单控制

5.5 验证结果

(1) 内网用户匹配白名单策略效果

通过菜单“数据中心 > 日志中心 > 控制日志 > 应用控制日志”，查看虚拟控制日志。内网用户使用白名单关键字内的 QQ 账户可以登录，不记录控制日志。使用白名单以外的 QQ 账户，登录账户阻断后，点击日志详情可以查看匹配的策略名称和阻断账户，如图 31 所示。

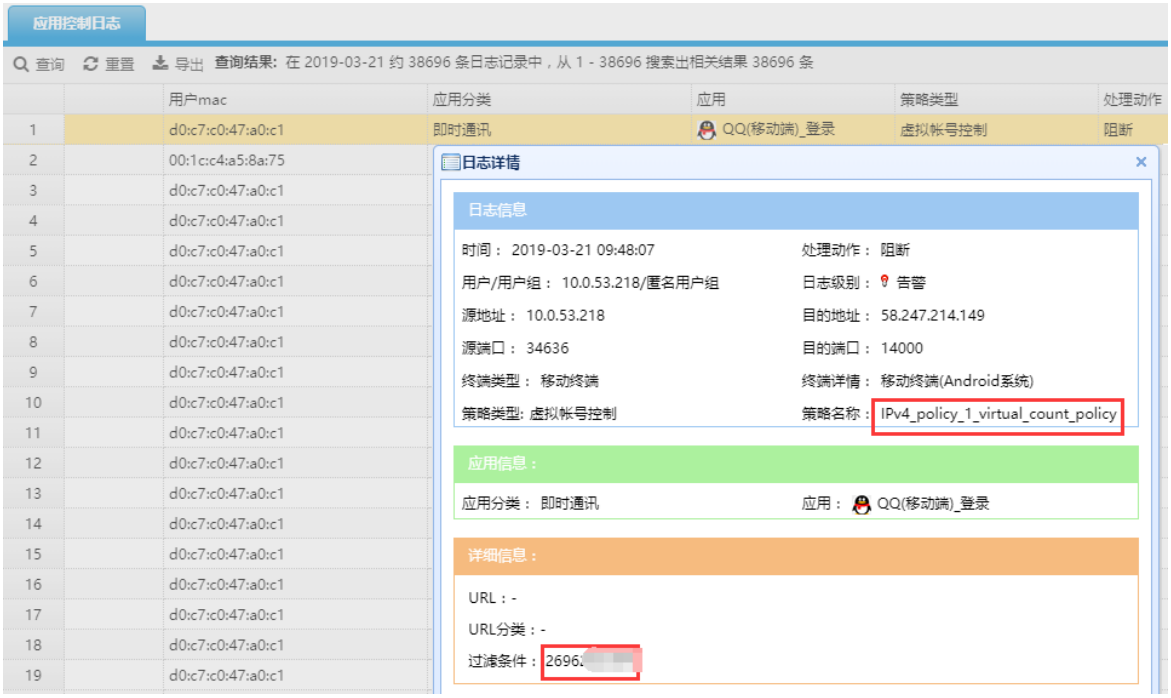
图31 内网用户匹配白名单日志



(2) 无线 WIFI 网段用户匹配黑名单策略效果

通过菜单“数据中心 > 日志中心 > 控制日志 > 应用控制日志”，查看虚拟控制日志。无线 WIFI 网段用户使用黑名单以外的关键字登录 qq，可以登录不记录控制日志。使用黑名单关键字的账户登录 qq 阻断后查看控制日志，点击日志条目详细可以看到匹配的策略名称和阻断账户进入如图 32 所示的页面。

图32 无线 WIFI 用户匹配黑名单日志

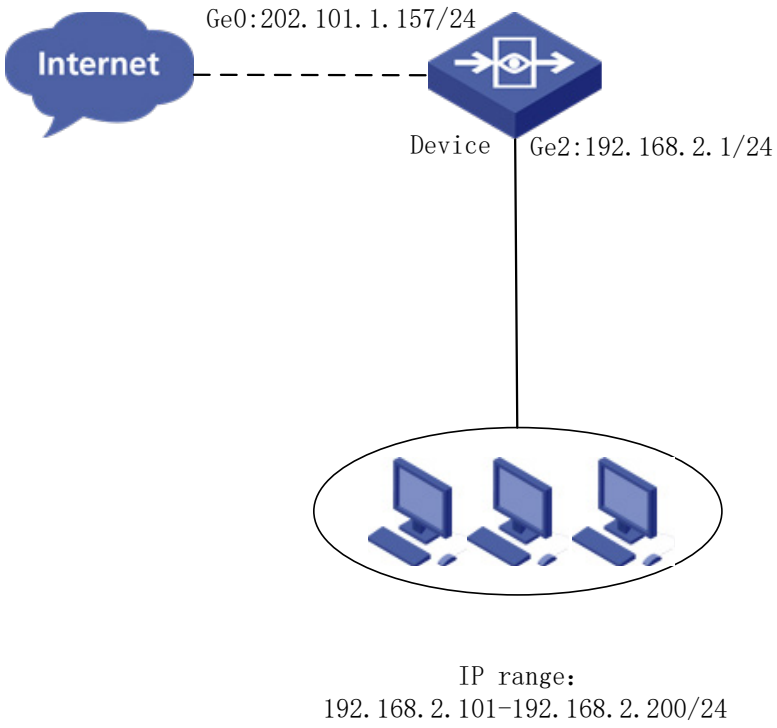


6 邮件控制功能配置举例

6.1 组网需求

如图 33 所示，针对内网用户 test 发送邮件大小超过 5M，则不允许发送，避免大量占用公司出口带宽。

图33 邮件控制组网图



6.2 配置思路

- 创建用户 test。
- 配置阻断策略，选择用户 test。
- 配置本地 web 认证。
- 开启邮件阻断策略，邮件阻断大小设置为 5M。

6.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

6.4 配置步骤

(1) 创建用户 test

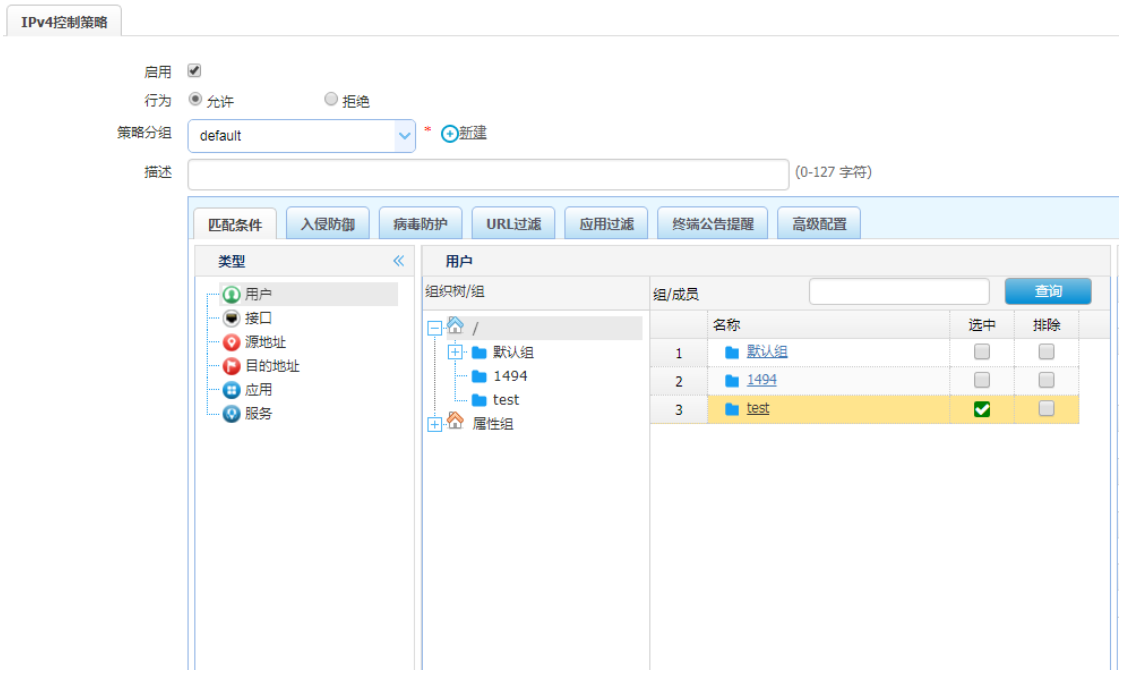
进入“用户管理 > 用户”，新建“test”用户，如图 34 所示。

图34 用户配置

(2) 配置 IPv4 控制策略

进入“策略配置 > IPv4 控制策略”，在“匹配条件”页面，选择用户“test”，并点击<提交>。如图35 所示。

图35 配置 IPv4 控制策略



(3) 配置邮件控制策略

在“IPv4 控制策略配置”页面，选择“应用过滤 > 邮件控制”，配置邮件控制，邮件大小设置为 5M，并点击<提交>按钮提交该页配置，如图 36 所示。

图36 配置邮件控制

(4) 配置认证策略

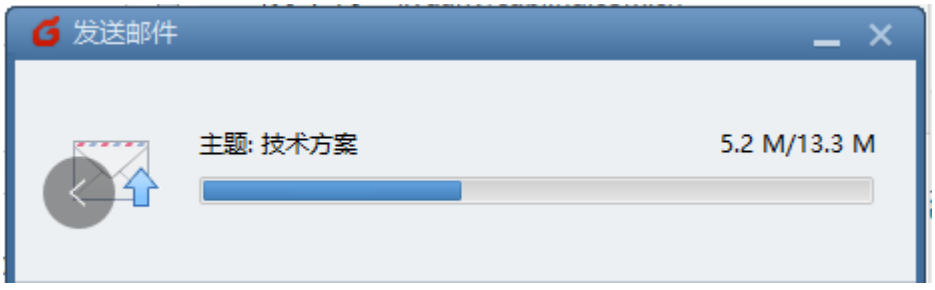
进入“用户管理> 认证管理 > 认证策略”，配置本地 WEB 认证策略，如图 37 所示。

图37　配置本地 WEB 认证

6.5 验证配置

(1)　用户 test 通过本地认证后过设备发送大于 5M 的邮件，邮件发送失败，如图 38 所示。

图38 邮件发送



(2)　设备应用控制记录阻断日志，可以查看详情，如图 39 所示。

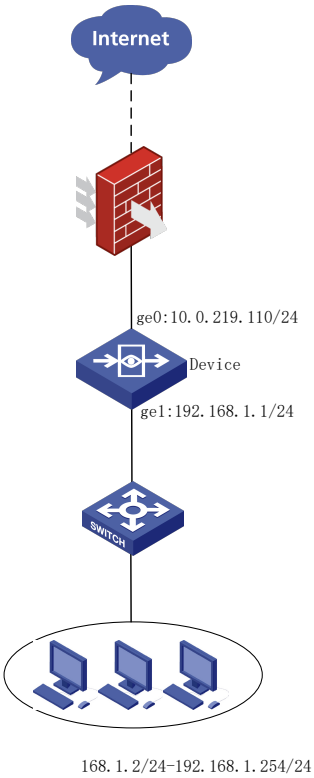
图39 应用控制记录阻断日志

7 终端公告推送功能配置举例

7.1 组网需求

如图 40 所示，某公司为了加强上网管理，拟定了一个上网准则公告，需要周期性进行网络内部推送，使用设备的的 ge0 和 ge1 接口以三层路由模式部署在网络中，设备上联出口 FW，下联二层交换机。设备上开启移动终端公告推送功能，检测上网行为并周期推送公告提醒。

图40 终端公告推送组网



7.2 配置思路

- 配置设备接口地址及路由。
- 配置地址对象。
- 配置用户识别范围。
- 配置自定义公告内容。
- 开启移动终端公告推送功能。

7.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

7.4 配置步骤

1. 配置接口地址

如图 41、图 42 所示，进入“网络配置>接口配置”页面，点击编辑 ge0、ge1 操作，把 ge0、ge1 的地址分别配置为 10.0.219.110/24、192.168.1.1/24。

图41 配置 ge0 接口

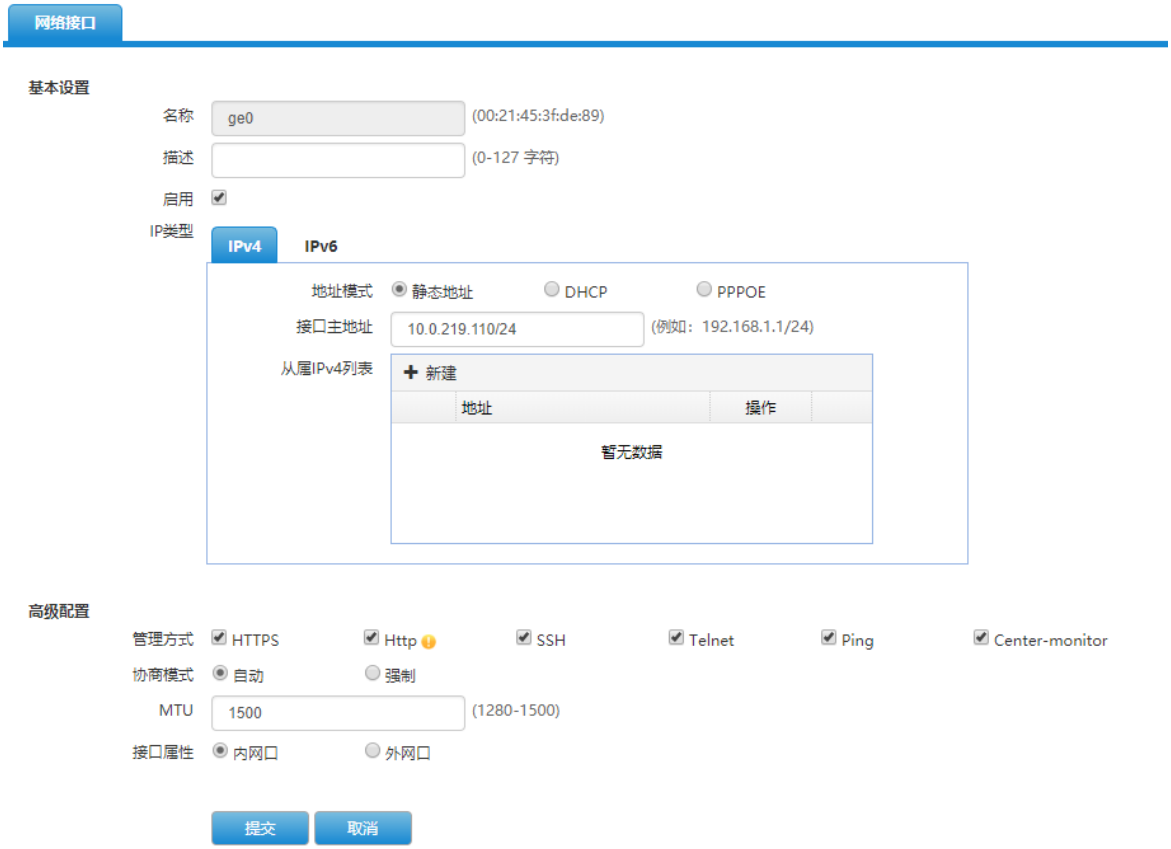
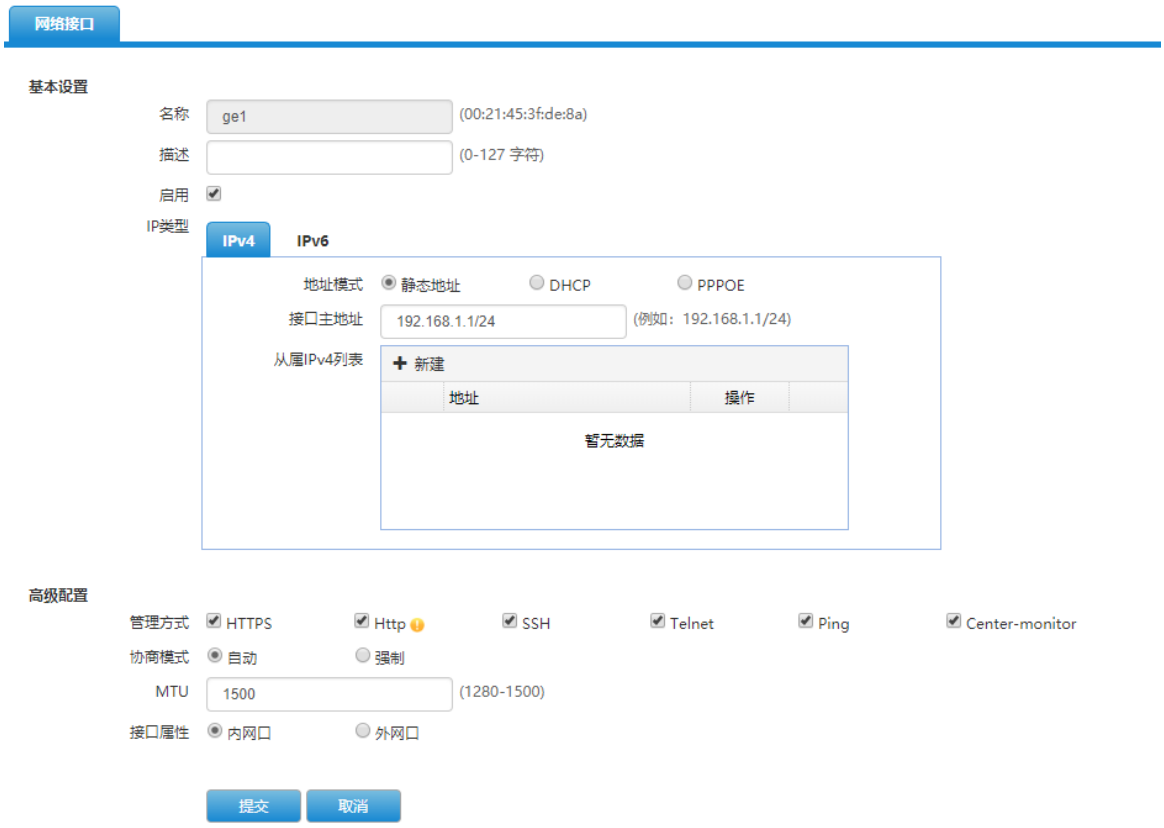

网络接口
基本设置
名称
ge0
(00:21:45:3f:de:89)
描述
(0-127 字符)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPOE
接口主地址
10.0.219.110/24
(例如：192.168.1.1/24)
从属IPv4列表
新建
地址
操作
暂无数据
高级配置
管理方式
HTTPS
Http
SSH
Telnet
Ping
Center-monitor
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口
提交
取消

图42 配置 ge1 接口



2. 配置静态路由

如图 43 所示，进入“网络配置>路由管理>静态路由”页面，新建一条访问外网的默认路由。

图43 配置静态路由

3. 配置地址对象

如图 44 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”页面，点击<新建>按钮创建内网用户地址对象，设置地址为 192.168.1.0/24，点击<提交>。

图44 配置地址对象

4. 配置用户识别范围

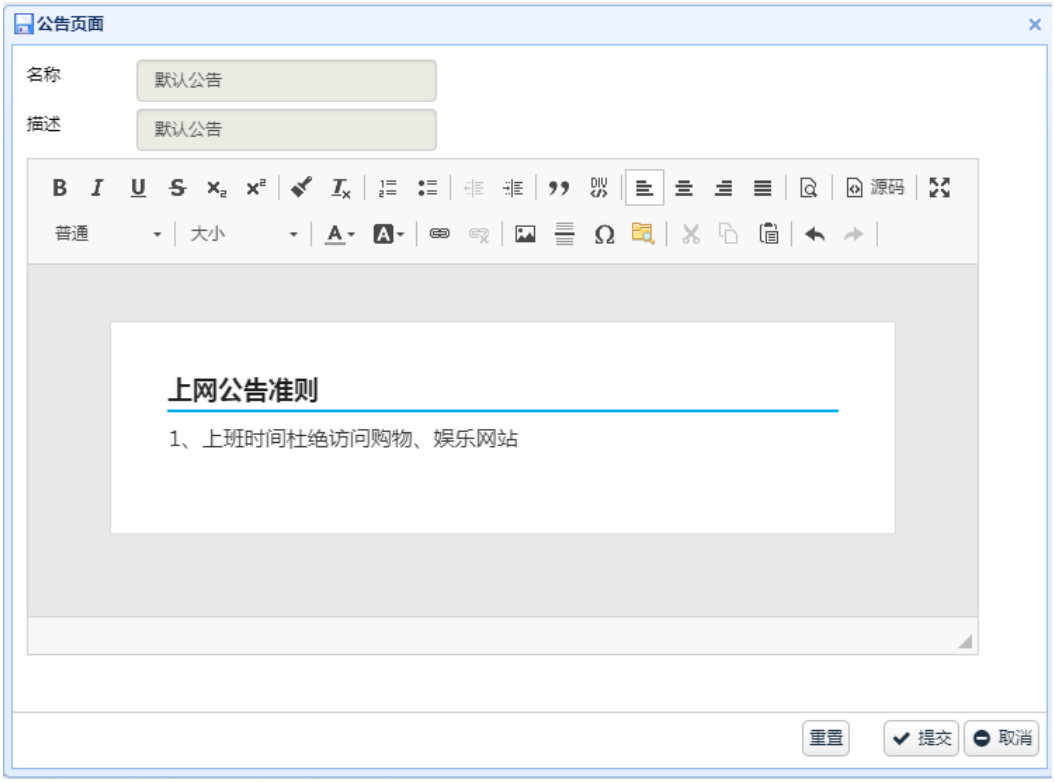
如图 45 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“内网用户”，其它配置默认，提交配置。

图45 用户识别范围

5. 配置自定义公告内容

如图 46 所示，进入“策略配置>对象管理>公告页面”，点击名称中“默认公告”，弹出自定义公告编辑页面。

图46 自定义公告



6. 开启终端公告推送功能

如图 47 所示，进入“策略配置 > IPv4 控制策略”页面，新建 IPv4 控制策略，源 IP 选择“内网用户”并开启终端公告推送功能。

图47 移动终端推送配置

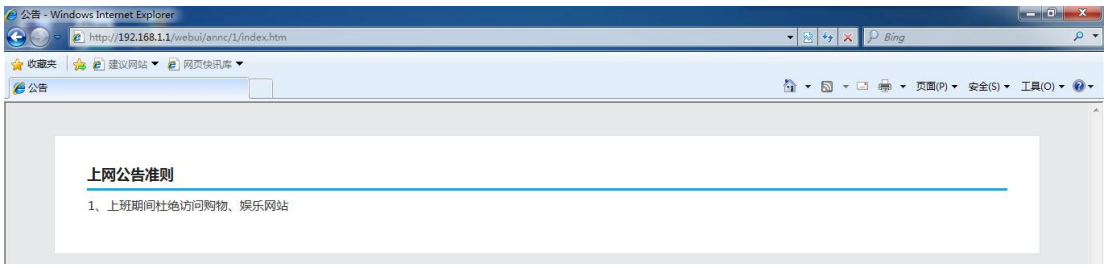
7.5 配置注意事项

- 内网接口管理方式必须开启 http，终端才能正常访问公告页面。

7.6 验证配置

如图 48 所示，某员工使用 1 台 PC 访问 http 网站，会被推送上网准则公告。

图48 推送公告

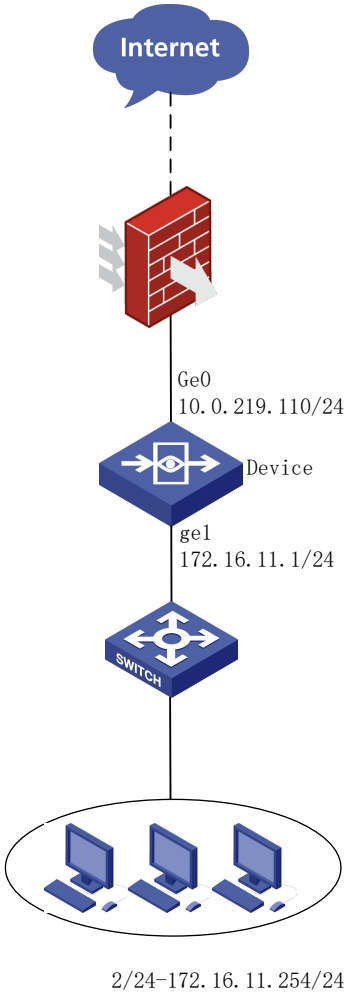


8 终端类型控制配置举例

8.1 组网需求

如图 49 所示，某公司内部网段 IP 地址 172.16.11.0/24，要求不允许移动终端及多终端访问外网，使用设备的的 ge0 和 ge1 接口作为路由模式，串接部署在网络中，设备上联出口 FW，下联路由器。设备上开启基于终端的 IPv4 控制策略,移动终端或多终端用户无法访问外网。

图49 基于终端类型的 IPv4 控制策略组网图



8.2 配置思路

- 配置接口
- 配置静态路由
- 配置地址对象
- 配置用户识别范围
- 配置 IPv4 控制策略

8.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

8.4 配置注意事项

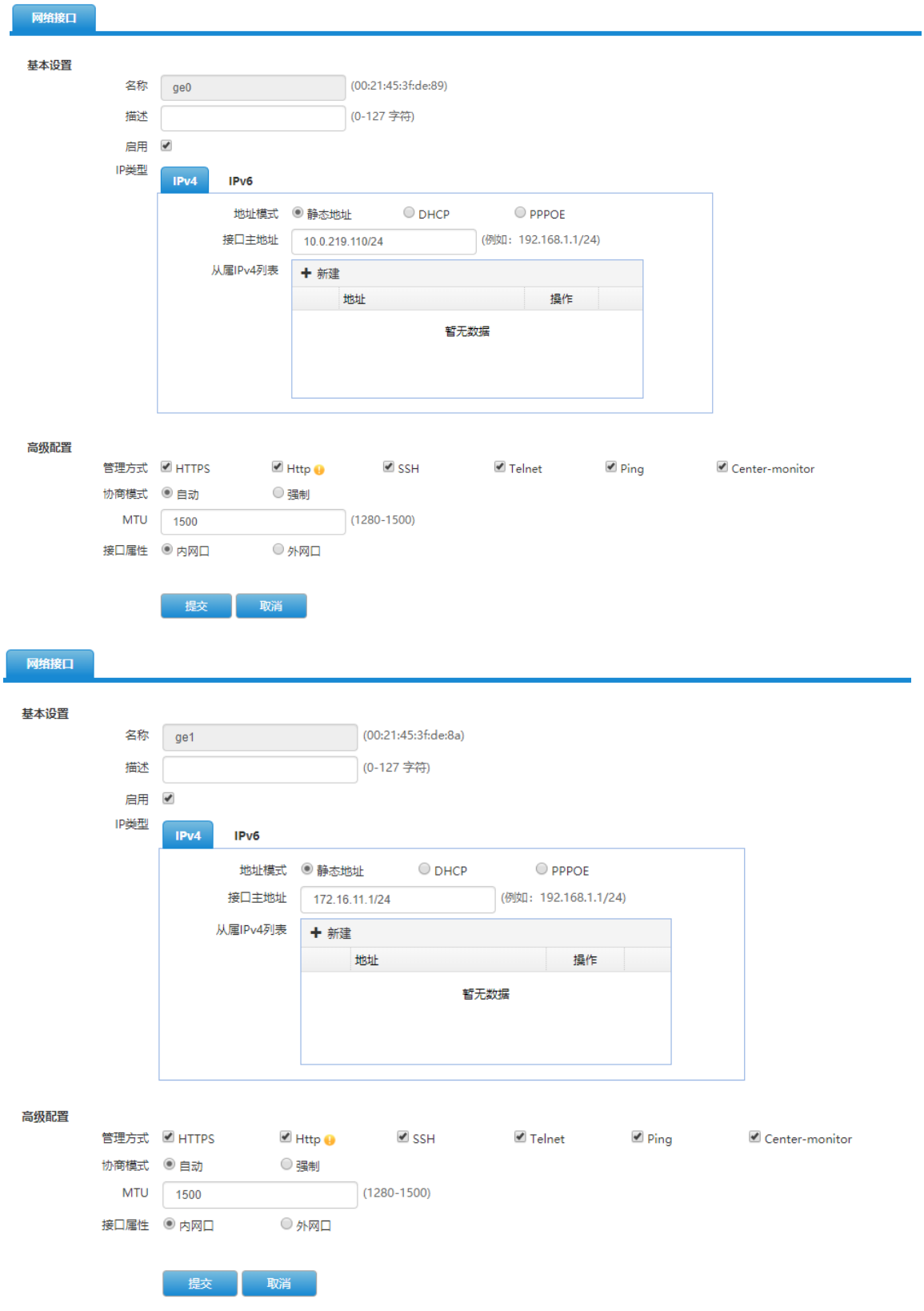
8.5 配置步骤

8.5.1 配置设备

1. 配置接口

如图 50 所示，进入“网络配置>接口配置”页面，进入物理接口页面，点击<编辑>按钮，ge0 和 ge1 分别配置 10.0.219.110/24 和 172.16.11.1/24。

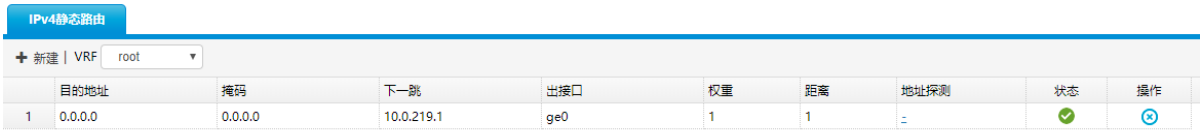
图50 配置接口


网络接口
基本设置
名称
ge0
(00:21:45:3f:de:89)
描述
(0-127 字符)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPOE
接口主地址
10.0.219.110/24
(例如：192.168.1.1/24)
从属IPv4列表
新建
地址
操作
暂无数据
高级配置
管理方式
HTTPS
Http
SSH
Telnet
Ping
Center-monitor
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口
提交
取消
网络接口
基本设置
名称
ge1
(00:21:45:3f:de:8a)
描述
(0-127 字符)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPOE
接口主地址
172.16.11.1/24
(例如：192.168.1.1/24)
从属IPv4列表
新建
地址
操作
暂无数据
高级配置
管理方式
HTTPS
Http
SSH
Telnet
Ping
Center-monitor
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口
提交
取消

2. 配置静态路由

如图 51 所示，进入“网络配置>路由管理>静态路由”，点击<新建>，配置一条缺省路由。

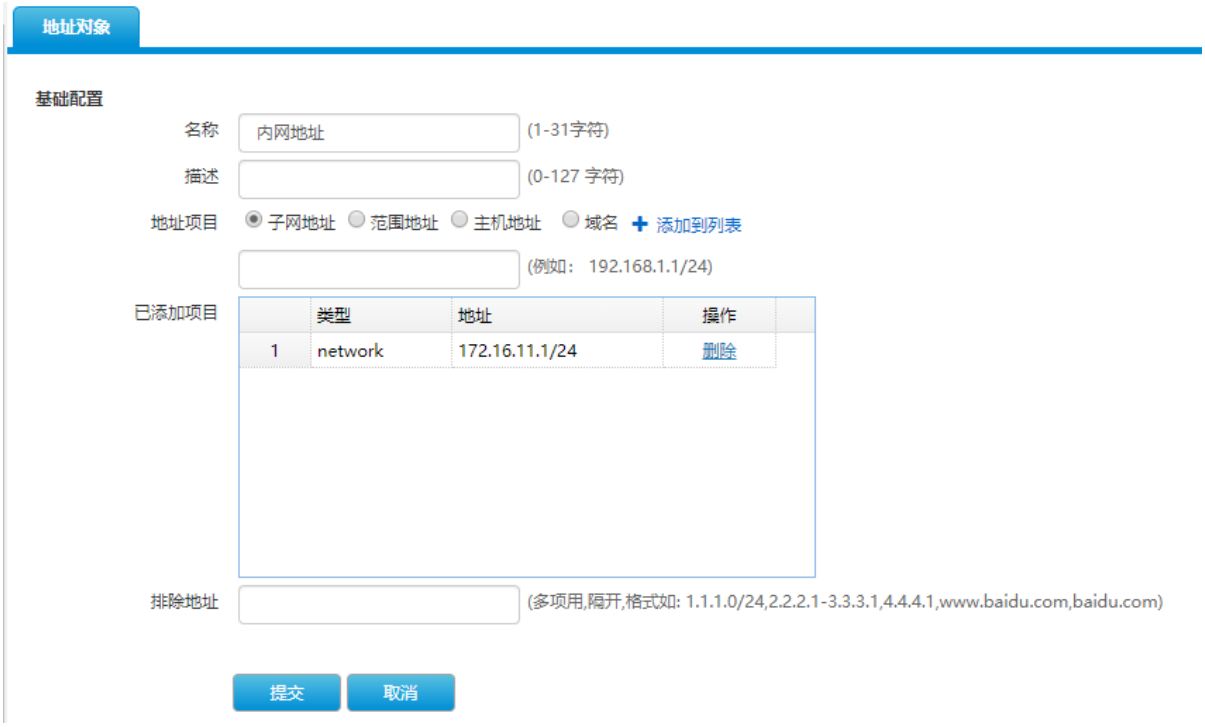
图51 配置静态路由



3. 配置地址对象

如图 52 所示，进入“策略配置>对象管理>地址对象”，进入 IPv4 地址对象页面，点击<新建>，新建一个“内网地址”地址对象，地址范围：172.16.11.1/24。

图52 配置地址对象



4. 配置用户识别范围

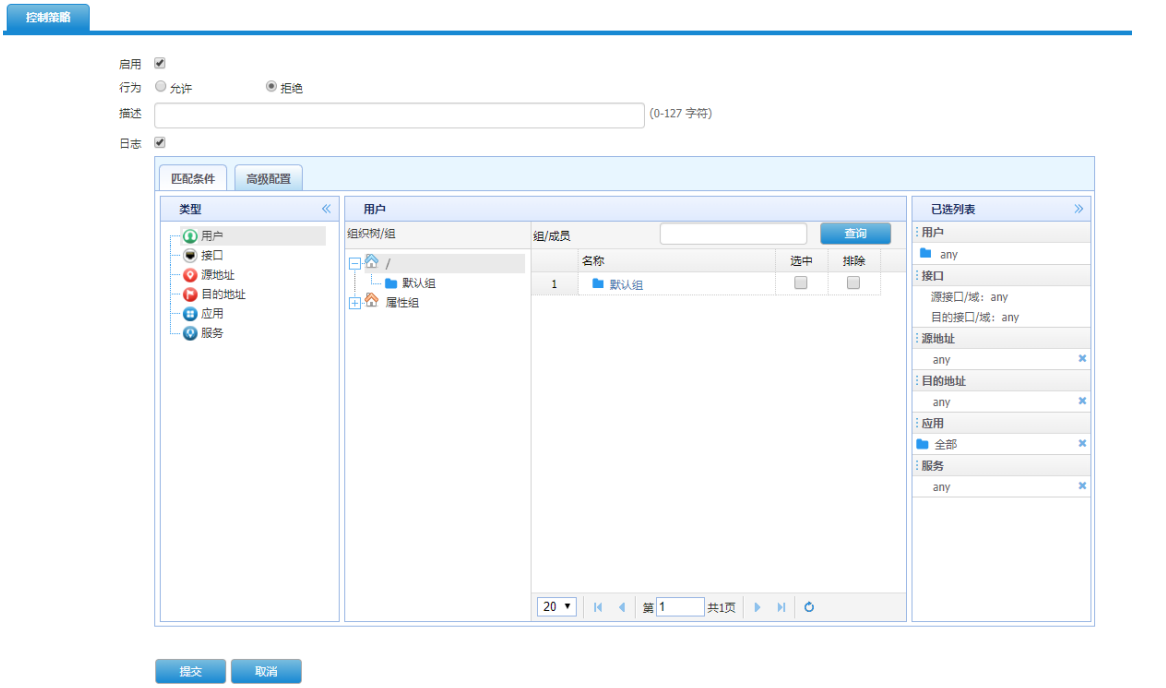
如图 53 所示，进入“用户管理>认证管理>高级选项”，进入全局配置页面，修改<识别范围>为“内网地址”，其余配置为默认配置。

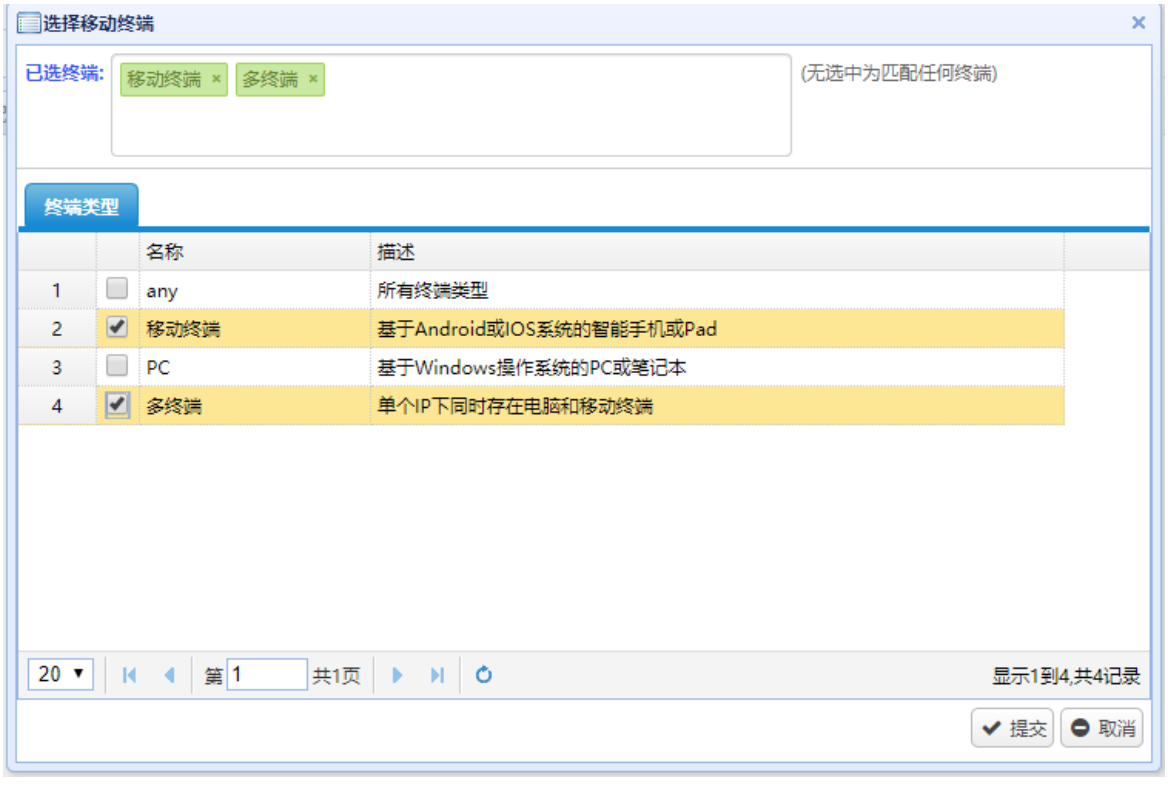
图53 配置用户识别范围

5. 配置 IPv4 控制策略

如图 54 所示，进入“策略配置 >策略配置 > IPv4 控制策略”，进入 IPv4 控制策略页面，点击<新建>，配置一条 IPv4 控制拒绝策略，终端选择多终端和移动终端。

图54 配置 IPv4 控制策略





8.6 验证配置

如图 55 所示，移动终端访问页面，提示访问出错

图55 移动终端无法上网

如图 56 所示，进入“策略配置 >策略配置 > IPv4 控制策略”，进入 IPv4 控制策略页面，可以查到策略匹配记录。

图56 IPv4 控制策略计数

使用 PC 可以正常上网，未被阻断。

目录

1 简介

本文档介绍设备的行为审计配置举例，包括 HTTP 类行为审计、邮件类行为审计、即时通讯类行为审计、网络基础协议类行为审计、娱乐股票类行为审计和网络应用其它应用行为审计。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解行为审计特性。

3 使用限制

设备对于采用私有算法进行加密的应用，无法审计其内容，例如无法审计 QQ 聊天内容。

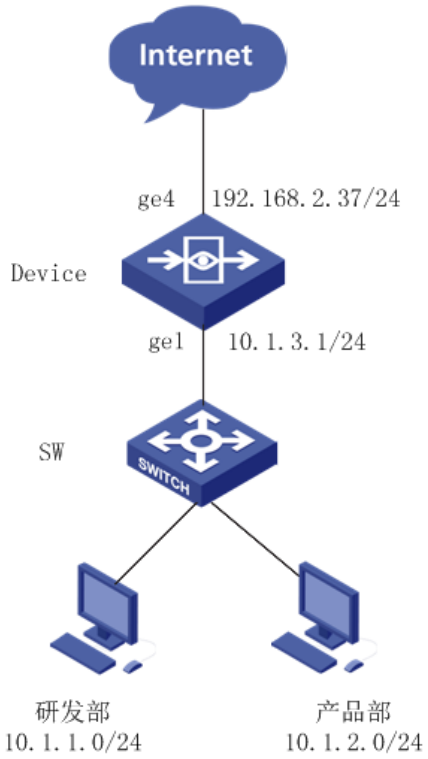
4 配置举例

4.1 组网需求

如图 1 所示，某公司内网存在研发部和产品部，IP 地址分别为 10.1.1.0/24 和 10.1.2.0/24。使用设备的的 ge1 和 ge4 接口跑三层转发，串接部署在核心交换机和出口路由器之间，启用行为审计功能，具体应用需求如下：

- 针对研发部，审计 HTTP 类行为、邮件类行为，其它应用行为不进行审计。
- 针对产品部，审计所有上网应用行为。

图1 IPv4 行为审计功能配置组网图



4.2 配置思路

- 根据源 IP 地址不同，配置两条 IPv4 策略分别对研发部和产品部进行审计。
- 在 IPv4 审计策略审计对象页面上，根据需求配置审计策略。
- 在用户管理高级选项全局配置页面上，配置具体用户识别访问。
- 在解密策略上配置网页及邮件类解密策略。
- 当需要将审计日志发送至外部日志服务器时，需要注意审计日志中配置的日志级别需要高于日志过滤中配置的发送级别。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- 一般情况下，目前应用都是应用行为进行审计，如果是 HTTPS 访问的应用，则需要优先配置 HTTPS 解密策略，优先进行解密才能进一步进行审计。HTTPS 解密策略的配置请参考“解密策略典型配置举例”。
- IPv4 审计策略匹配是由上至下进行匹配，策略匹配到之后将不会往下继续匹配。

4.5 配置步骤

4.5.1 配置设备

1. 配置地址对象

如图 2 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，IP 地址配置为 10.1.1.0/24，创建研发部地址对象，点击<提交>。按照同样的方法配置产品部地址对象。

图2 配置地址对象

如图 3 所示，创建成功的地址对象配置如下：

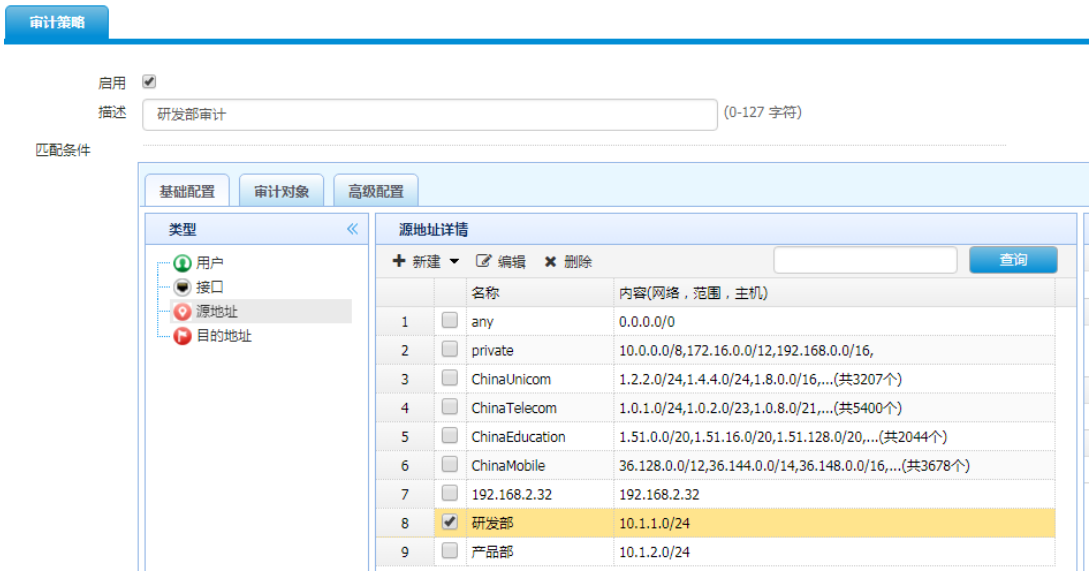
图3 地址对象配置成功

2. 配置研发部 IPv4 审计策略

(1) 配置研发部 IPv4 审计策略

如图 4 所示，进入“策略配置>IPv4 审计策略”，点击<新建>，“源地址”配置为研发部，然后点击“审计对象”页面。

图4 配置研发部 IPv4 审计策略



(2) 配置研发部审计对象

如图 5 和图 6 所示，在 IPv4 审计策略页面的“审计对象”页面，勾选“HTTP 类审计”和“邮件类审计”对象，其它配置保持默认，点击<提交>。

图5 配置 HTTP 类审计对象

图6 配置邮件类审计对象

如图 7所示，在“IPv4 审计策略”页面中查看，研发部审计策略配置完成。

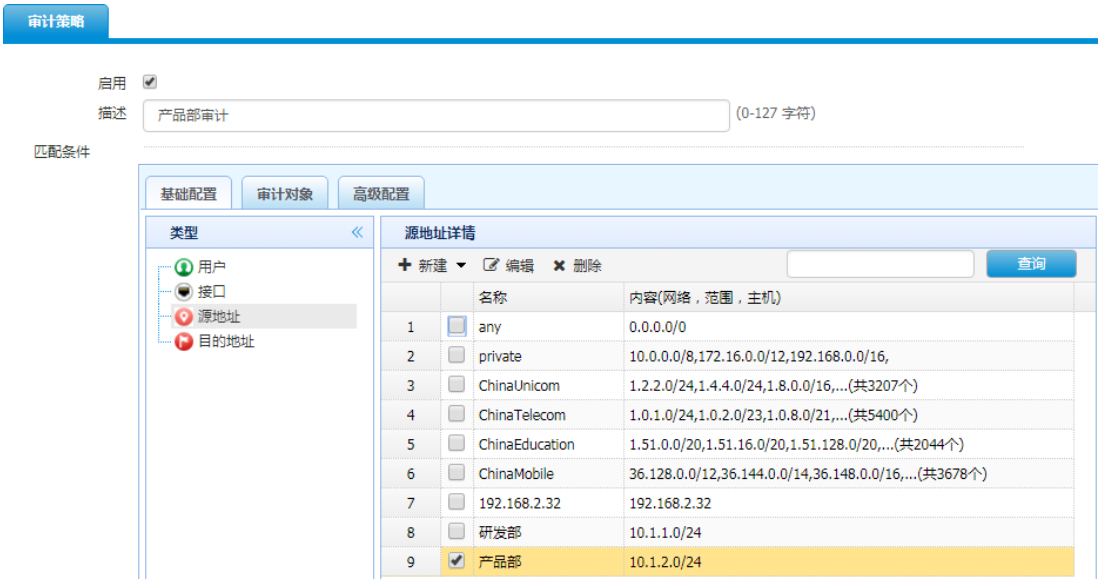
图7 研发部 IPv4 审计策略配置完成

3. 配置产品部 IPv4 审计策略

(1) 配置产品部 IPv4 策略

如图 8所示，进入“策略配置>IPv4 审计策略”，点击<新建>，选择源地址为产品部，然后点击“审计对象”页面。

图8 配置产品部 IPv4 审计策略



(2) 配置产品部全部应用审计策略

如图 9 所示，在 IPv4 审计策略配置页面 “审计对象”中，勾选所有类审计对象，其它配置保持默认，并点击<提交>。

图9 配置所有审计对象

如图 10 所示，创建成功的产品部审计策略配置如下，点击<提交>完成配置。

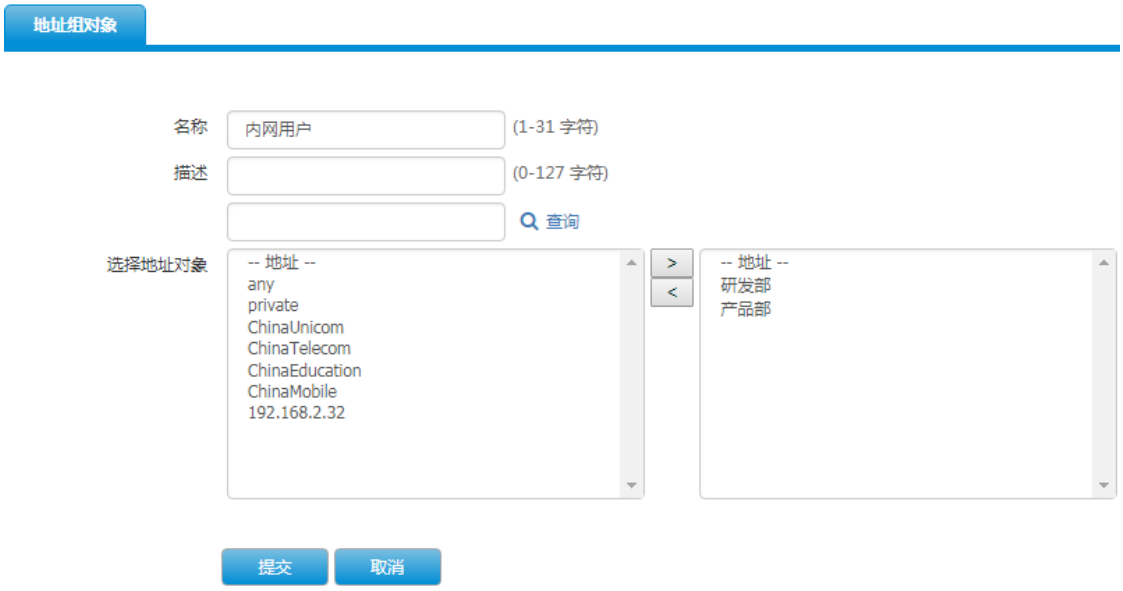
图10 产品部 IPv4 审计策略配置成功

4. 配置用户识别范围

(1) 配置地址对象组

如图 11 所示，进入“策略配置>对象管理>地址对象>地址组对象”，点击<新建>，配置一个地址对象组，将配置的研发部和产品部都选上，点击<提交>。

图11 地址组对象配置



如图 12 所示，在地址组对象页面查看，创建地址组对象完成。

图12 地址组对象配置完成

(2) 配置用户识别范围

如图 13 所示，进入“用户管理>认证管理>高级选项>全局配置”，识别范围选择地址组对象配置的内网用户，识别方式选择强制模式，点击<提交>按钮，用户识别配置完成。

图13 用户识别配置完成

5. 配置 HTTP 解密策略

(1) 配置 HTTPS 对象

如图 14 所示，进入“策略配置>对象管理>URL 对象>HTTPS 对象”，点击<新建>按钮，新建一条 HTTPS 对象，根据需求选择预定义对象和配置自定义 https 对象。

图14 新建 HTTPS 对象

如图 15 所示，HTTPS 对象配置完成之后，点击<提交>按钮，HTTPS 对象配置完成。

图15 HTTPS 对象配置完成

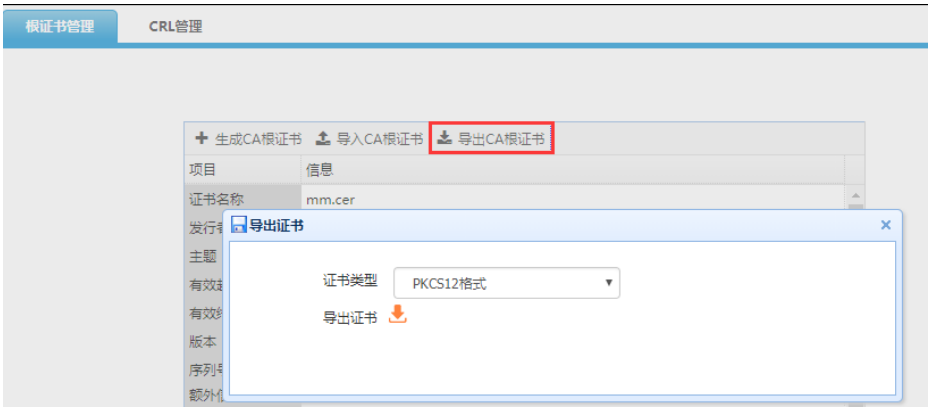
(2) 生成 CA 证书

如图 16 所示，进入“策略配置>对象管理>CA 服务器>根 CA 配置管理”，点击<生成 CA 根证书>。

图16 生成 CA 根证书

如图 17 所示，在生成 CA 证书以后，导出证书。.

图17 导出 CA 证书



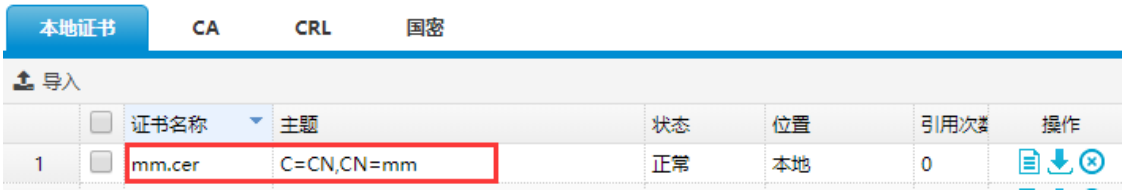
(3) 导入本地证书

如图 18 所示，进入“上策略配置>对象管理>本地证书>证书>本地证书”，点击<导入>，选择之前生成的 CA 证书。

图18 导入证书

如图 19 所示，导入成功的证书如下：

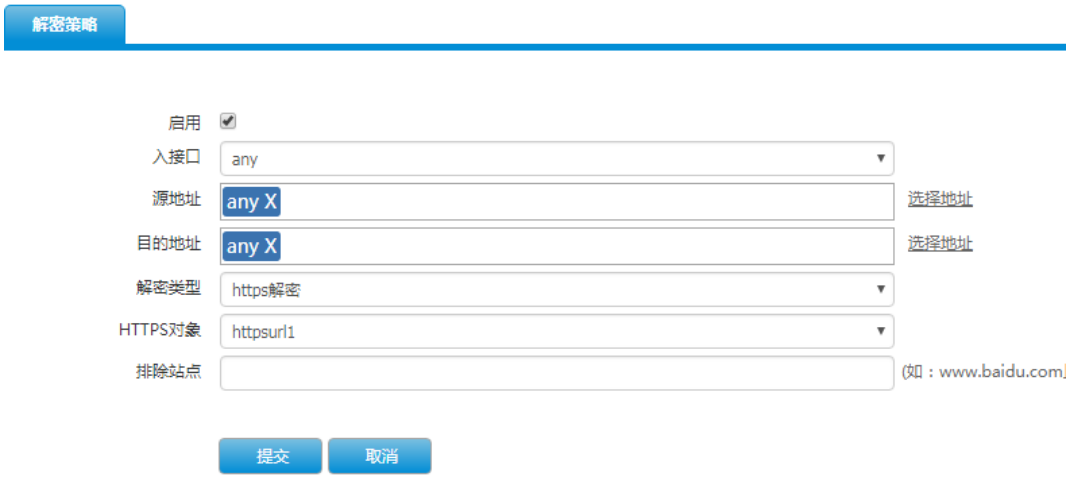
图19 导入证书成功



(4) 配置解密策略

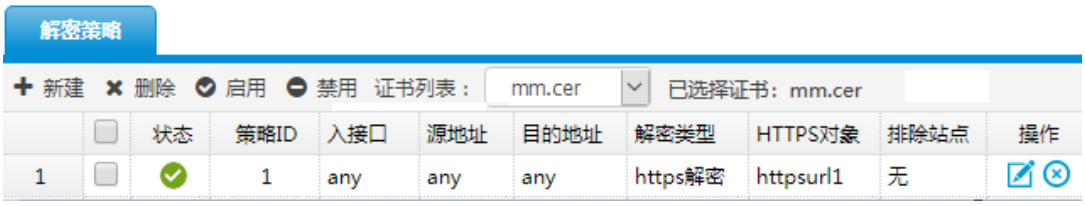
如图 20 所示，进入“策略配置>策略配置>SSL 解密策略”，点击<新建>按钮，配置一条 HTTPS 解密策略，根据需求配置指定的源目地址，解密类型选择 https 解密，解密 对象选择步骤 1 上配置的 https 对象，点击<提交>按钮。

图20 HTTPS 解密策略配置



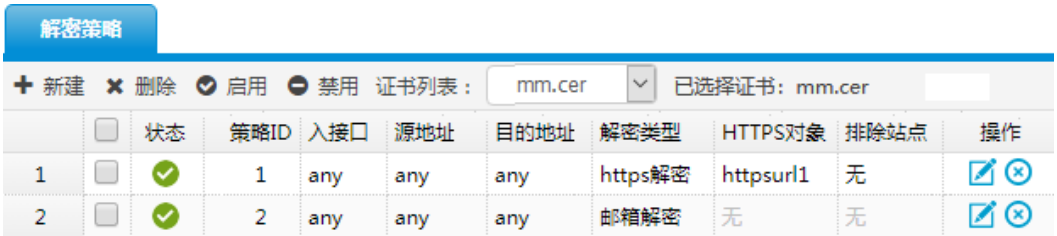
如图 21 所示，点击<提交>按钮之后，https 解密策略配置完成。

图21 HTTPS 解密策略配置完成



如图 22 所示，按步骤 2 的方法再配置一条邮件解密策略，解密类型选择邮箱解密，配置完成如下图所示。

图22 HTTPS 邮箱解密配置完成



4.6 验证配置

(1) 验证研发部 IPv4 审计策略效果

如图 23 所示，进入“数据中心>日志中心>审计日志>访问网站日志”，查看已经审计到研发部（IP 地址为 10.1.1.0/24）用户的网页浏览日志行为，并正确地记录了日志。

图23 查看研发部访问网站日志

	用户	用户mac	URL分类	网页标题	URL	级别	时间	操作
1	10.1.1.2	28:d2:44:3a:23:2d	门户网站与搜索引擎	网易账号中心		信息	2019-03-19 19:13:34	详细
2	10.1.1.2	28:d2:44:3a:23:2d	新闻媒体	新浪网		信息	2019-03-19 19:13:34	详细
3	10.1.1.2	28:d2:44:3a:23:2d	门户网站与搜索引擎	网易账号中心		信息	2019-03-19 19:13:27	详细
4	10.1.1.2	28:d2:44:3a:23:2d	新闻媒体	新浪网		信息	2019-03-19 19:13:24	详细
5	10.1.1.2	28:d2:44:3a:23:2d	机动车	新版狐首|微门户区域-北京-搜狐汽车		信息	2019-03-19 19:13:21	详细
6	10.1.1.2	28:d2:44:3a:23:2d	网上交易	京东广告		信息	2019-03-19 19:13:20	详细
7	10.1.1.2	28:d2:44:3a:23:2d	门户网站与搜索引擎	网易账号中心		信息	2019-03-19 19:13:12	详细
8	10.1.1.2	28:d2:44:3a:23:2d	门户网站与搜索引擎	网易账号中心		信息	2019-03-19 19:13:12	详细
9	10.1.1.2	28:d2:44:3a:23:2d	BBS站点	腾讯微博_你的心声，世界的回声		信息	2019-03-19 19:12:59	详细
10	10.1.1.2	28:d2:44:3a:23:2d	门户网站与搜索引擎	搜狐网		信息	2019-03-19 19:12:32	详细
11	10.1.1.2	28:d2:44:3a:23:2d	商业	淘宝网-淘！我喜欢		信息	2019-03-19 19:12:26	详细
12	10.1.1.2	28:d2:44:3a:23:2d	新闻媒体	腾讯·大燕网北京站		信息	2019-03-19 19:12:26	详细
13	10.1.1.2	28:d2:44:3a:23:2d	新闻媒体	搜狐		信息	2019-03-19 19:11:54	详细
14	10.1.1.2	28:d2:44:3a:23:2d	门户网站与搜索引擎	百度一下，你就知道		信息	2019-03-19 19:11:37	详细

如图 24 所示，进入“数据中心>日志中心>审计日志>社区日志”查看，查看已经审计到研发部（IP 地址为 10.1.1.0/24）用户的网络社区登录发帖内容，并正确地记录了日志。

图24 查看研发部网络社区日志

	用户	用户mac	应用	账号	行为	内容	终端类型	级别	时间	操作
1	10.1.1.2	28:d2:44:3a:23:2d	新浪微博_发表	6012097691	发表	最近有啥新鲜事没？	PC	信息	2019-03-19 19:30:38	详细
2	10.1.1.2	28:d2:44:3a:23:2d	新浪微博_登录	6012097691	登录	-	PC	信息	2019-03-19 19:30:15	详细
3	10.1.1.2	28:d2:44:3a:23:2d	百度贴吧_发表	bet[illegible]163.c	发表	从失败中总结教训与	PC	信息	2019-03-19 19:29:20	详细
4	10.1.1.2	28:d2:44:3a:23:2d	腾讯微博_发表	107[illegible]	发表	看天气预报今天晚上	PC	信息	2019-03-19 19:28:35	详细
5	10.1.1.2	28:d2:44:3a:23:2d	天涯论坛_发表	sapl[illegible]	发表	崇洋媚外	PC	信息	2019-03-19 19:27:55	详细
6	10.1.1.2	28:d2:44:3a:23:2d	天涯论坛_发表	sap[illegible]	发表	崇洋媚外	PC	信息	2019-03-19 19:27:55	详细
7	10.1.1.2	28:d2:44:3a:23:2d	腾讯微博_登录	1[illegible]9	登录	-	PC	信息	2019-03-19 19:26:55	详细
8	10.1.1.2	28:d2:44:3a:23:2d	百度贴吧_登录	bet[illegible]@163.c	登录	-	PC	信息	2019-03-19 19:26:42	详细
9	10.1.1.2	28:d2:44:3a:23:2d	天涯论坛_登录	sap[illegible]	登录	-	PC	信息	2019-03-19 19:26:28	详细

如图 25 所示，进入“数据中心>日志中心>审计日志>搜索引擎日志”，查看已经审计到研发部（IP 地址为 10.1.1.0/24）用户的网页搜索关键字日志行为，并正确地记录了日志。

图25 查询研发部搜索引擎审计日志

	用户	用户mac	应用	行为	内容	终端类型	级别	时间	操作
1	10.1.1.2	28:d2:44:3a:23:2d	360搜索_搜索	搜索	最新天气预报	PC	信息	2019-03-19 19:49:12	详细
2	10.1.1.2	28:d2:44:3a:23:2d	百度_搜索	搜索	北京植物园	PC	信息	2019-03-19 19:48:28	详细
3	10.1.1.2	28:d2:44:3a:23:2d	百度_搜索	搜索	北京植物园	PC	信息	2019-03-19 19:48:17	详细
4	10.1.1.2	28:d2:44:3a:23:2d	必应_搜索	搜索	玉渊潭公园	PC	信息	2019-03-19 19:47:42	详细
5	10.1.1.2	28:d2:44:3a:23:2d	必应_搜索	搜索	玉渊潭公园	PC	信息	2019-03-19 19:47:34	详细
6	10.1.1.2	28:d2:44:3a:23:2d	有道搜索_搜索	搜索	despaction	PC	信息	2019-03-19 19:47:30	详细
7	10.1.1.2	28:d2:44:3a:23:2d	必应_搜索	搜索	玉渊潭公园	PC	信息	2019-03-19 19:47:17	详细
8	10.1.1.2	28:d2:44:3a:23:2d	必应_搜索	搜索	玉渊潭公园	PC	信息	2019-03-19 19:47:17	详细
9	10.1.1.2	28:d2:44:3a:23:2d	搜搜_搜索	搜索	北京一日游	PC	信息	2019-03-19 19:47:04	详细
10	10.1.1.2	28:d2:44:3a:23:2d	百度_搜索	搜索	4月份旅游攻略	PC	信息	2019-03-19 19:46:55	详细

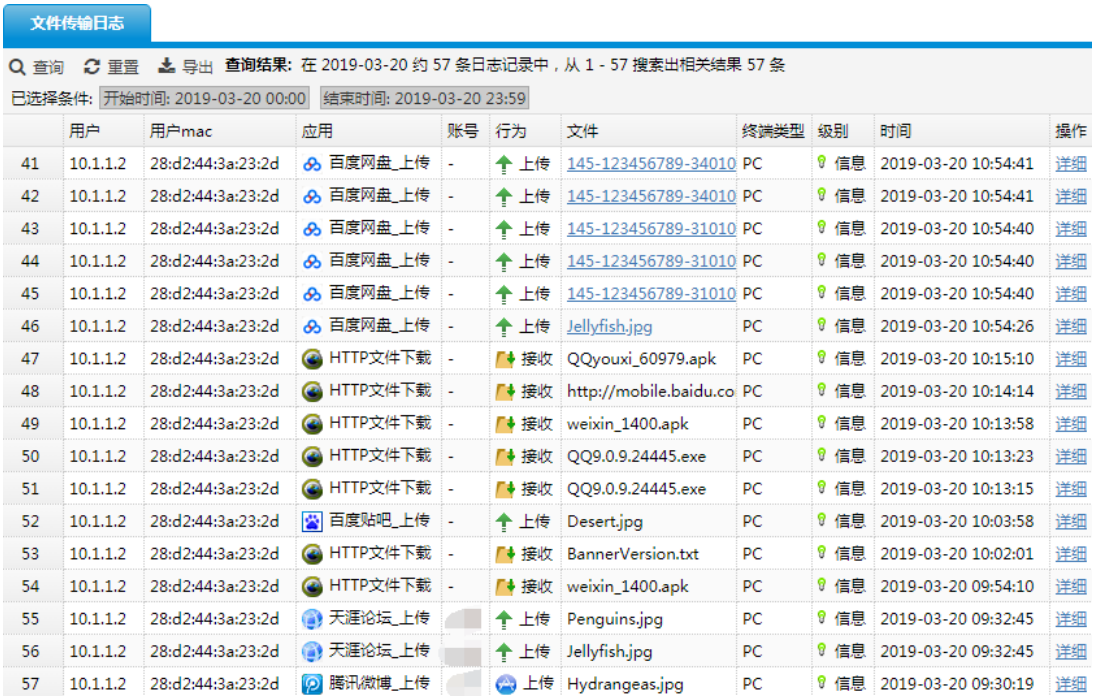
如图 26 所示，进入“数据中心>日志中心>审计日志>邮件日志”，查看已经审计到研发部（IP 地址为 10.1.1.0/24）用户的收发邮件日志行为，并正确地记录了日志。

图26 研发部收发邮件日志

	用户	用户mac	应用	行为	发件人	收件人	主题	内容	级别	时间	操作
1	10.1.1.2	28:d2:44:3a:23:2d	QQ邮箱_收邮件	收邮件	[redacted]@163.c	[redacted] <1076861	Chrysanth	查看	信息	2019-03-20 15:57:51	详
2	10.1.1.2	28:d2:44:3a:23:2d	QQ邮箱_收邮件	收邮件	[redacted]@163.c	[redacted]9 <1076861	都是范德	查看	信息	2019-03-20 15:57:49	详
3	10.1.1.2	28:d2:44:3a:23:2d	QQ邮箱_收邮件	收邮件	[redacted]3@163.c	[redacted]9 <1076861	新建 XLS	查看	信息	2019-03-20 15:57:49	详
4	10.1.1.2	28:d2:44:3a:23:2d	QQ邮箱_收邮件	收邮件	[redacted]@163.c	[redacted]9 <1076861	Chrysanth	查看	信息	2019-03-20 15:57:49	详
5	10.1.1.2	28:d2:44:3a:23:2d	126邮箱_收邮件	收邮件	[redacted]3@126	[redacted]3@163	施蒂利克	查看	信息	2019-03-20 15:43:35	详
6	10.1.1.2	28:d2:44:3a:23:2d	126邮箱_收邮件	收邮件	[redacted]3@yea	[redacted]3@163	sdfdsfds	查看	信息	2019-03-20 15:43:32	详
7	10.1.1.2	28:d2:44:3a:23:2d	126邮箱_收邮件	收邮件	[redacted]@yea	[redacted]03@163	sdfdsfds	查看	信息	2019-03-20 15:43:28	详
8	10.1.1.2	28:d2:44:3a:23:2d	126邮箱_收邮件	收邮件	[redacted]@163	[redacted]@163	时刻到了	查看	信息	2019-03-20 15:43:22	详
9	10.1.1.2	28:d2:44:3a:23:2d	126邮箱_登录	登录	[redacted]126.c	-	-	-	信息	2019-03-20 15:42:51	详
10	10.1.1.2	28:d2:44:3a:23:2d	163邮箱_发邮件	发邮件	[redacted]03	[redacted]79@qq.com	Chrysanth	查看	信息	2019-03-20 15:23:09	详
11	10.1.1.2	28:d2:44:3a:23:2d	163邮箱_发邮件	发邮件	[redacted]3	[redacted]79@qq.com	新建 XLS	查看	信息	2019-03-20 15:22:11	详
12	10.1.1.2	28:d2:44:3a:23:2d	163邮箱_发邮件	发邮件	[redacted]3	[redacted]3@qq.com"	Fw:你的快	查看	信息	2019-03-20 14:54:10	详

如图 27 所示，进入“数据中心>日志中心>审计日志>文件传输日志”，查看已经审计到研发部（IP 地址为 10.1.1.0/24）用户的 web 网盘上传下载文件以及 http 文件上传下载行为，并正确地记录了日志。

图27 研发部网盘上传下载日志



(2) 验证产品部 IPv4 审计策略效果

如图 28 所示，进入“数据中心>日志中心>审计日志>IM 聊天软件日志”，点击页面左上角的<查询>，可以看到产品部已经被正确记录了即时通讯日志，而研发部并没有记录除了 HTTP 类、邮件类以外的其它应用日志。

图28 产品部 IM 聊天软件日志

4.7 配置文件

!

address 研发部

ip subnet 10.1.1.0/24

```
!
address 产品部
 ip subnet 10.1.2.0/24
!
address-group 内网用户
 member 研发部
 member 产品部
!
https-object httpsurl1
  https-object add domain uploadphotos.baidu.com
  https-object add domain nav.fetiononline.com
  https-object add domain ssl-comments.youku.com
  https-object add domain comments.youku.com
  https-object add domain ptlogin2.minigame.qq.com
  https-object add domain www.9188.com
  https-object add domain www.vip.com
  https-object add domain www.yhd.com
  https-object add domain passport.yhd.com
  https-object add category BBS 站点
  https-object add category 商业
  https-object add category 娱乐
  https-object add category 游戏
  https-object add category 网络资源
  https-object add category 求职招聘
  https-object add category 网上交易
  https-object add category 新闻媒体
  https-object add category 在线聊天
  https-object add category 门户网站与搜索引擎
  https-object add category 参考
  https-object add category 旅游
  https-object add category WEB 通信
!
policy decrypt any any any https httpsurl1 1
policy decrypt any any any mail 2
policy listen block disable
!
audit_policy any any 研发部 any any always web_access any 1
    audit-behaviour network_community
```

```
    audit-behaviour web_search
    audit-behaviour send_web_mail
    audit-behaviour http_send_file
    audit-behaviour http_download_file
    audit-behaviour send_mail
    audit-behaviour receive_mail
    audit-behaviour receive_web_mail
    audit-behaviour web_mail_upload_attachment
    audit-behaviour web_mail_download_attachment
    audit-behaviour web_disk_upload_file
    audit-behaviour web_disk_download_file
    description 研发部审计
    log level info
audit_policy any any 产品部 any any always all any 2
    description 产品部审计
    log level info
audit associate enable
!
ip route 0.0.0.0/0 192.168.2.1
ip route 10.1.1.0/24 10.1.3.2
ip route 10.1.2.0/24 10.1.3.2
!
user-param recognition scope 内网用户 strict
!
```

目录

1 简介

本文档介绍设备的 IPv6 控制策略配置举例，IPv6 控制策略可以基于用户、源目接口、源目地址、应用、服务、URL、时间等多维度进行控制。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPv6 控制策略特性。

3 使用限制

- 设备版本对于纯 IPv6 环境下加密的应用无法进行解密，所以不能对加密相关应用进行识别及控制。

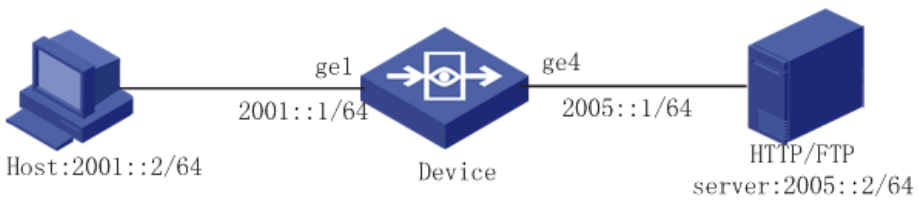
4 配置举例

4.1 组网需求

如图 1 所示，某部门内网用户使用 IPV6 网段地址过设备访问公司内部部署的 IPV6 的 HTTP 服务器和 FTP 服务器，先需要对 IPV6 服务器访问进行限制，工作时间（9:00-18:00）不允许访问 FTP 服务器和 HTTP 服务器，只有其它时间访问这两个服务器进行上传下载正常。具体应用需求如下：

- 工作时间不能通过 IPV6 地址访问这两个服务器。

图1 IPv6 控制策略功能配置组网图



4.2 配置思路

- Host 主机上配置 IPv6 地址；
- 设备接口上配置 IPv6 地址。
- 设备配置 IPv6 地址对象。
- 设备配置时间对象。
- 设备配置用户识别范围。

- 设备基于 IPv6 地址对象配置 IPv6 控制策略。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

IPv6 控制策略匹配是由上至下进行匹配，策略匹配到之后将不会往下继续匹配。

4.5 配置步骤

4.5.1 配置设备

1. 配置接口 IPv6 地址

如图所示，进入“网络配置>接口配置>物理接口”，在 ge1 和 ge4 口上配置 IPv6 地址。

图2 配置接口 IPv6 地址

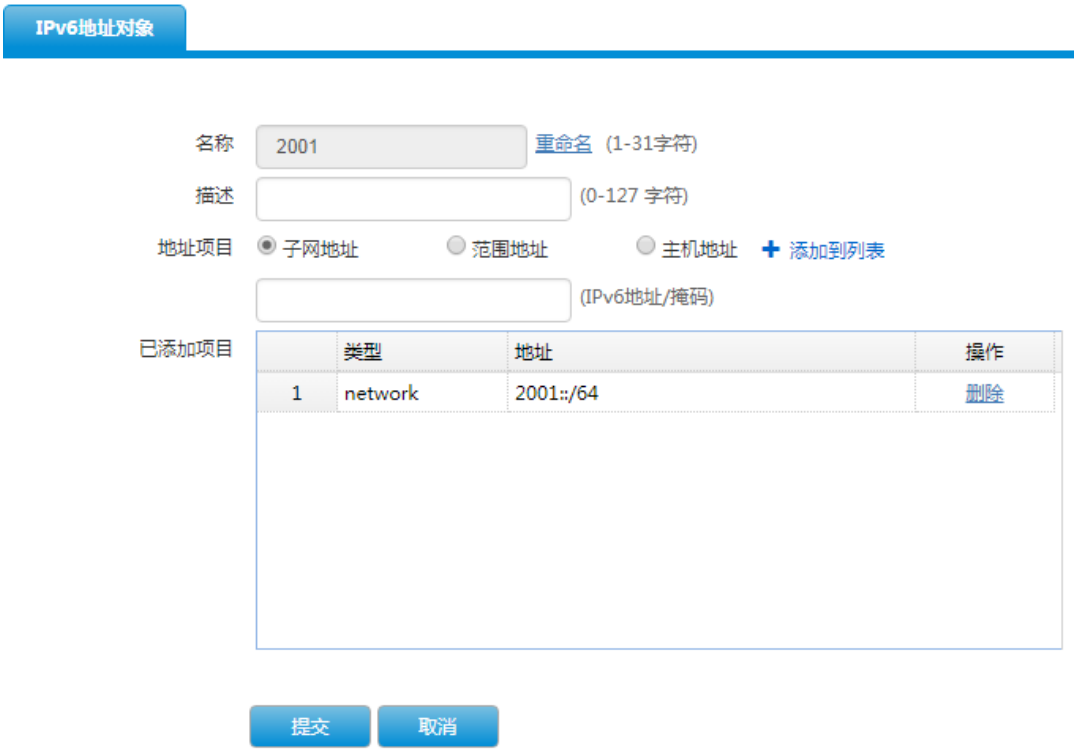
物理接口 | 子接口 | 网桥接口 | 聚合接口 | 隧道接口 | 无线接口 | 安全域 | 虚拟网线

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0		90.90.1.37/24		00:21:45:3f:de:9a	route	full	100	up		
2	ge1		10.1.1.1/24	2001::1/64	00:21:45:3f:de:9b	route	full	1000	up		
3	ge2				00:21:45:3f:de:9c	route	full	1000	down		
4	ge3				00:21:45:3f:de:9d	route	full	1000	up		
5	ge4		192.168.2.37/24	2005::1/64	00:21:45:3f:de:9e	route	full	100	up		
6	ge5				00:21:45:3f:de:9f	route	full	1000	up		

2. 配置地址对象

如图 3 所示，进入“策略配置>对象管理>地址对象>IPv6 地址对象”，点击<新建>，IP 地址配置为 2001::/64，创建内网 IPv6 地址对象，点击<提交>。按同样的办法配置服务器网段 2005::/64 的 IPv6 地址对象。

图3 配置地址对象



如图 4 所示，创建成功的地址对象配置如下：

图4 地址对象配置成功

3. 配置时间对象

如图 5 所示，进入“策略配置>对象管理>时间对象>日计划”，配置日计划时间对象，工作时间选择9:00-18:00。

图5 日计划时间对象

4. 配置用户识别范围

如图 6 所示，进入“用户管理>认证管理>高级选项>全局配置”，识别范围选择 any，识别方式选择强制模式，点击<提交>按钮，用户识别配置完成。

图6 用户识别配置完成

5. 配置 IPv6 控制策略策略

(1) 配置 IPv6 控制策略匹配条件

如图 7 所示，进入“策略配置>IPv6 控制策略”，点击<新建>，“源地址”配置为 2001，目的地址配置为 2005 如图 8 所示，时间对象选择工作时间如图 9 所示。

图7 配置 IPv6 控制策略源地址

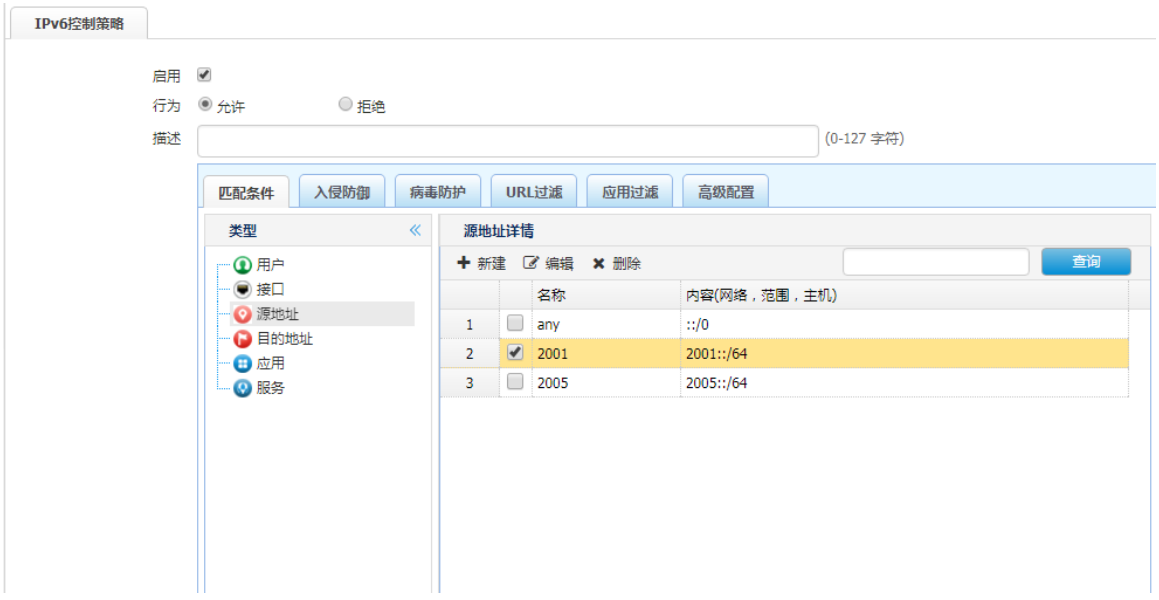


图8 配置 IPv6 控制策略目的地址

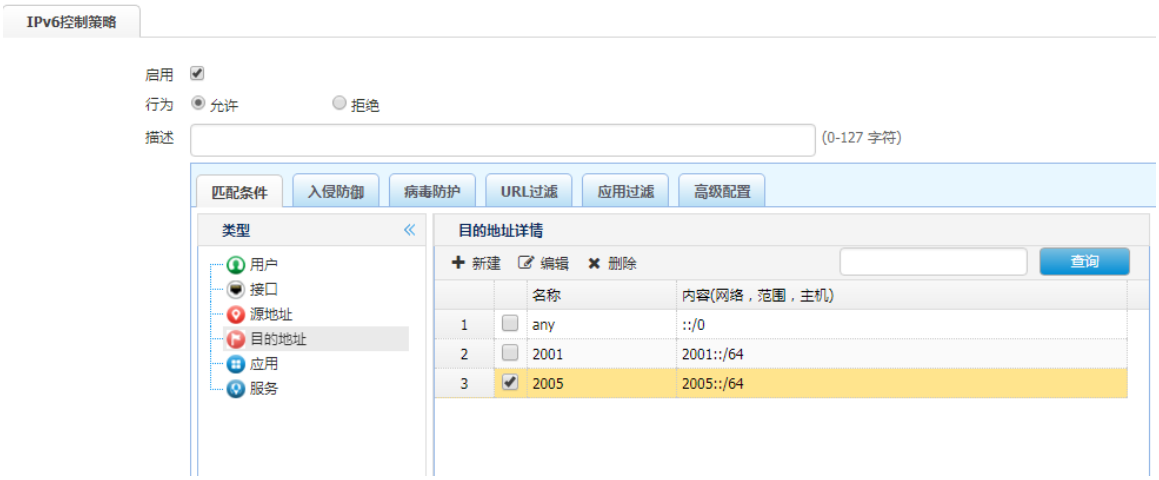
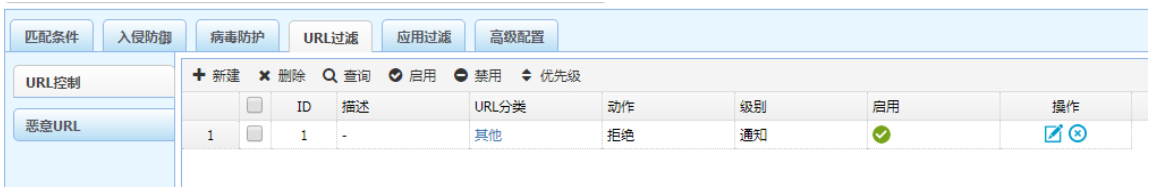


图9 配置 IPv6 控制策略时间

(2) 配置 URL 过滤策略

如图 10 所示，在 IPv6 控制策略的“URL 过滤”页面，点击“URL 控制”<新建>一条 URL 控制策略，URL 分类选择其它，动作选择拒绝，日志级别选择通知级别，点击<提交>。

图10 配置 URL 控制策略



(3) 配置应用过滤策略

如图 11 所示，在 IPv6 控制策略的“应用过滤”页面，点击<新建>一条应用控制策略，应用分类选择文件传输大类，动作选择拒绝，日志级别选择通知级别，点击<提交>。

图11 配置应用过滤策略

如图 12 所示，点击策略最下面的<提交>按钮，IPv6 控制策略配置完成。

图12 IPv6 控制策略配置完成

4.6 验证配置

(1) 如图 13 所示，测试终端 ping 服务器的 IPv6 地址可正常通信。

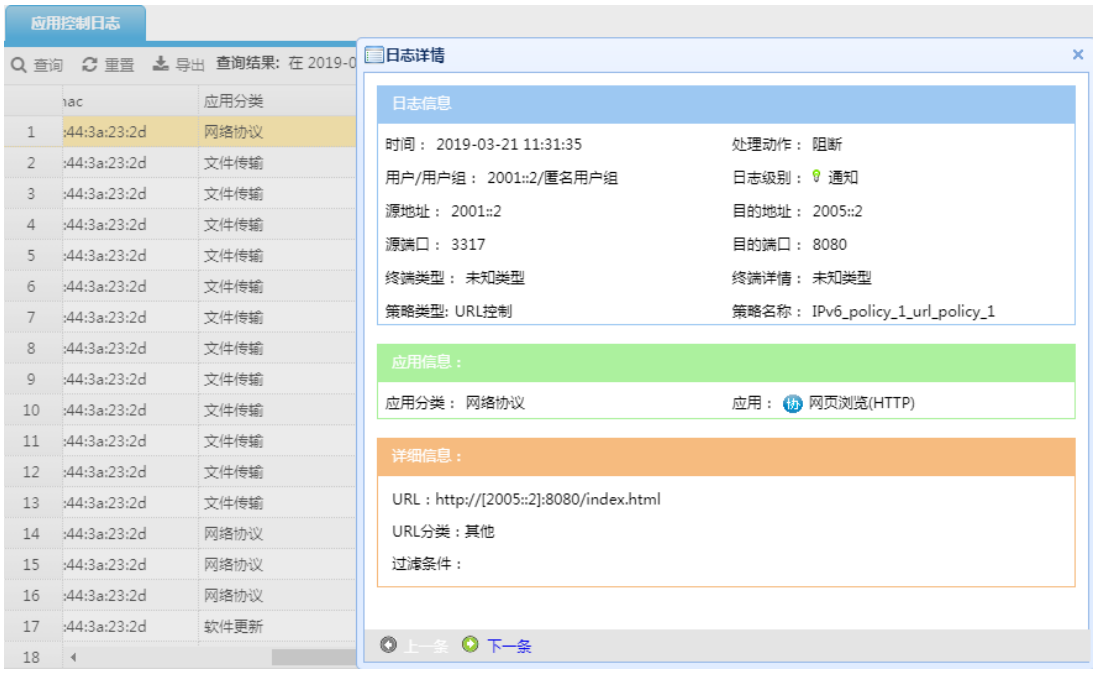
图13 测试终端 ping IPv6 服务器地址

(2) 如图 14 所示，工作时间段，测试 PC 访问 IPv6 服务器的 HTTP 服务被拒绝，有相应的阻断提示信息。

图14 访问 IPv6 服务器的 HTTP 服务被拒绝

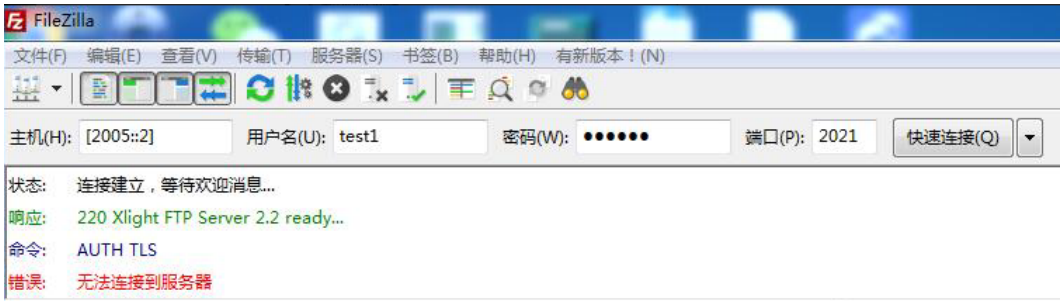
(3) 如图 15 所示，进入“数据中心>日志中心>控制日志>应用控制日志”，有匹配 IPv6 控制策略中 URL 控制策略的阻断日志。

图15 URL 过滤控制阻断日志



(4) 如图 16 所示，测试终端通过 FTP 客户端登录 IPv6 服务器的 FTP server，登录失败。

图16 终端登录 FTP 服务器失败



(5) 如图 17 所示，进入“数据中心>日志中心>控制日志>应用控制日志”，有匹配 IPv6 控制策略中应用过滤策略的阻断日志。

图17 应用控制阻断日志

	用户	用户mac	应用分类	应用	策略类型	处理动作	终端类型	级别	时间
1	2001::2	28:d2:44:3a:23:2d	文件传输	FTP文件传输协议	应用控制	阻断	未知类型	通知	2019-03-21
2	2001::2	28:d2:44:3a:23:2d	文件传输	FTP文件传输协议	应用控制	阻断	未知类型	通知	2019-03-21
3	2001::2	28:d2:44:3a:23:2d	文件传输	HTTP文件下载	应用控制	阻断	未知类型	通知	2019-03-21

4.7 配置文件

```
!
interface ge1
 ip address 10.1.3.1/24
 ipv6 address 2001::1/64
 allow access https
 allow access http
 allow access ping
 allow access ssh
 allow access telnet
!
interface ge4
 traffic-mode extern
 ip address 192.168.2.37/24
 ipv6 address 2005::1/64
 allow access https
 allow access http
```

```
 allow access ping
 allow access ssh
 allow access telnet
!
address6 2001
 ipv6 subnet 2001::/64
!
address6 2005
 ipv6 subnet 2005::/64
!
schedule-day 工作时间
 periodic start 09:00 end 18:00
!
policy6 any any 2001 2005 any any any 工作时间 permit 1
  log policy-deny enable
  app-policy control 1 action deny log-level notice
  app-policy control 1 application File_Transfer
  app-policy control 1 enable
  website-policy 1 other-url deny notice FilterUrl
   website-policy enable 1
policy6 default-action permit
!
```

目录

1 简介

本文档介绍设备的链路负载均衡配置举例，包括负载均衡出接口，免负载均衡地址，负载均衡策略的链路负载均衡配置。

在配置链路负载均衡前，先了解如下几个定义：

- 负载均衡：负载均衡建立在现有网络结构之上，扩展了网络设备和服务器的带宽、增加了吞吐量，同时提升了网络的数据处理能力、灵活性和可用性，具有低成本且有效透明的优点。负载均衡在应用模式上可分为服务器负载均衡和链路负载均衡，全局负载均衡。
- 物理链路：运营商提供的实际链路。
- 链路带宽：运营商提供给此链路的实际带宽。
- 链路阈值：流量超过此链路阈值时会进行相应带宽调度。
- 链路权重：多条链路在同一调度策略中，根据加权调度算法将目标流量根据权重比进行分发。
- 优先级：多条链路在同一调度策略中，根据由上到下的优先级顺序将目标流量进行分发。
- 健康检查：检查运营商链路的质量。
- 会话保持：匹配源目 ip 的同一会话在老化时间内走同一条链路。使用源地址 hash，这样就可以保证同一源地址的所有请求使用唯一接口完成转发。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解链路负载均衡的特性。

3 使用限制

链路负载均衡策略，对于新建流量生效。

4 配置举例

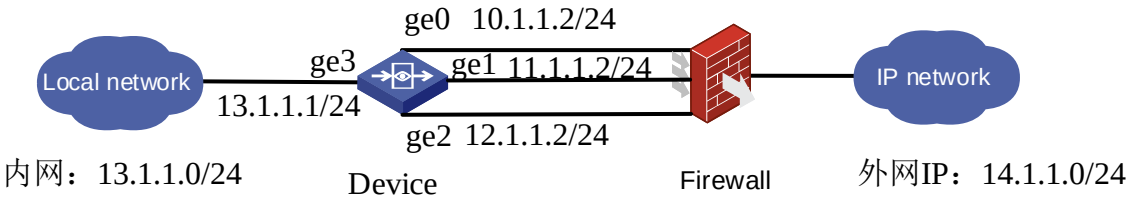
4.1 组网需求

如图 1 所示，某公司内网办公网段 IP 地址为 13.1.1.0/24。使用设备的的 ge3 口连接内网设备，ge3 网关地址 13.1.1.1/24，在设备产品开启链路负载均衡功能，出接口 ge0 内网 ip：10.1.1.2/24，出接口 ge1 内网 ip：11.1.1.2/24，出接口 ge2 内网 ip：12.1.1.2/24。具体应用需求如下：

- 将设备的配置三个负载均衡出接口，分别为出接口 ge0，ge1，ge2。
- 负载均衡的三个出接口分别添加健康检查功能。
- 配置负载均衡策略 1，负载均衡策略选择按照优先级进行负载均衡，匹配条件为电信运营商，添加出接口 ge0。

- 配置负载均衡策略 2，负载均衡策略选择按照优先级进行负载均衡，匹配条件为联通运营商，添加出接口 ge1。
- 配置负载均衡策略 3，负载均衡策略选择按照优先级进行负载均衡，匹配条件为移动运营商，添加出接口 ge2。
- 配置负载均衡策略 4，负载均衡策略选择按照权重进行负载均衡，匹配条件为默认，添加三个出接口分别为出接口 ge0，ge1，ge2。

图1 链路负载均衡功能组网图



4.2 配置思路

- 配置链路负载均衡前，先配置链路负载均衡出接口。
- 为每个链路负载出接口添加健康检查策略，保证可以及时监控链路状态。
- 链路负载均衡策略添加相应的链路出接口，保证命中策略的流量能够按照选中接口进行转发。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证。

4.4 配置注意事项

- 负载均衡出接口为三层静态 ip 的接口，必须配置下一跳地址，出接口为 pppoe，dhcp，tunnel 接口，不需要手动配置下一跳地址。
- 链路负载均衡出接口，尽量为每一个出口链路配置可达的地址作为健康检查地址，这样可以及时发现出接口状态的变化。
- Isp 地址导入后，需要执行 isp address update ，导入的 isp 地址生效。

4.5 配置步骤

4.5.1 配置设备

1. 配置地址对象

如图 2 所示，进入“策略配置>对象管理>地址对象> IPv4 地址对象”，点击<新建>，IP 地址配置为 13.1.1.0/24 创建办公网段地址对象，点击<提交>。

图2 配置地址对象

2. 配置默认路由

如图 3 所示，在设备上进入“网络配置>路由管理>静态路由”，点击<新建>，配置三条默认路由。

图3 配置默认路由

	目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	操作
1	0.0.0.0	0.0.0.0	11.1.1.1	ge1	1	1	-		
2	0.0.0.0	0.0.0.0	12.1.1.1	ge2	1	1	-		
3	0.0.0.0	0.0.0.0	10.1.1.1	ge0	1	1	-		

3. 配置出接口的源 NAT

如图 4 所示，在设备上进入“策略配置>NAT 转换策略>源 NAT”，点击<新建>，配置三个源 NAT。

图4 配置出接口源 NAT

4. 配置负载均衡出接口（3 个出接口）

如图 5，图 6，图 7 所示，在设备上进入“策略配置>负载均衡策略>负载均衡出接口”，点击<新建>，配置三个负载均衡出接口。

图5 电信出接口

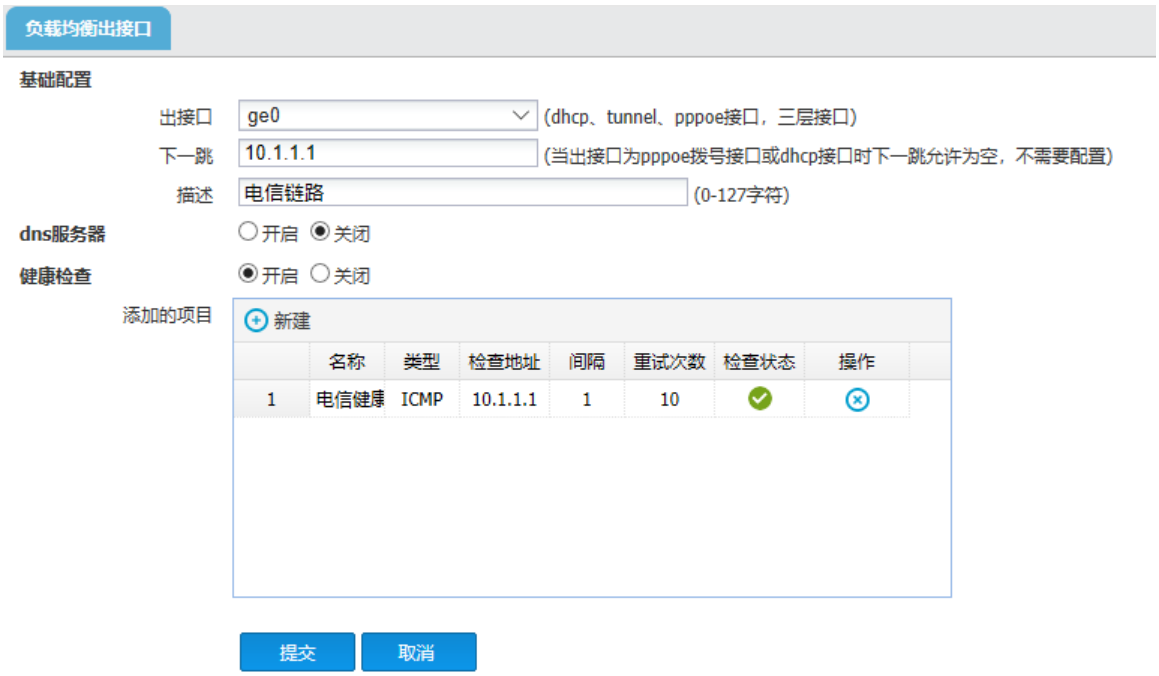


图6 联通出接口

图7 移动出接口

5. 配置负载均衡策略

如图 8，图 9，图 10，图 11 所示，在设备上进入“策略配置>负载均衡策略>负载均衡策略”，点击<新建>，配置四条负载均衡策略。

图8 电信链路负载均衡策略

图9 联通链路负载均衡策略

图10 移动链路负载均衡策略

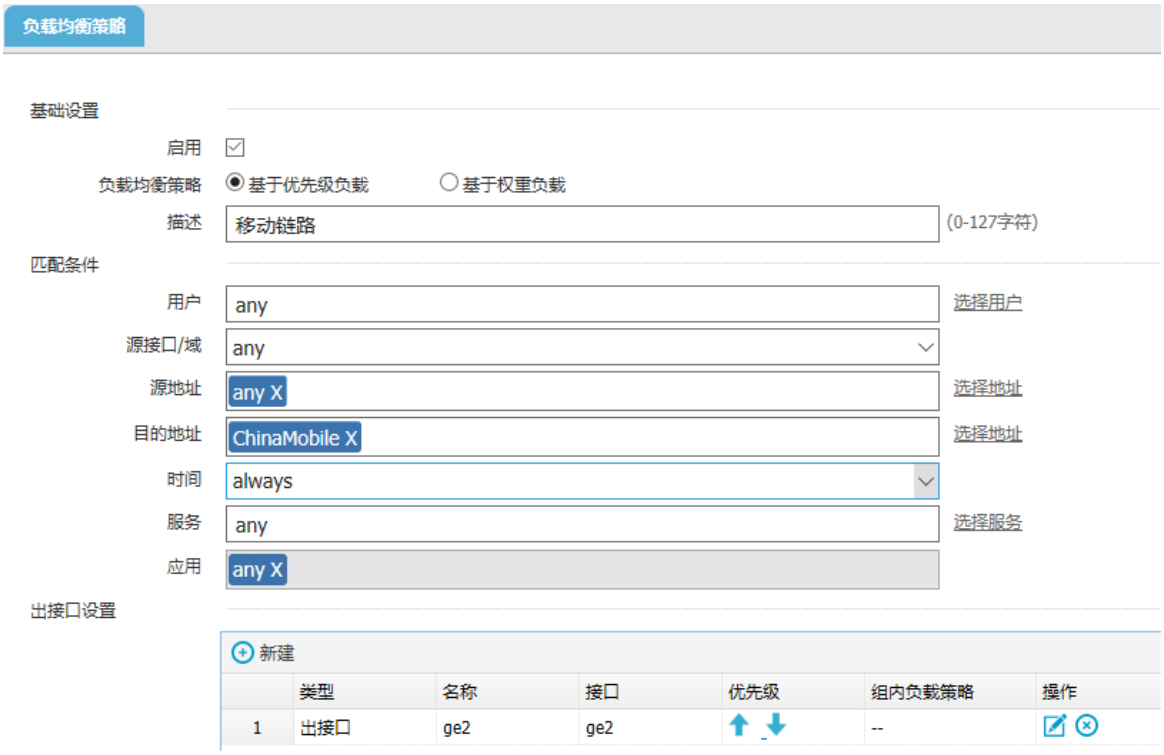


图11 默认链路负载均衡策略

4.6 验证配置

(1) 验证电信用户的流量从电信链路发送出去

如图 12 所示，观察所有用户访问 14.1.1.0/24 网段的流量全部从电信链路转发出去（前提：目的地址 14.1.1.0 网段，加入到 isp 电信运营商中）。

导入 ISP 地址后，需要 update 才能生效，命令如下：

```
UNIS# copy ftp 192.168.2.178 isp_addr.txt isp_address
Download file isp_addr.txt ....
100%[=======================================>] 34,559       --.-K/s    in 0.02s
Download file(isp_addr.txt) success.
UNIS# con terminal
UNIS(config)# isp address update
```

图12 负载均衡策略中观察电信策略的匹配次数

		状态	ID	描述	源接口	源地址	目的地址	服务	应用	用户	匹配次数	时间	负载策略	出接口详情	操作
1			1	电信链路	any	any	ChinaTelecon	any	any	any	2859777	always	优先级		
2			2	联通链路	any	any	ChinaUnicom	any	any	any	0	always	优先级		
3			3	移动链路	any	any	ChinaMobile	any	any	any	0	always	优先级		
4			4	默认所有链路	any	any	any	any	any	any	0	always	权重		

(2) 验证联通用户的流量从联通链路发送出去

如图 13 所示，观察所有用户访问 14.1.1.0/24 网段的流量全部从联通链路转发出去（前提：目的地址 14.1.1.0 网段，加入到 isp 联通运营商中）。

图13 负载均衡策略中观察联通策略的匹配次数

		状态	ID	描述	源接口	源地址	目的地址	服务	应用	用户	匹配次数	时间	负载策略	出接口详情	操作
1			1	电信链路	any	any	ChinaTelecon	any	any	any	0	always	优先级		
2			2	联通链路	any	any	ChinaUnicom	any	any	any	703351	always	优先级		
3			3	移动链路	any	any	ChinaMobile	any	any	any	0	always	优先级		
4			4	默认所有链路	any	any	any	any	any	any	7	always	权重		

(3) 验证移动用户的流量从移动链路发送出去

如图 14 所示，观察所有用户访问 14.1.1.0/24 网段的流量全部从移动链路转发出去（前提：目的地址 14.1.1.0 网段，加入到 isp 移动运营商中）。

图14 负载均衡策略中观察移动策略的匹配次数

		状态	ID	描述	源接口	源地址	目的地址	服务	应用	用户	匹配次数	时间	负载策略	出接口详情	操作
1			1	电信链路	any	any	ChinaTelecon	any	any	any	0	always	优先级		
2			2	联通链路	any	any	ChinaUnicom	any	any	any	0	always	优先级		
3			3	移动链路	any	any	ChinaMobile	any	any	any	1225186	always	优先级		
4			4	默认所有链路	any	any	any	any	any	any	0	always	权重		

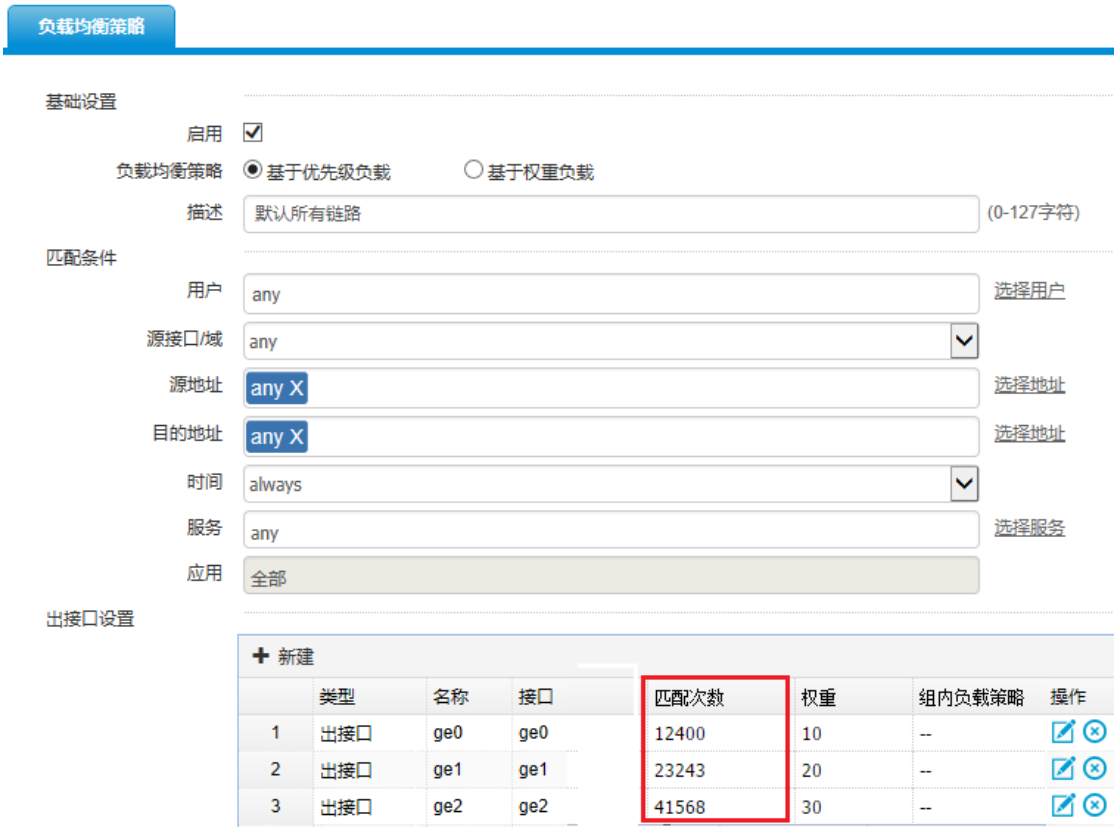
(4) 验证其它用户的流量按照出接口的带宽比，按比例发送出去

如图 15、图 16所示，观察所有用户访问 14.1.1.0/24 网段的流量全部从所有链路按配置比例 10:20:30 转发出去（前提：目的地址 14.1.1.0 网段，不属于任何运营商中）。

图15 负载均衡策略中观察默认策略的匹配次数

		状态	ID	描述	源接口	源地址	目的地址	服务	应用	用户	匹配次数	时间	负载策略	出接口详情	操作
1			1	电信链路	any	any	ChinaTelecon	any	any	any	0	always	优先级		
2			2	联通链路	any	any	ChinaUnicom	any	any	any	0	always	优先级		
3			3	移动链路	any	any	ChinaMobile	any	any	any	0	always	优先级		
4			4	默认所有链路	any	any	any	any	any	any	265380	always	权重		

图16 负载均衡策略中观察默认策略的匹配次数，每个接口是否按照比例 10：20：30 进行转发



4.7 配置文件

```
Device:WD-D# display running-config lb-policy
!
lb-policy wans interface ge1-0
 description 电信链路
 next-hop 10.1.1.1
 monitor enable
 monitor 电信健康检查 ping 10.1.1.1 1 10
lb-policy wans interface ge1-1
 description 联通链路
 next-hop 11.1.1.1
 monitor enable
 monitor 联通健康检查 ping 11.1.1.1 1 10
lb-policy wans interface ge1-2
 description 移动链路
 next-hop 12.1.1.1
 monitor enable
 monitor 移动健康检查 ping 12.1.1.1 1 10
!
lb-policy any any ChinaTelecom any any any always 1
 description 电信链路
```

```
 out-interface ge1-0 10
lb-policy any any ChinaUnicom any any any always 2
 description 联通链路
 out-interface ge1-1 10
lb-policy any any ChinaMobile any any any always 3
 description 移动链路
 out-interface ge1-2 10
lb-policy any any any any any any always 4
 mode weight-ratio
 description 默认所有链路
 out-interface ge1-0 10
 out-interface ge1-1 10
 out-interface ge1-2 10
!
Device:WD-D#
```

目录

1 简介

本文档介绍设备的日志功能配置举例，包括日志的记录、外发和管理。

设备共有五种类型日志，分别为系统日志、操作日志、安全日志、审计日志、终端日志，可以分别记录如下类型日志：

- 系统日志：记录系统状态变化信息，如接口状态变化、HA 状态变化、管理员登录登出日志等。
- 操作日志：记录管理员对系统的操作和修改日志。
- 安全日志：记录的日志包括异常包攻击日志、Flood 攻击日志、恶意 URL 日志以及应用控制日志等。
- 审计日志：记录的日志类型包括访问网站日志、IM 聊天软件日志、社区日志、搜索引擎日志、邮件日志、文件传输日志、娱乐/股票日志和其它应用日志。
- 终端日志：记录了用户终端相关的日志，如用户上下线日志、共享介入日志、移动终端日志等。

设备的日志级别表示日志的重要性，用户可以手工设置日志级别。目前设备的支持的日志级别从高到低，共有紧急、告警、严重、错误、警告、通知、信息和调试八种，当审计日志中配置的日志级别高于日志过滤中配置的发送级别时，日志方可被发送给第三方日志服务器。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解设备日志特性。

3 使用限制

- 设备的的审计日志和控制日志存储位置为硬盘，操作日志和系统日志存储位置为 Flash 芯片，其它日志（包括部分安全日志、终端日志）在设备有硬盘时存储到硬盘中，没有硬盘时存储在 Flash 芯片中。
- 当硬盘存储空间占用率达到 95%后，设备开始按照时间顺序，从时间最早的文件开始删除硬盘内的日志和邮件缓存文件，直到硬盘存储空间占用率达到 85%。

4 配置举例

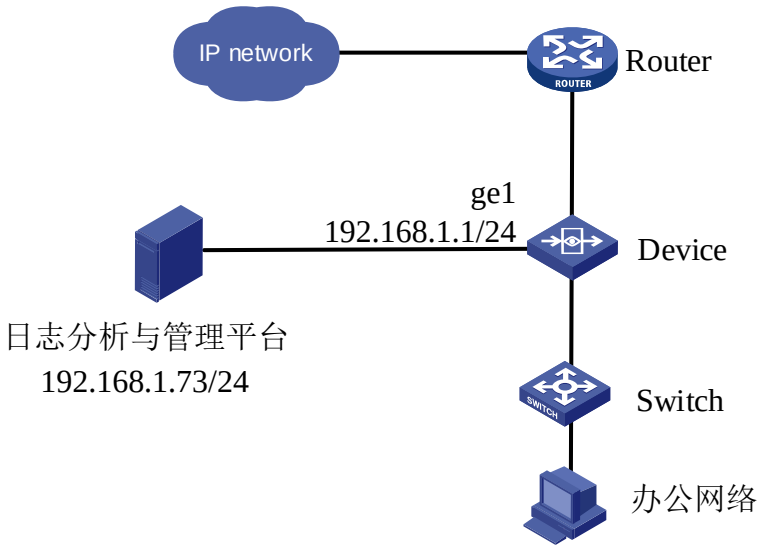
4.1 组网需求

如图 1 所示，设备的以透明模式串接在某公司网络的核心交换机和出口路由器之间，内网中部署日志分析与管理平台服务器，具体应用需求如下：

- 设备的开启日志审计功能，设备的使用的 IP 地址为 192.168.1.1/24，日志分析与管理平台使用的 IP 地址为 192.168.1.73/24，日志使用默认的 UDP 514 端口发送。

- 需要审计的日志为：应用审计日志、网站访问日志、安全防护日志和系统日志，上述日志的日志级别分别为信息、信息、警告、通知。
- 设备的在本地记录日志，同时将日志发送到日志分析与管理平台服务器。
- 将设备上的日志支持导出到 PC。

图1 日志功能配置组网图



4.2 配置前提

设备正确部署在网络中，内网用户可以正常上网。

4.3 配置思路

- 设备的配置 IPv4 审计策略。
- 设备的开启网络层攻击防护功能，安全防护日志会自动记录。
- 在日志服务器中填写日志分析与管理平台的 IP 地址。
- 在日志过滤中选择需要记录的日志类型以及发送日志的级别。

4.4 使用版本

本举例是在设备的的 E6442 版本和日志分析与管理平台的 R0304 版本上进行配置和验证的。

4.5 配置注意事项

- 当需要将审计日志发送至外部日志服务器时，需要注意审计日志中配置的日志级别需要高于日志过滤中配置的发送级别。
- 如果只需要在设备本地记录日志，则无需配置日志服务器。
- 配合日志分析与管理平台收集日志时，可选择将日志加密，防止日志遭到窃取。

- 所有日志均支持导出，其中系统日志、操作日志、网络层攻击日志、用户上下线日志、移动终端日志支持一次性导出，不支持选择导出日志的时间范围；其它日志不支持一次性全部导出所有日志内容，支持导出时间范围。
- 导出文件形式为压缩包，当导出日志中某一天无日志记录时不生成该日期的空内容导出文件。
- 用户导出的最大日志大小为 25 万条左右（对应的文件大小在 100M 左右，存在一些误差），因此当数据量较大时，用户选择了近三月的数据，可能只导出了几天或十几天的数据。所以导出的日志数量为导出规格的先决条件，其次才是选择的时间范围。
- 不支持负载及附件内容的导出（例如：邮件负载内容及附件）。
- 导出文件存储格式为 csv 格式，文件内容编码格式为 GBK，可直接使用 excel 打开，使用其它文本查看工具时请注意编码类型，以免中文内容显示为乱码。

4.6 配置步骤

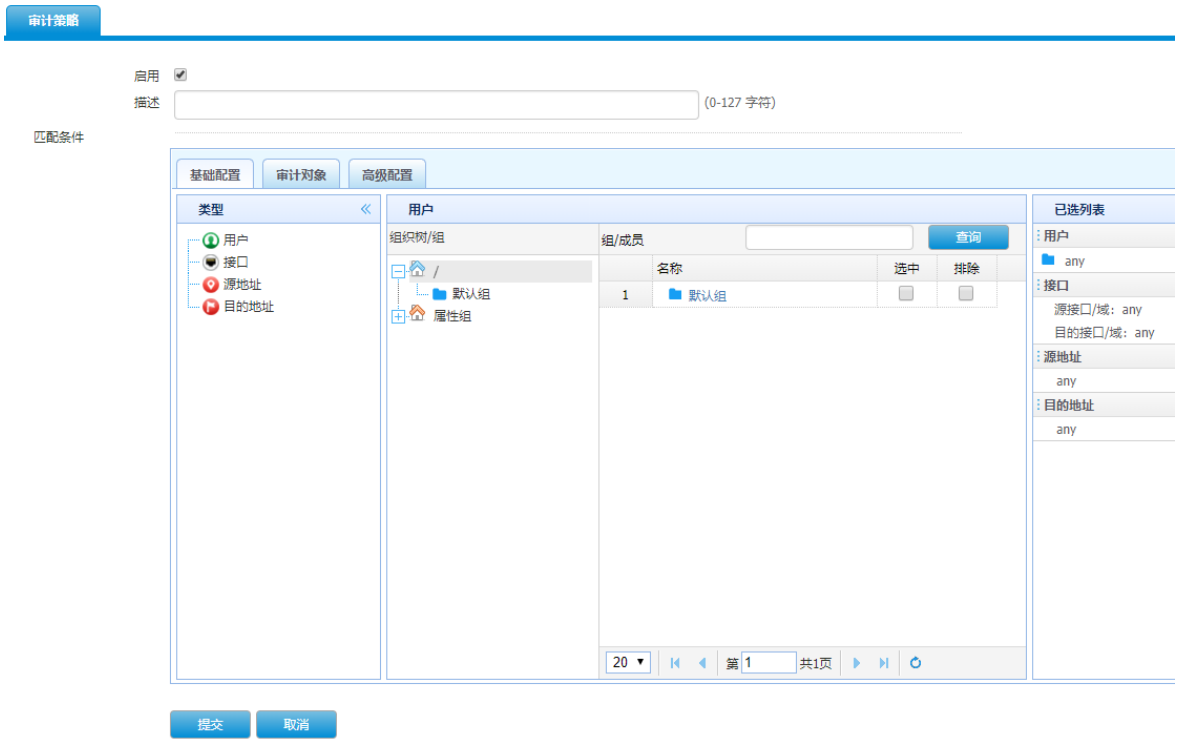
4.6.1 配置设备

1. 配置 IPv4 审计策略

(1) 配置 IPv4 策略

如图 2 所示，进入“策略配置>IPv4 审计策略”，单击<新建>，基础配置保持默认的全 any，接着配置“审计对象”。

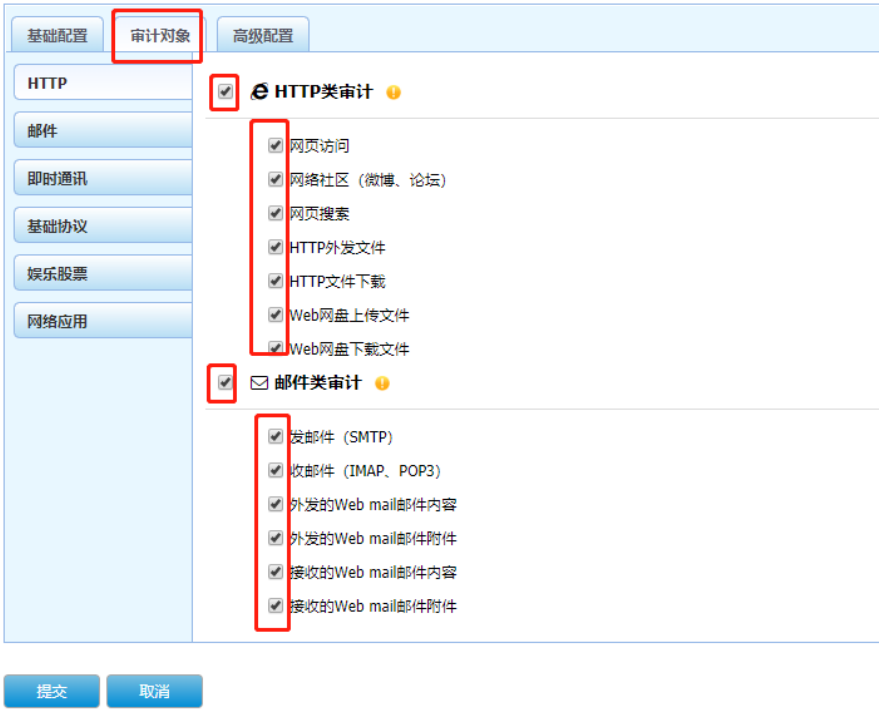
图2 配置 IPv4 审计策略基础配置



(2) 配置审计对象

如图 3 所示，在 IPV4 审计策略的审计对象部分，勾选所有的应用分类。

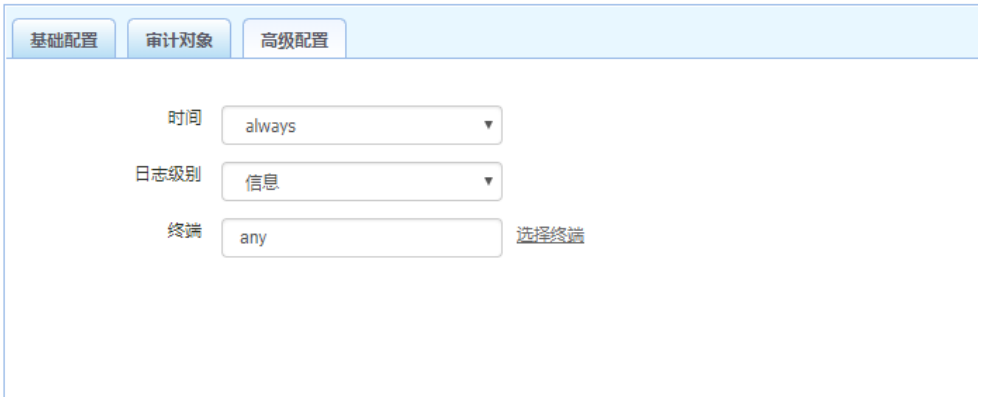
图3 配置应用审计策略



(3) 配置高级配置

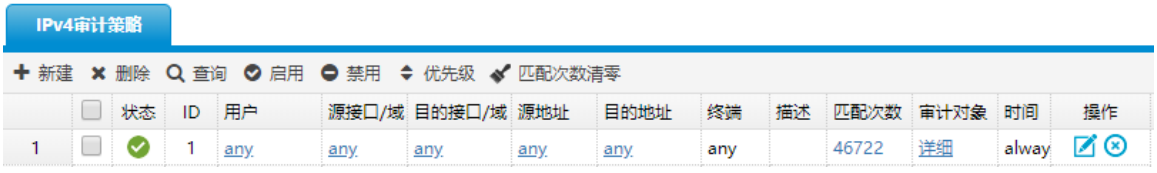
如图 4 所示，单击“高级配置”部分，选择时间为“always”，日志级别为“信息”，终端为“any”。最后提交配置。

图4 配置高级配置



如图 5 所示，创建成功的 IPv4 审计策略如下。

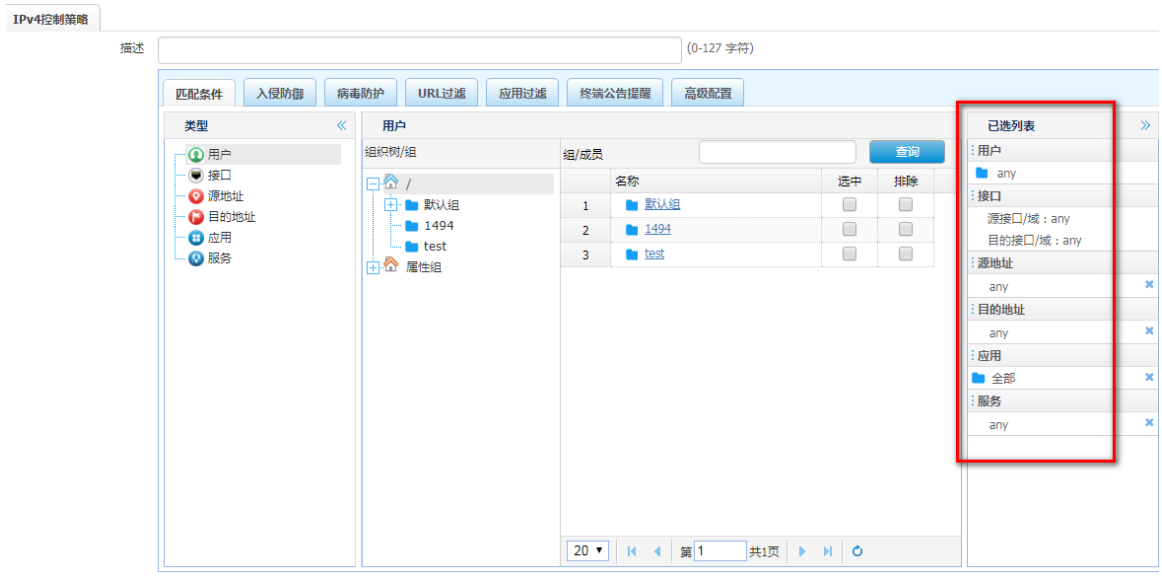
图5 IPv4 审计策略配置成功



2. 配置 IPv4 控制策略

如下图所示，进入“策略配置>IPv4 控制策略”，单击<新建>，在控制策略新建页面勾选“启用”，选择行为为“允许”，匹配条件保持默认即可。

图6 IPv4 控制策略-匹配条件



选择 URL 过滤页面，在 URL 控制项中单击<新建>，在弹出的配置框中勾选“启用规则”，URL 分了选择“全部”，处理动作选择“允许”，日志级别选择“信息”，然后单击<提交>，配置后如下图所示。

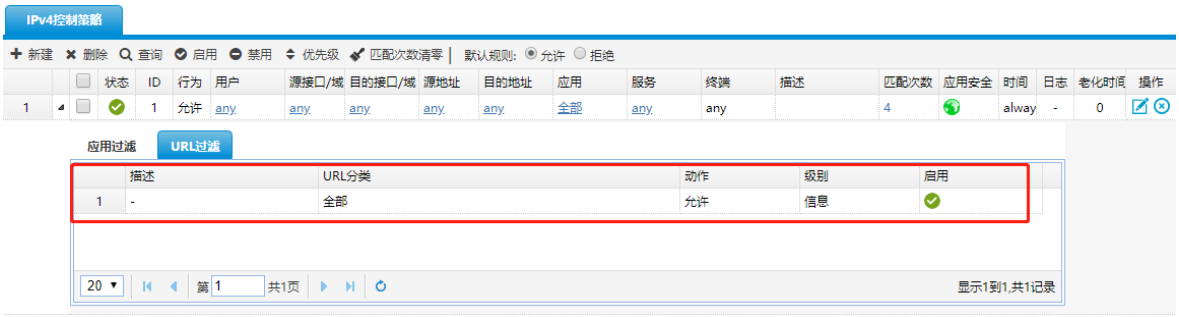
图7 IPv4 控制策略-URL 控制

在恶意 URL 项中勾选“过滤”选项，其它保持默认，最后提交配置。

图8 IPv4 控制策略-恶意 URL

配置完成后，IPv4 控制策略列表显示如下。

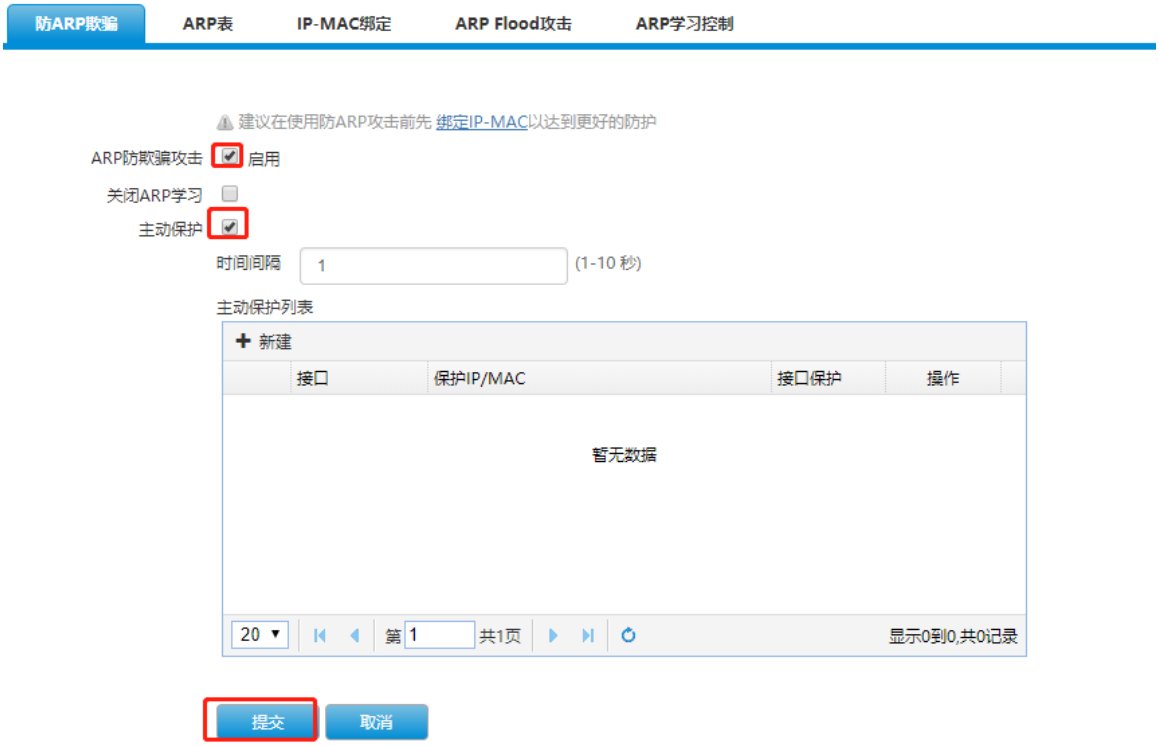
图9 IPv4 控制策略



3. 配置安全防护

如图 10 所示，进入“策略配置>安全设置>安全防护> ARP 攻击防护>防 ARP 欺骗”，在“ARP 防欺骗攻击”和“主动防护”上打钩，并单击<提交>。

图10 开启防 ARP 欺骗



如图 11 所示，进入“策略配置>安全设置>安全防护> ARP 攻击防护> ARP Flood 攻击”，在“启用”上打钩，单击<提交>。

图11 开启防 ARP Flood 攻击

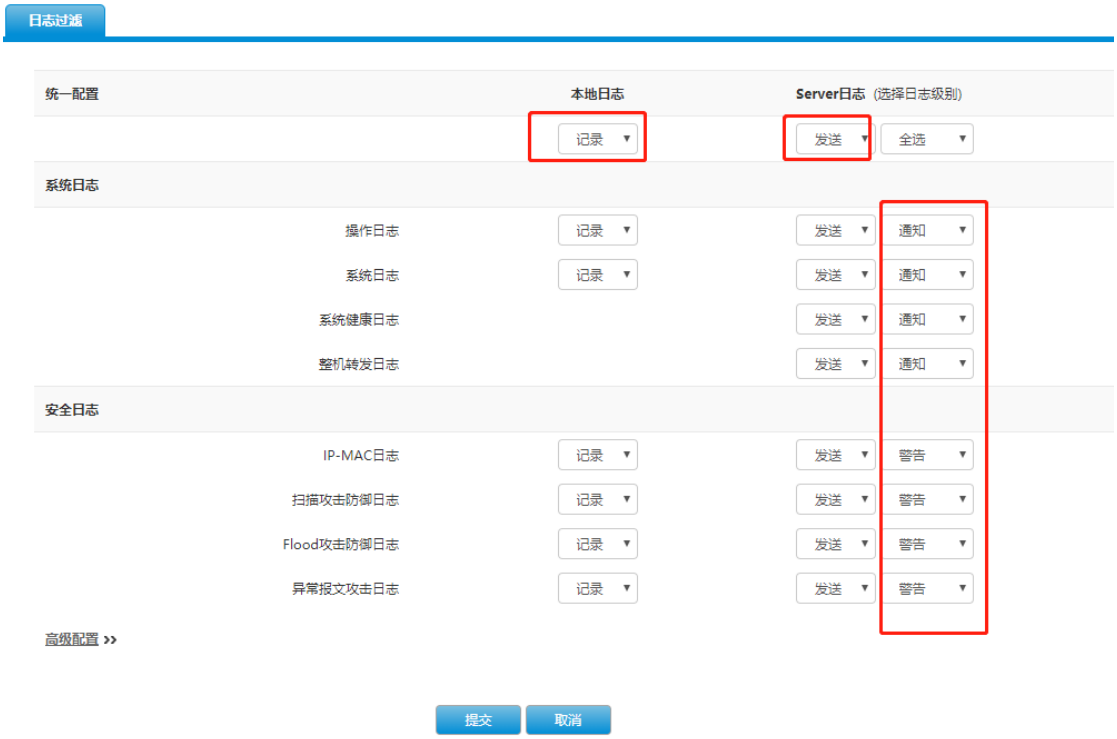
如图 12 所示，进入“策略配置>安全设置>安全防护>异常包攻击防御”，在相应的选项上打钩，并单击<提交>。

图12 开启防异常包攻击

4. 配置日志过滤

如图 13 所示，进入“系统管理>日志设定>日志过滤”，在本地日志处单击“记录”，系统日志级别选择“通知”，安全日志发送级别选择“警告”，单击<提交>。

图13 日志过滤配置



如图 14所示，单击“高级配置”，配置记录和发送上网行为日志，选择级别为“信息”，单击<提交>。

图14 日志过滤高级配置

5. 配置日志服务器

如图 15 所示，进入“系统管理>日志设定>日志服务器”，配置服务器 1 的 IP 地址的为 192.168.1.73，端口保持为默认的 514，并打开启用开关，单击<提交>。

图15 配置日志服务器

4.6.2 配置日志分析与管理平台

如图 16 所示，使用 https 方式登录设备日志分析与管理平台，默认用户名密码为 admin/admin，单击<登录>。

图16 登录日志分析与管理平台

如图 17 所示，进入“设备管控>设备管理>设备管理”，单击<新增>，选择“设备”，在弹出的配置框中，“设备 IP”配置为设备的的 IP 地址 192.168.1.1，“用户名”和“密码”配置为设备的的用户名密码，，单击<确定>。

图17 添加设备的

如图 18 所示，添加成功的设备的配置如下。

图18 添加设备成功

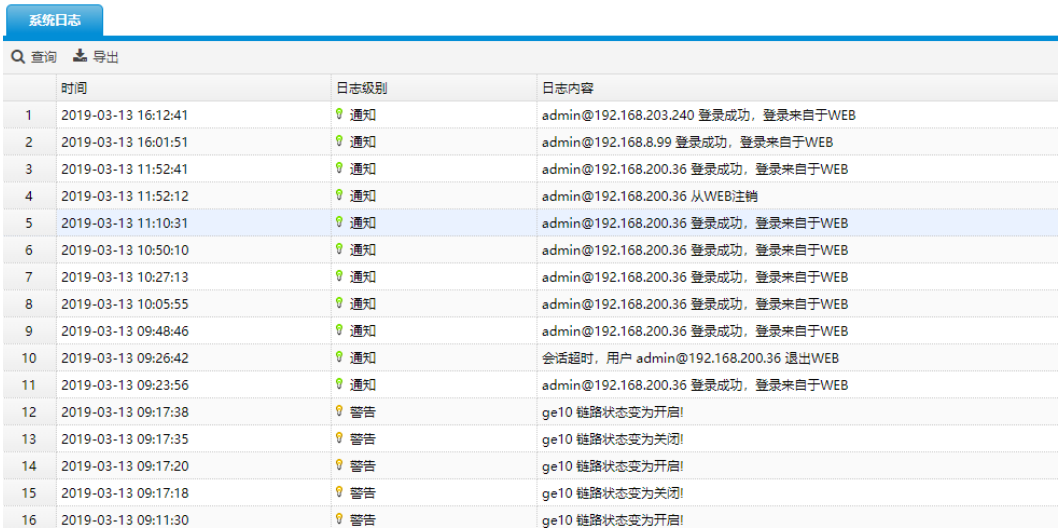
4.7 验证配置

4.7.1 设备端验证

(1) 验证本地日志

如图 19 所示，在设备的本地，进入“数据中心>日志中心>系统日志”，可以看到本地收集系统日志正常。

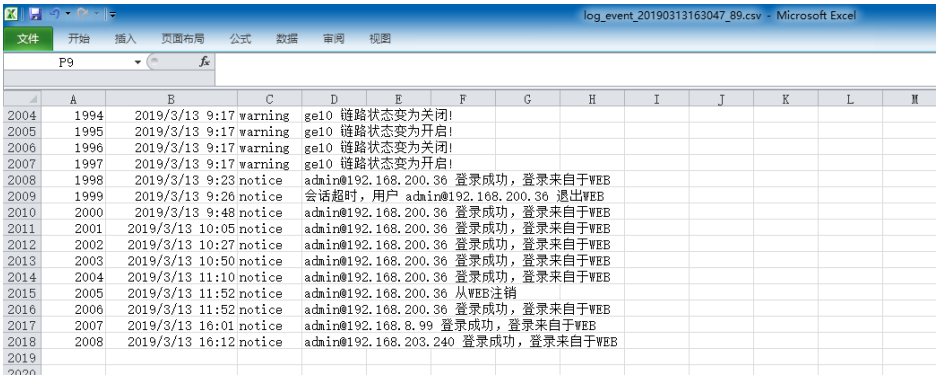
图19 系统日志



	时间	日志级别	日志内容
1	2019-03-13 16:12:41	通知	admin@192.168.203.240 登录成功，登录来自于WEB
2	2019-03-13 16:01:51	通知	admin@192.168.8.99 登录成功，登录来自于WEB
3	2019-03-13 11:52:41	通知	admin@192.168.200.36 登录成功，登录来自于WEB
4	2019-03-13 11:52:12	通知	admin@192.168.200.36 从WEB注销
5	2019-03-13 11:10:31	通知	admin@192.168.200.36 登录成功，登录来自于WEB
6	2019-03-13 10:50:10	通知	admin@192.168.200.36 登录成功，登录来自于WEB
7	2019-03-13 10:27:13	通知	admin@192.168.200.36 登录成功，登录来自于WEB
8	2019-03-13 10:05:55	通知	admin@192.168.200.36 登录成功，登录来自于WEB
9	2019-03-13 09:48:46	通知	admin@192.168.200.36 登录成功，登录来自于WEB
10	2019-03-13 09:26:42	通知	会话超时，用户 admin@192.168.200.36 退出WEB
11	2019-03-13 09:23:56	通知	admin@192.168.200.36 登录成功，登录来自于WEB
12	2019-03-13 09:17:38	警告	ge10 链路状态变为开启!
13	2019-03-13 09:17:35	警告	ge10 链路状态变为关闭!
14	2019-03-13 09:17:20	警告	ge10 链路状态变为开启!
15	2019-03-13 09:17:18	警告	ge10 链路状态变为关闭!
16	2019-03-13 09:11:30	警告	ge10 链路状态变为开启!

单击<导出>，可以导出 CSV 格式的日志，打开后可以看到和实际的日志一致。

图20 导出的日志



	A	B	C	D	E	F	G	H	I	J	K	L	M
2004	1994	2019/3/13 9:17	warning	ge10 链路状态变为关闭!									
2005	1995	2019/3/13 9:17	warning	ge10 链路状态变为开启!									
2006	1996	2019/3/13 9:17	warning	ge10 链路状态变为关闭!									
2007	1997	2019/3/13 9:17	warning	ge10 链路状态变为开启!									
2008	1998	2019/3/13 9:23	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2009	1999	2019/3/13 9:26	notice	会话超时，用户 admin@192.168.200.36 退出WEB									
2010	2000	2019/3/13 9:48	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2011	2001	2019/3/13 10:05	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2012	2002	2019/3/13 10:27	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2013	2003	2019/3/13 10:50	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2014	2004	2019/3/13 11:10	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2015	2005	2019/3/13 11:52	notice	admin@192.168.200.36 从WEB注销									
2016	2006	2019/3/13 11:52	notice	admin@192.168.200.36 登录成功，登录来自于WEB									
2017	2007	2019/3/13 16:01	notice	admin@192.168.8.99 登录成功，登录来自于WEB									
2018	2008	2019/3/13 16:12	notice	admin@192.168.203.240 登录成功，登录来自于WEB									
2019													

如图 21 所示，在设备的本地，进入“数据中心>日志中心>审计日志>IM 聊天软件日志”，可以看到本地收集 IM 聊天软件日志正常。

图21 设备的本地记录 IM 聊天软件日志

单击<导出>，在弹出的过滤框中选择需要导出的日志的时间范围，单击<导出>，即可将对应时间段的日志压缩包下载到本地。解压缩后，可以看到带有日期信息的 CSV 文件。

图22 导出过滤

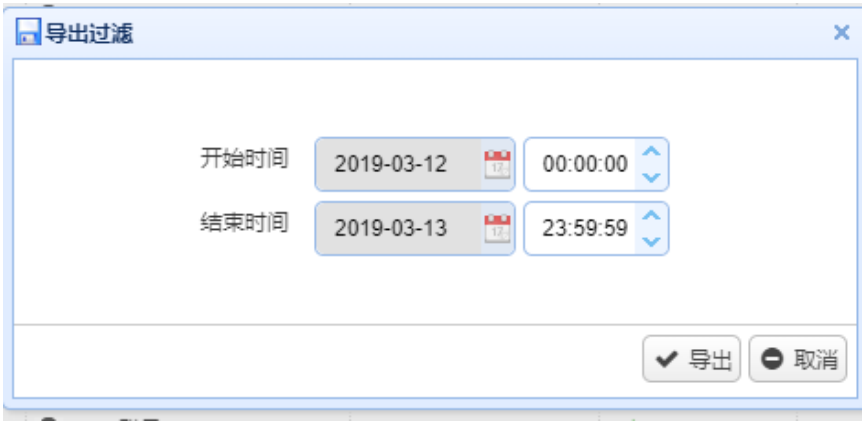
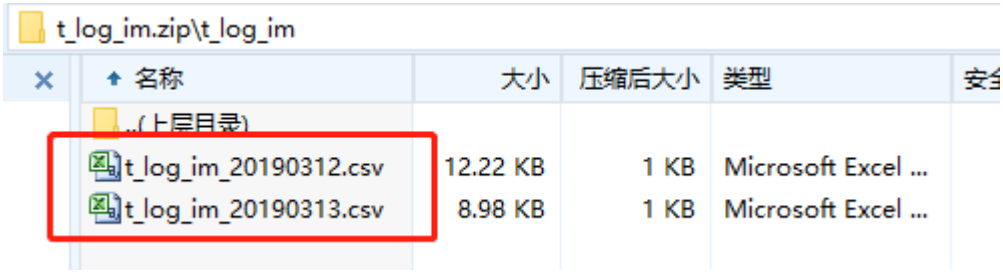
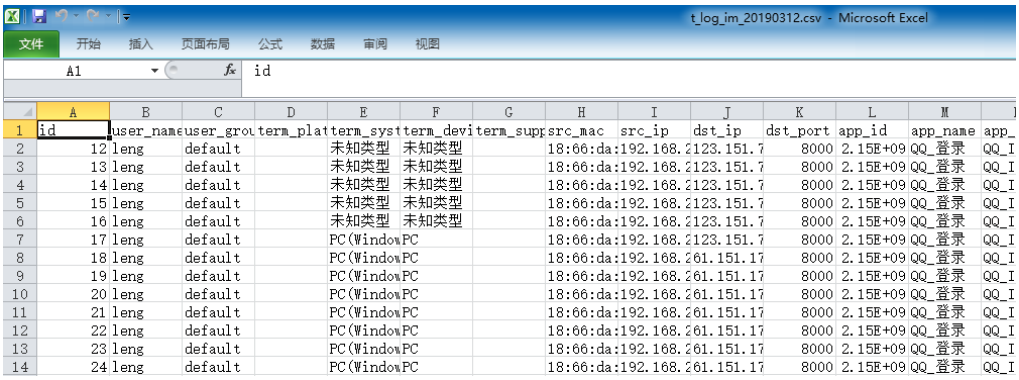


图23 审计日志导出的文件



CSV 文件中的日志内容与实际日志内容一致。

图24 审计日志导出内容



t_log_im_20190312.csv - Microsoft Excel

文件 开始 插入 页面布局 公式 数据 审阅 视图

A1 id

	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	id	user_name	user_grou	term_plat	term_syst	term_devi	term_supp	src_mac	src_ip	dst_ip	dst_port	app_id	app_name	app_
2	12	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
3	13	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
4	14	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
5	15	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
6	16	leng	default		未知类型	未知类型		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
7	17	leng	default		PC(Window	PC		18:66:da:	192.168.2	123.151.7	8000	2.15E+09	QQ_登录	QQ_I
8	18	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
9	19	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
10	20	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
11	21	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
12	22	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
13	23	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I
14	24	leng	default		PC(Window	PC		18:66:da:	192.168.2	61.151.17	8000	2.15E+09	QQ_登录	QQ_I

如图 25 所示，，在设备的本地，进入“数据中心>日志中心>审计日志>访问网站日志”，可以看到本地收集网站访问日志正常。和 IM 聊天软件日志一样，该日志也支持选择时间范围进行导出，不再赘述。

图25 设备的本地记录网站访问日志

访问网站日志

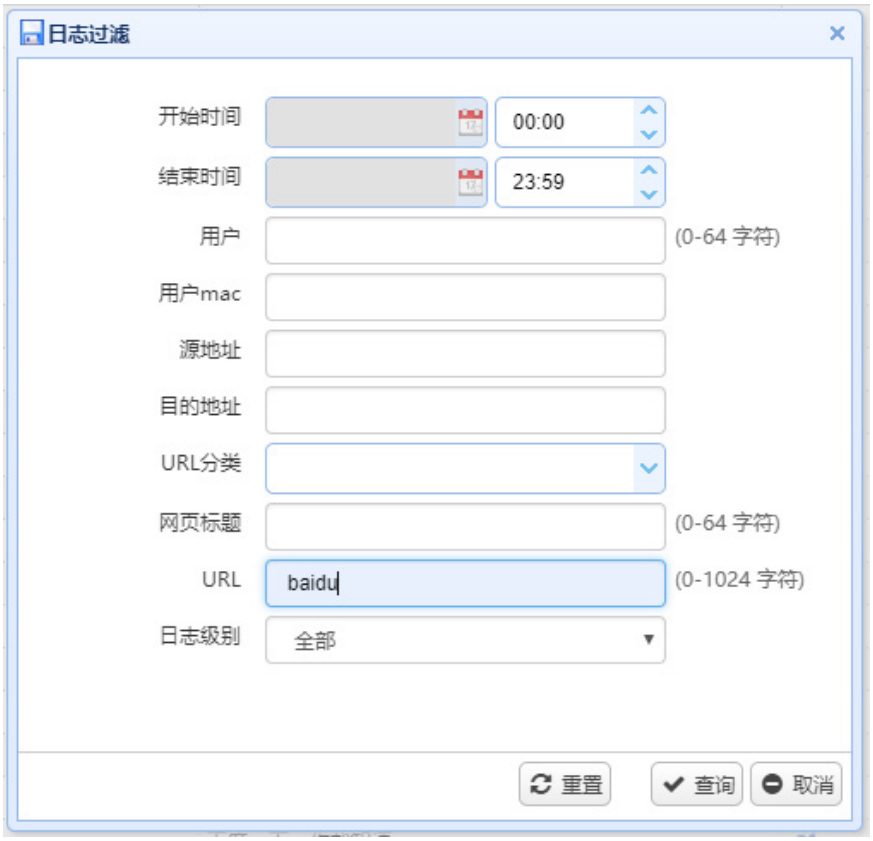
查询 重置 导出 **查询结果:** 在 2019-03-13 约 814 条日志记录中，从 1 - 814 搜索出相关结果 814 条

	用户	用户mac	URL分类	网页标题	URL	级别	时间	操作
1	leng	18:66:da:e5:81:cb	IP站点	入侵检测与防御系统		信息	2019-03-13 17:09:18	详细
2	leng	18:66:da:e5:81:cb	IP站点	入侵检测与防御系统		信息	2019-03-13 17:09:17	详细
3	leng	18:66:da:e5:81:cb	IP站点	入侵检测与防御系统		信息	2019-03-13 17:08:26	详细
4	leng	18:66:da:e5:81:cb	IP站点	入侵检测与防御系统		信息	2019-03-13 17:08:25	详细
5	leng	18:66:da:e5:81:cb	IP站点	入侵检测与防御系统		信息	2019-03-13 17:08:04	详细
6	leng	18:66:da:e5:81:cb	网络资源	百度一下，你就知道		信息	2019-03-13 17:06:53	详细
7	leng	18:66:da:e5:81:cb	网络资源	百度一下，你就知道		信息	2019-03-13 17:06:24	详细
8	leng	18:66:da:e5:81:cb	网络资源	百度一下，你就知道		信息	2019-03-13 17:05:47	详细

(2) 验证本地日志查询

如图 26 所示，在上述访问网站日志页面单击查询，可根据多种条件进行过滤查询，将“URL”配置为 baidu，单击<查询>。

图26 访问网站日志查询



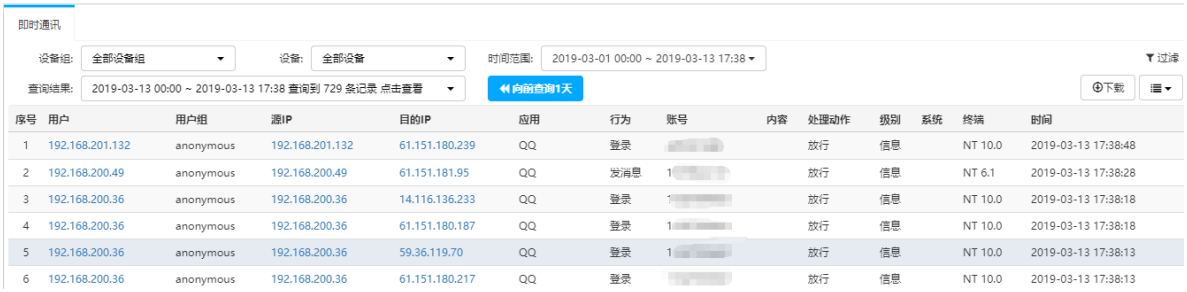
如图 27 所示，可以看到日志正确返回 URL 均中含有 baidu 的日志。

图27 查询到 URL 中含有 baidu 的日志

4.7.2 日志分析与管理平台端验证

如图 28 所示，在日志分析与管理平台，进入“日志审计>内容审计日志>即时通讯”，在日志过滤页面过滤对应的设备，即可以看到日志分析与管理平台正确收集到了聊天日志。

图28 日志分析与管理平台聊天日志



4.8 配置文件

```
!
policy any any any any any any any always any permit 1
  app-policy control 1 action permit log-level info
  app-policy control 1 application any
  app-policy control 1 enable
  website-policy malware enable
  website-policy 1 any accept info FilterUrl
   website-policy enable 1
policy default-action permit
policy white-list enable
!
!policy-decrypt
!
policy listen block disable
!
audit_policy any any any any any always all any 1
     log level info
audit associate enable
!
anti-arp spoof enable
anti-arp broadcast enable
anti-arp flood enable
!
!
anony_user log disable
ap ipmac enable
ip defend attack ping-of-death
ip defend attack tear-drop
ip defend attack jolt2
ip defend attack land-base
ip defend attack winnuke
```

```
ip defend attack tcp-flag
ip defend attack smurf
ip defend attack ip-option
ip defend attack ip-spoof
!
ip defend synflood interface bvi0 destination 1500
ip defend udpflood interface bvi0 destination 1500
ip defend icmpflood interface bvi0 destination 1500
ip defend dnsflood interface bvi0 destination 1500
ip defend synflood interface bvi0 source 1500
ip defend udpflood interface bvi0 source 1500
ip defend icmpflood interface bvi0 source 1500
ip defend dnsflood interface bvi0 source 1500
!
!flow-account
!
log command_log server disable
log server addr 192.168.203.240
log server second addr 192.168.200.36
log server enable
!
```

目录

1 简介

本文档介绍设备的用户认证配置举例，包括本地用户 Web 认证、Radius 联动 Web 认证和 LDAP 联动 Web 认证。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户认证特性。

3 使用限制

设备的 E6442 版本仅支持与 AD 域服务器联动认证，与 openldap 服务器联动仅支持用户同步不支持认证，在配置使用时请使用 AD 域服务器联动认证。

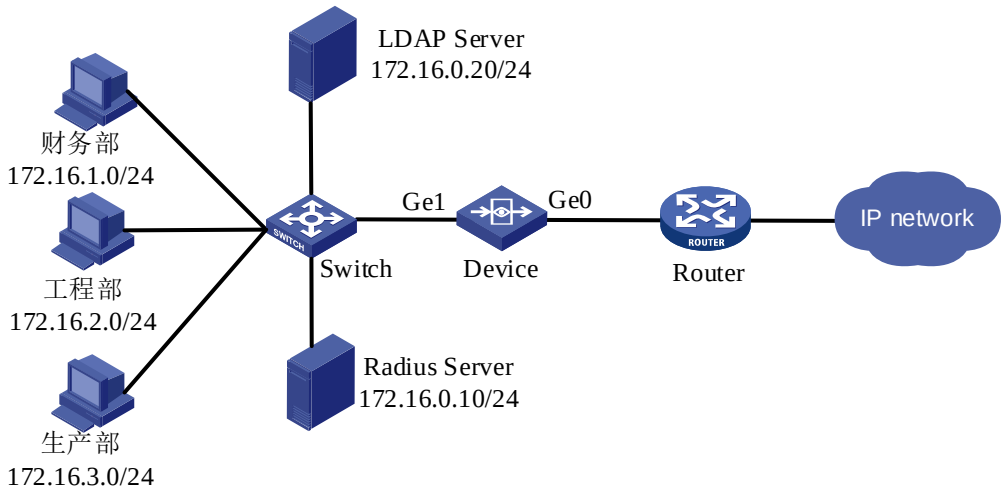
4 配置举例

4.1 组网需求

如图 1 所示，某公司的财务部、工程部和生产部实行用户认证上网，其网段分别是 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24。内网 Radius 服务器的地址为 172.16.0.10/24、LDAP 服务器的地址为 172.16.0.20/24。使用设备的的 ge0 和 ge1 接口透明模式部署在网络中，在设备上配置用户认证功能。具体要求如下：

- 财务部进行 Web 认证上网，用户名和密码存储在设备的本地。
- 工程部进行 Web 认证上网，用户名和密码存储在 Radius 服务器上。
- 生产部进行 Web 认证上网，用户名和密码存储在 LDAP 服务器上。
- 财务部、工程部和生产部的每个 Web 认证用户需要支持两个终端同时并发登录，要求用户成功登录后跳转到 http://www.baidu.com。

图1 用户认证功能配置组网图



4.2 配置思路

- 配置 Radius 和 LDAP 服务器对象，设备上的相关参数配置需要和服务器保持一致。
- 配置地址对象。
- 配置本地认证用户，RADIUS 和 LDAP 认证用户直接在相应的服务器创建即可。
- 配置用户认证策略。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- 设备的配置 Web 认证时，允许用户的 TCP 三次握手报文、DNS 报文以及 ICMP 报文通过，当检测到用户 HTTP 报文时拦截并弹出认证页面。所以，在使用 Web 认证功能时，需要保证终端可以进行正常的 HTTP 访问。
- 如果需要实现访问某些资源时免 Web 认证，请在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的目的 IP 地址排除即可。

4.5 配置步骤

4.5.1 配置设备

1. 添加服务器

(1) 配置工程部 Radius 服务器

如图 2 所示，进入“用户管理>认证管理>认证服务器”，点击<新建>，选择 Radius 服务器，配置“服务器地址”为 172.16.0.10，“服务器密码”和“端口”需要和 Radius 服务器保持一致，点击<提交>。

图2 添加工程部 radius 服务器

(2) 配置生产部 LDAP 服务器

如图 3 所示，进入“用户管理>认证管理>认证服务器>”，点击<新建>选择 LDAP 服务器，配置“服务器地址”为 172.16.0.20，“端口”和“通用名标识”和“Base DN”需要和 LDAP 服务器保持一致，点击<提交>。

图3 添加生产部 LDAP 服务器

2. 配置 Web 认证用户

(1) 配置市场部本地认证用户

如图 4 所示，进入“用户管理>用户组织结构”，点击“新建>用户”，配置用户名称为“user1”，配置和确认密码后，点击<提交>。

图4 配置市场部本地认证用户

(2) 配置工程部 Radius 认证用户

设备本地不需要创建 Radius 认证用户，直接在 Radius 服务器上创建即可。

(3) 配置生产部 LDAP 认证用户

设备本地不需要创建 LDAP 认证用户，直接在 LDAP 服务器上创建即可。

如图 5 所示，添加完成的认证用户对象配置如下。

图5 Web 认证用户对象配置完成

3. 配置用户认证地址对象

(1) 配置财务部地址对象

如图 6 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，命名为“财务部地址对象”，“地址项目”选为子网地址，配置地址为 172.16.1.0/24，点击<提交>。

图6 配置财务部地址对象

(2) 配置工程部地址对象

如图 7 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，命名为“工程部地址对象”，“地址项目”选为子网地址，配置地址为 172.16.2.0/24，点击<提交>。

图7 配置工程部地址对象

(3) 配置生产部地址对象

如图 8 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，命名为“生产部地址对象”，“地址项目”选为子网地址，配置地址为 172.16.3.0/24，点击<提交>。

图8 配置生产部地址对象

如图 9 所示，创建完成的地址对象配置如下。

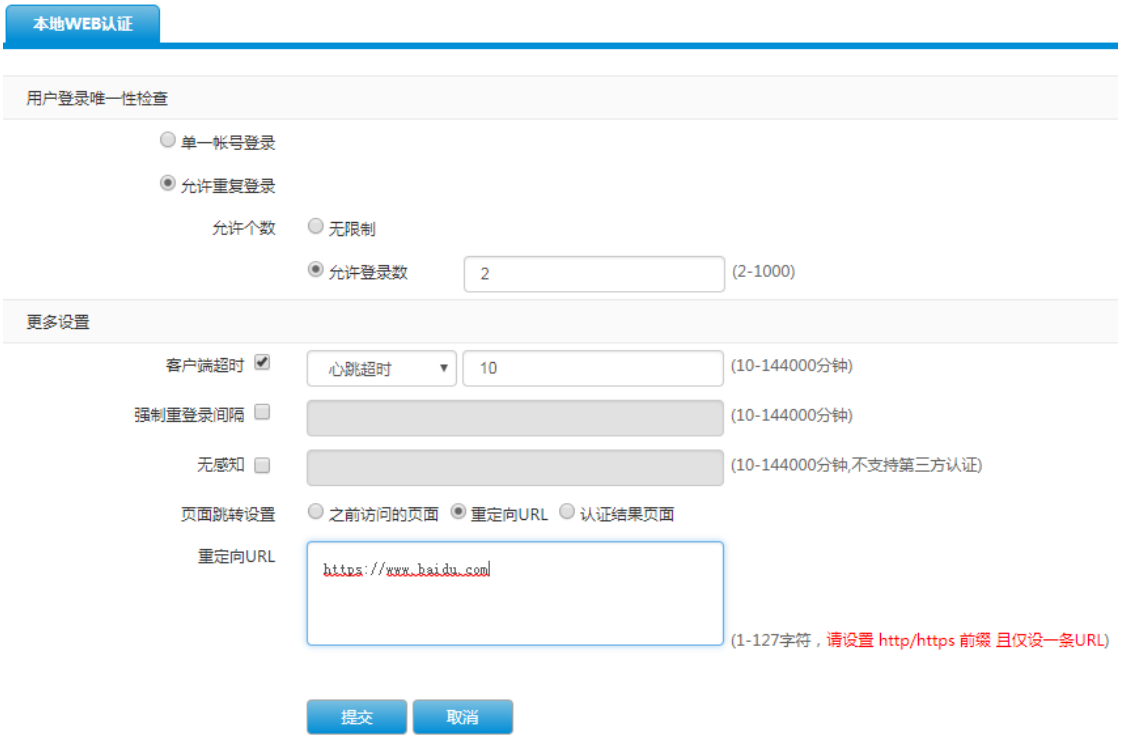
图9 用户认证地址对象配置完成

	名称	内容(网络，范围，主机)	排除地址	描述	引用	操作
1	any	0.0.0.0/0		任何地址	14	
2	private	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,		私有地址	0	
3	ChinaUnicom	1.24.0.0/13,1.56.0.0/13,1.188.0.0/14,...		中国联通	0	
4	ChinaTelecom	1.0.1.0/24,1.0.2.0/23,1.0.8.0/21,...		中国电信	0	
5	ChinaEducation	1.51.0.0/16,1.184.0.0/15,42.244.0.0/14,...		教育网	0	
6	ChinaMobile	61.232.0.0/14,61.236.0.0/15,110.96.0.0/11,...		中国移动	0	
7	财务部地址对象	172.16.1.0/24			0	
8	工程部地址对象	172.16.2.0/24			0	
9	生产部地址对象	172.16.3.0/24			0	

4. 配置 Web 认证参数

如图 10 所示，进入“用户管理>认证管理>认证方式>本地 Web 认证”，勾选“允许重复登录”，配置“允许登录数”为 2，配置重定向 URL 为 https://www.baidu.com，点击<提交>。

图10 配置 Web 认证



5. 配置 IPv4 控制策略

如图 11 所示，进入“策略配置>IPv4 控制策略”，将默认规则修改为允许。

图11 配置 IPv4 控制策略

6. 配置用户认证策略

(1)　配置财务部用户认证策略

如图 12 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“财务部地址对象”，认证方式选择“Web 认证”，其它选项保持默认，点击<提交>。

图12 配置财务部用户认证策略

(2)　配置工程部用户策略

如图 13 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“工程部地址对象”，认证方式选择“Web 认证”，其它选项保持默认，点击<提交>。

图13 配置工程部用户认证策略

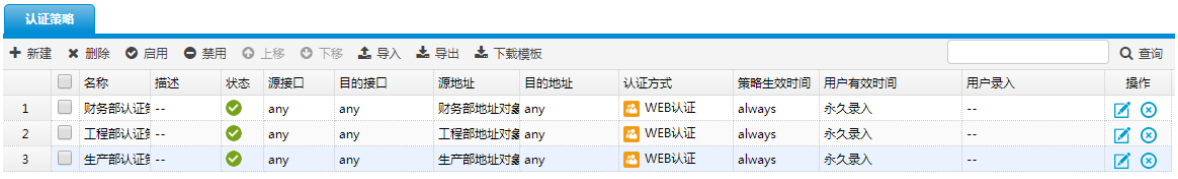
(3) 配置生产部用户认证策略

如图 14 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“生产部地址对象”，认证方式选择“Web 认证”，其它选项保持默认，点击<提交>。

图14 配置生产部用户认证策略

如图 15 所示，添加完成的用户策略配置如下。

图15 用户策略配置完成



7. 启用第三方认证

如图 16、图 17 所示，进入“用户管理>认证管理>高级选项>全局配置”，当与 Radius 服务器认证对接时，启用 Radius 方式，当与 LDAP 服务器认证对接时，启用 LDAP 服务器。

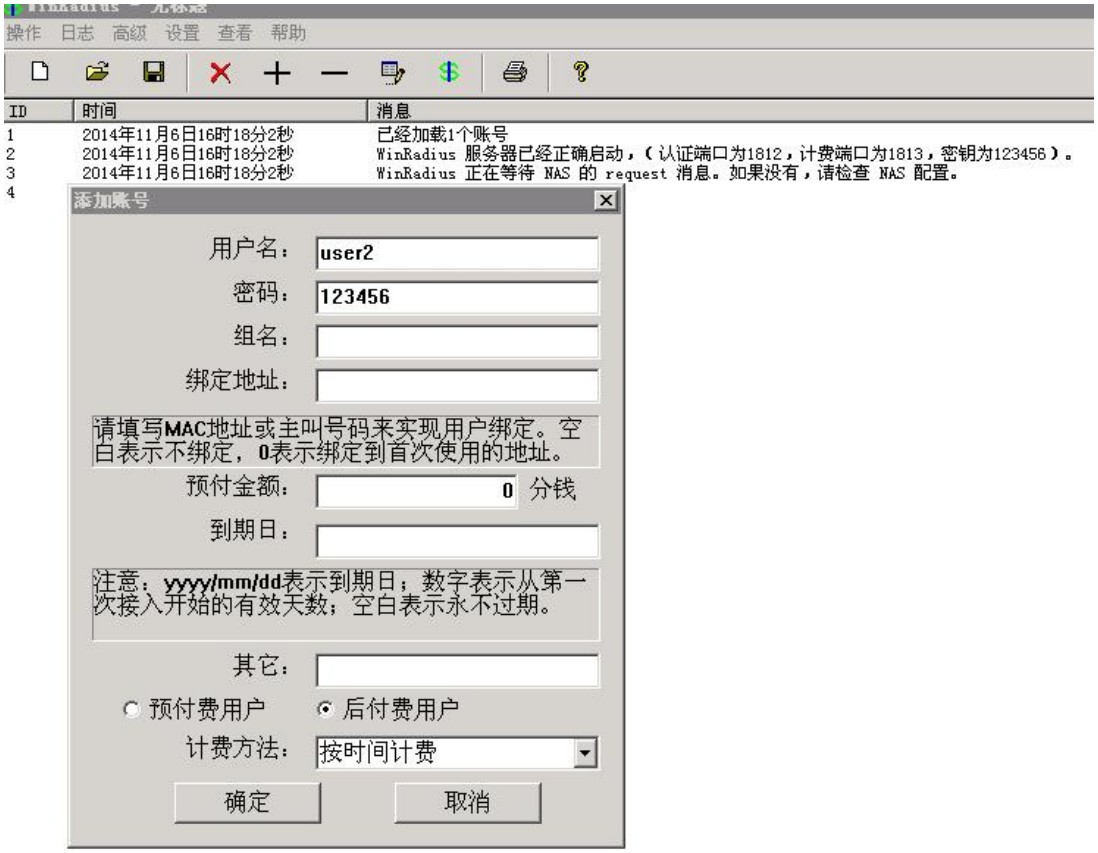
图16 启用第三方认证 Radius

图17 启用第三方认证 LDAP

8. 配置 Radius 服务器

如图 18 所示，以 WinRadius 为例搭建 Radius 服务器，点击<操作>，配置用户名为 user2，密码为 123456，点击<确定>。

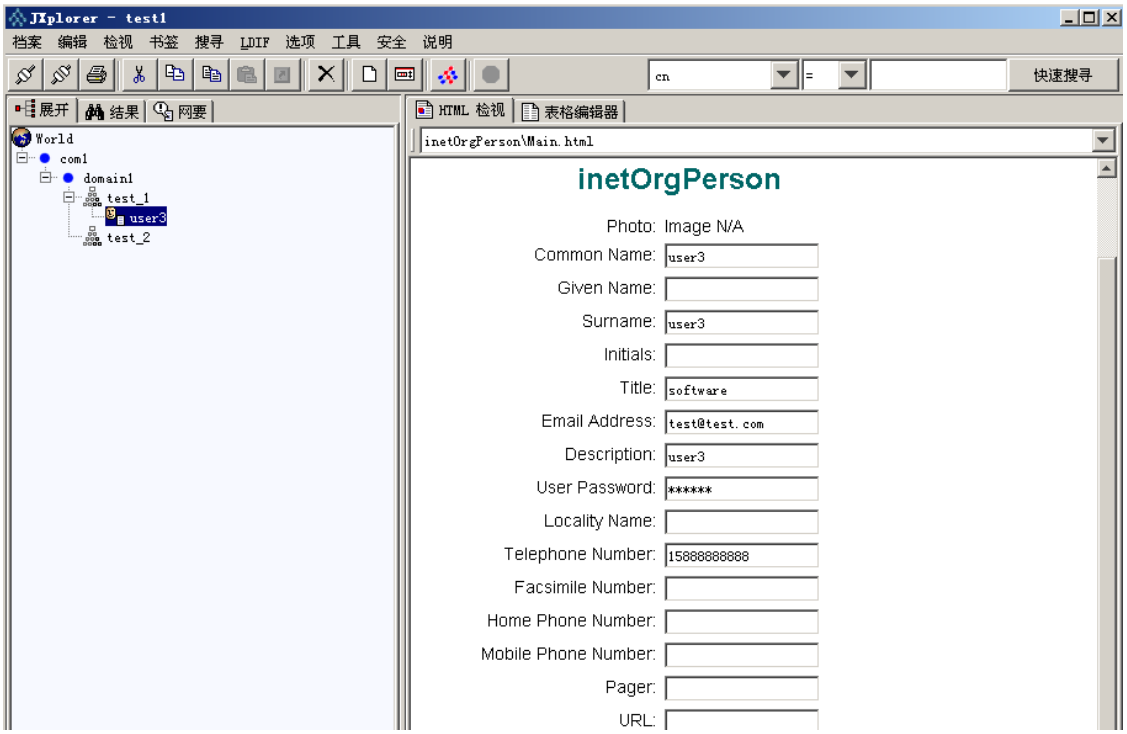
图18 配置 Radius 服务器



9. 配置 LDAP 服务器

如图 19 所示，在 LDAP 服务器上配置 Common Name 和 Sumname 为 user3，User Password 为 123456。

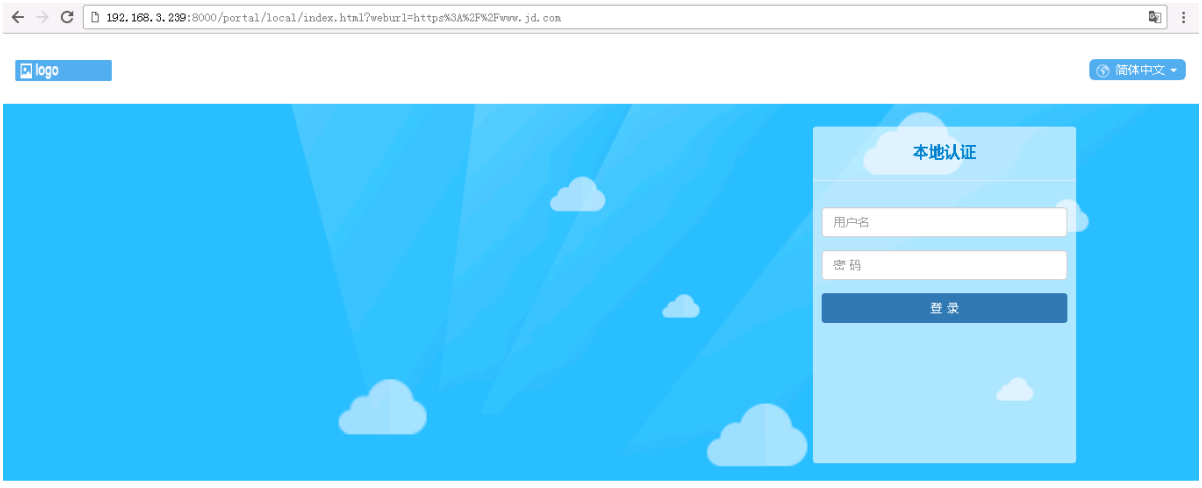
图19 配置 LDAP 服务器



4.6 验证配置

如图 20 所示，在每个网段使用终端进行 HTTP 访问，弹出如下本地 Web 认证页面，填写用户名和密码进行认证。

图20 本地 Web 认证页面



如图 21 所示，财务部（172.16.1.0/24）本地用户 user1 测试认证成功。

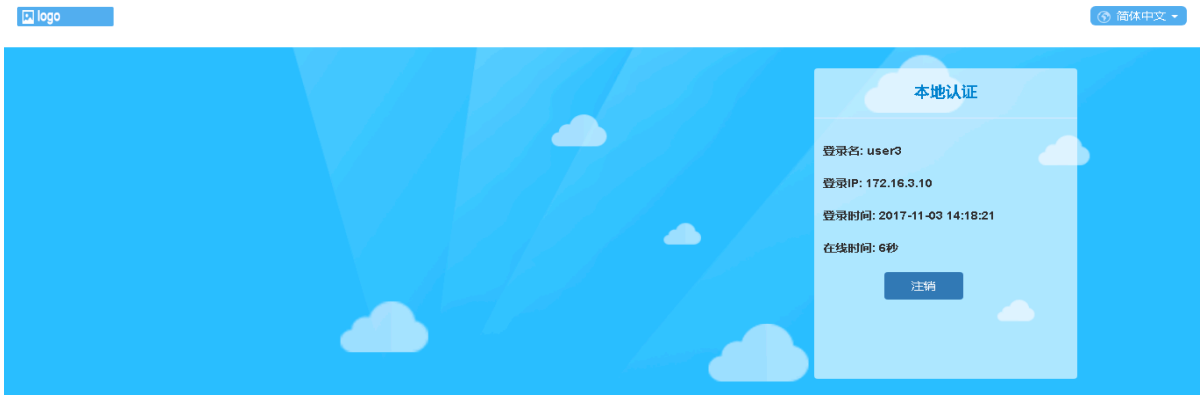
图21 财务部本地 Web 认证成功

如图 22 所示，工程部（172.16.2.0/24）Radius 联动用户 user2 测试认证成功。

图22 Radius 联动用户 Web 认证成功

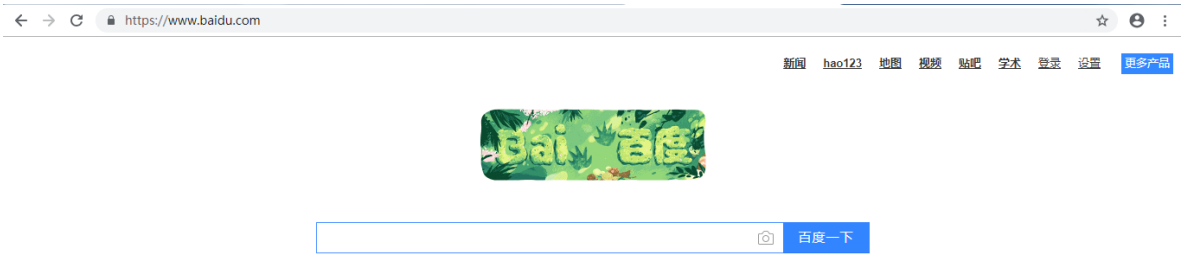
如图 23 所示，生产部（172.16.3.0/24）LDAP 联动用户 user3 测试认证成功。

图23 LDAP 联动用户 Web 认证成功



如图 24 所示，用户 Web 认证通过后跳转到配置的 https://www.baidu.com。

图24 Web 认证通过后重定向到 www.baidu.com



4.7 配置文件

```
!
admin auth certificate
radius-server Radius 172.16.0.10 secret
kTgxl5p34DqlzzT+XZ0R14cv6Qal7urj9YogDjQGHYyVxSLYIpmOxTPwro4b0aN 1812
ldap LDAP
 ldap 172.16.0.20 389
 cnid cn
 dn ou=test_1,dc=domain,dc=com1
 bindtype simple user cn=administrator,cn=users,dc=domain,dc=com1 secret
BgJYypIYXs1/LNbP9R5HFuFBPq2wzxUUDLphPZPbxeceoRv3HJMyd9xT0dkiOvR
!
address 财务部地址对象
 ip subnet 172.16.1.0/24
!
address 工程部地址对象
 ip subnet 172.16.2.0/24
!
address 生产部地址对象
 ip subnet 172.16.3.0/24
!
user user1
 bind-group organization
 authenticate local kTgxl5p34DqlzzT+XZ0R14cv6Qal7urj9YogDjQGHYyVxSLYIpmOxTPwro4b0aN
change-password enable first-log-change-pwd disable
!
user-policy listen authentication disable
user-policy https-portal enable
user-policy any any 财务部地址对象 any always local-webauth enable 财务部认证策略 no-record
forever
user-policy any any 工程部地址对象 any always local-webauth enable 工程部认证策略 no-record
forever
user-policy any any 生产部地址对象 any always local-webauth enable 生产部认证策略 no-record
forever
!
```

```
policy default-action permit
policy white-list enable
!
user-webauth login-multi number 2
user-webauth hello-url https://www.baidu.com
!user-portal-server
```

目录

1 简介

本文档介绍设备的用户认证策略配置举例，认证策略页面实现对策略的新增、删除、导入、导出等操作，对于非本地/域用户支持认证后加入指定用户组功能，仅支持组织结构，暂不支持属性组。

用户有效时间指的是第三方用户录入方式：

- 永久录入：第三方用户认证成功后录入指定组，永久有效。
- 有效期至：第三方用户认证成功后录入指定组，设备运行时间到配置的时间当天 23:59 后，录入的用户状态变为不启用，认证策略也变为不启用。
- 临时录入：第三方用户认证成功后录入指定组，用户注销下线后，录入的用户组里用户自动删除。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户认证特性。

3 使用限制

- 设备 E6442 版本仅支持简单模式的 LDAP 联动认证，不支持匿名和通用模式的 LDAP 联动认证，在配置时请使用简单模式的 LDAP 联动认证。
- 认证策略录入配置主要针对第三方用户，目的是将存在于第三方的用户加入设备，便于做策略限制等。此功能不影响本地已有用户，只会新增用户，不会修改已有用户信息。
- 认证策略用户录入未配置用户组时不会录入用户。
- 第三方录入用户，如果用户未下线，该用户无法编辑，在线用户注销后，用户可以编辑。
- 认证策略有效期录入用户，当认证策略里用户有效期过期后用户状态变为未启用状态，如果重新启用用户的话需要更换用户有效期为有效时间。

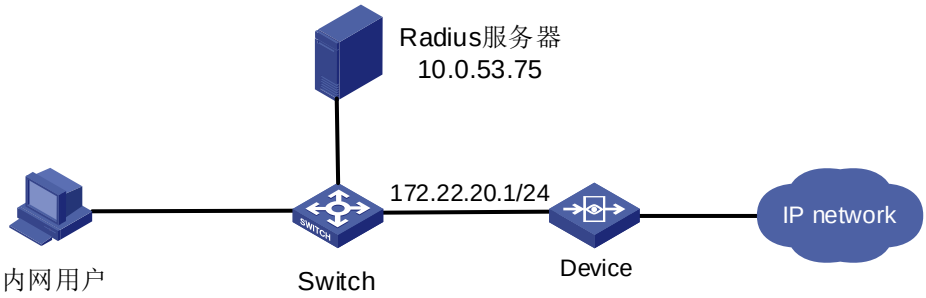
4 配置举例

4.1 组网需求

如图 1 所示，某公司内网搭建有第三方 Radius 服务器，用户名全部存放在 radius 服务器上，要求内网用户使用 radius 服务器上的用户进行认证，认证成功后用户录入设备做其它策略控制。具体要求如下：

- 内网用户进行 Web 认证上网，用户名和密码存储在 Radius 服务器上，认证成功后用户永久录入设备。

图1 用户认证功能配置组网图



4.2 配置思路

- 配置 Radius 服务器对象，设备上的相关参数配置需要和服务器保持一致。
- 配置地址对象；
- 创建用户组，作为用户认证后的录入组；
- 配置 IPv4 控制策略允许上网；
- 全局配置启用第三方认证选择 radius 服务器；
- 配置用户策略触发认证。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- 设备的配置 Web 认证时，允许用户的 TCP 三次握手报文通过，当检测到用户 HTTP 报文时拦截并弹出认证页面。所以，在使用 Web 认证功能时，需要保证终端可以进行正常的 HTTP 访问。
- 如果需要实现访问某些资源时免 Web 认证，请在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的 IP 地址排除。目前仅支持排除 IP 地址，不支持排除域名。

4.5 配置步骤

4.5.1 配置设备

1. 添加服务器

通过菜单“用户管理>认证管理>认证服务器>Radius”，点击<新建>，配置“服务器地址”为 10.0.53.85，“服务器密码”和“端口”需要和 Radius 服务器保持一致，点击<提交>。进入如图 2 所示的页面。

图2 添加 radius 服务器

2. 配置地址对象

通过菜单“策略配置>对象管理 > 地址对象”，点击<新建>地址对象，配置内网用户和无线 wifi 地址对象。如图 3 所示。

图3 添加内网用户地址对象

3. 配置用户组对象

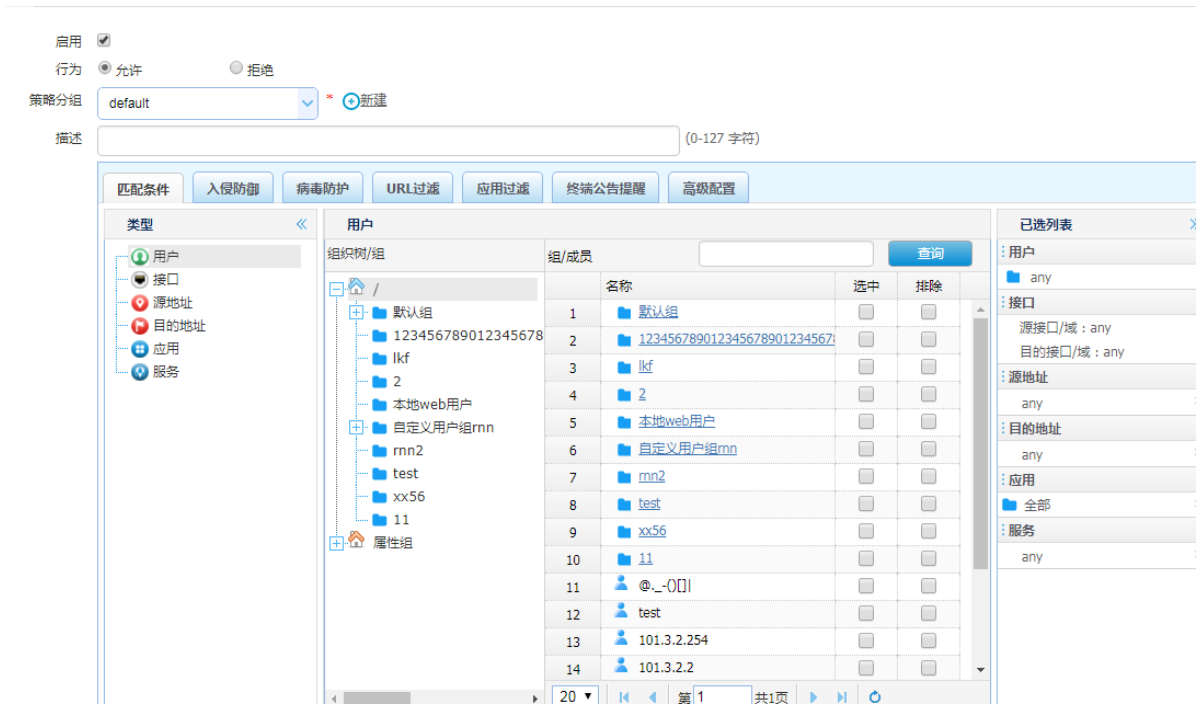
通过菜单“用户管理>用户组织结构”，单击<新建>用户组，配置 radius 用户组和无线 wifi 用户组，如图 4 示。

图4 配置 Radius 用户组

4. 配置 IPv4 控制策略

通过菜单“策略配置>IPv4 控制策略”，点击<新建>IPv4 控制策略，进入如图 5 所示的页面。

图5 IPV4 控制策略配置



5. 全局配置启用第三方认证选择 radius 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 radius 服务器，如图 6 所示。

图6 全局模式启用第三方 radius 配置效果图

6. 配置用户策略

(1) 配置内网用户认证策略，用户永久录入。

通过菜单进入“用户管理>认证管理>认证策略”，点击<新建>，源地址配置为“内网用户地址对象”，相关行为配置为“本地 Web 认证”，用户录入选择创建的“Radius-group”，有效期为永久录入，点击<提交>。如图 7 所示。

图7 配置内网用户认证用户策略

4.6 验证配置

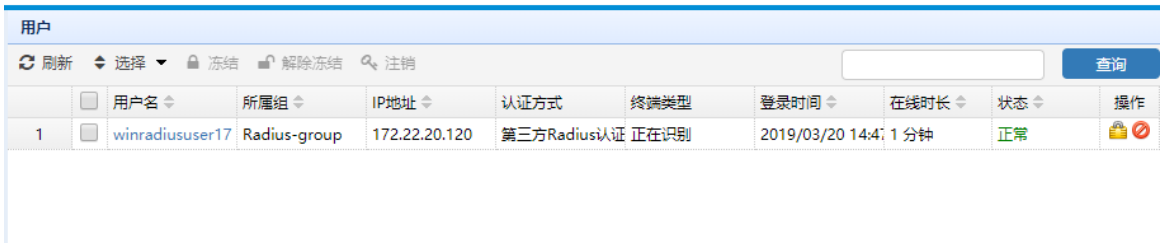
4.6.1 内网用户使用 radius 用户认证

如图 8 所示，内网终端进行 HTTP 访问，弹出如下本地 Web 认证页面，使用 radius 服务器上用户名、密码进行认证。

图8 内网用户使用第三方 radius 用户认证成功

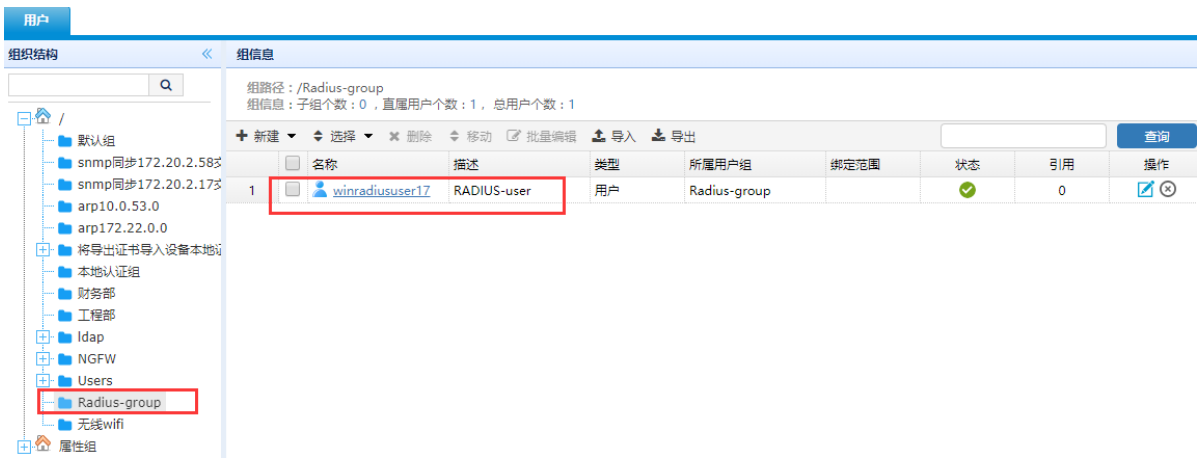
如图 9 所示，设备在线用户显示第三方 radius 用户认证。

图9 Radius 联动用户 Web 认证成功



通过菜单“用户管理>用户组织结构”，查看 Radius-group 用户组下，winradiusuer17 用户已录入，如图 10 所示。

图10 Radius 用户组下录入用户



如图 11 所示，编辑用户查看用户永不过期。

图11 radius 录入用户显示为永不过期

目 录

1 简介

本文档介绍设备用户同步配置举例，用户同步包含 LDAP 同步、ARP 扫描、SNMP 同步。同步成功录入设备的用户支持策略调用、QOS 控制、策略路由等模块的引用控制。本文档主要针对用户同步中的 LDAP 同步和 SNMP 同步进行典型配置举例介绍。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解用户同步特性。

针对 SNMP 同步在配置前，需要做如下准备：

- 交换机上已开启 SNMP 代理功能。
- 设备的与交换机网络可达。

3 使用限制

- LDAP 同步条目 128。
- SNMP 同步条目 64。
- Arp 扫描条目 64。
- LDAP 仅支持简单模式的联动认证，不支持匿名和通用模式的联动认证。
- LDAP 服务器用户名长度大于 63 字符后无法录入。
- LDAP 服务器同步目前支持 389 明文传输，不支持 636 密文传输（不能与加密服务器交互，无法进行身份验证）。
- 只支持 Windows AD 域用户同步，不支持匿名同步用户。只支持 OpenLdap 服务器用户同步，不支持 OpenLdap 认证（OpenLdap 同步的用户没有 dn 属性无法参与认证）。
- AD 服务器上用户名超长(大于 63 字符)，含有异常字符（汉字数字字母以及@._-()[]|以外的特殊字符）可以同步，不能录入到本地用户结构，同步过程中会依次在本地用户结构添加用户、用户组，本地满规格时无法录入，同步规格和本地用户规格相同。
- LDAP BaseDN 如果写根 OU 的话，同步 LDAP 服务器的时候会把根 OU 下的所有子 OU 以及用户全部同步下来。
- IPSec 和 sslvpn 使用 LDAP 认证时，需保证本地存在该用户。
- 多个用户同步条目存在时，同步任务为串行，上面同步条目同步完成后在进行下面同步条目的同步。
- LDAP 同步周期起始时间（0-23），间隔时间（1-24），例如起始时间 8，间隔 2，代表该同步条目每天 8 点开始同步，每隔 2 小时同步一次，晚上 12 点结束当天的同步任务。
- AD 域用户更新密码后，使用同步的 LDAP 认证时，新旧密码都可以认证。在 server 2008 级别的 AD 下，旧密码生存期为 5 分钟，在 server 2003 级别的 AD 下，旧密码生存期为 60 分钟。

这个 5 分钟就是为了防止 AD 同步延时问题，防止 DC 数量比较多时，用户登录所在的站点内还没有成功的更新到密码的修改的情况。这样，即使新密码没有生效，旧密码依然可用。

测试 2003 的服务器，旧密码有效期为 60 分钟，自测 60 分钟后密码失效，此为 AD 域服务器的保护机制，不修改。

- 手动创建用户组、用户创建为本地用户，和 LDAP 服务器上组、用户名称一样，点 LDAP 同步，这个用户没法用 LDAP 认证，LDAP 同步当存在重名用户时，只移动用户，不覆盖。
- LDAP 组里第一个 LDAP 服务器密码不对，用户在第二个服务器，此时用户认证浏览器无响应，目前不能处理跨域的 LDAP 组认证，需要保障 LDAP 组下地址可达，服务器密码正确。
- arp 扫描只支持扫描设备同网段用户。
- 新建 SNMP 同步条目的 MAC 地址是与设备相连的交换机的地址。
- 设备的配置的团体名需要跟交换机上的团体名一致，团体字中不能包含中文。
- 开启 SNMP 同步及 IP-MAC 绑定后，交换机下的新用户 IP-MAC 如果不能及时学习到，数据直接放通，在线用户列表中的 MAC 会显示成三层交换机的 MAC。
- 在配置多个交换机时扫描开始后串行逐个扫描，待所有交换机扫描完毕后等待配置的更新时间后再开始下一轮扫描。
- 对于每次扫描结果如何处理：如果旧表中有对应 MAC，则更新老化时间，如果没有，则新增。对于旧表中有但没有新学习到的 MAC，等老化后删除。
- SNMP 同步分两步：

  1. SNMP 协议跟交换机交互报文，来学习 IP-MAC 条目，并将 IP-MAC 条目存到文件中（网络好时报文交互快，学的也快）。

  2.从文件中读 IP-MAC，进行新旧对比并更新老化时间。
- 正常情况下，开启 SNMP 同步功能后启动老化定时器，30 分钟执行一次老化，然后更新定时器的时间进行下一次老化，如果条目达到 59000 条，触发定时器快速老化（记录本次快速老化的时间），然后刷新定时器为 30 分钟；当再次达到 59000 条时，判断当前时间-上次快速老化时间小于 10 分钟，什么都不做；否则触发定时器快速老化（记录本次快速老化的时间），然后刷新定时器为 30 分钟。
- 快速老化机制：

  1.IP-MAC 表达到 59000 条时触发快速老化，将已经老化的 IP-MAC 全清掉，规格满直接丢新的条目。

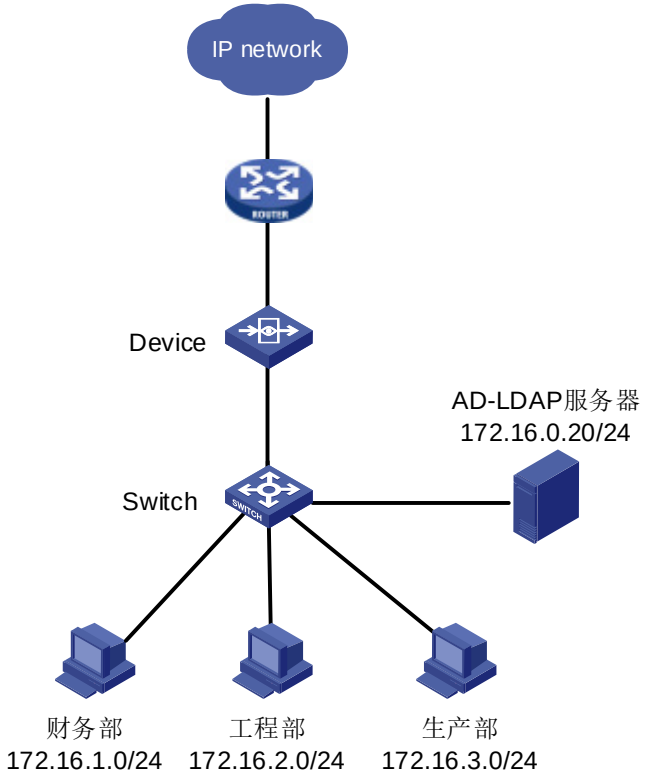
  2.两次快速老化的时间间隔是 10 分钟。

4 用户同步配置举例

4.1 组网需求

如图 1 所示，某公司的财务部、工程部员工实行固定设备使用静态绑定 IP/MAC 的方式上网，生产部员工使用 LDAP 服务器配置的用户账号认证上网，其网段分别是 172.16.1.0/24、172.16.2.0/24 和 172.16.3.0/24，LDAP 服务器的地址为 172.16.0.20/24。工程部 SNMP 服务器地址为 172.16.0.10/24。使用设备的 ge0 和 ge1 接口透明模式部署在网络中，在上配置用户同步。

图1 用户同步功能配置组网图



4.2 配置思路

按照组网图组网。

(1) 添加 LDAP 服务器

(2) 配置用户组

(3) 配置用户同步任务

(4) 配置用户认证地址对象

(5) 配置 WEB 认证参数

(6) 配置 IPv4 策略

(7) 全局配置启用第三方 LDAP 服务器

(8) 配置用户策略

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

1. 添加 LDAP 服务器

通过菜单“用户管理>认证管理>认证服务器”，点击<新建>LDAP 服务器。进入如图 2 所示的页面。

图2 LDAP 服务器配置

2. 配置用户组

通过菜单“用户管理>用户组织结构”，单击选择“新建>用户组”，配置财务部和工程部用户组，如图 3、图 4 所示。

图3 财务部用户组配置

图4 工程部用户组配置

3. 配置用户同步认证

(1) 配置 LDAP 同步

通过菜单“用户管理>用户同步”，单击选择“新建>LDAP 同步”，进入 LDAP 同步配置页面。配置 LDAP 同步任务名称，选择 LDAP 服务器，选择开启同步周期并配置同步周期（每天的某个整点），或者选择关闭周期同步，如图 5 所示。

图5 配置生产部 LDAP 同步

(2) 配置 SNMP 同步

通过菜单“用户管理>用户同步”，单击选择“新建>SNMP 同步”，进入 SNMP 配置页面。配置 SNMP 同步任务名称，IP 地址和 MAC 地址配置为 SNMP server 的 IP 地址和 MAC 地址，配置团体名和 SNMP 的版本号，选择开启周期同步并配置同步周期或者关闭周期同步（只在配置成功后同步一次），选择开启自动录入并配置同步结果的录入用户组，或者关闭自动录入由后期用户手动添加。如图 6 所示。

图6 配置工程部 SNMP 同步

(3) 配置 ARP 扫描

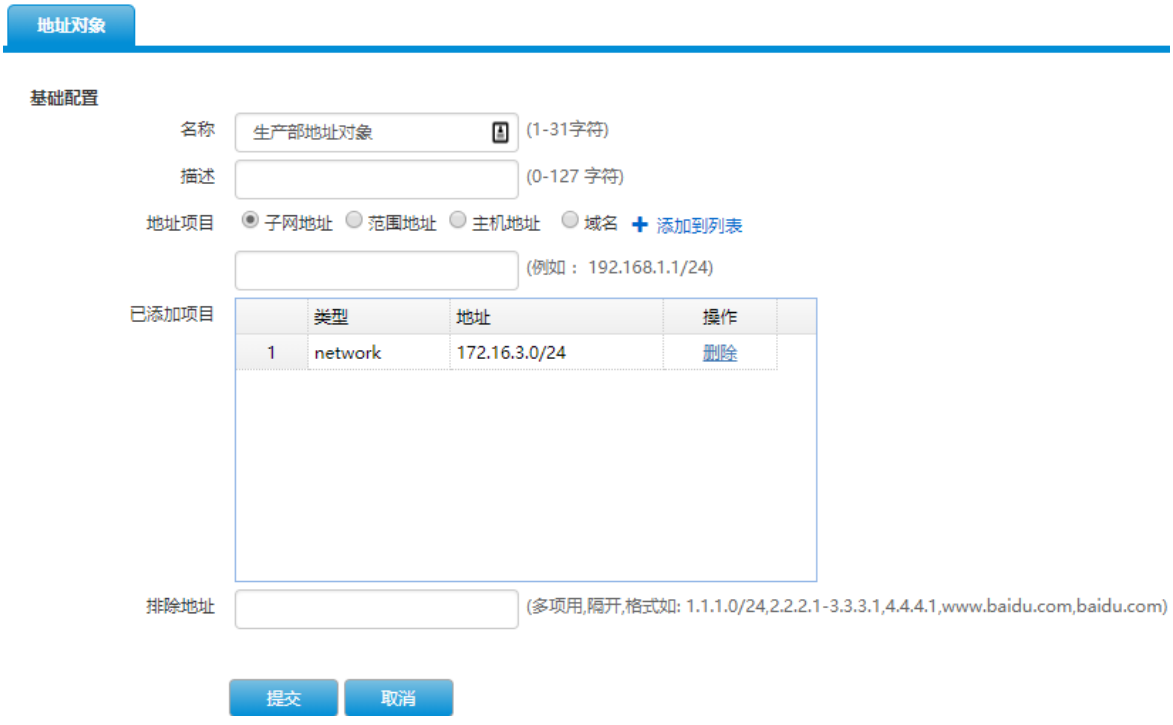
通过菜单“用户管理>用户同步”，单击选择“新建>ARP 扫描”，进入 ARP 扫描配置页面。配置“扫描网段”为财务部网段，选择配置是否开启周期同步，是否开启自动录入并选择录入用户的组织结构的用户组。如图 7 所示。

图7 配置财务部 ARP 扫描

4. 配置用户认证地址对象

通过菜单“策略配置 > 对象管理 > 地址对象”，单击“新建>地址对象”，配置生产部地址对象。如图 8 所示。

图8 地址对象配置



5. 配置 Web 认证参数

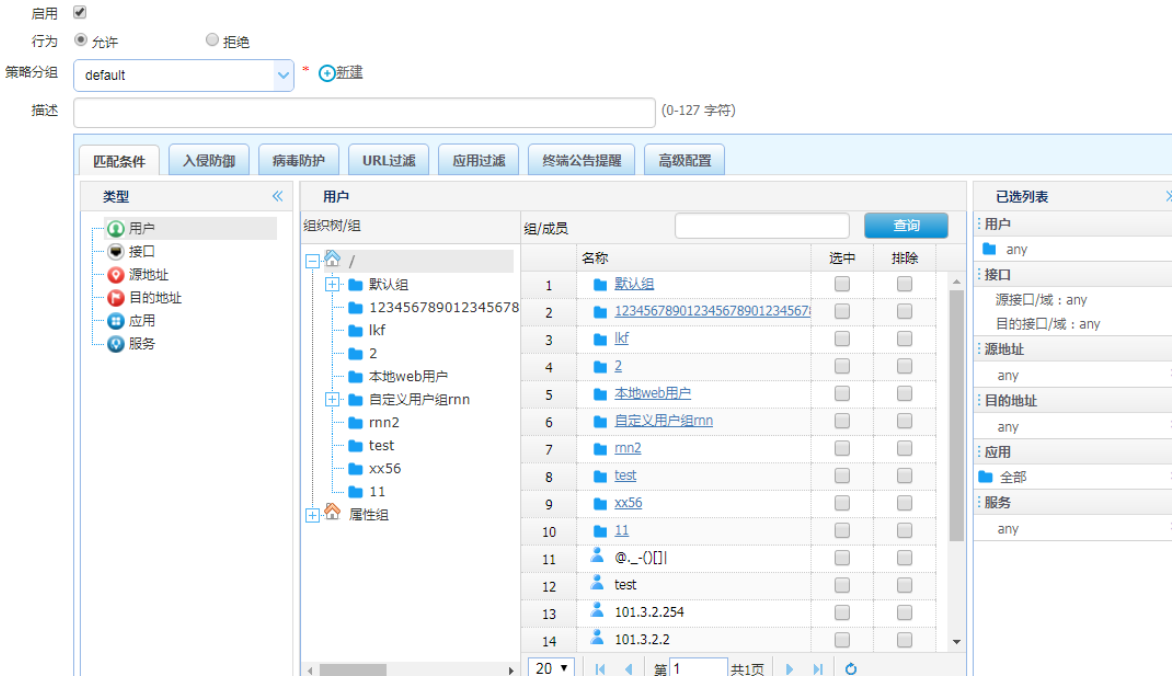
通过菜单“用户管理>认证管理>认证方式 > 本地 WEB 认证”，勾选“允许重复登录”，配置“允许登录数”为无限制，单击<提交>。如图 9 所示。

图9 配置 Web 认证

6. 配置安全策略

通过菜单“策略配置>IPv4 控制策略”，单击“新建>IPv4 控制策略”。如图 10 所示。配置用户组财务部、工程部和生产部（LDAP 同步下来的用户组）允许访问外网。

图10 IPV4 控制策略配置



7. 全局配置启用第三方认证选择 LDAP 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证，选择 LDAP 服务器，如图 11 所示。

图11 全局模式启用第三方 Ldap 配置

8. 配置用户策略

通过菜单进入“用户管理>认证管理>认证策略”，单击<新建>，源地址配置为“生产部地址对象”，认证方式配置为“Web 认证”，其它选项保持默认，单击<提交>。如图 12 所示。

图12 用户策略配置

4.5 验证配置

(1) 进入“用户管理>用户组织结构”，查看“财务部”用户组。财务部 ARP 同步成功后，财务部固定设备的用户全部自动录入，用户静态绑定对应的 IP，固定设备直接可以上网。如图 13 所示。

图13 财务部 ARP 同步用户

(2) 进入“用户管理>用户组织结构”，查看“工程部”用户组。工程部 SNMP 同步成功后，生产部固定设备的用户全部自动录入，用户静态绑定对应的 IP/MAC，固定设备直接可以上网。如图 14 所示。

图14 工程部 SNMP 同步用户

(3) 进入“用户管理>用户组织结构”，查看“生产部”用户组。从 LDAP 成功同步了生产部的用户，同步了用户组“生产部”以及用户组的直属用户 user1，user2，user3。如图 15 所示。

图15 生产部 LDAP 同步用户

(4) 在生产部网段（172.16.3.0/24）使用 PC 终端进行 HTTP 访问，弹出本地 Web 认证页面，使用 LDAP 联动用户 user3（此用户在 LDAP 服务器上真实存在且已经通过 LDAP 同步功能录入到了设备本地用户组）认证成功，认证成功后可以正常访问外网。如图 16 所示。

图16 生产部 LDAP 用户认证页面

目 录

1 简介

本文档介绍设备的短信认证功能配置举例，在配置前，先了解如下定义：

- 短信网关：与设备对接，给认证终端指定手机号下发授权验证码的设备，目前支持对接的短信网关厂商包括：亿美软通、凌凯、一信通、佳诺、阿里云、梦网科技、移动云 MAS。

本文档以亿美软通短信网关厂商对接进行举例说明。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

- 客户已经在对应的短信网关厂商进行了注册（如亿美软通）。
- 本文档假设您已了短信认证特性。

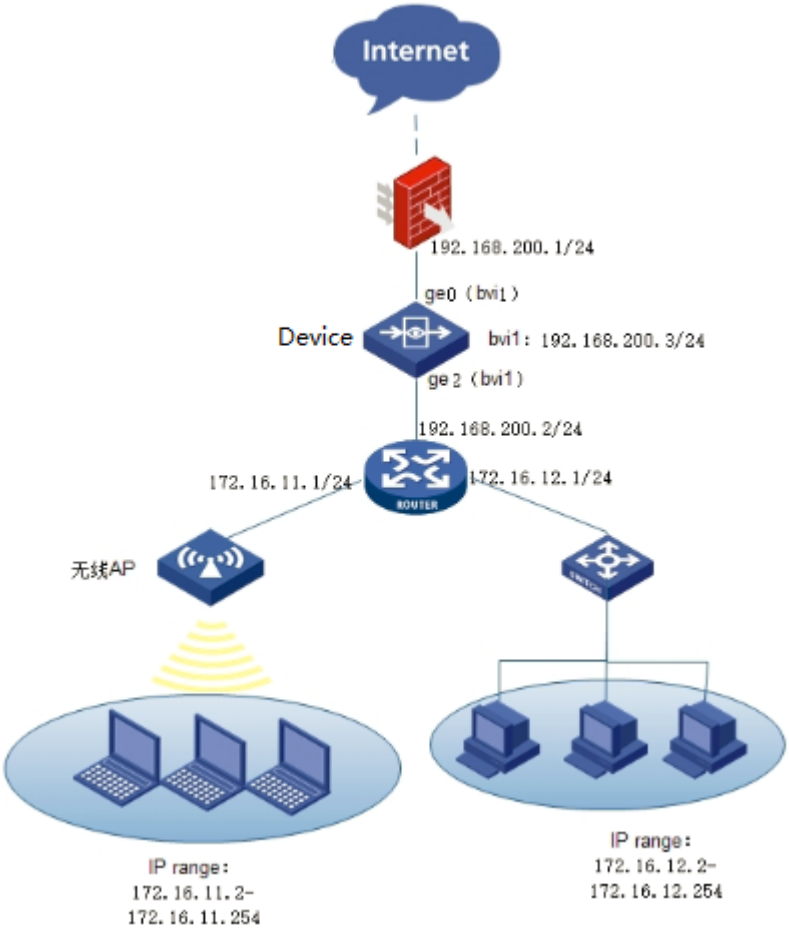
3 短信认证功能配置举例

3.1 组网需求1：透明桥三层组网

3.1.1 组网需求

如图 1所示，某公司内网无线办公网段 IP 地址 172.16.11.0/24，有线办公网段 IP 地址 172.16.12.0/24，其中 172.16.11.1/24 作为无线访问点的网关，172.16.12.1/24 作为有线访问点的网关。Router 上开启 DHCP，地址池分别为 172.16.11.2/24~172.16.11.254/24、172.16.12.2/24~172.16.12.254/24。使用设备的的 ge0 和 ge2 接口作为透明桥，串接部署在网络中，设备上联出口 FW，下联三层设备路由器。设备上开启短信认证功能,用户通过短信认证后才能访问网络。

图1 短信认证透明桥三层组网图



3.1.2 配置思路

- 注册短信网关厂商，获取授权。
- 配置短信认证功能。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

(1) 配置网桥接口

如图 2 所示，进入网络配置>接口配置>网桥接口，点击<新建>按钮创建网桥接口 bvi1，把 ge0、ge2 加入网桥，配置接口地址为 192.168.200.3/24。

图2 配置网桥接口

(2) 配置静态路由

如图 3 配置访问外网的默认路由及去往认证用户网段 172.16.11.0/24,172.16.12.0/24 路由。

图3 配置静态路由

	目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	操作
1	0.0.0.0	0.0.0.0	192.168.200.1	bvi1	1	1	-		
2	172.16.11.0	255.255.255.0	192.168.200.2	bvi1	1	1	-		
3	172.16.12.0	255.255.255.0	192.168.200.2	bvi1	1	1	-		

(3) 配置短信认证地址对象

如图 4 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,172.16.12.0/24，点击<提交>。

图4 配置短信认证地址对象

(4) 配置短信认证参数

如图 5 所示，进入“用户管理 > 认证管理 > 认证方式 > 短信认证 >”页面，配置短信认证参数。

图5 短信认证配置

(5) 配置短信认证策略

如图 6 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge2，源地址选择“认证用户”，认证方式使用“短信认证”，提交策略。

图6 认证策略页面

(6) 配置用户识别范围

如图 7 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，其它配置默认，提交配置。

图7 用户识别范围

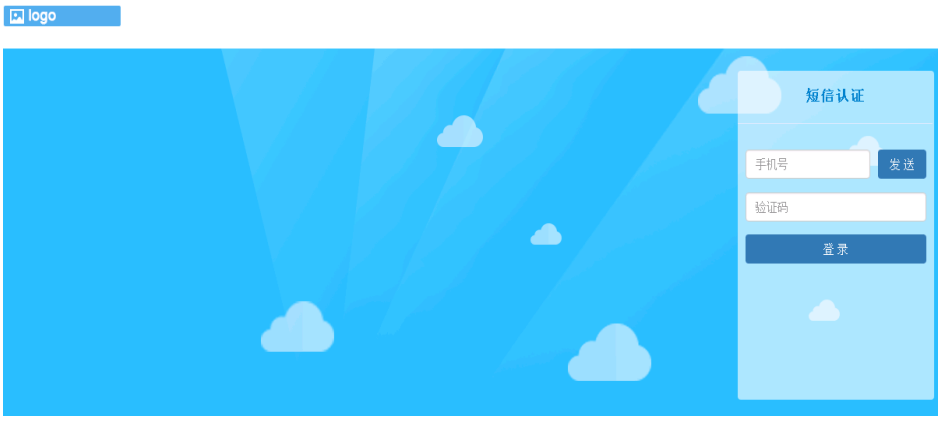
3.1.5 配置注意事项

- Router 设备需要开启 DHCP 功能，地址池范围为 172.16.11.2/24~172.16.11.254/24。172.16.12.2/24~172.16.12.254/24。
- 认证用户网段必须在用户识别范围中，否则导致不能正常认证。

3.1.6 验证配置

如图 8 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图8 认证 portal 页面

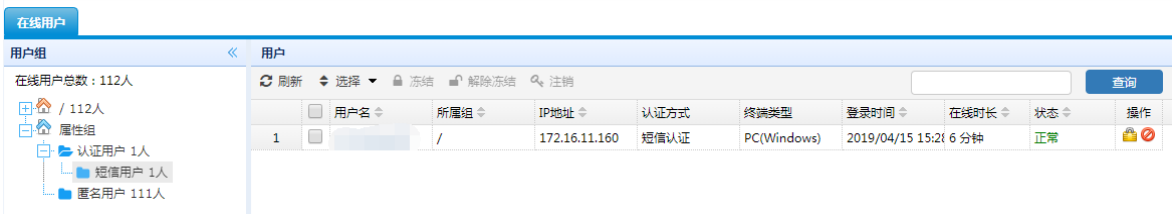


如图 9 所示，输入手机号，点击<发送>获取验证码，待手机获取到短信网关发送的验证码后，输入正确的验证码，点击登录即可完成认证。

图9 短信认证

如图 10 所示，在“数据中心>系统监控>在线用户”管理中查看该用户已认证成功。

图10 在线用户

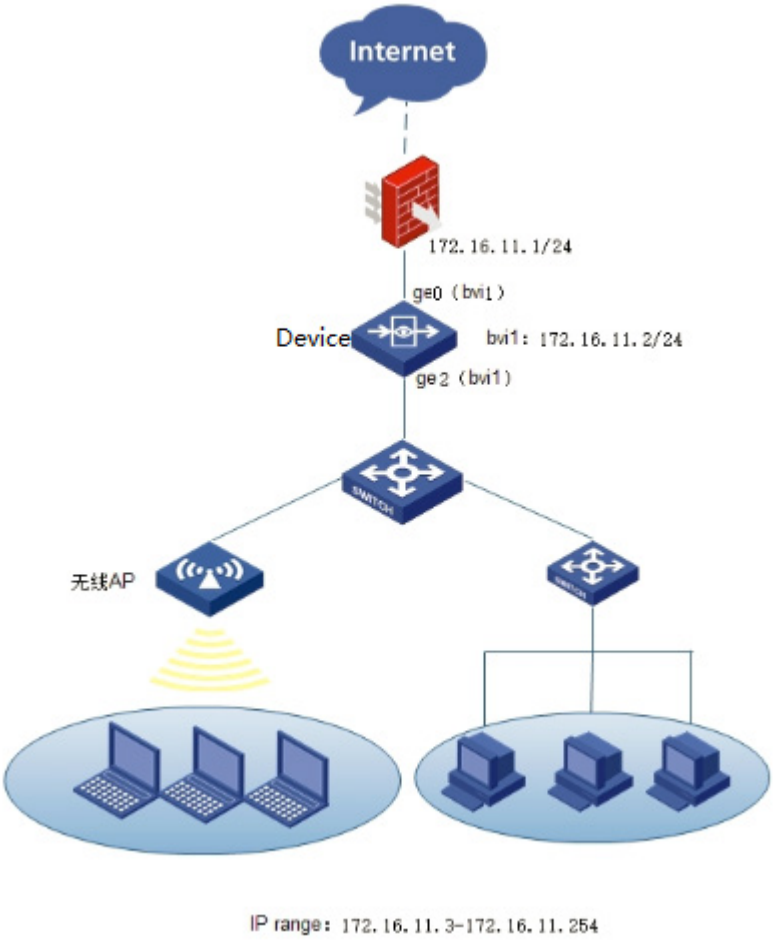


3.2 组网需求2：透明桥二层组网

3.2.1 组网需求

如图 11 所示，某公司内网办公网段 IP 地址 172.16.11.0/24，其中 172.16.11.1/24 作为认证用户的网关。FW 上开启 DHCP，地址池为 172.16.11.3/24~172.16.11.254/24。使用设备的的 ge0 和 ge2 接口作为透明桥，串接部署在网络中，设备上联出口 FW，下联二层交换机。设备上开启短信认证功能，用户通过短信认证后才能上网。

图11 短信认证透明桥二层组网图



3.2.2 配置思路

- 注册短信网关厂商，获取授权。
- 配置短信认证功能。

3.2.3 使用版本

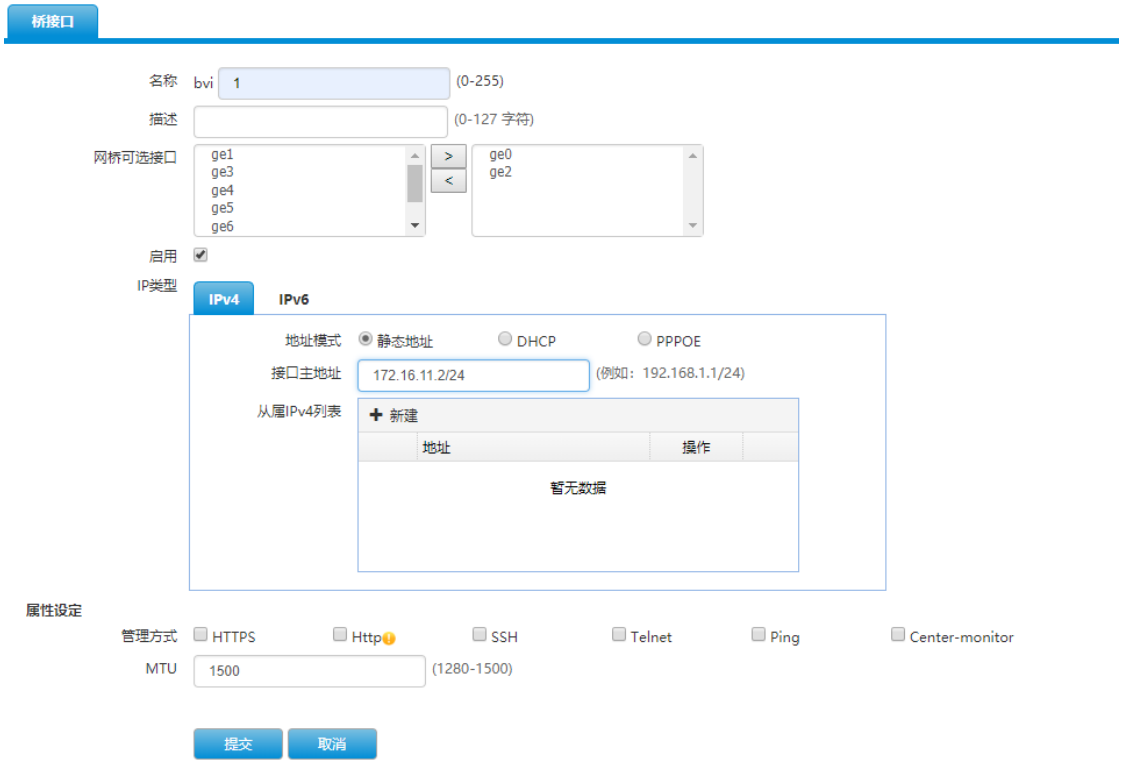
本举例是在 E6442 版本上进行配置和验证的。

3.2.4 配置步骤

(1) 配置网桥接口

如图 12 所示，进入“网络配置>接口配置>网桥接口”，点击<新建>按钮创建网桥接口 bvi1，把 ge0、ge2 加入网桥，配置接口地址为 172.16.11.2/24。

图12 配置网桥接口



(2) 配置静态路由

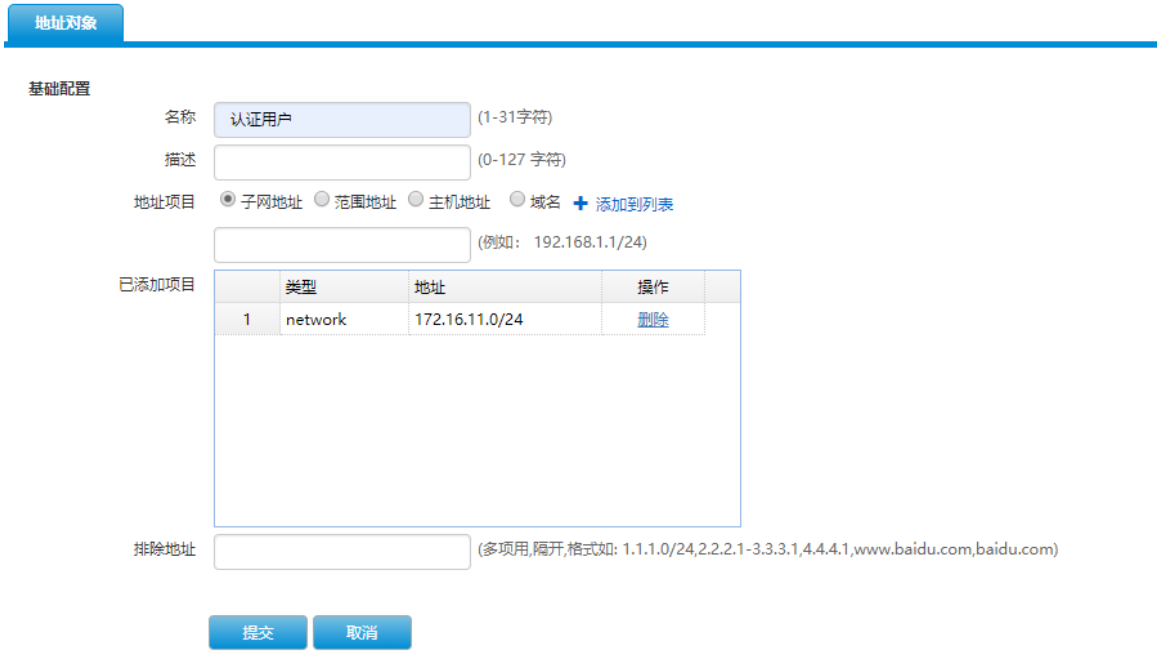
如图 13 配置访问外网的默认路由。

图13 配置静态路由

(3) 配置短信认证地址对象

如图 14 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

图14 配置短信认证地址对象



(4) 配置短信认证参数

如图 15 所示，进入“用户管理 > 认证管理 > 认证方式 > 短信认证”页面，配置短信认证参数。

图15 短信认证配置

(5) 配置短信认证策略

如图 16 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge2，源地址选择“认证用户”，认证方式使用“短信认证”，提交策略。

图16 认证策略页面

(6) 配置用户识别范围

如图 17 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，其它配置默认，提交配置。

图17 用户识别范围

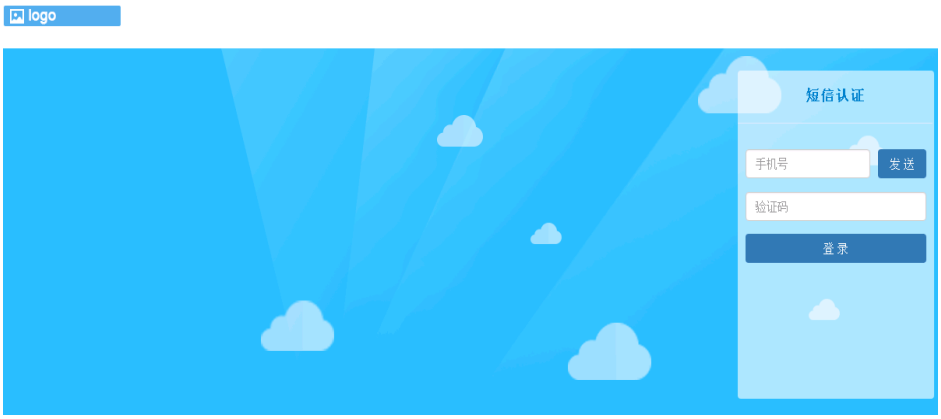
3.2.5 配置注意事项

- FW 设备需要开启 DHCP 功能，地址池范围为 172.16.11.3/24~172.16.11.254/24。
- 设备在透明部署模式下配置短信认证时，bvi 接口需要配置管理地址和认证用户同网段，以便正常给认证用户推送 portal 页面。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。

3.2.6 验证配置

如图 18 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图18 认证 portal 页面

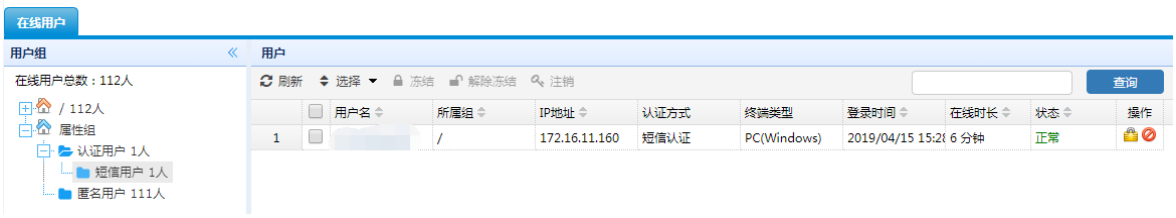


如图 19 所示，输入手机号，点击<发送>获取验证码，待手机获取到短信网关发送的验证码后，输入正确的验证码，点击登录即可完成认证。

图19 短信认证

如图 20 所示，在“数据中心>系统监控>在线用户”管理中查看该用户已认证成功。

图20 在线用户



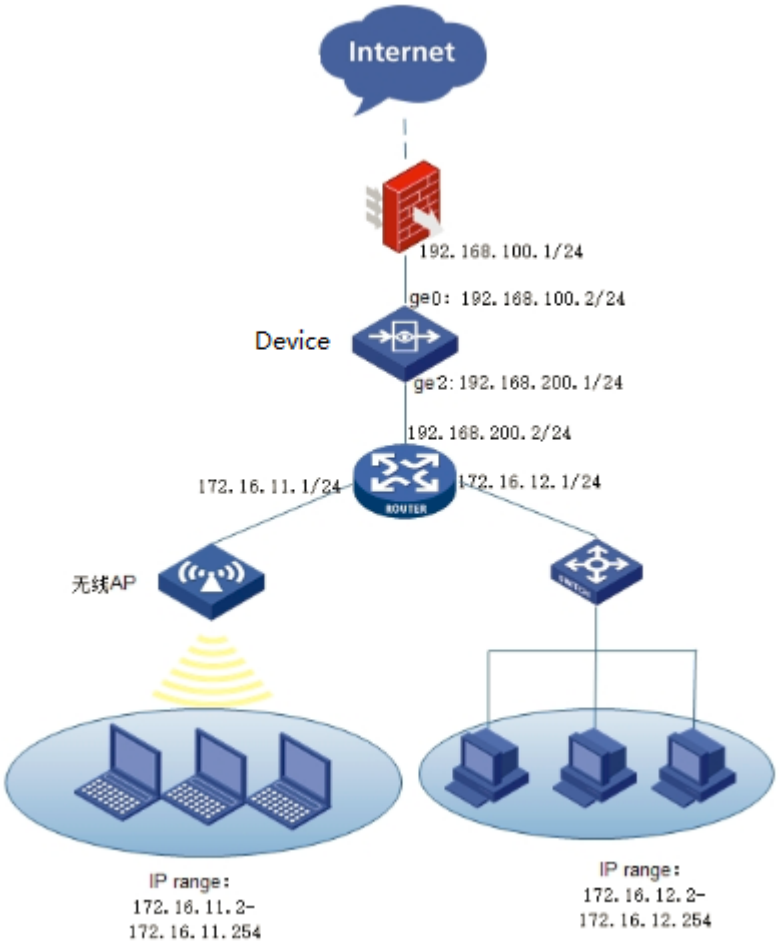
3.3 组网需求3：路由模式三层组网

3.3.1 组网需求

如图 21 所示，某公司内网无线办公网段 IP 地址 172.16.11.0/24，有线办公网段 IP 地址 172.16.12.0/24，其中 172.16.11.1/24 作为无线访问点的网关，172.16.12.1/24 作为有线访问点的网关。Router 上开启 DHCP，地址池分别为：

172.16.11.2/24~172.16.11.254/24、172.16.12.2/24~172.16.12.254/24。使用设备的的 ge0 和 ge2 接口以三层路由模式部署在网络中，设备上联出口 FW，下联三层设备路由器。设备上开启短信认证功能，用户通过短信认证后才能上网。

图21 短信认证路由模式三层组网图



3.3.2 配置思路

- 注册短信网关厂商，获取授权。
- 配置短信认证功能。

3.3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.3.4 配置步骤

(1) 配置路由接口

如图 22、图 23 所示，进入“网络配置>接口配置”，点击编辑 ge2、ge0 操作，把 ge0、ge2 的地址分别配置为 192.168.100.2/24、192.168.200.1/24。

图22 配置 ge2 接口

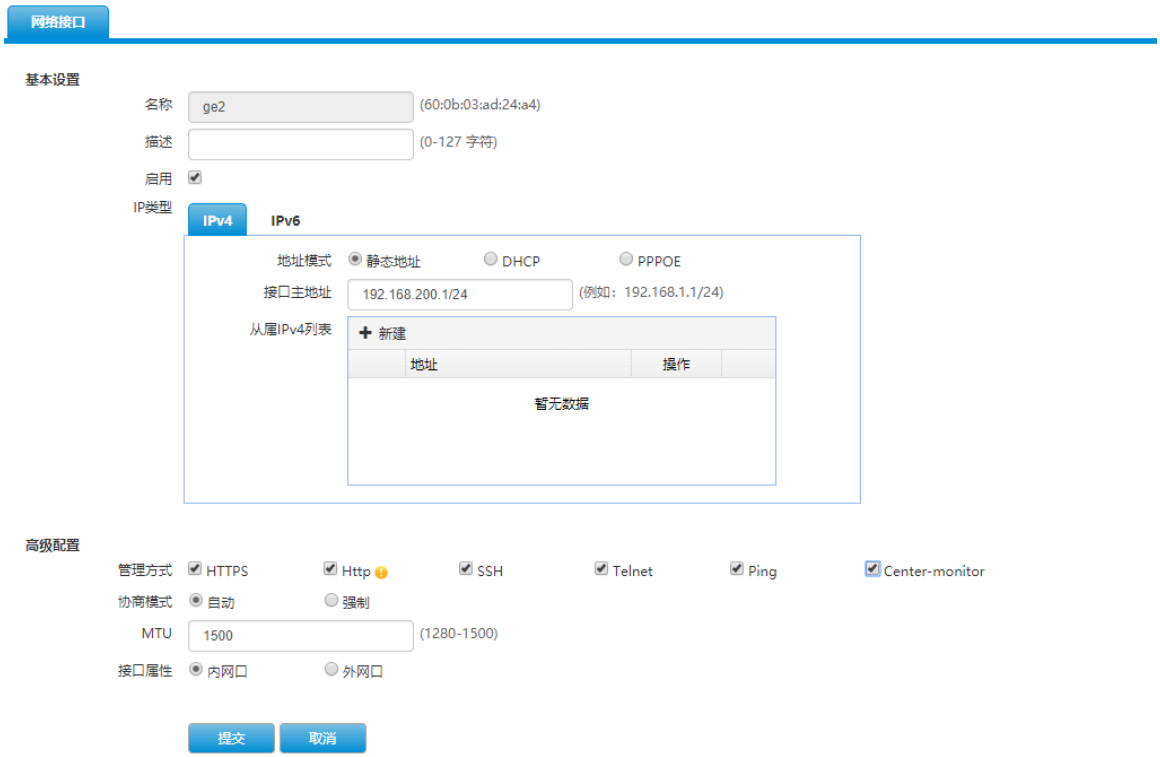
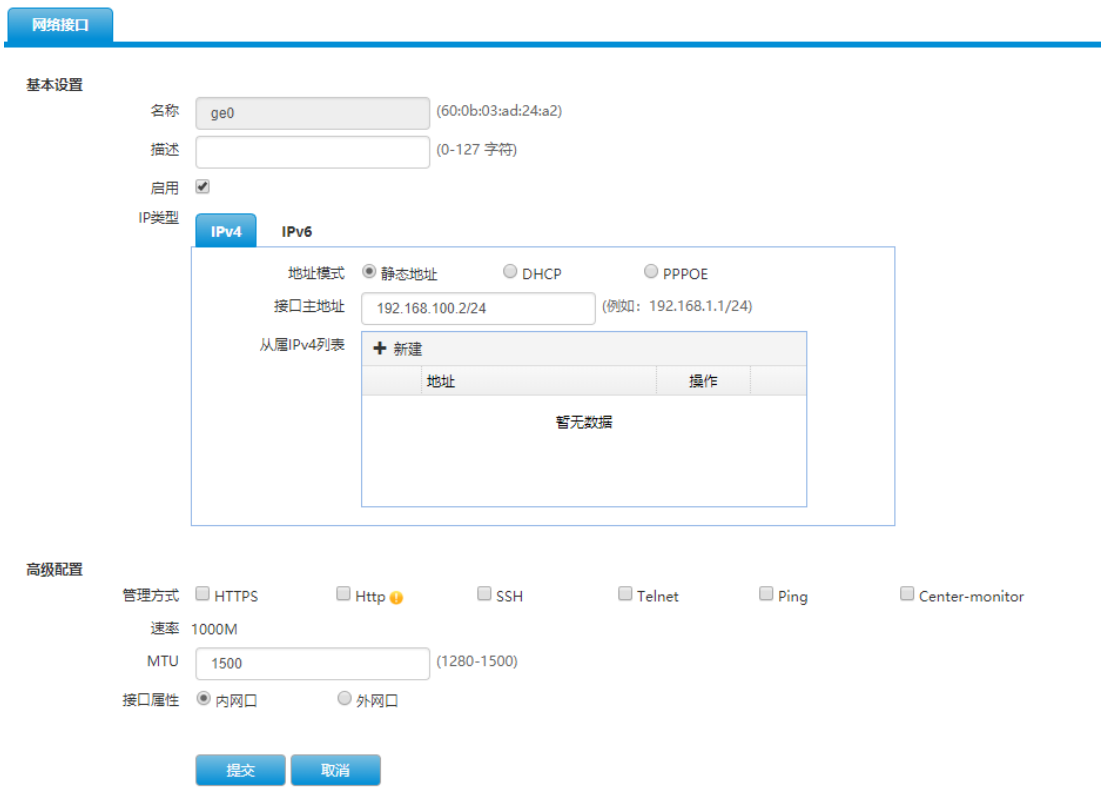


图23 配置 ge0 接口



(2)　配置静态路由

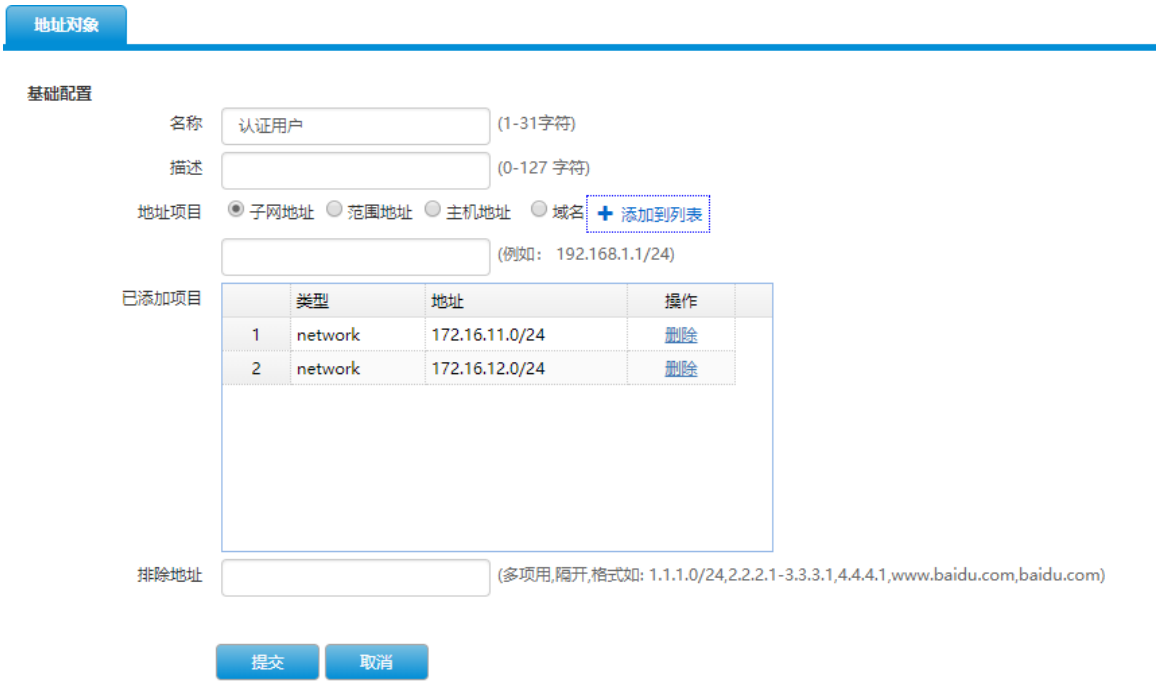
如图 24 配置访问外网的默认路由及去往认证用户网段 172.16.11.0/24,172.16.12.0/24 路由。

图24 配置静态路由

(3)　配置短信认证地址对象

如图 25 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,172.16.12.0/24，点击<提交>。

图25 配置短信认证地址对象



(4)　配置短信认证参数

如图 26 所示，进入“用户管理 > 认证管理 > 认证方式 > 短信认证”页面，配置短信认证参数。

图26 短信认证配置

(5) 配置短信认证策略

如图 27 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge2，源地址选择“认证用户”，认证方式使用“短信认证”，提交策略。

图27 认证策略页面

(6) 配置用户识别范围

如图 28 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，其它配置默认，提交配置。

图28 用户识别范围

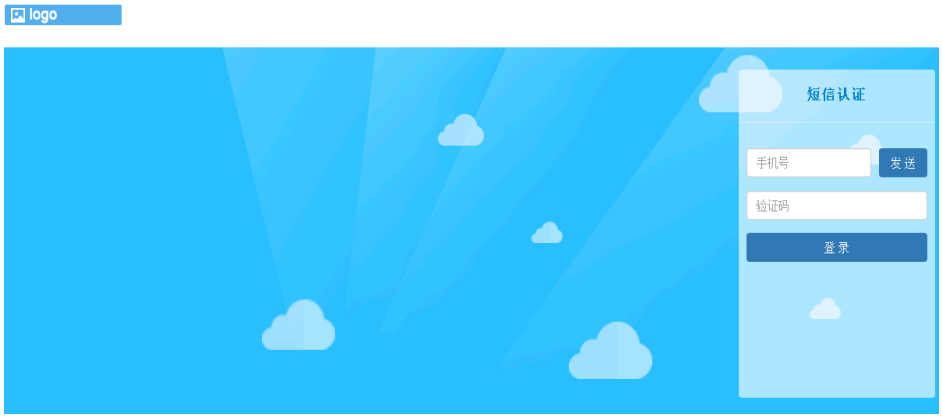
3.3.5 配置注意事项

- Router 设备需要开启 DHCP 功能，地址池范围为 172.16.11.2/24~172.16.11.254/24。172.16.12.2/24~172.16.12.254/24。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。

3.3.6 验证配置

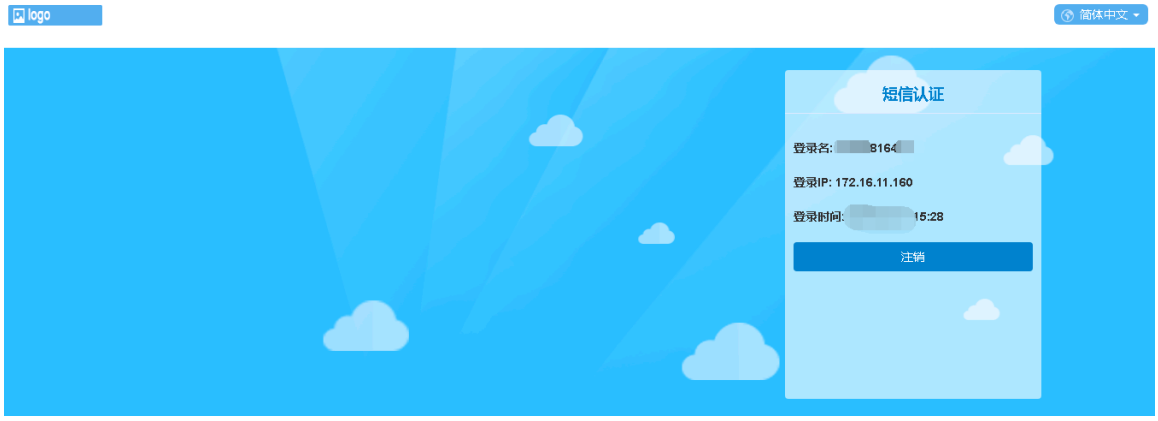
如图 29 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图29 认证 portal 页面



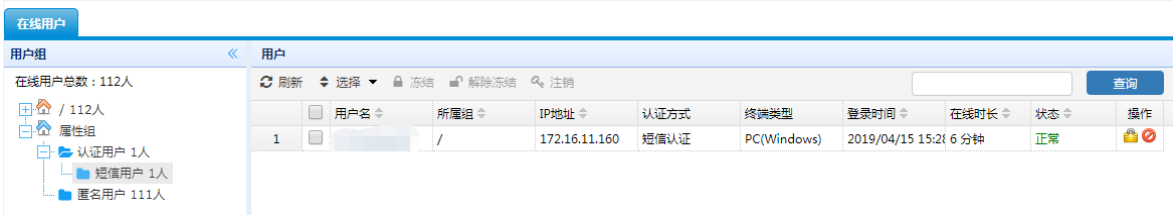
如图 30 所示，输入手机号，点击<发送>获取验证码，待手机获取到短信网关发送的验证码后，输入正确的验证码，点击登录即可完成认证。

图30 短信认证



如图 31 所示，在“数据中心>系统监控>在线用户”管理中查看该用户已认证成功。

图31 在线用户

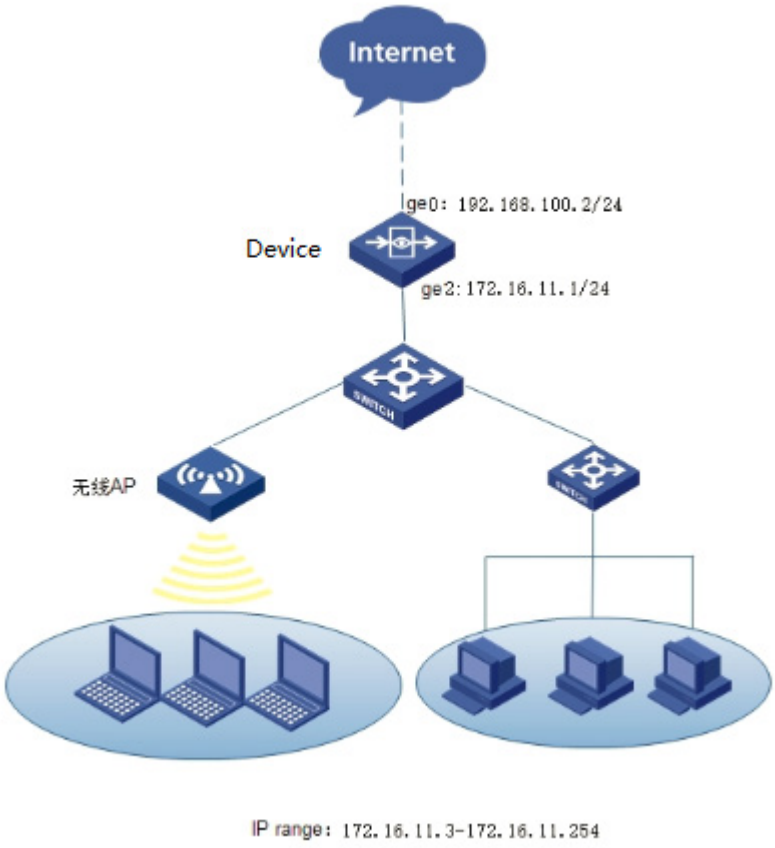


3.4 组网需求4：路由模式二层组网

3.4.1 组网需求

如图 32 所示，某公司内网办公网段 IP 地址 172.16.11.0/24，其中 172.16.11.1/24 作为认证用户的网关。地址池为 172.16.11.3/24~172.16.11.254/24。使用设备的的 ge0 和 ge2 接口以三层路由模式部署在网络中，设备作为出口网关设备，下联二层交换机。设备上开启短信认证功能，用户通过短信认证后才能上网。

图32 短信认证路由模式二层组网图



3.4.2 配置思路

- 注册短信网关厂商，获取授权。
- 配置短信认证功能。

3.4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

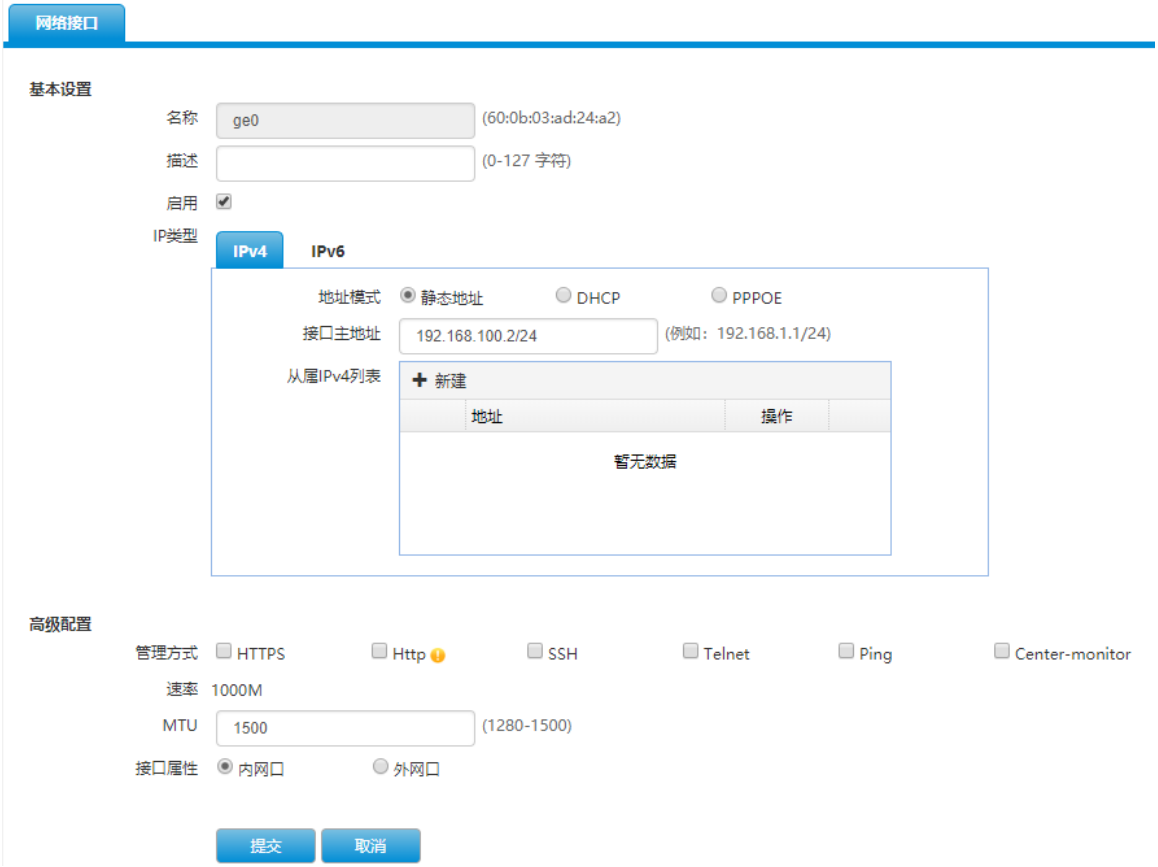
3.4.4 配置步骤

(1) 配置路由接口

如图 33、图 34 所示，进入“网络配置>接口配置”，点击编辑 ge0、ge2 操作，把 ge0、ge2 的地址分别配置为 192.168.100.2/24、172.16.11.1/24。

图33 配置 ge2 接口

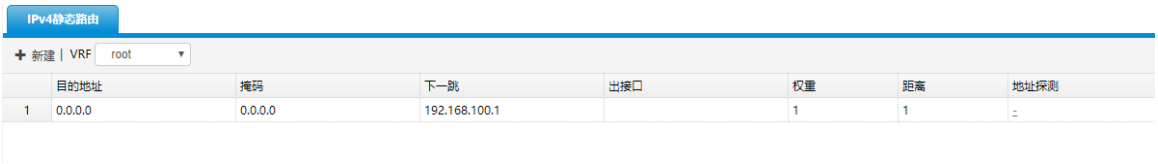
图34 配置 ge0 接口



(2) 配置静态路由

如图 35 配置访问外网的默认路由。

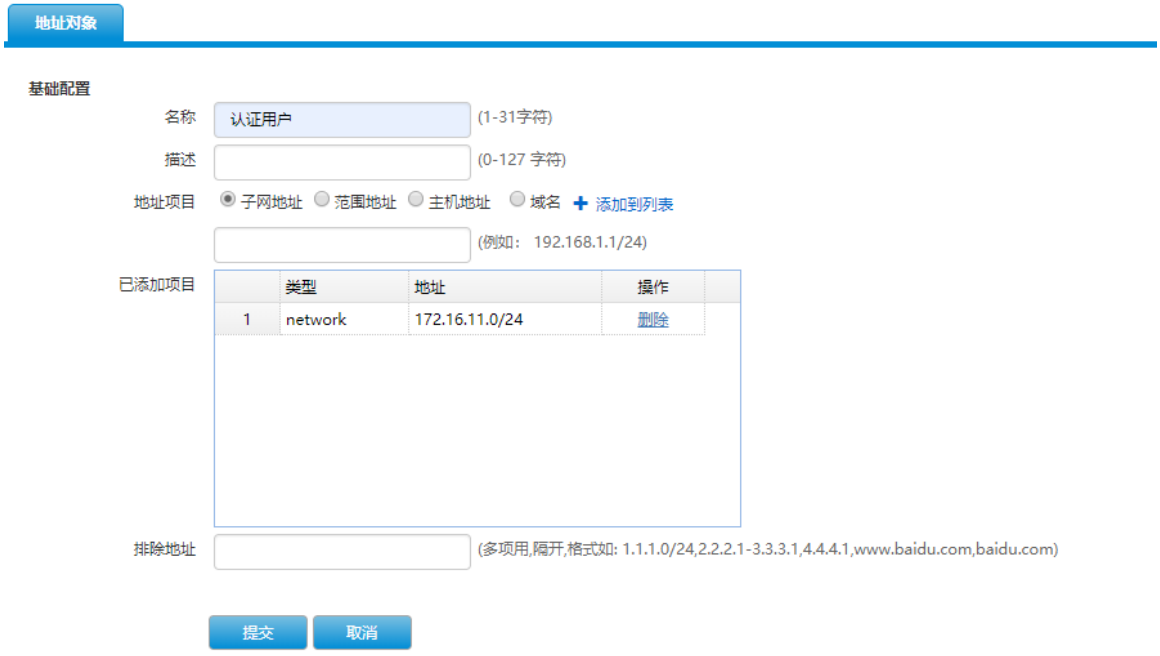
图35 配置静态路由



(3) 配置短信认证地址对象

如图 36 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

图36 配置短信认证地址对象



(4) 配置短信认证参数

如图 37 所示，进入“用户管理 > 认证管理 > 认证方式 > 短信认证 ”页面，配置短信认证参数。

图37 短信认证配置

(5) 配置短信认证策略

如图 38 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge2，源地址选择“认证用户”，认证方式使用“短信认证”，提交策略。

图38 认证策略页面

(6) 配置用户识别范围

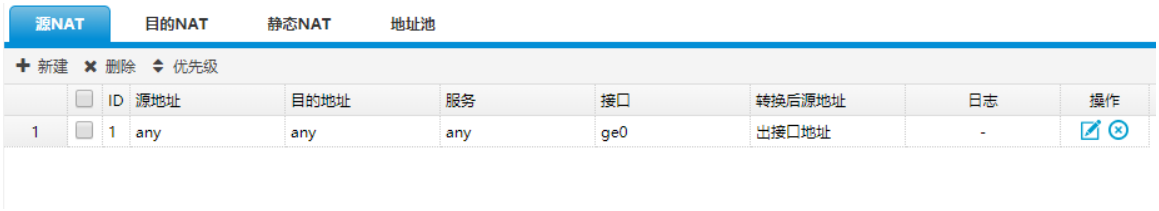
如图 39 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，其它配置默认，提交配置。

图39 用户识别范围

(7) 配置源 NAT

如图 40 所示，进入“策略配置>策略配置>NAT 转换策略”页面，在源 NAT 页面创建策略，接口选择 ge0，其它配置默认，提交配置。

图40 配置源 NAT



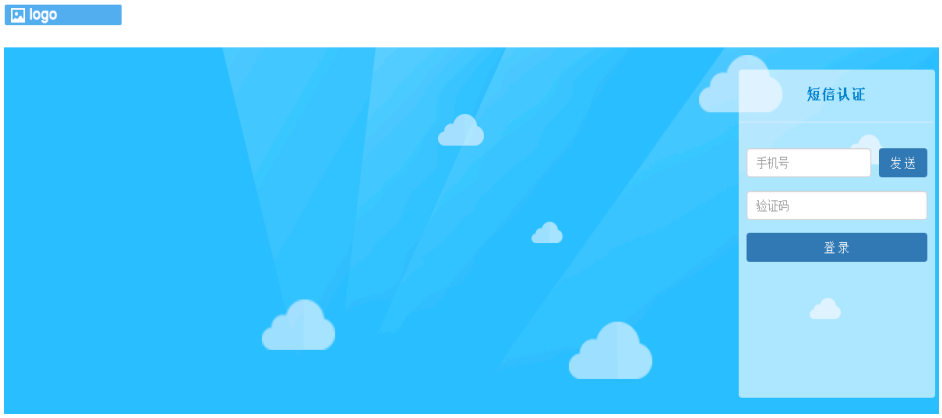
3.4.5 配置注意事项

- 设备或二层交换机上需要开启 DHCP 功能，地址池范围为：172.16.11.2/24~172.16.11.254/24。172.16.12.2/24~172.16.12.254/24。认证用户的网关地址指向 172.16.11.1。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。

3.4.6 验证配置

如图 41 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图41　认证 portal 页面

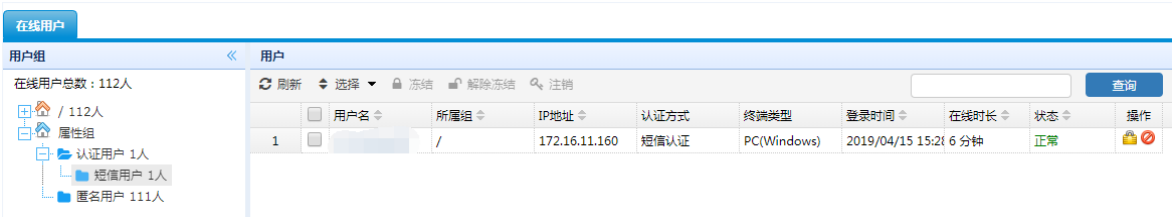


如图 42 所示，输入手机号，点击<发送>获取验证码，待手机获取到短信网关发送的验证码后，输入正确的验证码，点击登录即可完成认证。

图42 短信认证

如图 43 所示，在“数据中心>系统监控>在线用户”管理中查看该用户已认证成功。

图43 在线用户



目录

1 简介

LDAP 是轻量目录访问协议(Lightweight Directory Access Protocol)的缩写，其实是一种目录服务，类似于我们所使用诸如 NIS(Network Information Service)、DNS (Domain Name Service)等网络目录。

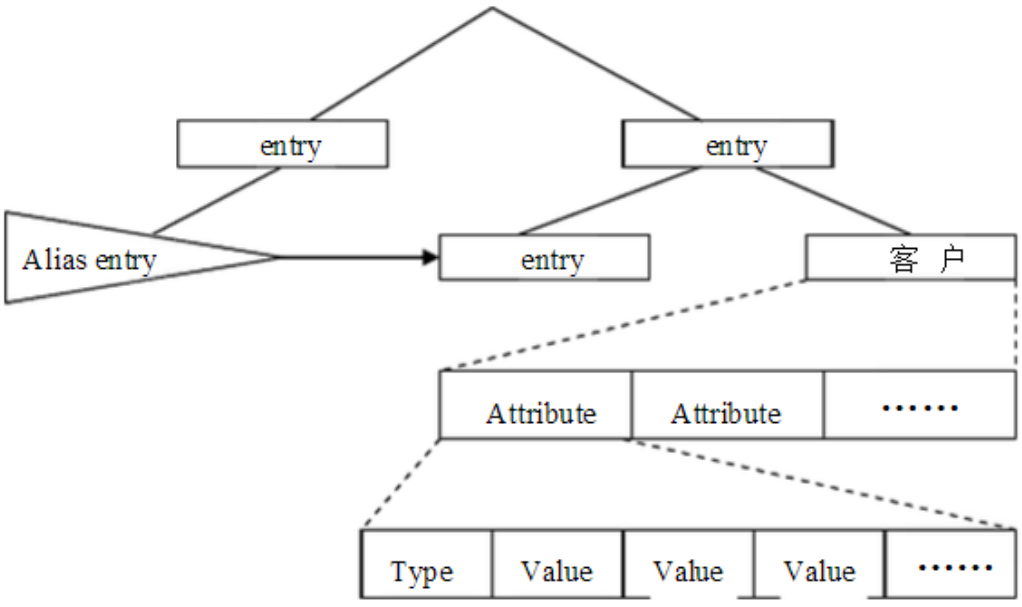
信息被集中存储在服务器上的 LDAP 目录中，信息模型以条目（entry）为基础（如图 1），一个条目是属性的集合，并且具有全局唯一 DN(distinguished name)用来唯一标识；条目类似数据库中的一条记录。

LDAP 目录以树状的层次结构来存储数据（这很类同于 DNS），最顶层即根部称作“基准 DN”，形如"dc=ldap,dc=com"或者"o=ldap.com"，前一种方式更为灵活也是 Windows AD 中使用的方式。在根目录的下面有很多的文件和目录，为了把这些大量的数据从逻辑上分开，LDAP 像其它的目录服务协议一样使用 OU （Organization Unit），可以用来表示公司内部机构，如部门等，也可以用来表示设备、人员等。同时 OU 还可以有子 OU，用来表示更为细致的分类。

LDAP 中每一条记录都有一个唯一的区别于其它记录的名字 DN（Distinguished Name）,其处在“叶子”位置的部分称作 RDN；如 dn:cn=user,ou=test,dc=ldap,dc=com 中 user 即为 RDN，RDN 在一个 OU 中必须是唯一的。

LDAP 支持 TCP/IP 协议，基于 C/S 模式客户端通过 TCP 连接到 Server 服务器，通过此连接发送请求和接收响应。

图1 LDAP 目录



在配置 LDAP 服务器前，先了解如下几个定义（图 2）以及它的详细说明（表 1）：

图2 LDAP 服务器页面

表1 LDAP 服务器页面的详细说明

项目	说明
服务器名称	LDAP服务器名称
服务器IP	LDAP服务器地址
端口	LDAP服务器端口，默认389明文，暂不支持636加密同步
通用名显示	1、cn 全称 common name ：配置cn时，同步、认证都使用标识名 2、sAMAccountName 同步和认证使用登录名
Base DN	用于获取同步信息的服务器域名路径
管理员	拥有管理权限的域服务器管理员
管理员密码	管理员对应密码

LDAP 同步配置显示如图 3 所示。

在导航栏中选择“用户管理>用户同步”，单击<新建>按钮，配置 LDAP 同步，LDAP 同步详细参数如表 2 所示。

图3 LDAP 服务器配置界面

表2 LDAP 同步界面的详细说明

参数	说明
名称	LDAP同步条目名称。
描述	LDAP同步描述信息
LDAP服务器	选择引用的LDAP服务器
同步类型	1、OU 同步AD域下ou用户 2、 安全组同步Ad域下组用户
自动同步	启用或禁用自动同步功能
起始时间	LDAP同步条目创建后开始同步的时间
间隔时间	LDAP同步条目创建后按照时间间隔进行同步
用户组	LDAP同步用户的用户组

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 LDAP 服务器特性。

3 使用限制

- LDAP 同步下来的用户如果在 AD 域上被删除，则在设备上进行删除用户；如果该用户有引用策略且为用户自己的引用策略同时删除用户并解引用；否则，只删除该用户在用户组中引用的该用户。
- 同步过程中如果由于网络异常（例如断网）导致同步的用户（组）不完整，则认为该次同步失败，将不完整数据丢弃。
- 同步下来的用户如果无法识别，则将该用户丢弃，不在设备上进行任何操作。Windows AD 服务器上用户名超长(大于 63 字符)；（汉字数字字母以及@._-()[]|以外的特殊字符）.
- 最多可以配置 128 条 LDAP 服务器策略，最多可以配置 100 条 LDAP 组策略，每个 LDAP 组下最多可以引用 5 条 LDAP 服务器。
- LDAP 仅支持简单模式的联动认证，不支持匿名和通用模式的联动认证。
- LDAP 服务器用户名长度大于 63 字符后无法录入。
- LDAP 服务器同步目前支持 389 明文传输，不支持 636 密文传输（加密跟服务器交互不了 身份验证不了）。
- 只支持 Windows AD 域用户同步，不支持匿名同步用户。不支持 OpenLdap 服务器（openldap 同步的用户没有 dn 属性无法参与认证）。
- AD 服务器上用户名超长(大于 63 字符)，含有异常字符（汉字数字字母以及@._-()[]|以外的特殊字符）可以同步，不能录入到本地用户结构，同步过程中会依次在本地用户结构添加用户、用户组，本地满规格时无法录入，同步规格和本地用户规格相同。
- LDAP BaseDN 如果写根 OU 的话，同步 LDAP 服务器的时候会把根 OU 下的所有子 OU 以及用户全部同步下来。
- IPSec 和 sslvpn 使用 LDAP 认证时，需保证本地存在该用户。
- 多个用户同步条目存在时，同步任务为串行，上面同步条目同步完成后在进行下面同步条目的同步。
- LDAP 同步周期起始时间（0-23），间隔时间（1-24），例如起始时间 8，间隔 2，代表该同步条目每天 8 点开始同步，每隔 2 小时同步一次，晚上 12 点结束当天的同步任务。
- AD 域用户更新密码后，使用同步的 ldap 认证时，新旧密码都可以认证。在 server 2008 级别的 AD 下，旧密码生存期为 5 分钟，在 server 2003 级别的 AD 下，旧密码生存期为 60 分钟。
- 这个 5 分钟就是为了防止 AD 同步延时问题，防止 DC 数量比较多时，用户登录所在的站点内还没有成功的更新到密码的修改的情况。这样，即使新密码没有生效，旧密码依然可用。

  测试 2003 的服务器，旧密码有效期为 60 分钟，自测 60 分钟后密码失效，此为 AD 域服务器的保护机制，不修改。

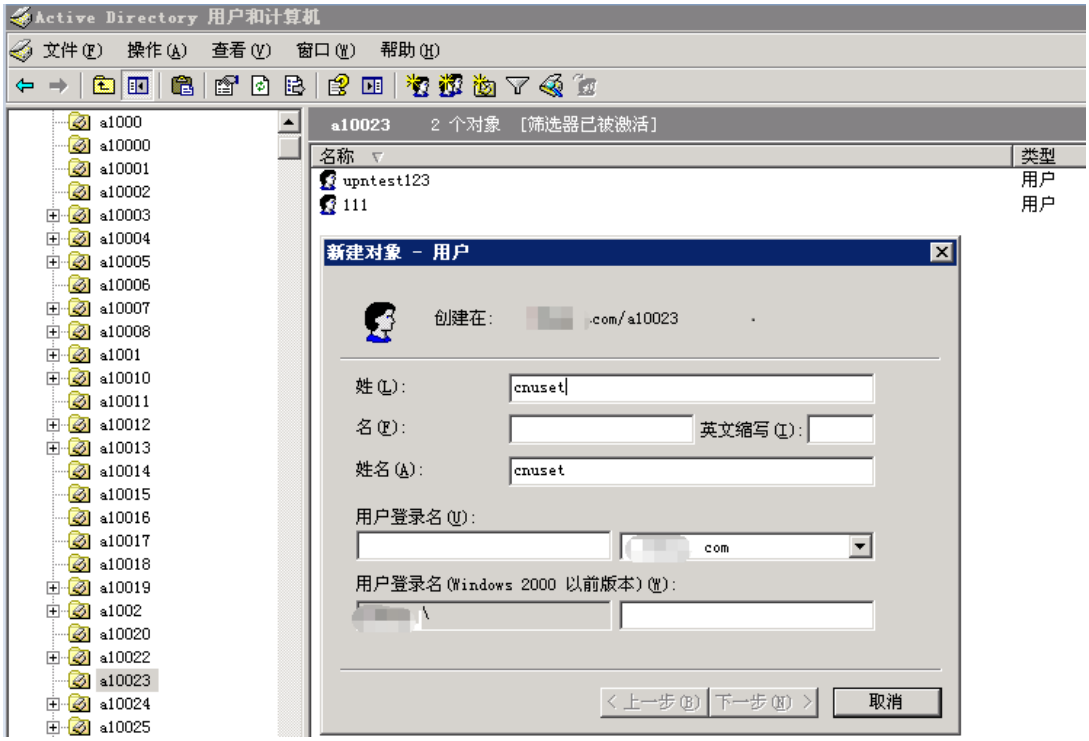
- LDAP 同步下来的用户如果在 AD 域上被删除，则在设备上进行删除用户；如果该用户有引用策略且为用户自己的引用策略同时删除用户并解引用；否则，只删除该用户在用户组中引用的该用户。
- 同步过程中如果由于网络异常（例如断网）导致同步的用户（组）不完整，则认为该次同步失败，将不完整数据丢弃。
- 同步下来的用户如果无法识别，则将该用户丢弃，不在设备上进行任何操作。Windows AD 服务器上用户名超长(大于 63 字符)；（汉字数字字母以及@._-()[]|以外的特殊字符）.
- 手动创建用户组、用户创建为本地用户，和 ldap 服务器上组、用户名称一样，点 ldap 同步，这个用户没法用 ldap 认证，ldap 同步当存在重名用户时，只移动用户，不覆盖。
- ldap 组里第一个 ldap 服务器密码不对，用户在第二个服务器，此时用户认证浏览器无响应，目前处理不了跨域的 ldap 组认证，需要保障 ldap 组下地址可达，服务器密码正确。

3.1 LDAP认证的两种方式

图4 LDAP 用户认证方式有两种类型分别为 CN 和 sAMAccountName

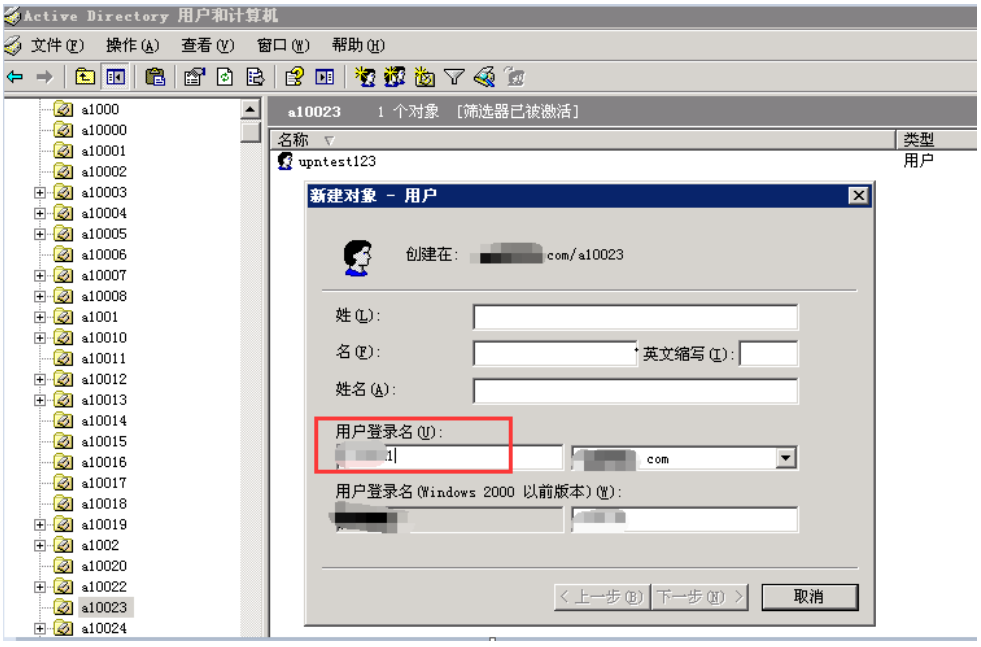
3.1.1 CN：使用的是显示名进行认证

图5 通用名标识配置为 CN 时服务器用户配置



3.1.2 sAMAccountName：使用的是登录名进行认证

图6 通用名标识配置为 sAMAccountName 时服务器用户配置

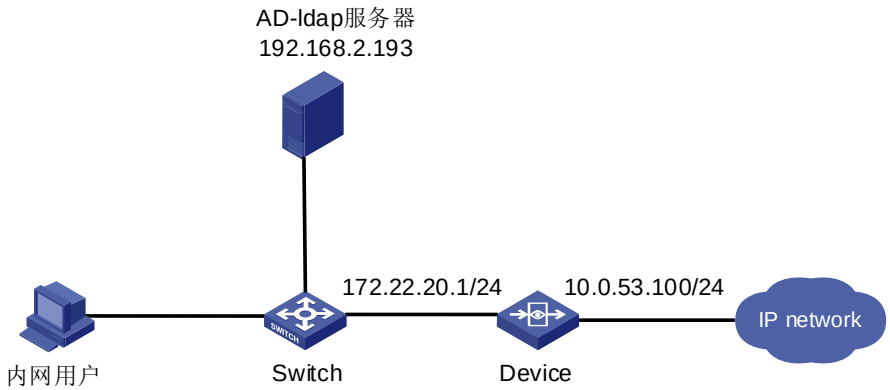


4 LDAP 使用通用名标识 CN 认证配置举例

4.1 组网需求

如图 7 所示，在公司内网搭建有 LDAP 服务器，LDAP 服务器上用户是以标识名的方式进行创建的，要求内网用户使用 AD-ldap 服务器同步下来的用户进行认证后上网。

图7 LDAP 组网图



4.2 配置思路

按照组网图组网。

(1) 新建 LDAP 服务器,通用名标识为 cn；

(2) 新建 LDAP 同步，并同步用户；

(3) 全局配置启用第三方认证选择 ldap 服务器；

(4) 新建用户认证策略。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

(1) 新建 LDAP 服务器,通用名标识为 cn。

在导航栏中选择“用户管理>认证管理>认证服务器”，单击<新建>按钮，配置 LDAP 服务器，如图 8 所示。

图8 标识为为 CN 的 LDAP 服务器配置

配置完成后如下图 9 所示。

图9 LDAP 服务器配置效果图

(2) 新建 LDAP 同步。

在导航栏中选择“用户管理>用户同步”，单击<新建>按钮，配置 LDAP 同步，如图 10 所示。

图10 LDAP 同步配置

(3) 全局配置启用第三方认证选择 ldap 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，如图 11 所示。

图11 全局模式启用第三方 Ldap 配置效果图

(4) 新建用户认证策略

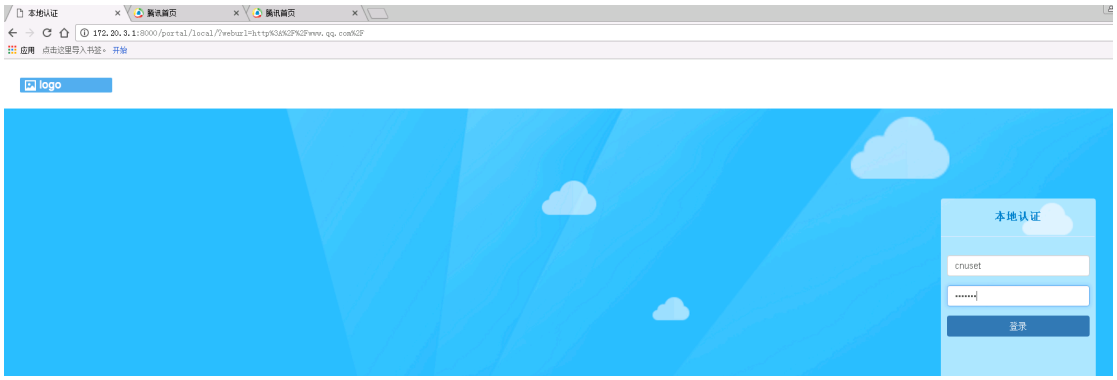
在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 12 所示。

图12 用户认证策略配置效果图

4.5 验证配置

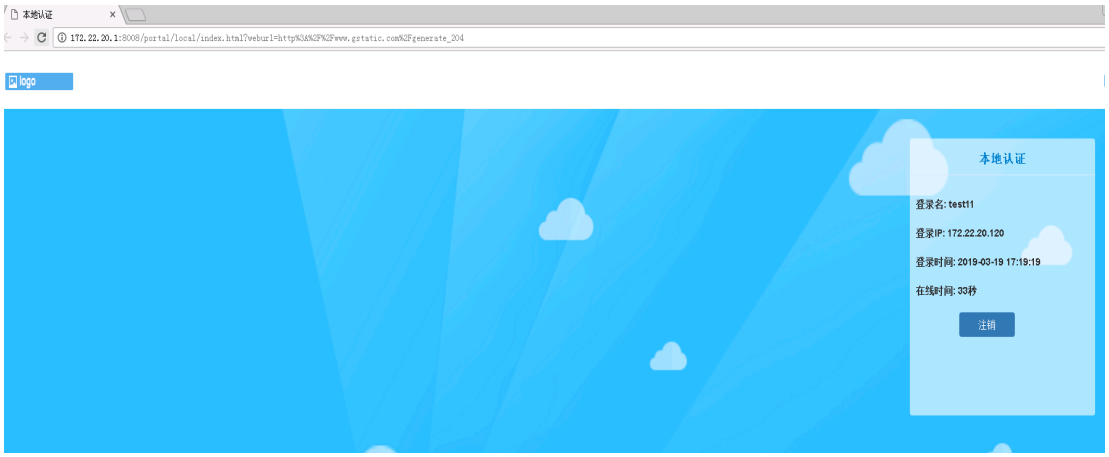
如图 13 所示，访问 www.qq.com，设备弹出本地认证界面。输入 LDAP 同步下来的用户名和密码进行认证。

图13 PC 访问网页弹出本地认证页面，后使用同步下来的 LDAP 用户进行认证。



如图 14 所示，通用名标识为 CN 的 LDAP 认证效果图。

图14 认证成功效果图

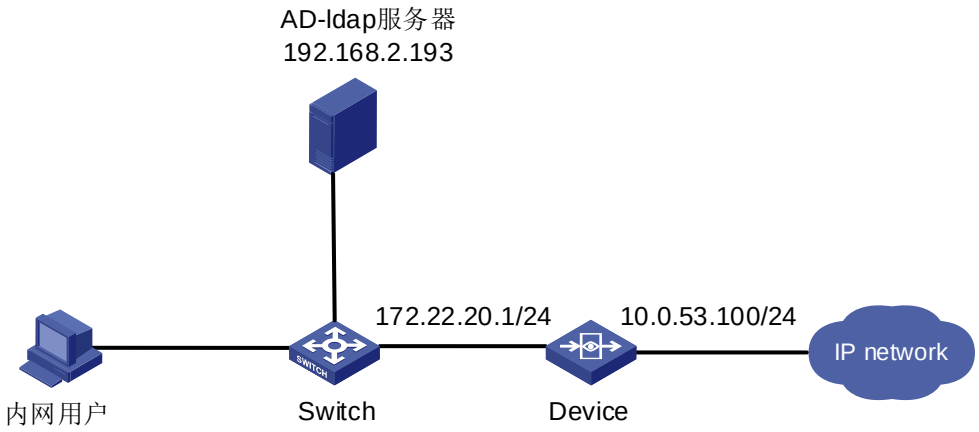


5 LDAP 使用通用名标识 sAMAccountName 认证配置举例

5.1 组网需求

如图 15 所示，在公司内网搭建有 LDAP 服务器，LDAP 服务器上用户是以用户登录名的方式进行创建的，要求内网用户使用 AD-ldap 服务器同步下来的用户进行认证后上网。

图15 LDAP 组网图



5.2 配置思路

按照组网图组网。

(1) 新建 LDAP 服务器,通用名标识为 sAMAccountName；

(2) 新建 LDAP 同步，并同步用户；

(3) 全局配置启用第三方认证选择 ldap 服务器；

(4) 新建用户认证策略。

5.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置设备

(1) 新建 LDAP 服务器，通用名称标识为 sAMAccountName，并同步。

在导航栏中选择“用户管理>认证管理>认证服务器”，选择“新建 LDAP 服务器”，如图 16 所示。

图16 标识名为 sAMAccountName 的 LDAP 服务器配置

配置完成后如图 17 所示。

图17 LDAP 服务器配置效果图

(2) 新建 LDAP 同步

在导航栏中选择“用户管理>用户同步”，选择“新建> LDAP 同步”，配置 LDAP 同步，如图 18 所示。

图18 LDAP 同步

(3) 全局模式启用第三方 ldap 配置

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，，如图 19 所示。

图19 启用第三方 ldap 配置界面

(4)　新建用户认证策略

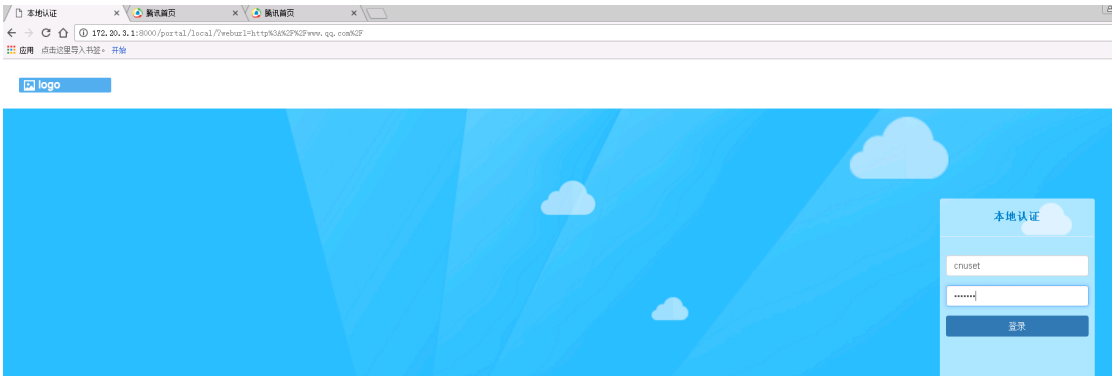
在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 20 所示。

图20 用户认证策略配置效果图

5.5 验证配置

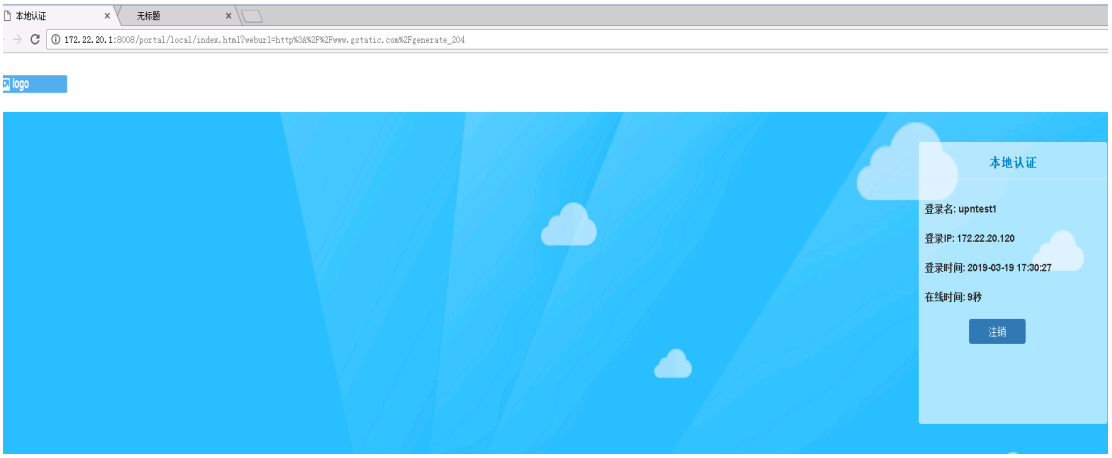
如图 21 所示，访问 www.qq.com，设备弹出本地认证界面。输入 LDAP 同步下来的用户名和密码进行认证。

图21 PC 访问网页弹出本地认证页面，后使用同步下来的 LDAP 用户进行认证。



如图 22 所示，通用名标识为 sAMAccountName 的 LDAP 认证效果图。

图22 认证成功效果图

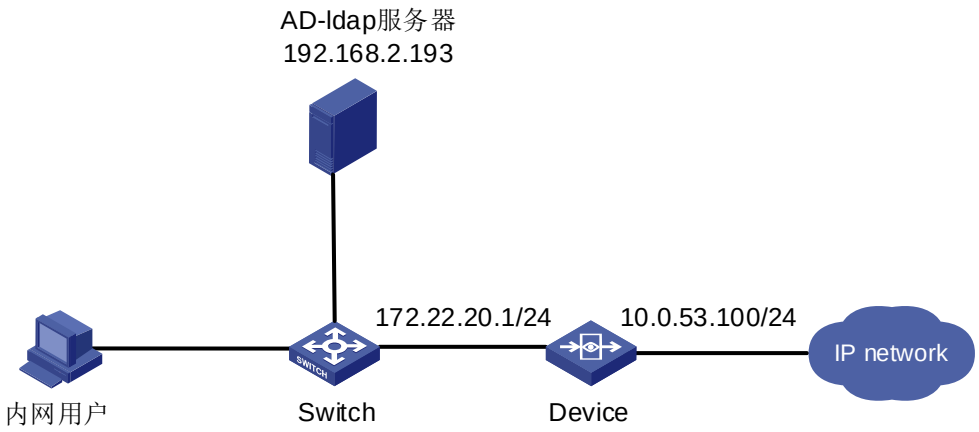


6 LDAP 控制认证用户名是否区分大小写配置举例

6.1 组网需求

如图 23 所示，在公司内网搭建有 LDAP 服务器，LDAP 服务器上用户是以用户登录名的方式进行创建的，要求内网用户使用 AD-ldap 服务器同步下来的用户进行认证后上网，启用 ldap 控制用户名不区分大小写认证。

图23 LDAP 组网图



6.2 配置思路

按照组网图组网。

(1) 新建 LDAP 服务器,通用名标识为 sAMAccountName，并同步。

(2) 新建 LDAP 同步，并同步用户。

(3) 全局配置启用第三方认证选择 ldap 服务器。

(4) 新建用户认证策略。

(5) 启用 ldap 认证用户不区分大小写。

6.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

6.4 配置步骤

6.4.1 配置设备

(1) 新建 LDAP 服务器,通用名标识为 sAMAccountName

在导航栏中选择“用户管理>认证管理>认证服务器”，单击<新建>按钮，配置 LDAP 服务器，如图 24 所示。

图24 显示名为 sAMAccountName 的 LDAP 服务器配置

配置完成后如图 25 所示。

图25 LDAP 服务器配置效果图

(2) 新建 LDAP 同步，并同步用户。

在导航栏中选择“用户管理>用户同步”，选择“新建> LDAP 同步”，配置 LDAP 同步，如图 26 所示。

图26 LDAP 同步

(3) 全局配置启用第三方认证选择 ldap 服务器

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，如图 27 所示。

图27 启用第三方 ldap 配置界面

(4)　新建用户认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 28 所示。

图28 用户认证策略配置效果图

(5)　启用 LDAP 认证用户名不区分大小写，如图 29 所示。

图29 LDAP 认证用户名不区分大小写配置图

```
Host(config)# ldap-auth easy-name-match
  disable  Disable
  enable   Enable
Host(config)# ldap-auth easy-name-match enable
Host(config)#
```

说明

默认情况下设备认证过程中用户名称不区分大小写，而 LDAP 服务器在检验用户名时不区分大小写，如在 LDAP 服务器上配置用户名为 aaa，用户在认证时输入 AAA，也可以认证通过，但在设备侧上线时记录的用户名是 AAA，由于设备从 LDAP 服务器同步下来的用户名是 aaa，其它策略在调用 aaa 做控制后，由于上线时的用户为 AAA，导致策略无法匹配上，为了解决这一问题，设备侧开启认证用户名称区分大小写，即使用户输入了 AAA，上线时也会显示为 aaa，与本地存的用户名一模一样，保证了后续用户对象正常匹配。

6.5 验证配置

PC 访问网页弹出本地认证页面，后使用同步下来的 LDAP 用户进行认证。（原同步下来的用户为 upntest1，启用 ldap 认证用户名区分大小写后，认证用户名输入 UPNtest1 进行认证）

(1)　关闭 LDAP 认证用户区分大小写

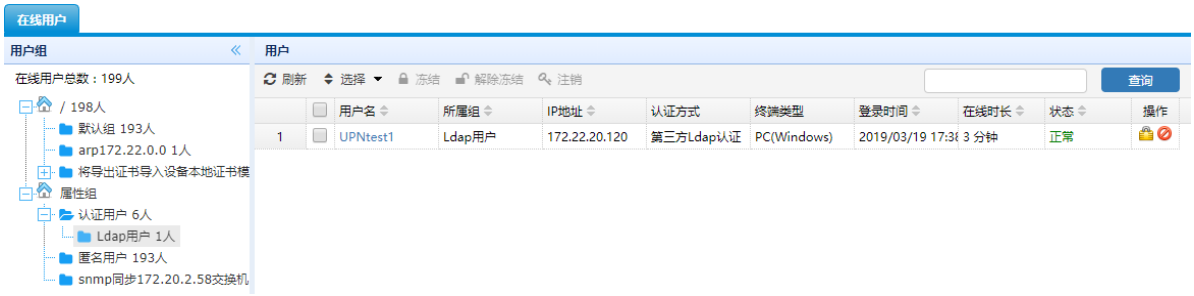
```
[redacted]WD-D(config)# display ldap-auth easy-name-match switch
ldap-auth easy-name-match disable
```

关闭 ldap 认证用户名区分大小写，认证页面显示如图 30 所示。

图30 登录页面

关闭 ldap 认证用户名区分大小写，设备在线用户显示如图 31 所示。

图31 在线用户页面



(2) 开启 LDAP 认证用户区分大小写

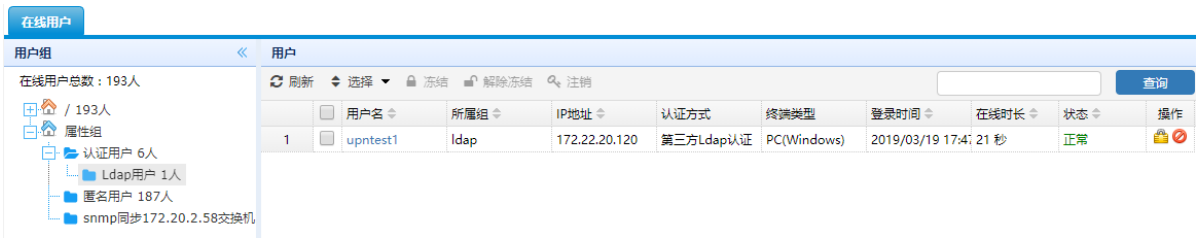
```
[redacted](config)# ldap-auth easy-name-match enable
[redacted](config)#  display ldap-auth easy-name-match switch
ldap-auth easy-name-match enable
```

开启 ldap 认证用户名区分大小写，认证页面显示如图 32 所示。

图32 登录页面

开启 ldap 认证用户名区分大小，设备在线用户显示如图 33 所示。

图33 在线用户页面

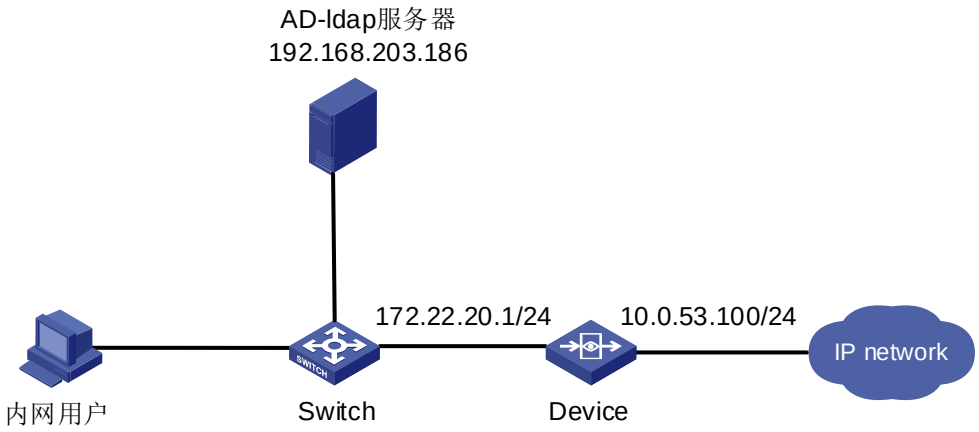


7 LDAP 使用同步安全组认证配置举例

7.1 组网需求

如图 34 所示，在公司内网搭建有 LDAP 服务器，LDAP 服务器上用户是以标识名的方式进行创建的，要求内网用户使用 AD-ldap 服务器上安全组下的用户进行认证后上网。

图34 LDAP 组网图



7.2 配置思路

按照组网图组网。

(1) 新建 LDAP 服务器；

(2) 新建 LDAP 同步，同步类型为按安全组同步，并同步用户；

(3) 全局配置启用第三方认证选择 ldap 服务器；

(4) 新建用户认证策略。

7.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

7.4 配置步骤

7.4.1 配置设备

(1) 新建 LDAP 服务器，通用名称标识为 cn。

在导航栏中选择“用户管理>认证管理>认证服务器”，选择“新建>LDAP 服务器”，配置 LDAP 服务器，如图 35 所示。

图35 标识名为 cn 的 LDAP 服务器配置

(2) 新建 LDAP 同步，同步类型为按安全组同步。

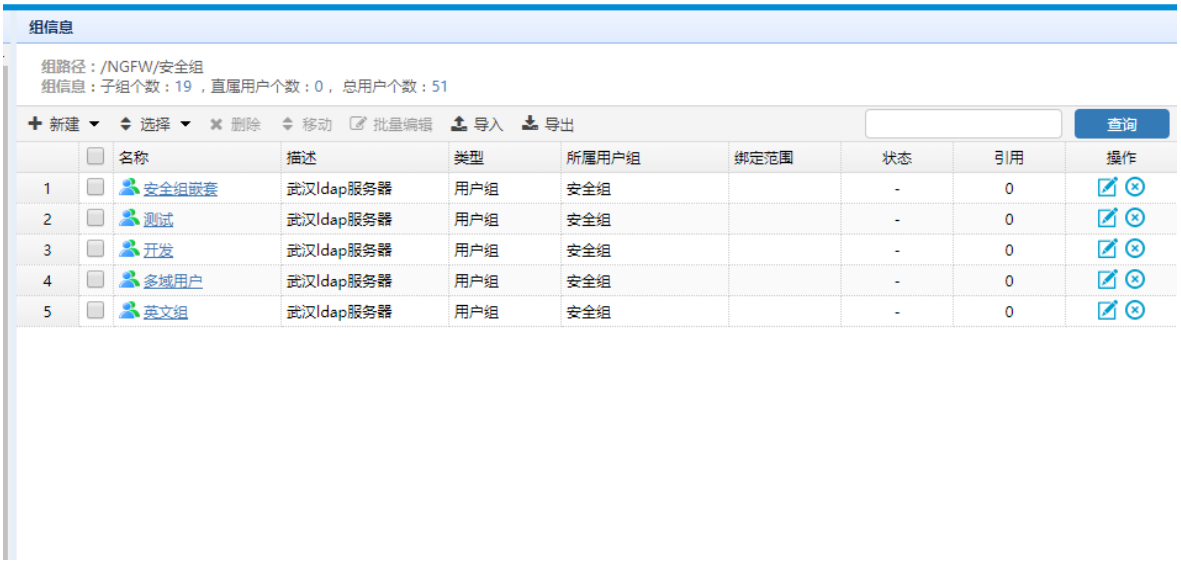
在导航栏中选择“用户管理>用户同步”，选择“新建> LDAP 同步”，配置 LDAP 同步，如图 36 所示。

图36 LDAP 同步

(3) 查看 LDAP 同步用户

在导航栏中选择“用户管理>用户组织结构”，查看 LDAP 同步用户,如图 37 所示。

图37 LDAP 同步的用户



(4) 全局模式启用第三方 ldap 配置

在导航栏中选择“用户管理>认证管理>高级选项”，进入全局配置页面，启用第三方认证选择 Ldap 服务器，如图 38 所示。

图38 全局模式配置效果图

(5) 新建用户认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入用户认证策略的配置页面，单击<新建>按钮，配置认证策略，如图 39 所示。

图39 用户认证策略配置效果图

2. 验证配置效果

如图 40 所示，PC 访问 www.qq.com，弹出本地认证界面。输入 LDAP 同步下来的安全组用户的用户名和密码进行认证。

图40 PC 访问网页弹出本地认证页面，后使用同步下来的 LDAP 安全组用户进行认证。

如图 41 所示，安全组用户的 LDAP 认证效果图。

图41 认证成功效果图

目 录

1 简介

本文档介绍设备的访客二维码认证功能配置举例，在配置前，先了解如下定义：

- 审核人：指定用户或用户组（此用户必须是已认证上线用户）作为审核人，二维码认证用户需要审核人扫码二维码来完成上网认证。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

- 本文档假设您已了访客二维码认证特性。

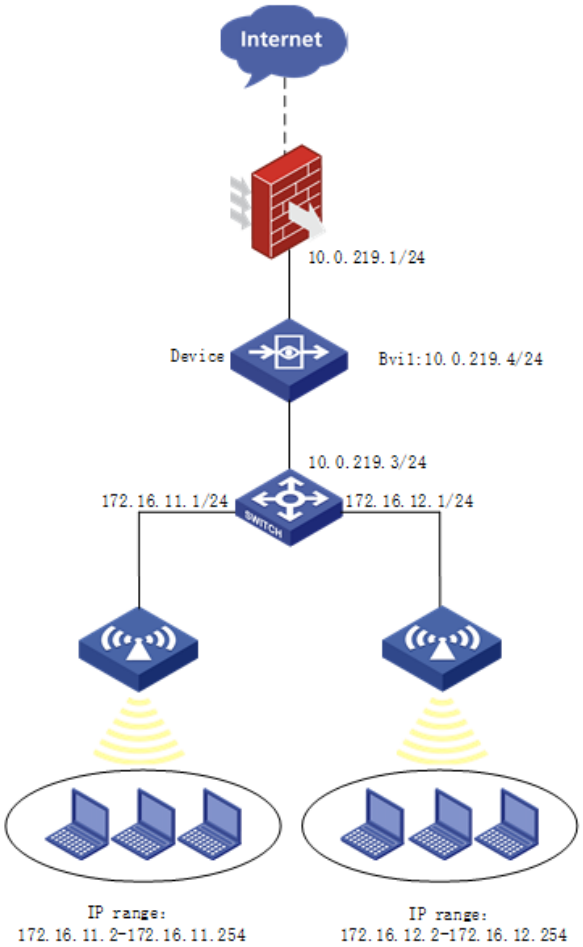
3 访客二维码认证功能配置举例

3.1 组网需求1：透明桥组网

3.1.1 组网需求

如图 1 所示，某公司无线访客用户网段 IP 地址 172.16.11.0/24，无线办公用户网段 IP 地址 172.16.12.0/24，其中 172.16.11.1/24 作为无线访客用户的网关，172.16.12.1/24 作为无线办公用户的网关。三层设备交换机上开启 DHCP，地址池分别为 172.16.11.2/24~172.16.11.254/24、172.16.12.2/24~172.16.12.254/24。使用设备的 ge0 和 ge1 接口作为透明桥，串接部署在网络中，设备上联出口 FW，下联三层交换机。设备上开启访客二维码认证功能，访客用户通过访客二维码认证后才能访问网络。

图1 访客二维码认证透明桥组网图



3.1.2 配置思路

- 配置访客二维码认证功能。
- 配置本地认证功能。

3.1.3 使用版本

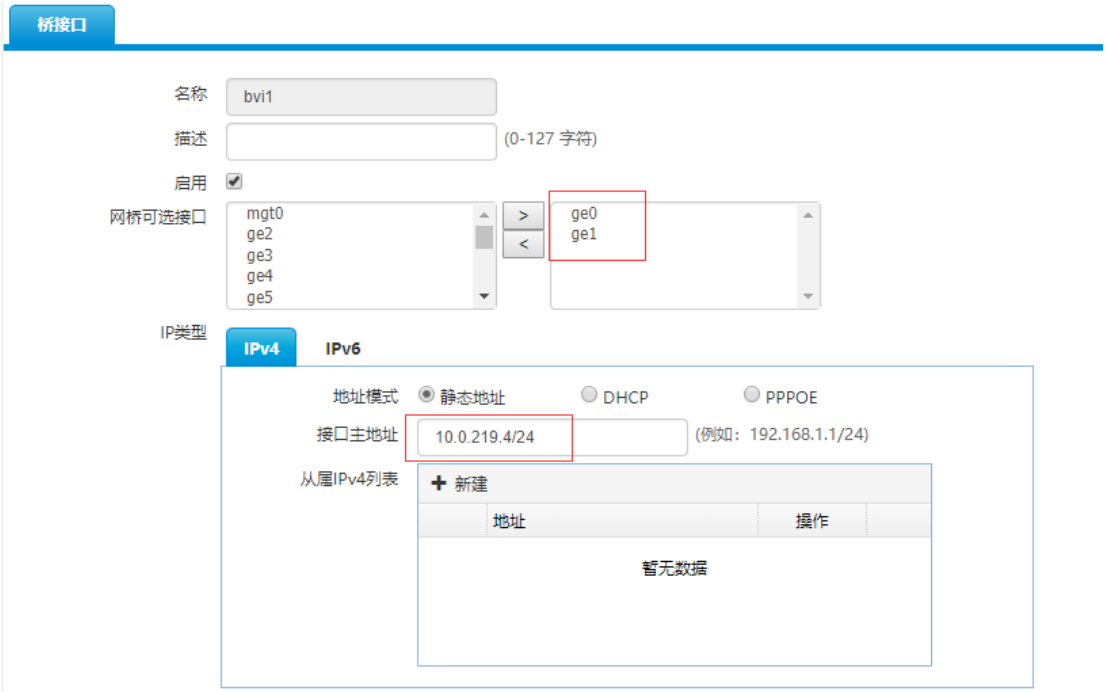
本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

1. 配置网桥接口

如图 2 所示，进入“网络配置>接口配置>网桥接口”页面，点击<新建>按钮创建网桥接口 bvi1，把 ge0、ge1 加入网桥，配置接口地址为 10.0.219.4/24。

图2 配置网桥接口



2. 配置静态路由

如图 3 配置访问外网的默认路由及去往认证用户网段 172.16.11.0/24，172.16.12.0/24 的路由。

图3 配置静态路由

	目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	操作
1	0.0.0.0	0.0.0.0	10.0.219.1	bvi1	1	1	-		
2	172.16.11.0	255.255.255.0	10.0.219.3	bvi1	1	1	-		
3	172.16.12.0	255.255.255.0	10.0.219.3	bvi1	1	1	-		

3. 配置地址对象

如图 4 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”页面，点击<新建>按钮创建无线访客用户、无线办公用户地址对象，地址分别为 172.16.11.0/24 和 172.16.12.0/24，点击<提交>。

图4 配置认证用户地址对象

如图 5 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”页面，点击<新建>按钮创建内网用户地址对象，地址为 172.16.11.0/24 和 172.16.12.0/24，点击<提交>。

图5 配置内网用户地址对象

4. 配置本地用户

如图 6 所示，进入“用户管理>用户组织结构”页面，新建用户，用于无线办公用户进行本地认证。

图6 新建用户

5. 配置访客二维码认证参数

如图 7 所示，进入“用户管理 > 认证管理 > 认证方式 > 访客二维码认证 ”页面，配置访客二维码认证参数。

图7 访客二维码认证配置

6. 配置本地认证策略

如图 8 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge0，源地址选择“无线办公用户”，认证方式使用“本地认证”，提交策略。

图8 本地认证策略配置页面

7. 配置访客二维码认证策略

如图 9 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge0，源地址选择“无线访客用户”，认证方式使用“访客二维码认证”，提交策略。

图9 访客二维码认证认证策略配置页面

8. 配置用户识别范围

如图 10所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“内网用户”，其它配置默认，提交配置。

图10 用户识别范围

3.1.5 配置注意事项

- 三层交换机需要开启 DHCP 功能，地址池范围为 172.16.11.2/24~172.16.11.254/24。172.16.12.2/24~172.16.12.254/24。
- 认证用户网段必须在用户识别范围中，否则导致不能正常认证。

3.1.6 验证配置

如图 11 所示，无线访客用户访问网页上网时，浏览器弹出 portal 页面。

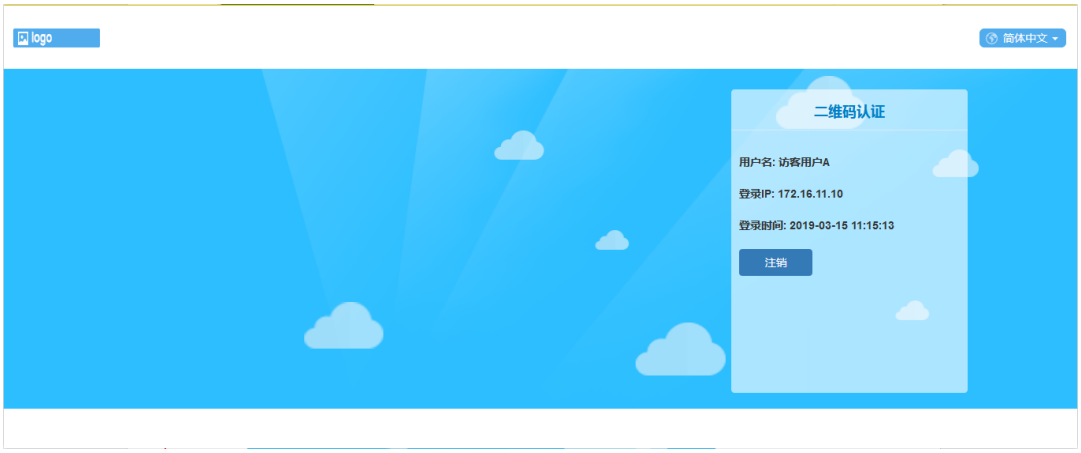
图11 认证 portal 页面

如图 12 所示，无线办公用户的手机通过本地认证上网后，可以通过手机扫一扫功能，扫描二维码认证中二维码图，会在手机上弹出审核页面，输入用户名后，点击确认，二维码用户即可认证成功。

图12 审核页面

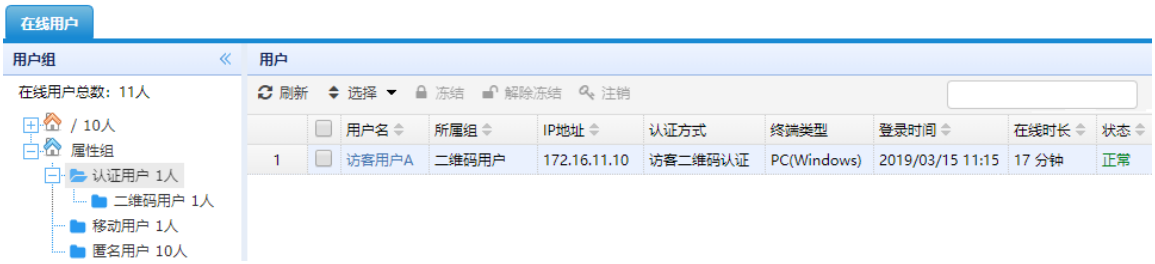
如图 13 所示，审核通过后二维码认证页面可自动跳到认证成功。（点击完成按钮，可以跳转到所访问的 web 页面，如果配置了重定向 url，那就跳转到重定向 url 页面）

图13 认证成功



如图 14 所示，在“数据中心>系统监控>在线用户”页面，查看到该用户已认证成功。

图14 在线用户

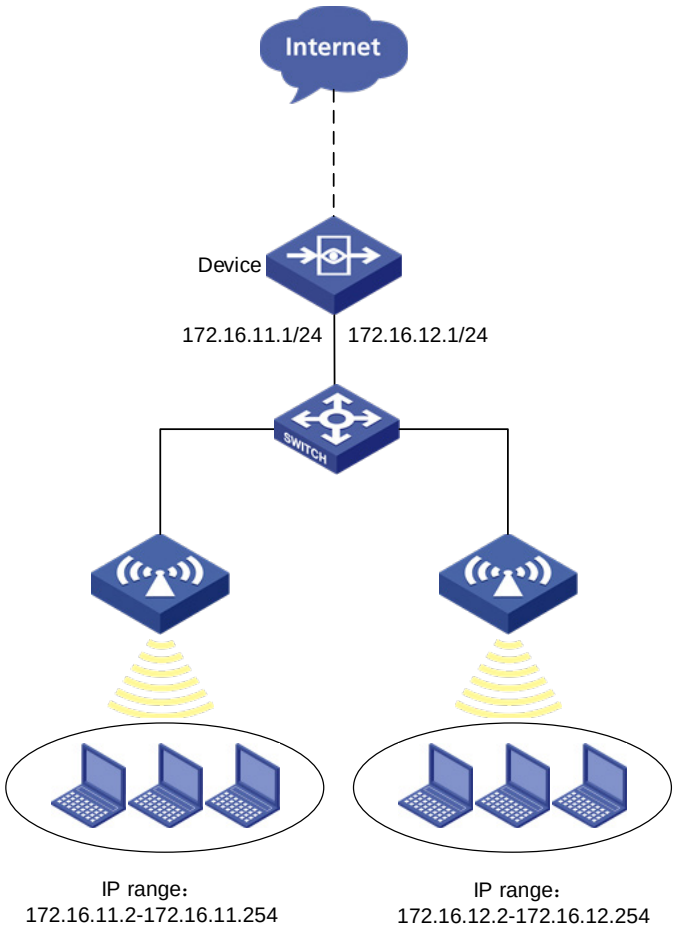


3.2 组网需求2：路由模式组网

3.2.1 组网需求

如图 15 所示，某公司无线访客用户网段 IP 地址 172.16.11.0/24，无线办公用户网段 IP 地址 172.16.12.0/24，其中 172.16.11.1/24 作为无线访客用户的网关，172.16.12.1/24 作为无线办公用户的网关。三层设备交换机上开启 DHCP，地址池分别为 172.16.11.2/24~172.16.11.254/24、172.16.12.2/24~172.16.12.254/24。使用设备的的 ge0 和 ge1 接口以三层路由模式部署在网络中，设备作为出口网关设备，下联二层交换机。设备上开启访客二维码认证功能，用户通过访客二维码认证后才能上网。

图15 访客二维码认证路由模式组网图



3.2.2 配置思路

- 配置访客二维码认证功能。
- 配置本地认证功能。

3.2.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.2.4 配置步骤

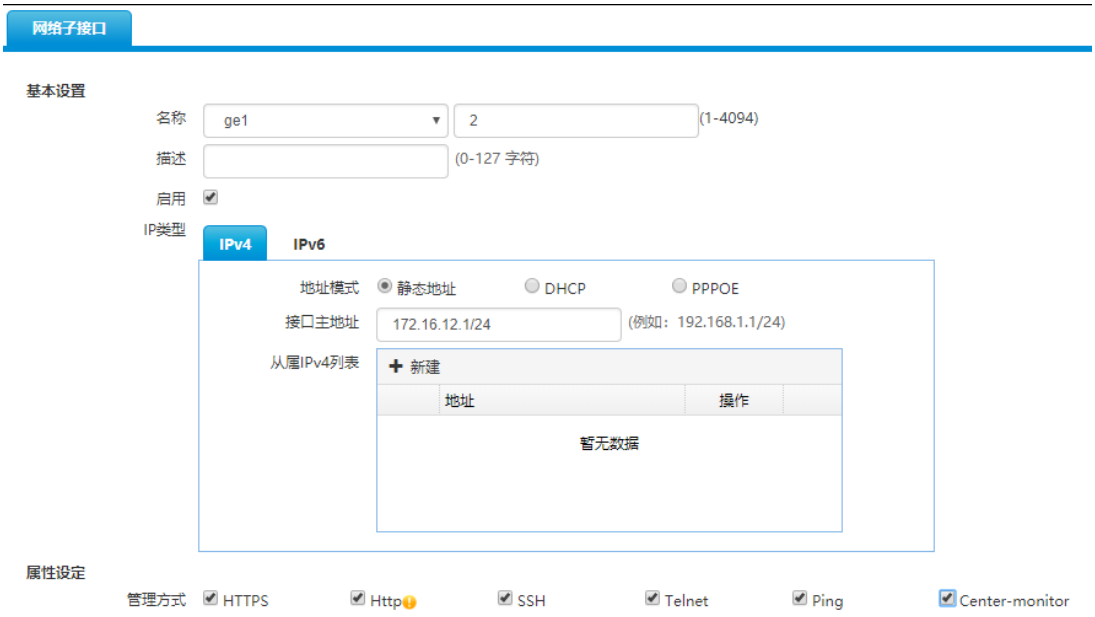
1. 配置路由接口

如图 16、图 17、图 18 所示，进入“网络配置>接口配置”页面，点击编辑 ge0 操作，把 ge0 的地址配置为 10.0.219.3/24。进入“网络配置>接口配置>子接口”页面，新建 ge1.1、ge1.2 子接口，把 ge1.1 和 ge1.2 的地址分别配置为 172.16.11.1/24 和 172.16.12.1/24。

图16 配置 ge0 接口

图17 配置 ge1.1 子接口

图18 配置 ge1.2 子接口



2. 配置静态路由

如图 19 配置访问外网的默认路由。

图19 配置静态路由

3. 配置对象

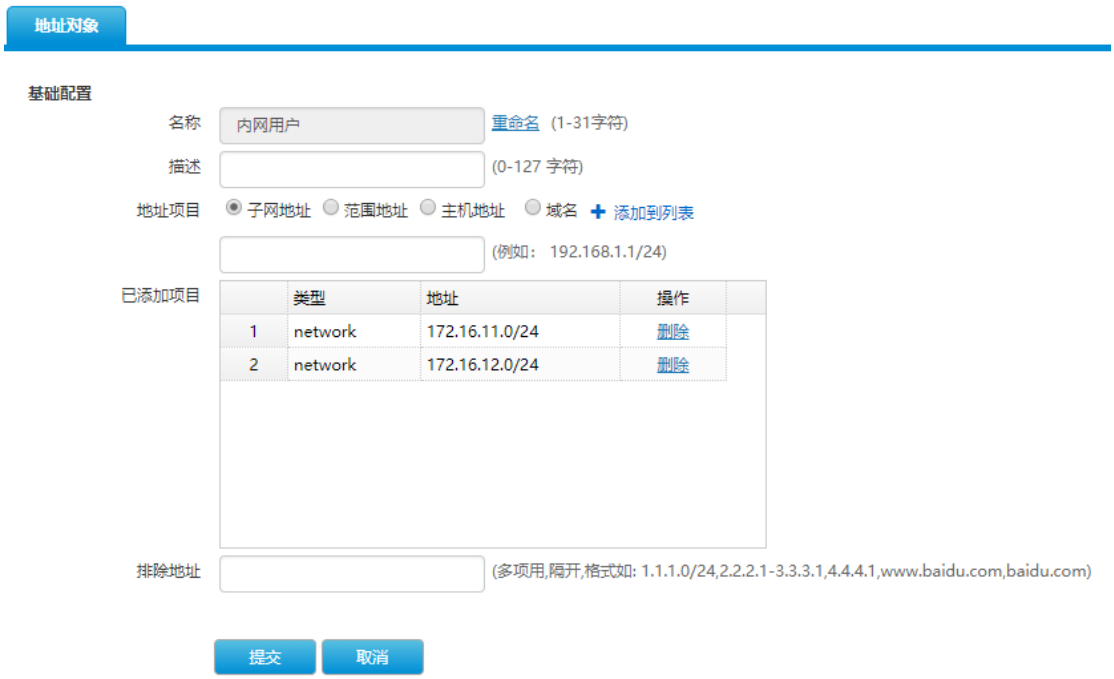
如图 20、图 21 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”页面，点击<新建>按钮创建无线访客用户、无线办公用户地址对象，分别地址为 172.16.11.0/24 和 172.16.12.0/24，点击<提交>。

图20 配置无线访客用户地址对象

图21 配置无线办公用户地址对象

如图 22 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”页面，点击<新建>按钮创建内网用户地址对象，地址为 172.16.11.0/24 和 172.16.12.0/24，点击<提交>。

图22 配置内网用户地址对象



4. 配置访客二维码认证参数

如图 23所示，进入“用户管理 > 认证管理 > 认证方式 > 访客二维码认证 ”页面，配置访客二维码认证参数。

图23 访客二维码认证配置

5. 配置本地认证策略

如图 24 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge1.2，源地址选择“无线办公用户”，认证方式使用“本地认证”，提交策略。

图24 本地认证策略页面

6. 配置访客二维码认证策略

如图 25 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，源接口选择内网口 ge1.1，源地址选择“无线访客用户”，认证方式使用“访客二维码认证”，提交策略。

图25 二维码认证策略页面

7. 配置用户识别范围

如图 26所示，进入“用户管理>认证管理>高级选项”页面，识别范围选择“内网用户”，其它配置默认，提交配置。

图26 用户识别范围

8. 配置源 NAT

如图 27 所示，进入“策略配置>NAT 转换策略”页面，在源 NAT 页面创建策略，接口选择 ge0，其它配置默认，提交配置。

图27 配置源 NAT

3.2.5 配置注意事项

- 设备或二层交换机上需要开启 DHCP 功能，地址池范围为：172.16.11.2/24~172.16.11.254/24。172.16.12.2/24~172.16.12.254/24。
- 认证用户网段必须在用户识别范围中，否则会导致不能正常认证。

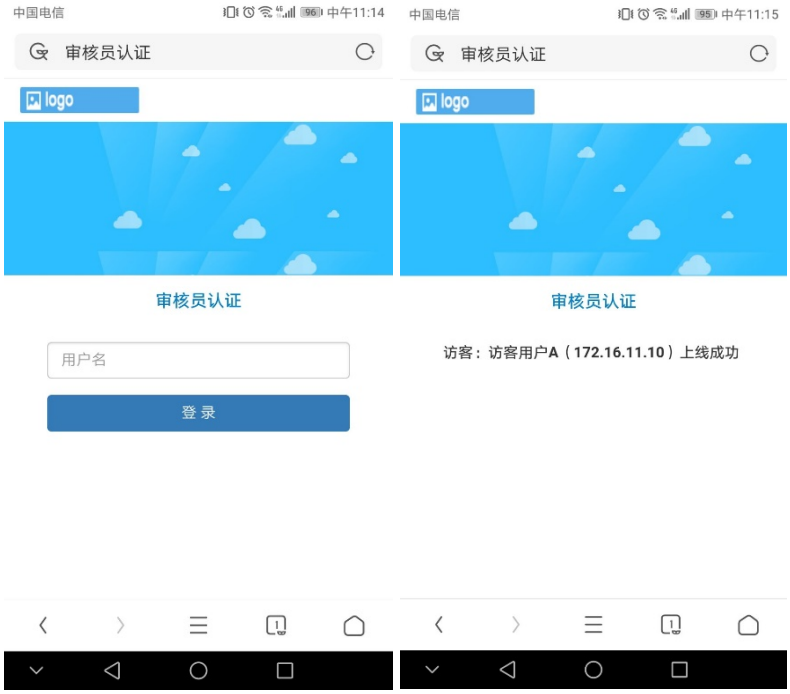
3.2.6 验证配置

如图 28 所示，终端访问网页上网时，浏览器弹出 portal 页面。

图28 认证 portal 页面

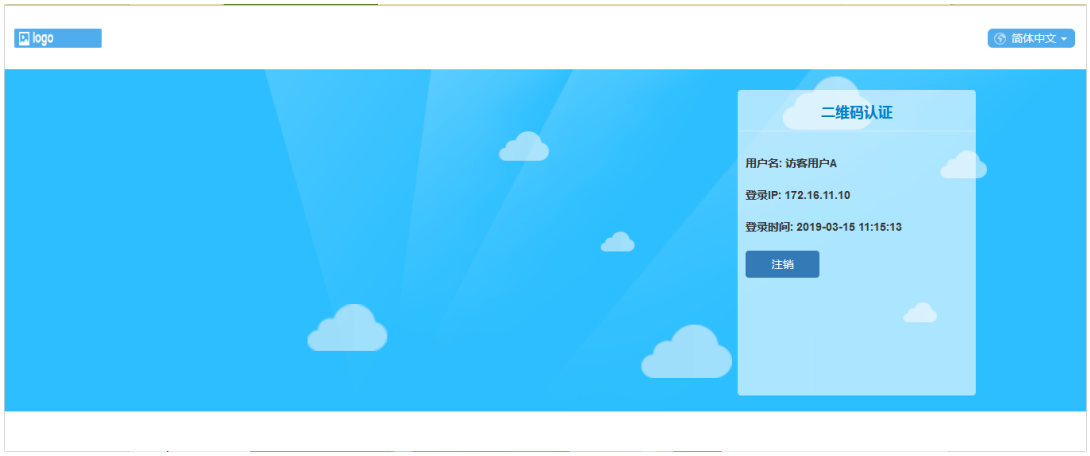
如图 29 所示，无线办公用户的手机通过本地认证上网后，可以通过手机扫一扫功能，扫描二维码认证中二维码图，会在手机上弹出审核页面，输入用户名后，点击确认，二维码用户既可以审核成功。

图29 审核页面



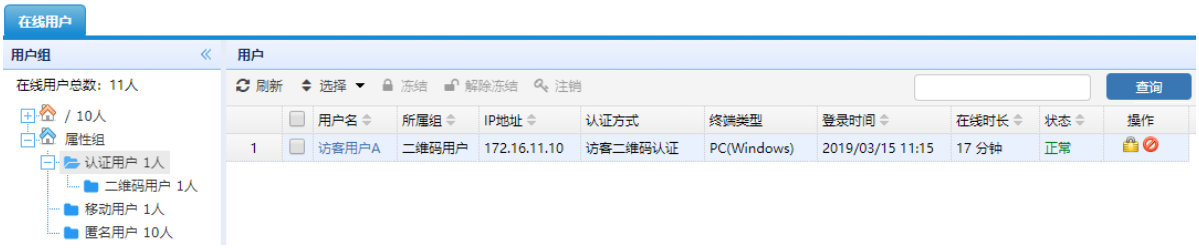
如图 30 所示，审核通过后二维码认证页面可自动跳到认证成功（点击完成按钮，可以跳转到所访问的 web 页面，如果配置了重定向 url，那就跳转到重定向 url 页面）。

图30 二维码认证成功



如图 31 所示，在“数据中心>系统监控>在线用户”页面，可查看该用户已认证成功。

图31 在线用户


在线用户
用户组
在线用户总数：11人
/ 10人
属性组
认证用户 1人
二维码用户 1人
移动用户 1人
匿名用户 10人
用户
刷新
选择
冻结
解除冻结
注销
查询
用户名
所属组
IP地址
认证方式
终端类型
登录时间
在线时长
状态
操作
1
访客用户A
二维码用户
172.16.11.10
访客二维码认证
PC(Windows)
2019/03/15 11:15
17 分钟
正常

目 录

1 简介

本文档介绍设备的虚拟网线 Web 认证功能配置举例，在配置前，先了解如下定义：

- 虚拟网线：虚拟网线免去了 MAC 学习和二层交换，相比于传统的桥接方式效率更高。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

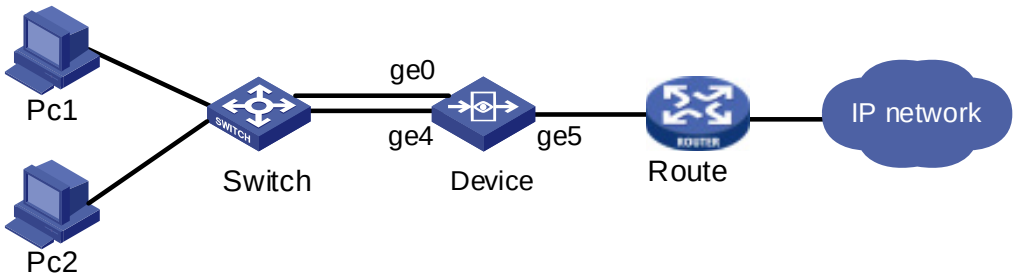
- 本文档假设您已了解虚拟网线和 Web 认证特性。

3 虚拟网线 Web 认证功能配置举例

3.1 组网需求

如图 1 所示，某公司原有网络为二层交换机连接路由器访问互联网，使用虚拟网线方案新增设备部署，用于对内网用户进行认证，认证后才能访问互联网。

图1 虚拟网线 Web 认证组网图



3.2 配置思路

- 配置 ge0 口管理 IP
- 配置 ge4 和 ge5 为虚拟网线
- 配置 Web 认证

3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.4 配置步骤

(1) 配置 ge0 接口 IP

如图 2 所示，进入“网络配置>接口配置>物理接口”页面，点击 ge0 口后面的<编辑>按钮，配置接口地址为 192.168.1.254/24。

图2 配置接口

(2) 配置虚拟网线

如图 3 所示，进入“网络配置>接口配置>虚拟网线”页面，点击<新建>按钮，配置接口 ge4、ge5 为虚拟网线。

图3 配置虚拟网线

(3) 配置本地用户

如图 4 所示，进入“用户管理>用户组织结构”页面，新建用户，用于用户进行 Web 认证。

图4 新建用户

(4) 配置本地认证策略

如图 5 所示，进入“用户管理>认证管理>认证策略”页面，选择新建认证策略，认证方式使用“Web 认证”，提交策略。

图5 认证策略页面

3.5 配置注意事项

- 虚拟网线无法配置 IP，需要有单独接口配置管理 IP。
- 设备管理 IP 需要和认证 PC 可以正常通信，不然会导致认证页面无法打开，用户无法认证上网情况出现。

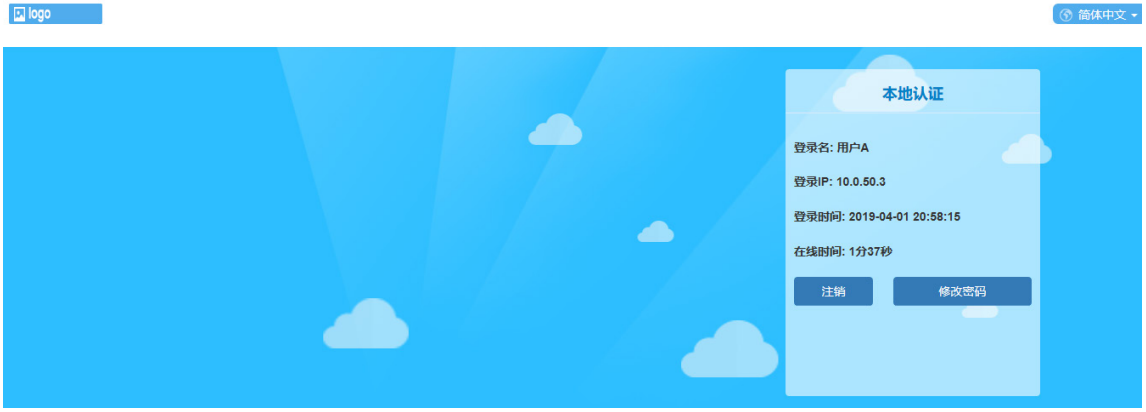
3.6 验证配置

如图 6 所示，用户访问网页上网时，浏览器弹出 portal 页面。

图6　认证 portal 页面

如图 7 所示，输入用户账号密码，点击登录后，用户认证成功。

图7 认证成功

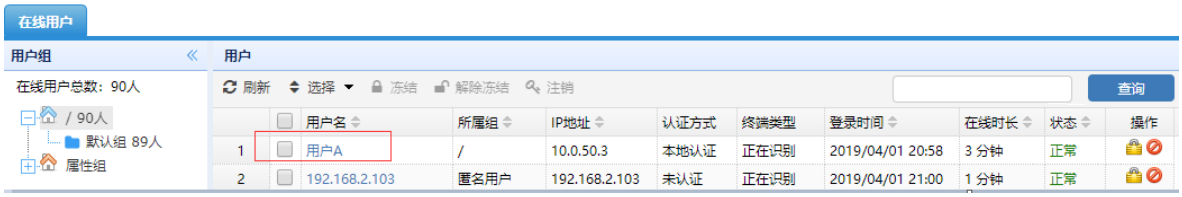


如图 8 所示，自动跳转到认证前访问的 Web 页面（点击完成按钮，可以跳转到所访问的 Web 页面，如果配置了重定向 url，那就跳转到重定向 url 页面）。

图8 自动跳转页面

如图 9 所示，在“数据中心>系统监控>在线用户”页面，查看到该用户已认证成功。

图9 在线用户



目 录

1 简介

本文档介绍设备的 iMC 联动 Portal 认证配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 iMC 联动 Portal 认证特性。

3 使用限制

- iMC 下发用户组信息到设备的时，只支持下发“接入策略”模块中的“下发用户组”参数，而不能支持“用户”模块中的“用户分组”参数。
- 在设备的不参与 Portal 认证的组网模式中，iMC 仅支持将用户组信息发送到一个第三方设备（一个 IP 地址），不支持发送到多个第三方设备。
- 设备的参与 iMC 联动 portal 认证时，只支持认证，不能支持计费相关特性。

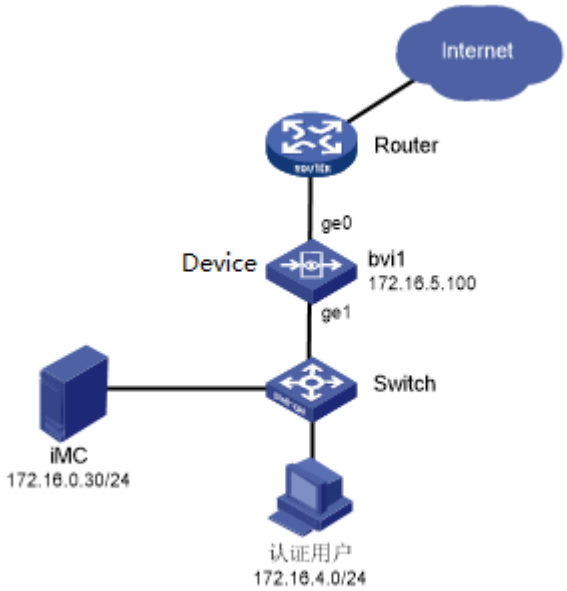
4 IMC 联动认证配置举例

4.1 组网需求

如图 1 所示，某公司对内网用户实行 iMC 联动 Portal 认证上网，认证网段是 172.16.4.0/24。内网 iMC 服务器的 IP 地址为 172.16.0.30/24。使用设备 设备的 ge0 和 ge1 接口透明桥模式部署在网络中，设备 设备的 bvi1 接口地址配置为 172.16.5.100。在设备 设备上配置 iMC 联动 Portal 认证功能。具体要求如下：

- 设备 设备参与 Portal 认证和 Radius 认证，并把所有 iMC 联动 Portal 认证用户加入到用户组“2”中。
- 172.16.4.0/24 网段中的认证用户在认证之前，只允许访问 192.168.3.1 的所有服务和 iMC 服务器，其它访问全部被禁止。
- 172.16.4.0/24 网段中的认证用户在认证之后可以正常访问内网和互联网。

图1 IMC 联动认证功能配置组网图



4.2 配置思路

- 在设备 设备上配置 iMC 对应的 Radius 服务器。
- 在设备 设备上配置 iMC 对应的 Portal 服务器。
- 在设备 设备上配置地址对象，注意在认证目的地址中排除 iMC 服务器地址和 192.168.3.1。
- 在设备 设备上配置用户策略。
- 在设备 设备上配置用户组。
- 配置 iMC 服务器。

4.3 使用版本

本举例是在设备的 E6442、iMC PLAT 7.1 (E0303)、iMC EIA 7.1(E0302P13)和 iMC EIP 7.1 (E0302P13)版本上进行配置和验证的。

4.4 配置注意事项

- 当设备参与 Portal 和 Radius 认证时，iMC 会自动同步用户组信息到设备上，此时 iMC 上无需进行额外配置，设备上需要配置用户组，并确保上述用户组的名称与 iMC 上接入策略中下发用户组的名称保持一致。
- 如果需要实现访问某些资源时免 Portal 认证，需要在对应用户策略的目的地址对象中配置排除地址，将需要免认证访问的 IP 地址排除，其中 iMC 服务器和 Portal 服务器的地址必须排除。目前仅支持排除 IP 地址，不支持排除域名。

4.5 配置步骤

4.5.1 配置设备 产品

1. 配置 iMC 对应的 Radius 服务器

如图 2 所示，进入“用户管理 > 认证管理 > 认证服务器”，点击<新建>，选择<Radius 服务器>，配置“服务器地址”为 172.16.0.30，“服务器密码”和“端口”需要和 iMC 服务器的配置保持一致，点击<提交>。

图2 配置 iMC 对应的 Radius 服务器

如图 3 所示，添加完成的 iMC 服务器配置如下。

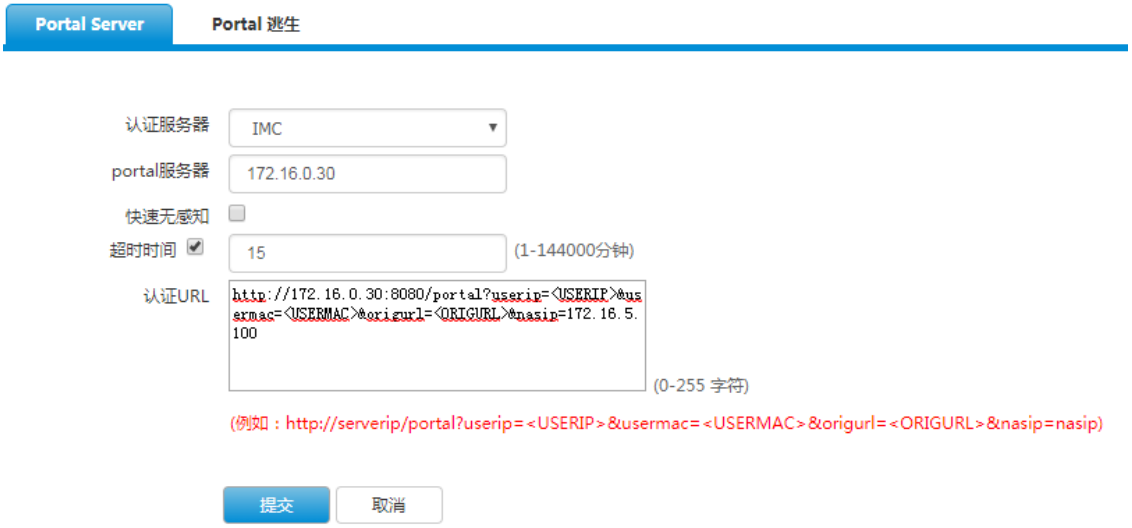
图3 iMC 对应的 Radius 服务器配置完成

2. 配置 iMC 对应的 Portal 服务器

如图 4 所示，进入“用户管理 > 认证管理 > 认证方式 > Portal Server”，“认证服务器”配置为 IMC，“Portal 服务器”配置为 172.16.0.30，“超时时间”保持默认，“认证 URL”将示例中的 serverip 替换为实际地址为：

http://172.16.0.30:8080/portal?userip=<USERIP>&usermac=<USERMAC>&origurl=<ORIGURL>&nasip=172.16.5.100，点击<提交>。

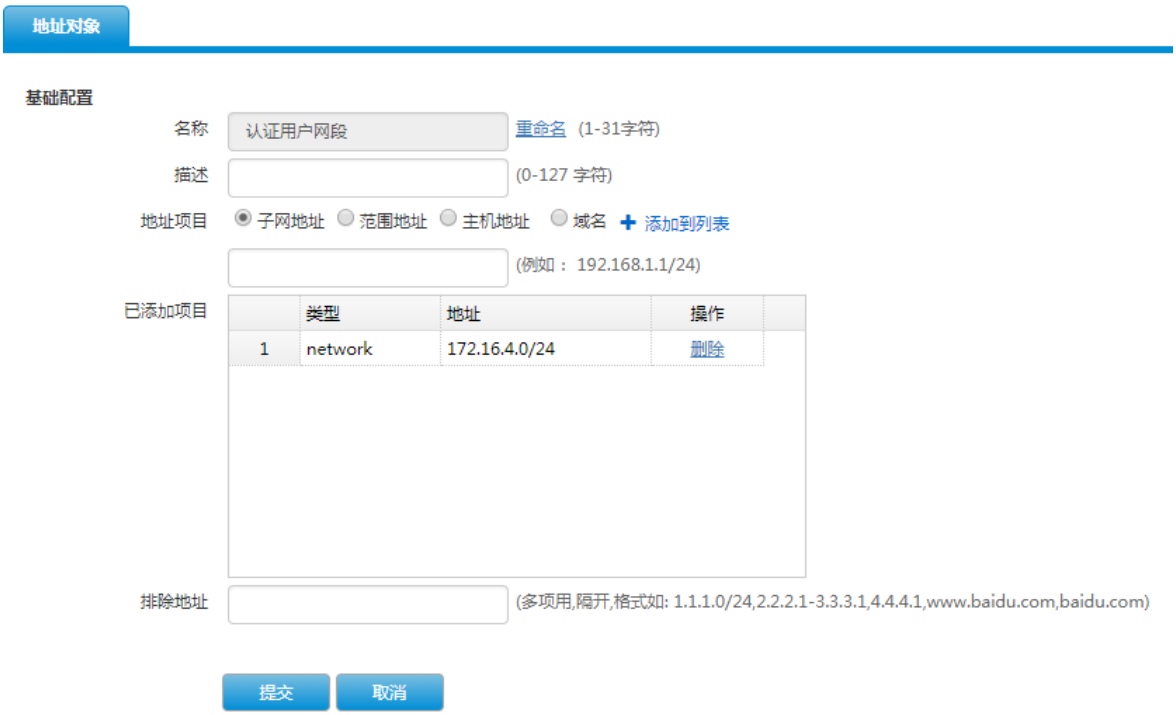
图4 配置 iMC 对应的 Portal 服务器



3. 配置地址对象

如图 5 所示，进入“策略配置 > 对象管理 > 地址对象 > Ipv4 地址对象”，点击<新建>，命名为“认证用户网段”，“地址项目”选为子网地址，配置地址为 172.16.4.0/24，点击<提交>。

图5 配置认证用户网段地址对象



如图 6 所示，进入“策略配置 > 对象管理 > 地址对象 > Ipv4 地址对象”，点击<新建>，命名为“认证目的地址”，“地址项目”选为子网地址，配置地址为 0.0.0.0/0，“排除地址”配置为 172.16.0.30 和 192.168.3.1，点击<提交>。

图6 配置认证目的地址对象

如图 7 所示，添加完成的地址对象配置如下。

图7 地址对象配置完成

4. 配置用户认证策略

如图 8 所示，进入“用户管理 > 认证管理 > 认证策略”，点击<新建>，源地址配置为“认证用户网段”，目的地址配置为“认证目的地址”，相关行为配置为“Portal Server 认证”，其它选项保持默认，点击<提交>。

图8 配置认证策略

如图 9 所示，添加完成的用户策略配置如下。

图9 用户认证策略配置完成

5. 配置用户组

如图 10 所示，进入“用户管理 > 用户组织结构”，点击<新建>，选择<用户组>，命名为“2”，点击<提交>。

图10 配置用户组

如图 11 所示，添加完成的用户组配置如下。

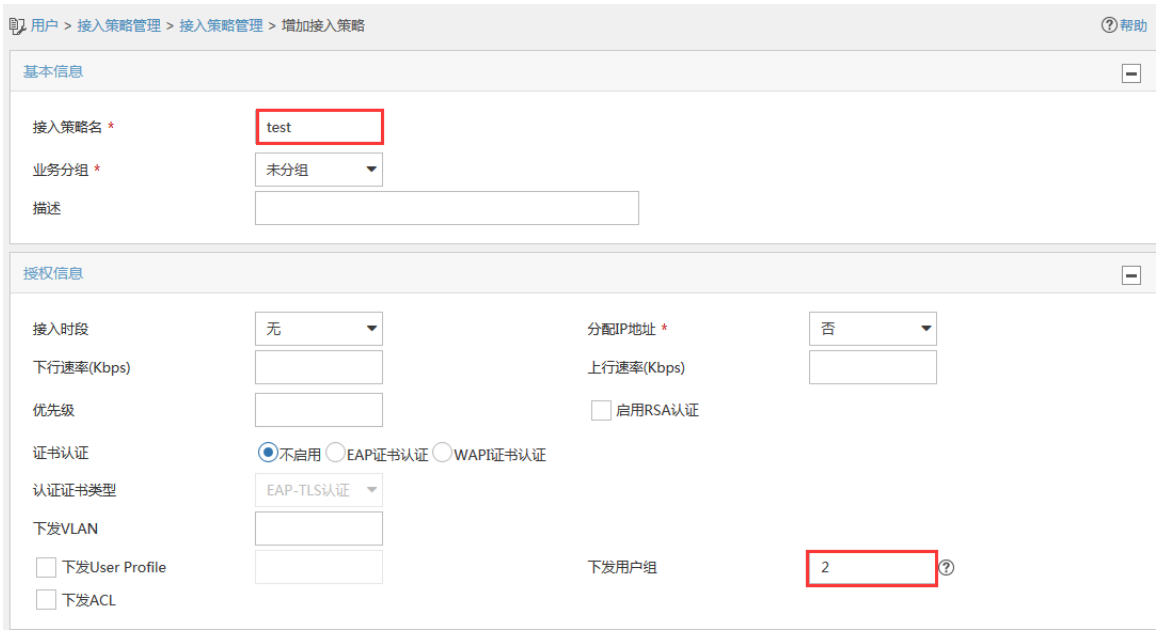
图11 用户组配置完成

4.5.2 配置 iMC 服务器

1. 配置接入策略

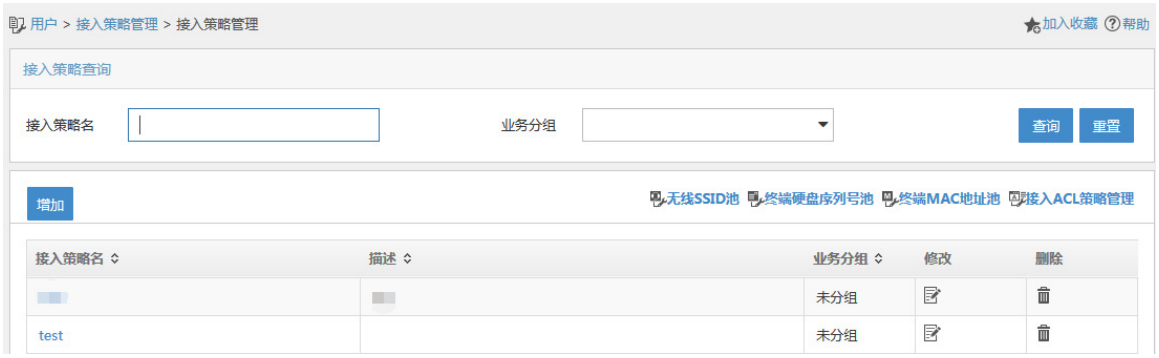
如图 12 所示，进入“用户 > 接入策略管理 > 接入策略管理 > 增加接入策略”，“接入策略名”配置为 test，“下发用户组”配置为 2，其它选项保持默认，点击<确定>。

图12 配置接入策略



如图 13所示，添加完成的接入策略如下。

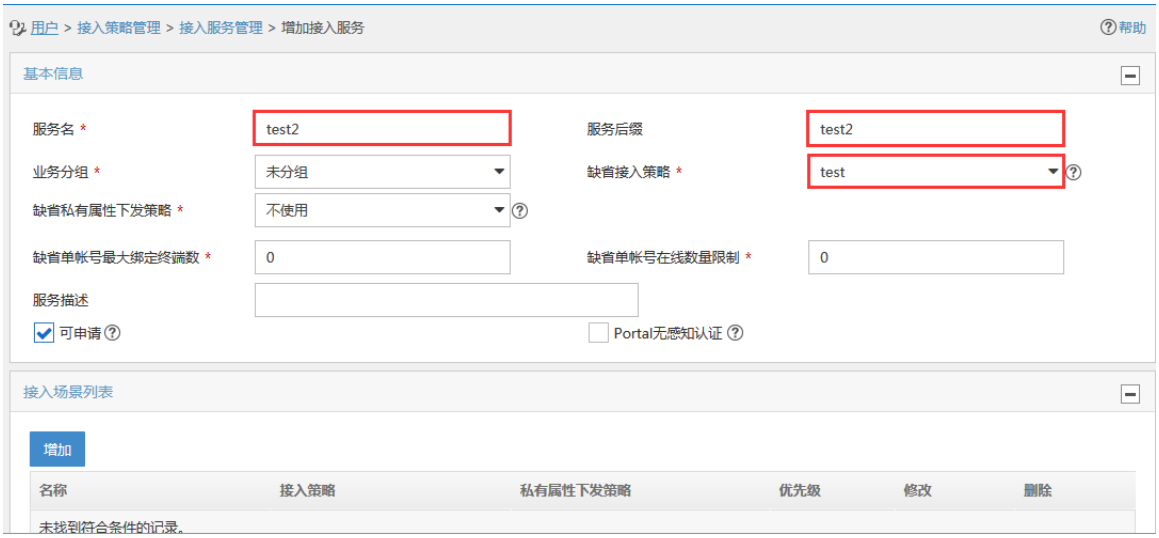
图13 接入策略配置完成



2. 配置接入服务

如图 14所示，进入“用户 > 接入策略管理 > 接入服务管理 > 增加接入服务”，“服务名”配置为 test2，“服务后缀”配置为 test2，“缺省接入策略”配置为 test，其它选项保持默认，点击<确定>。

图14 配置接入服务



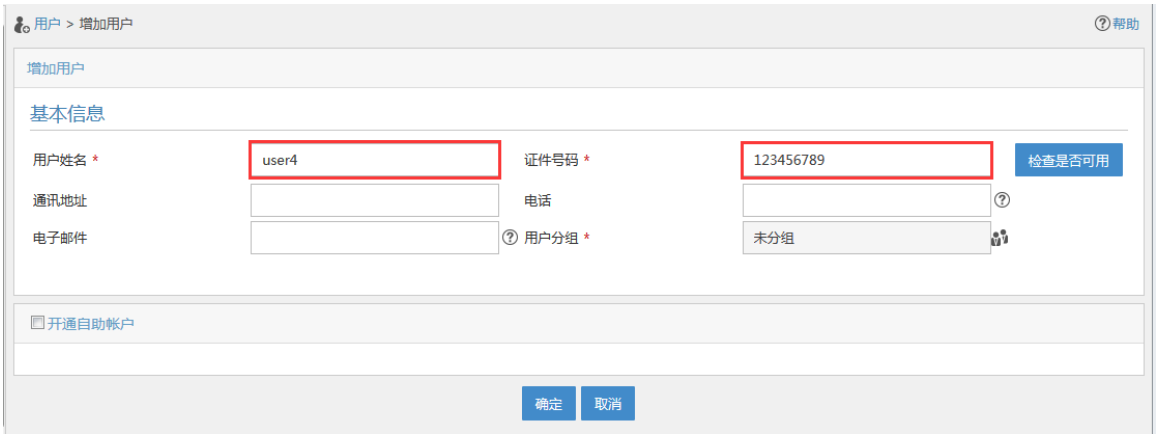
如图 15所示，添加完成的接入服务配置如下。

图15 接入服务配置完成

3. 配置用户和接入用户

如图 16所示，进入“用户 > 增加用户”，“用户姓名”配置为 user4，证件号码配置为 123456789，其它选项保持默认，点击<确定>。

图16 增加用户

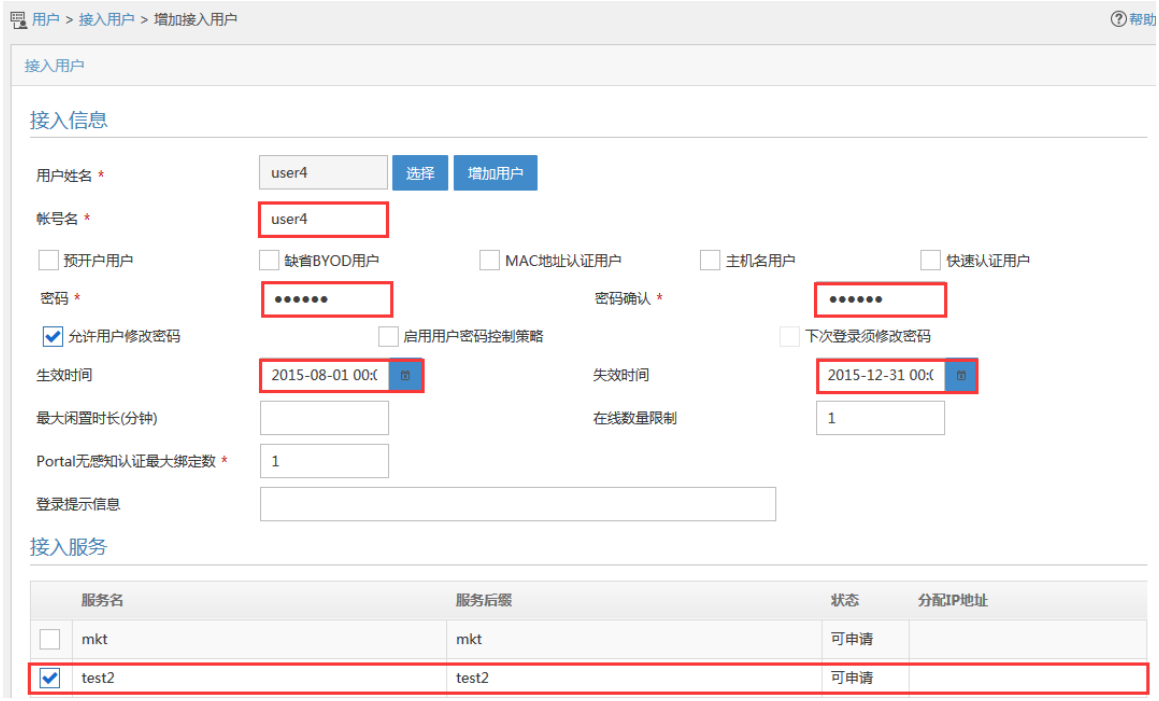


如图 17 所示，增加的用户配置如下。在此页面上点击<增加用户>。

图17 增加用户配置完成

如图 18 所示，进入“用户 > 接入用户 > 增加接入用户”，“账号名”配置为 user4，“密码”和“密码确认”均配置为用户密码，“生效时间”和“失效时间”根据实际情况配置，“接入服务”选择 test，其它选项保持默认，点击<确定>。

图18 配置接入用户



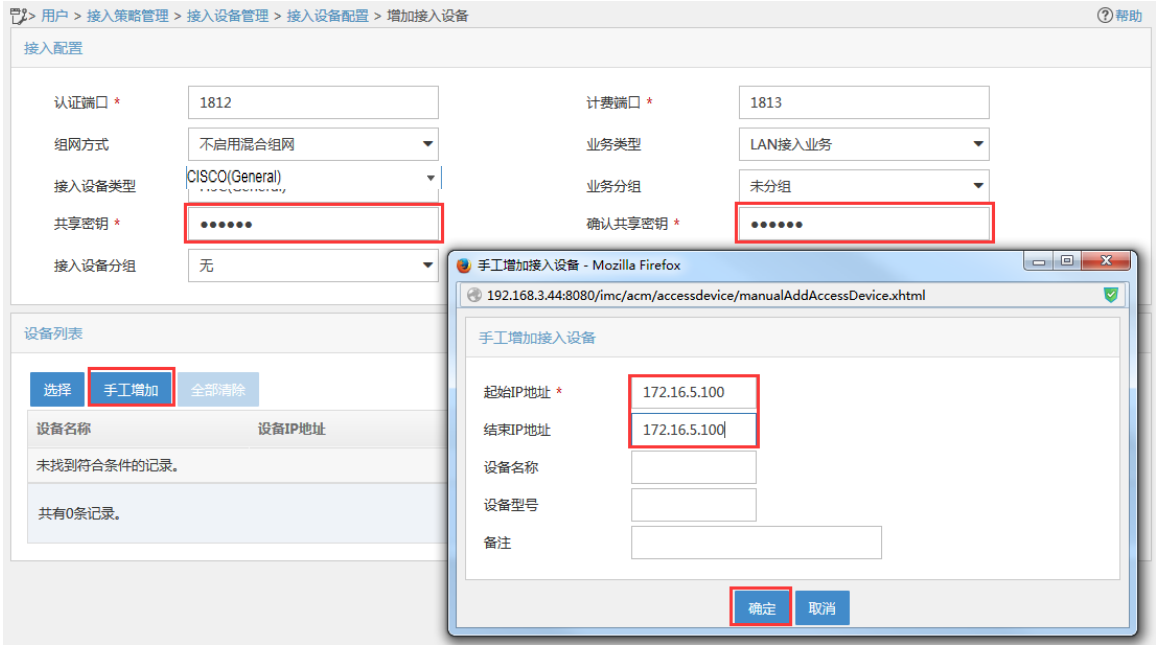
如图 19 所示，添加完成的接入用户配置如下。

图19 接入用户配置完成

4. 配置接入设备

如图 20 所示，进入“用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备”，点击<手工增加>，“共享密钥”和“确认共享密钥”均配置为和设备 A 设备匹配的密码，“起始 IP 地址”和“结束 IP 地址”均配置为 172.16.5.100（设备 A 设备的 bvi1 接口地址），其它选项保持默认，点击<确定>。

图20 配置接入设备



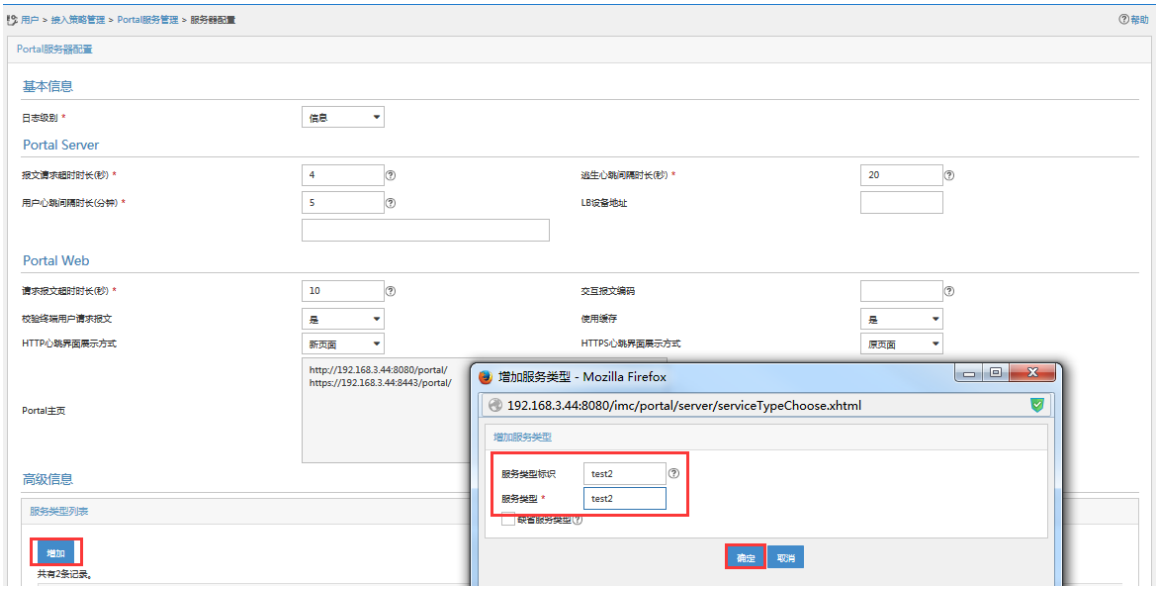
如图 21 所示，添加完成的接入设备配置如下。

图21 接入设备配置完成

5. 配置 Portal 服务器

如图 22 所示，进入“用户 > 接入策略管理 > Portal 服务管理 > 服务器配置”，点击<增加>，“服务类型标识”和“服务类型”均配置为 test，其它选项保持默认，点击<确定>。

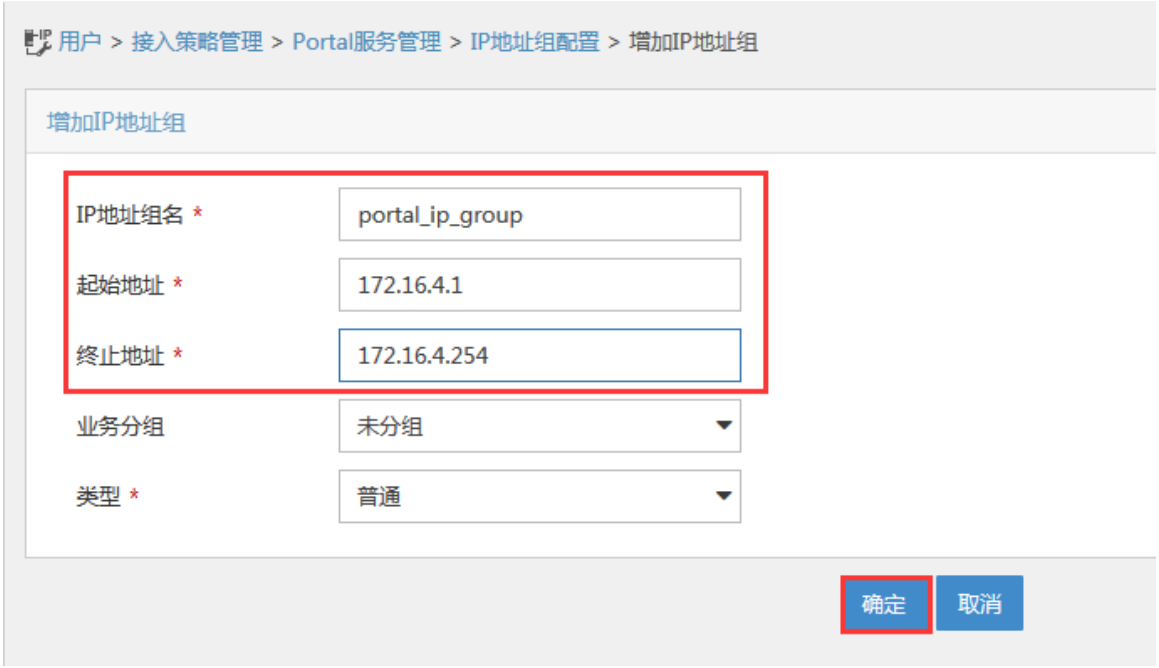
图22 配置 Portal 服务器



6. 配置 IP 地址组

如图 23 所示，进入“用户 > 接入策略管理 > Portal 服务管理 > IP 地址组配置 > 增加 IP 地址组”，“IP 地址组名”配置为 portal_ip_group，“起始地址”配置为 172.16.4.1，“终止地址”配置为 172.16.4.254，其它配置保持默认（如果是 NAT 组网，需要将“类型”配置为 NAT，并配置转换后的起始地址和终止地址），点击<确定>。

图23 配置 IP 地址组



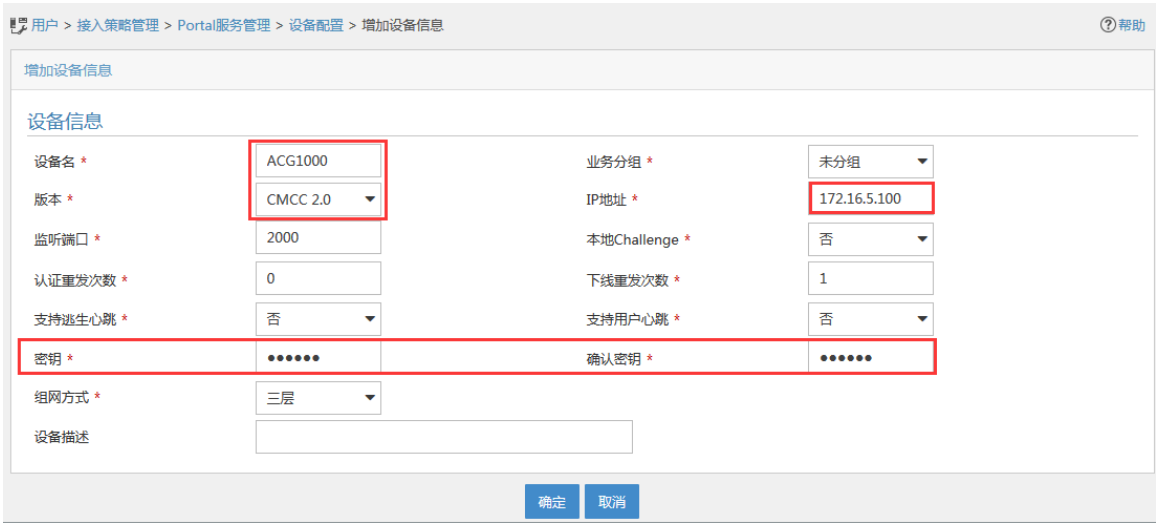
如图 24 所示，添加成功的 IP 地址组配置如下。

图24 IP 地址组配置成功

7. 配置设备信息和端口组信息

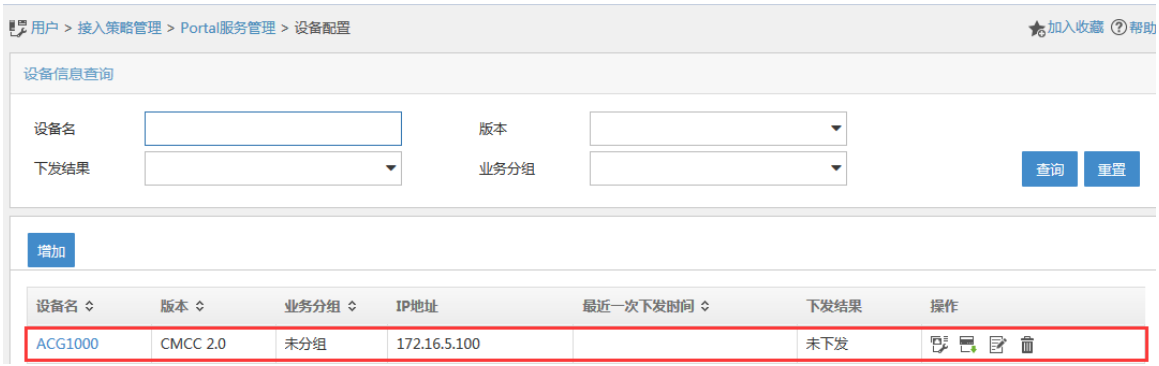
如图 25 所示，进入“用户 > 接入策略管理 > Portal 服务管理 > 设备配置 > 增加设备”，“设备名”配置为设备 1000，“IP 地址”配置为 172.16.5.100，“密钥”和“确认密钥”配置为和设备 A 设备匹配的密码，其它选项保持默认（虽然设备 A 透明部署，但“组网方式”仍保持为三层），点击<确定>。

图25 增加设备信息



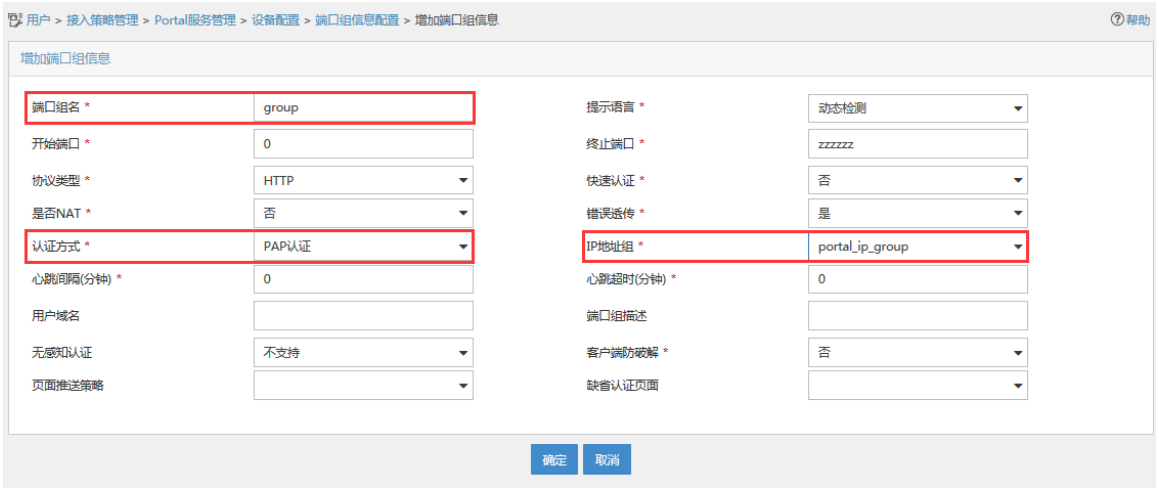
如图 26 所示，添加完成的设备的信息配置如下，并在此页面上单击<端口组信息管理>。

图26 设备的信息添加配置完成



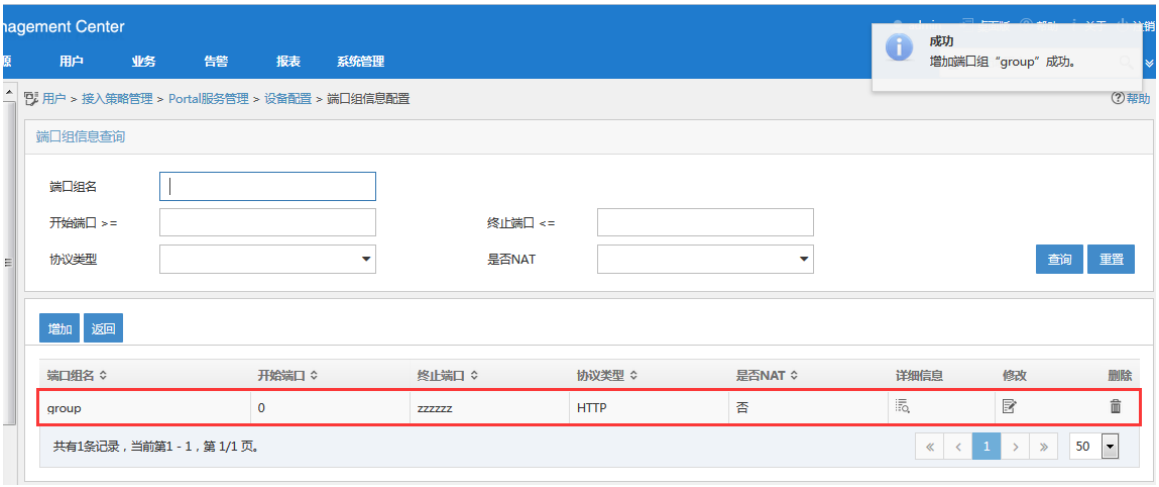
如图 27 所示，进入“用户 > 接入策略管理 > Portal 服务管理 > 设备配置 > 端口地址信息配置 > 增加端口组信息”，“端口组名”配置为 group，“认证模式”配置为 PAP 认证（设备目前只支持 PAP 认证），“IP 地址组”配置为 portal_ip_group，其它选项保持默认，点击<确定>。

图27 配置端口组信息



如图 28 所示，添加完成的端口组信息配置如下。

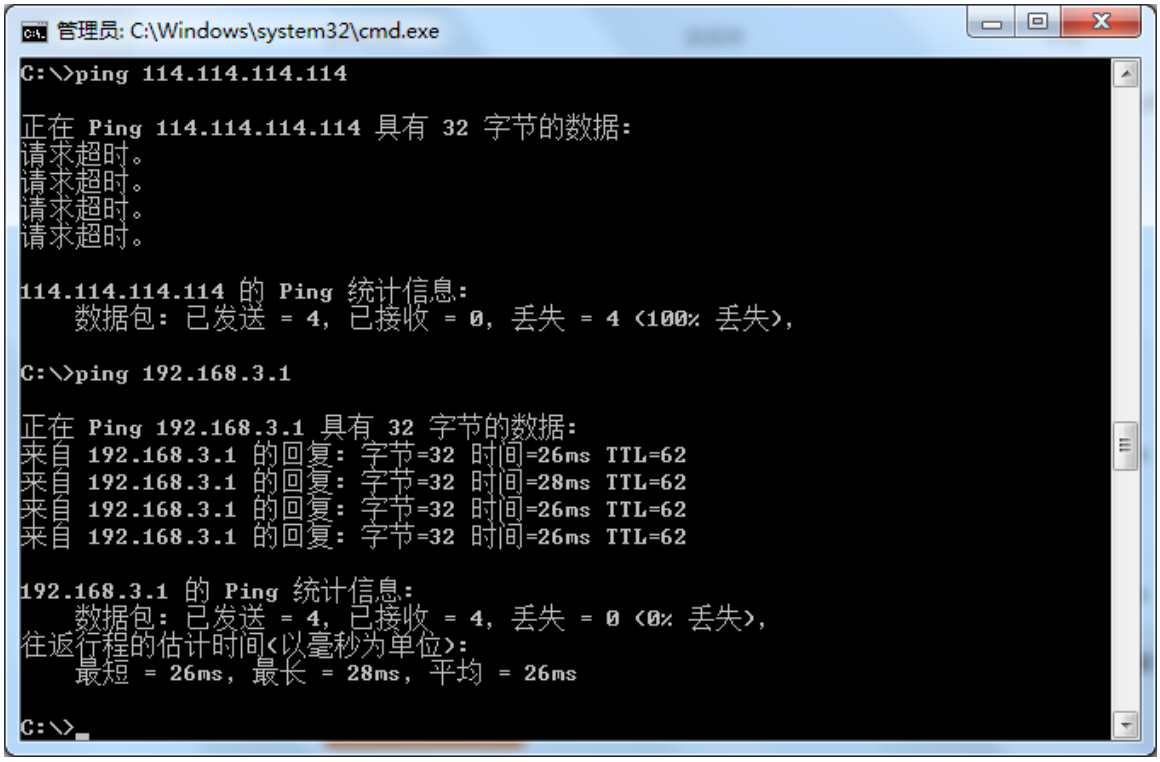
图28 端口组信息配置完成



4.6 验证配置

如图 29 所示，认证网段用户未进行认证时无法访问互联网，但是可以 ping 通 192.168.3.1。

图29 认证网段用户未认证前测试

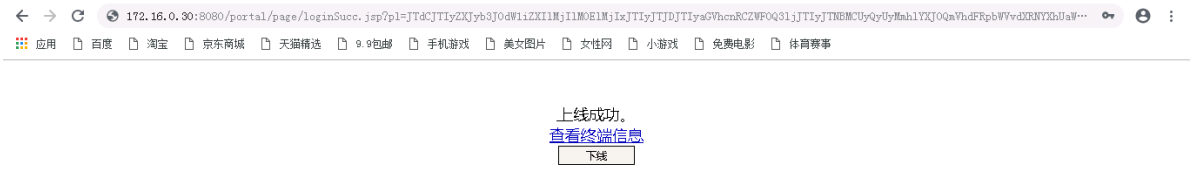


如图 30 所示，用户上网时会弹出 Portal 页面，在页面上输入用户名 user4 和密码，选择服务类型为 test2，单击<上线>。

图30 用户上网弹出 Portal 页面

如图 31 所示，认证成功，弹出计时页面。

图31 iMC 联动 Portal 认证成功



如图 32 所示，在设备上查看在线用户列表，发现 user4 已经被正确同步到用户组 2 中。

图32 用户组同步成功

目 录

1 简介

本文档介绍设备的 HA 主备功能典型应用场景配置举例，HA 是 High Availability 缩写，即高可用性，可防止网络中由于单个网关产品的设备故障或链路故障导致网络中断，保证网络服务的连续性和安全强度。

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

主备模式是指实现 HA 的两台设备中，一台作为主设备，另外一台作为备设备。主设备在进行业务配置和数据转发的同时，将相关的配置和数据信息实时同步到备设备。当主设备出现故障或主设备的链路中断时，备用设备成为主设备，接管原主设备的工作，实现网络业务的无缝切换。

在主备模式下，主设备响应各类报文请求，并且转发网络流量；备用设备不响应报文请求，也不转发网络流量。

HA 作为热备份，为了在状态切换的过程中，尽量减小对网络的影响。HA 会将主设备上的一些实时的状态同步给备设备。同步的内容主要包括三种：session 信息、设备配置、特征库。

- Session 信息：包括设备连接表、FDB、用户信息、PKI。
- 设备配置：同步的设备配置中不包含 HA 配置信息以及接口 manage ip 配置。
- 特征库：特征库包括 APP 特征库以及 URL 特征库。

主备模式下如下内容不会同步：

- HA 全局配置和接口 manage ip，两设备都需要单独配置。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。

2.1 组网需求1：HA主备路由模式三层组网

2.1.1 组网需求

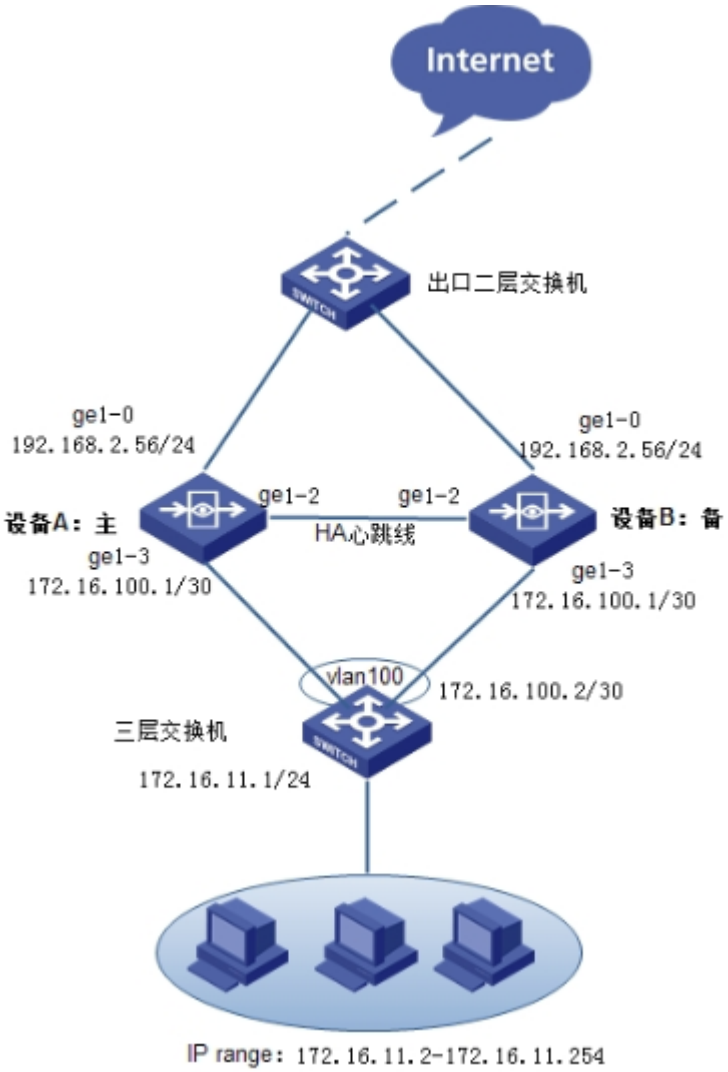
如图 1 所示，某公司内网办公网段：IP 地址 172.16.11.0/24，172.16.11.1/24 作为办公网段的网关，两台设备的：设备 A 和设备 B 工作在路由+NAT 模式，并以 HA 主备模式部署，实现热备份，接入网络，两台设备开启本地 web 认证，主设备 A 上的业务配置会实时同步给备设备 B，其中主设备 A 挂掉后，已经通过认证上网的用户，仍然能通过备设备 B 上网，不需要再次认证，具体应用需求如下：

- 办公网段：172.16.11.0/24 以数据默认走主设备 A 转发，当设备 A 发生故障后，备设备 B 切换为主，继续转发数据。

下联设备为三层交换机或路由器，因设备选型不一样，配置会不一样，配置不详细列出，配置需求概括如下：

- 三层交换机上联两个接口配置在一个 vlan 中，并设置 vlan 接口 ip:172.16.100.2/24，默认路由网关：172.16.100.1/24。
- 出口二层交换机所有接口在同一个 vlan 即可，不需要额外配置。

图1 HA 主备路由模式三层组网图



2.1.2 配置思路

- 设备 A 和设备 B 连接心跳线，并完成 HA 配置，保证 HA 主备协商成功，然后在设备 A 上开始做其它配置，以下配置都为设备 A 上的配置步骤。
- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 配置 NAT。
- 申请并导入 license 授权。
- 配置 DNS。

- 升级特征库。
- 配置 HA 全局配置，全局配置包含：工作模式、配置同步、运行状态同步、库同步、抢占模式（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

2.1.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 2 所示，进入网络配置>接口配置，点击 ge1-0、ge1-3 后的<编辑>按钮，配置 IP 192.168.2.56/24、172.16.100.1/30。

图2 配置接口 IP

(2) 配置静态路由

如图 3 所示，进入网络配置>路由管理>静态路由，配置访问外网的默认路由及内网认证用户网段 172.16.11.0/24。

图3 配置静态路由

(3) 配置认证用户地址对象

如图 4 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,点击<提交>。

图4 配置认证用户地址对象

(4) 配置源 NAT

如图 5 所示，进入“策略配置 > NAT 转换策略 > 源 NAT ”，新建 NAT 策略配置。

图5 配置源 NAT

(5) 申请并导入 license

如图 6 所示，进入“系统管理 > 系统维护 > 授权管理 ”，点击<导入许可证>。

图6 导入 license

(6) 配置 DNS

如图 7 所示，进入“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图7 配置 DNS

(7) 升级特征库

如图 8 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图8 升级特征库

(8) 配置用户识别范围

如图 9 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图9 用户识别范围

(9) 配置地址探测对象

如图 10 所示，进入策略配置>对象管理>地址对象>地址探测，点击<新建>按钮创建探测地址对象。

图10 用户识别范围

说明

地址探测支持 ping、TCP、DNS 三种方式。

(10) 配置 HA 全局配置

如图 11 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图11 HA 全局配置

说明

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。设备 B 会发送免费 ARP 更新下联交换机的 MAC 表项，用户数据会被转发到设备 B 进行处理。监控接口都为 UP 状态时，设备 A 会抢占为主，转发数据。
- 地址探测：地址探测失败后，设备 A 的 HA 状态变为备，业务切换到设备 B。当探测地址恢复后，设备 A 会重新抢占为主进行数据转发。

(11) 添加本地认证用户

如图 12 所示，进入“用户管理> 用户组织结构 ”页面，点击新建，创建用户账号 test。

图12 添加认证用户

(12) 配置本地 web 认证参数

如图 13 所示，进入“用户管理 > 认证管理 > 认证方式 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图13 配置本地 web 认证参数

(13) 配置认证策略

如图 14 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图14 认证策略页面

2. 设备 B 配置

在配置其它策略前，先保证设备 A 和设备 B 均开启了 HA 主备配置，设备 B 只需要做 HA 全局配置，设备 A 上的所有其它配置都会自动同步给设备 B，不需要人为配置。

(1) 配置 HA 全局配置

如图 15 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图15 HA 全局配置

2.1.5 配置注意事项

- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主备模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用接口主地址发包，但是发生状态切换变成备状态后，地址探测就会用管理地址发包了，如果不配置管理 IP，会导致原来的主设备永远不能重新变成主，即使新的主设备挂了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA 主状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

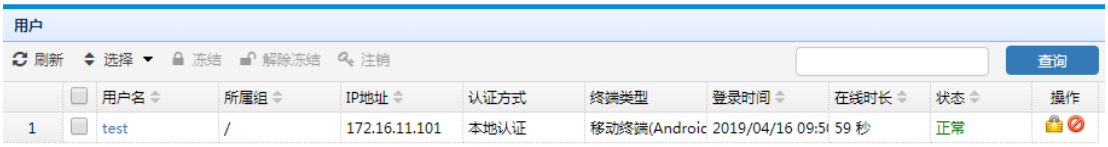
2.1.6 验证配置

1. 查看设备 B 的配置，发现设备 A 上的所有配置都实时同步给了设备 B。

2. 172.16.11.0/24 网段过设备 A 进行认证上网，在线用户会同步给设备 B，当设备 A 挂掉后，用户仍然可以通过设备 B 正常上网，不会断网，也不需要重新认证。

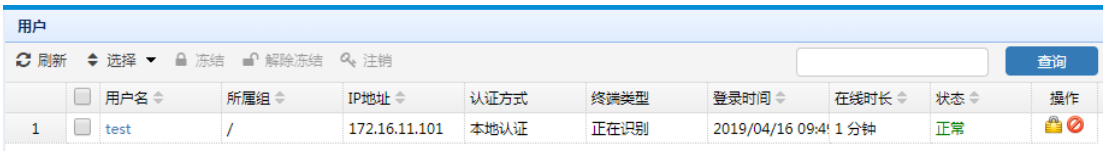
如图 16 所示，设备 A 在线用户。

图16 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。设备 A 恢复后，用户再次切回设备 A 上网。

图17 设备 B 在线用户



2.2 组网需求2：HA主备路由模式二层组网

2.2.1 组网需求

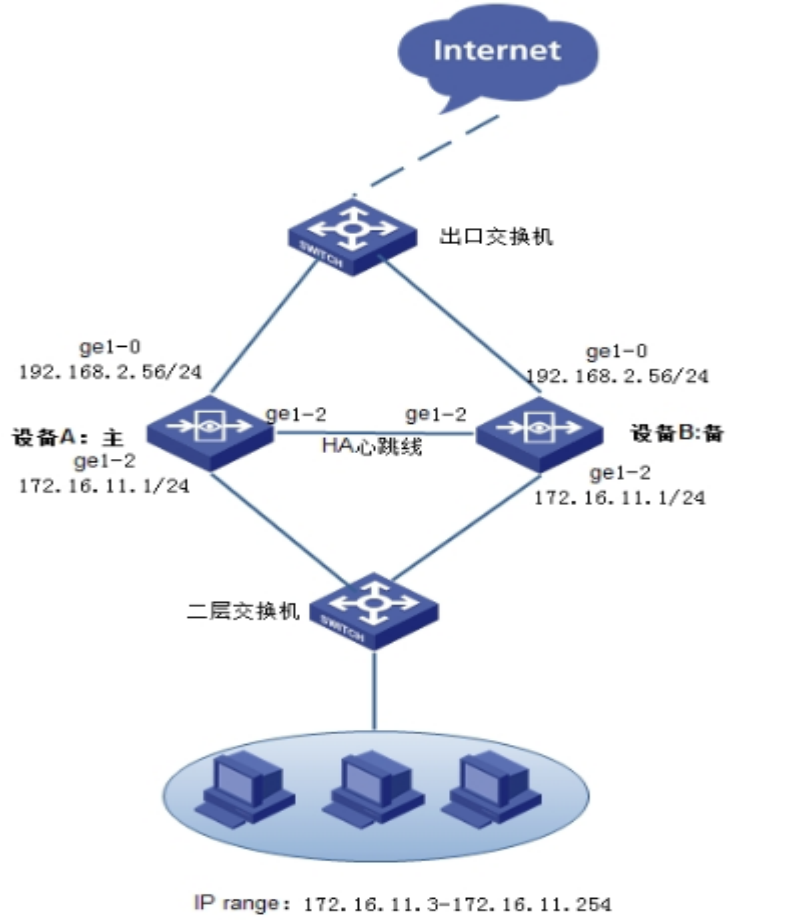
如图 18 所示，某公司内网办公网段：IP 地址 172.16.11.0/24，172.16.11.1/24 作为办公网段的网关，两台设备的：设备 A 和设备 B 工作在路由+NAT 模式，并以 HA 主备模式部署，实现热备份，接入网络，两台设备开启本地 web 认证，主设备 A 上的业务配置会实时同步给备设备 B，其中主设备 A 挂掉后，已经通过认证上网的用户，仍然能通过备设备 B 上网，不需要再次认证，具体应用需求如下：

- 办公网段：172.16.11.0/24 数据默认走主设备 A 转发，当设备 A 发生故障后，备设备 B 切换为主，继续转发数据。

下联设备为二层交换机，因设备选型不一样，配置会不一样，配置不详细列出，配置需求概括如下：

- 二层交换机上联两个接口配置在一个 vlan 中。
- 出口二层交换机所有接口在同一个 vlan 即可，不需要额外配置。

图18 HA 主备路由模式二层组网图



2.2.2 配置思路

- 设备 A 和设备 B 连接心跳线，并完成 HA 配置，保证 HA 主备协商成功，然后在设备 A 上开始做其它配置，以下配置都为设备 A 上的配置步骤。
- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 配置 NAT。
- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置 HA 全局配置，全局配置包含：工作模式、配置同步、运行状态同步、库同步、抢占模式（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.2.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

2.2.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 19 所示，进入网络配置>接口配置，点击 ge1-0、ge1-3 后的<编辑>按钮，配置 IP 192.168.2.56/24、172.16.11.1/24。

图19 配置接口 IP

(2)　配置静态路由

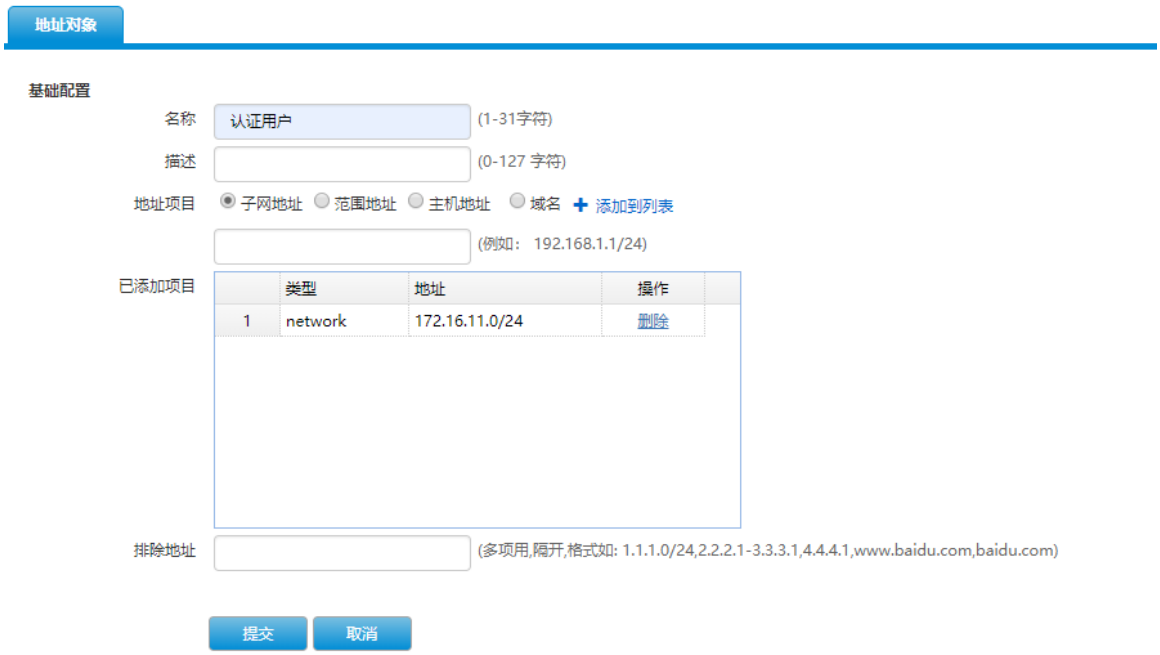
如图 20 所示，进入网络配置>路由管理>静态路由，配置访问外网的默认路由。

图20 配置静态路由

(3)　配置认证用户地址对象

如图 21 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

图21 配置认证用户地址对象



(4)　配置源 NAT

如图 22 所示，进入“策略配置 > NAT 转换策略 > 源 NAT ”，新建 NAT 策略配置。

图22 配置源 NAT

(5)　申请并导入 license

如图 23 所示，进入“系统管理 > 系统维护 > 授权管理 ”，点击<导入许可证>。

图23 导入 license

(6) 配置 DNS

如图 24 所示，进入“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图24 配置 DNS

(7) 升级特征库

如图 25 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图25 升级特征库

(8) 配置用户识别范围

如图 26 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图26 用户识别范围

(9) 配置地址探测对象

如图 27 所示，进入策略配置>对象管理>地址对象>地址探测，点击<新建>按钮创建探测地址对象。

图27 用户识别范围

说明

地址探测支持 ping、TCP、DNS 三种方式。

(10) 配置 HA 全局配置

如图 28 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图28 HA 全局配置

说明

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。设备 B 会发送免费 ARP 更新下联交换机的 MAC 表项，用户数据会被转发到设备 B 进行处理。监控接口都为 UP 状态时，设备 A 会抢占为主，转发数据。
- 地址探测：地址探测失败后，设备 A 的 HA 状态变为备，业务切换到设备 B。当探测地址恢复后，设备 A 会重新抢占为主进行数据转发。

(11) 添加本地认证用户

如图 29 所示，进入“用户管理> 用户组织结构 ”页面，点击新建，创建用户账号 test。

图29 添加认证用户

(12) 配置本地 web 认证参数

如图 30 所示，进入“用户管理 > 认证管理 > 认证方式 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图30 配置 web 认证参数

(13) 配置认证策略

如图 31 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图31 认证策略页面

2. 设备 B 配置

在配置其它策略前，先保证设备 A 和设备 B 均开启了 HA 主备配置，设备 B 只需要做 HA 全局配置，设备 A 上的所有其它配置都会自动同步给设备 B，不需要人为配置。

(1)　配置 HA 全局配置

如图 32 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图32 HA 全局配置

2.2.5 配置注意事项

- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主备模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用接口主地址发包，但是发生状态切换变成备状态后，地址探测就会用管理地址发包了，如果不配置管理 IP，会导致原来的主设备永远不能重新变成主，即使新的主设备挂了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA 主状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

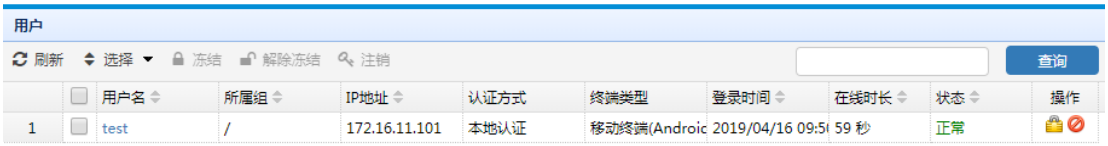
2.2.6 验证配置

1. 查看设备 B 的配置，发现设备 A 上的所有配置都实时同步给了设备 B。

2. 172.16.11.0/24 网段过设备 A 进行认证上网，在线用户会同步给设备 B，当设备 A 挂掉后，用户仍然可以通过设备 B 正常上网，不会断网，也不需要重新认证。

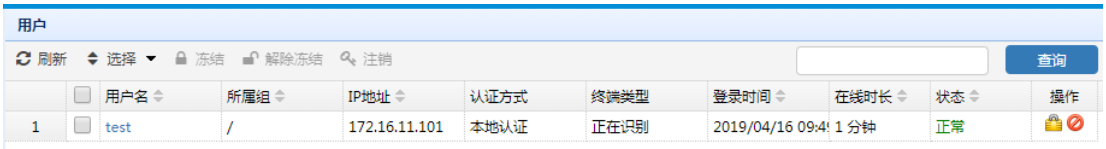
如图 33 所示，设备 A 在线用户。

图33 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。设备 A 恢复后，用户再次切回设备 A 上网。

图34 设备 B 在线用户



2.3 组网需求3：HA主备透明桥模式三层组网

2.3.1 组网需求

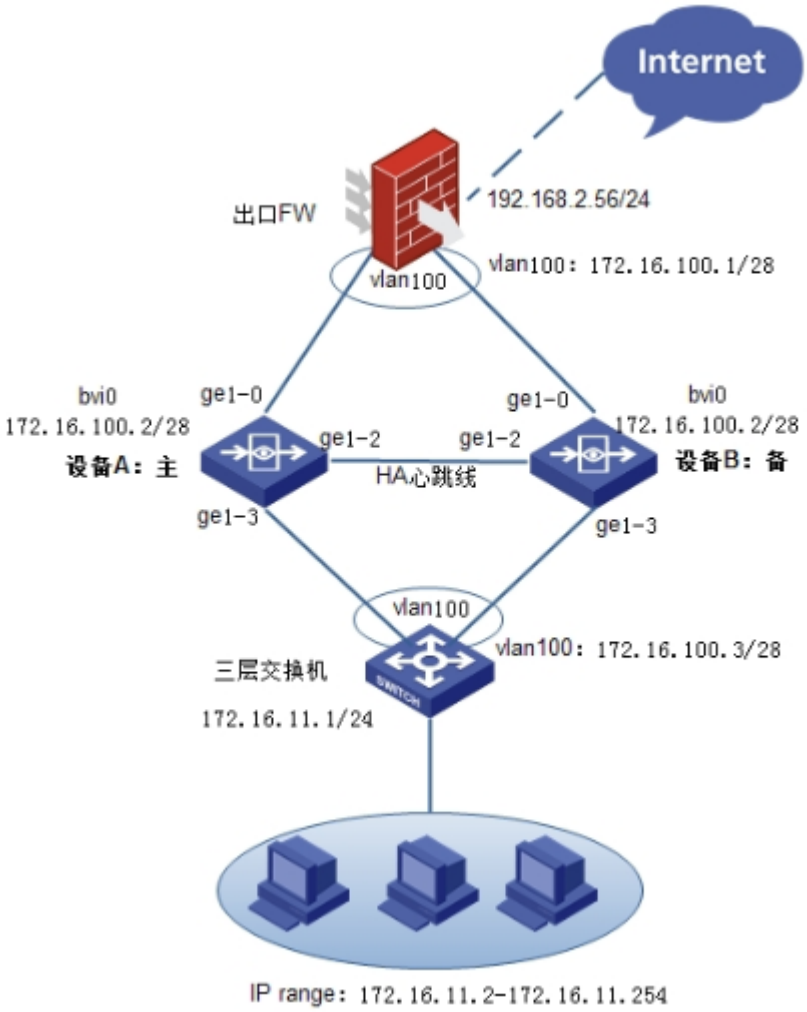
如图 35 所示，某公司内网办公网段：IP 地址 172.16.11.0/24，172.16.11.1/24 作为办公网段的网关，两台设备的：设备 A 和设备 B 为透明桥模式，并以 HA 主备模式部署，实现热备份，接入网络，两台设备开启本地 web 认证，主设备 A 上的业务配置会实时同步给备设备 B，其中主设备 A 挂掉后，已经通过认证上网的用户，仍然能通过备设备 B 上网，不需要再次认证，具体应用需求如下：

- 办公网段：172.16.11.0/24 以数据默认走主设备 A 转发，当设备 A 发生故障后，备设备 B 切换为主，继续转发数据。

下联设备为三层交换机或路由器，因设备选型不一样，配置会不一样，配置不详细列出，配置需求概括如下：

- 三层交换机上联两个接口配置在一个 vlan 中，并设置 vlan 接口 ip:172.16.100.3/24，默认路由网关：172.16.100.1/24。
- 出口 FW 下联两个接口在同一个 vlan，出接口配置访问公网的 IP 和路由，并配置源 NAT。

图35 HA 主备透明桥模式三层组网图



2.3.2 配置思路

- 设备 A 和设备 B 连接心跳线，并完成 HA 配置，保证 HA 主备协商成功，然后在设备 A 上开始做其它配置，以下配置都为设备 A 上的配置步骤。
- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置 HA 全局配置，全局配置包含：工作模式、配置同步、运行状态同步、库同步、抢占模式（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

2.3.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 36 所示，进入网络配置>接口配置>网桥接口，点击新建，将 ge1-0、ge1-3 加入桥口 bvi0，配置 IP 172.16.100.2/28。

图36 配置接口 IP

(2) 配置静态路由

如图 37 所示，进入网络配置>路由管理>静态路由，配置访问外网的默认路由及内网认证用户网段 172.16.11.0/24。

图37 配置静态路由

(3) 配置认证用户地址对象

如图 38 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,点击<提交>。

图38 配置认证用户地址对象

(4) 申请并导入 license

如图 39 所示，进入“系统管理 > 系统维护 > 授权管理 ”，点击<导入许可证>。

图39 导入 license

(5) 配置 DNS

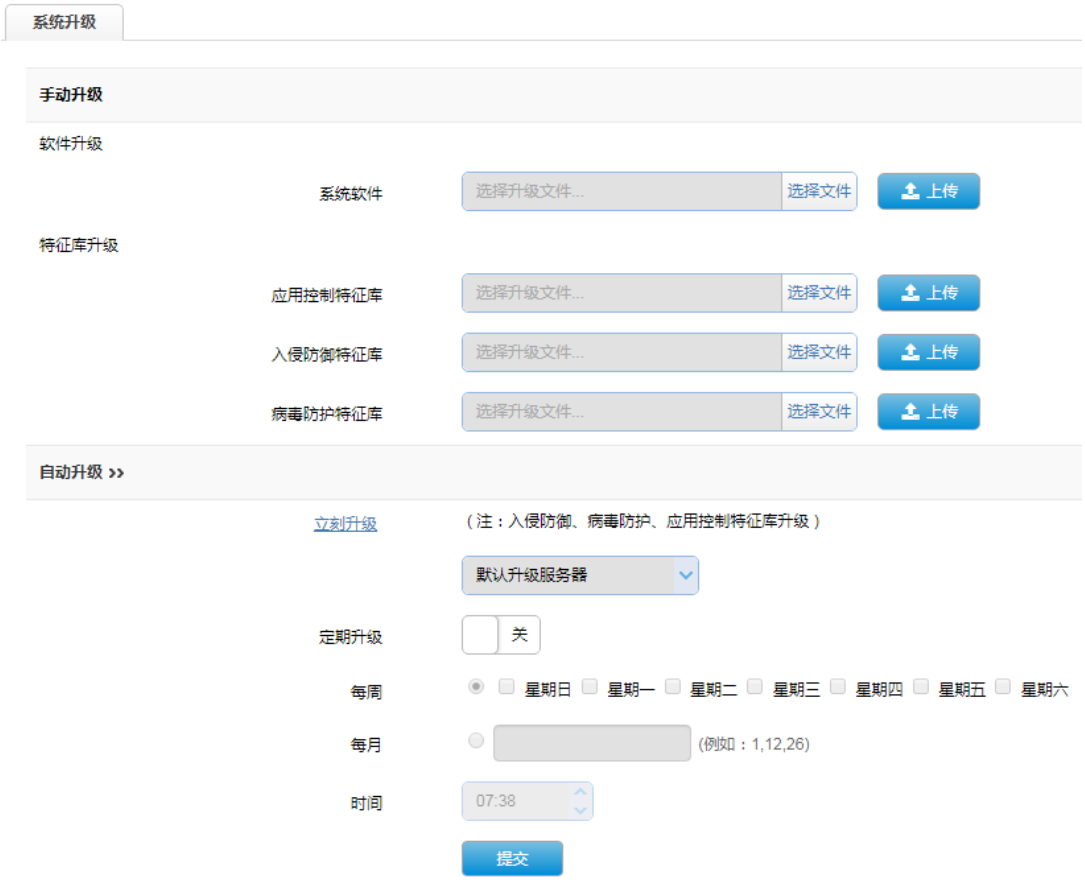
如图 40 所示，进入“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图40 配置 DNS

(6) 升级特征库

如图 41 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图41 升级特征库



(7) 配置用户识别范围

如图 42 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图42 用户识别范围

(8) 配置地址探测对象

如图 43 所示，进入策略配置>对象管理>地址对象>地址探测，点击<新建>按钮创建探测地址对象。

图43 用户识别范围

说明

地址探测支持 ping、TCP、DNS 三种方式。

(9) 配置 HA 全局配置

如图 44 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图44 HA 全局配置

说明

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。设备 B 会发送免费 ARP 更新下联交换机的 MAC 表项，用户数据会被转发到设备 B 进行处理。监控接口都为 UP 状态时，设备 A 会抢占为主，转发数据。
- 地址探测：地址探测失败后，设备 A 的 HA 状态变为备，业务切换到设备 B。当探测地址恢复后，设备 A 会重新抢占为主进行数据转发。

---

(10) 添加本地认证用户

如图 45 所示，进入“用户管理> 用户组织结构 ”页面，点击新建，创建用户账号 test。

图45 添加认证用户

(11) 配置本地 web 认证参数

如图 46 所示，进入“用户管理 > 认证管理 > 认证方式 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图46 配置本地 web 认证参数

(12) 配置认证策略

如图 47 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图47 认证策略页面

2. 设备 B 配置

在配置其它策略前，先保证设备 A 和设备 B 均开启了 HA 主备配置，设备 B 只需要做 HA 全局配置，设备 A 上的所有其它配置都会自动同步给设备 B，不需要人为配置。

(1) 配置 HA 全局配置

如图 48 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图48 HA 全局配置

2.3.5 配置注意事项

- HA 透明桥模式组网需要在 ha-config 模式下配置 fdb refresh enable，当发生 HA 状态切换时，由主切换为备的设备需要 up/down 一次桥接口中的成员接口，以促使上下游交换机刷新接口的 MAC 转发表，将流量同步切换到新的主设备上，只有 HA 桥模式需要开启此命令。
- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主备模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用接口主地址发包，但是发生状态切换变成备状态后，地址探测就会用管理地址发包了，如果不配置管理 IP，会导致原来的主设备永远不能重新变成主，即使新的主设备挂了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA 主状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

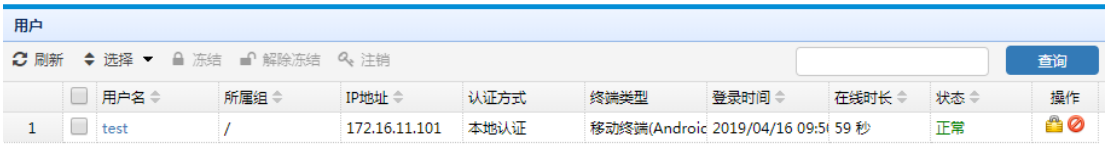
2.3.6 验证配置

1. 查看设备 B 的配置，发现设备 A 上的所有配置都实时同步给了设备 B。

2. 172.16.11.0/24 网段过设备 A 进行认证上网，在线用户会同步给设备 B，当设备 A 挂掉后，用户仍然可以通过设备 B 正常上网，不会断网，也不需要重新认证。

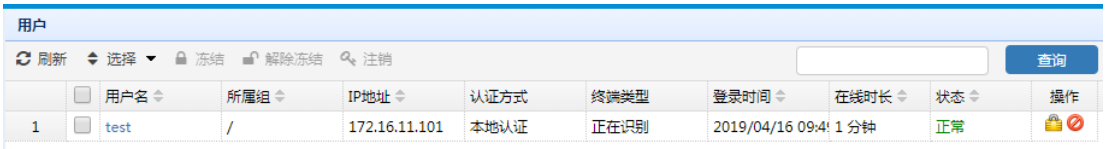
如图 49 所示，设备 A 在线用户。

图49 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。设备 A 恢复后，用户再次切回设备 A 上网。

图50 设备 B 在线用户



2.4 组网需求4：HA主备透明桥模式二层组网

2.4.1 组网需求

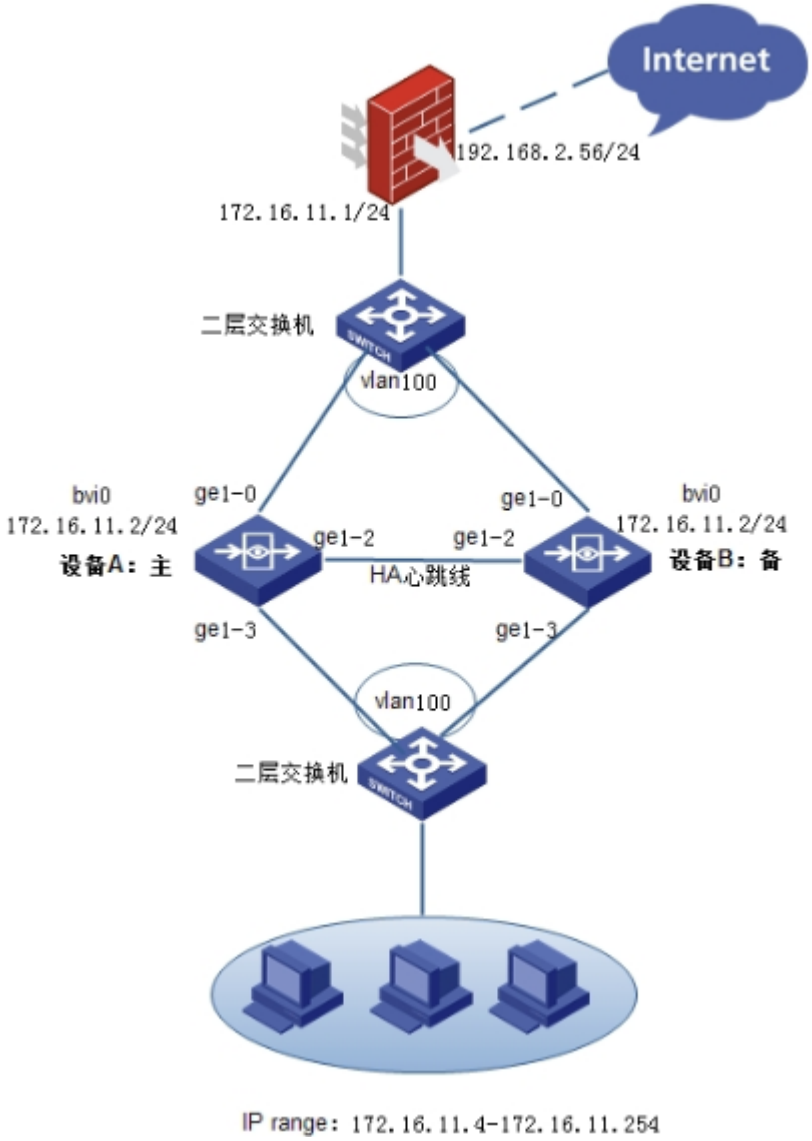
如图 51 所示，某公司内网办公网段：IP 地址 172.16.11.0/24，172.16.11.1/24 作为办公网段的网关，两台设备的：设备 A 和设备 B 为透明桥模式，并以 HA 主备模式部署，实现热备份，接入网络，两台设备开启本地 web 认证，主设备 A 上的业务配置会实时同步给备设备 B，其中主设备 A 挂掉后，已经通过认证上网的用户，仍然能通过备设备 B 上网，不需要再次认证，具体应用需求如下：

- 办公网段：172.16.11.0/24 以数据默认走主设备 A 转发，当设备 A 发生故障后，备设备 B 切换为主，继续转发数据。

上联和下联设备均为二层交换机，因设备选型不一样，配置会不一样，配置不详细列出，配置需求概括如下：

- 二层交换机所有接口配置在一个 vlan 中。
- 出口 FW 作为内网办公网段用户的网关。

图51 HA 主备透明桥模式二层组网图



2.4.2 配置思路

- 设备 A 和设备 B 连接心跳线，并完成 HA 配置，保证 HA 主备协商成功，然后在设备 A 上开始做其它配置，以下配置都为设备 A 上的配置步骤。
- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置 HA 全局配置，全局配置包含：工作模式、配置同步、运行状态同步、库同步、抢占模式（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。

- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

2.4.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 52 所示，进入网络配置>接口配置>网桥接口，点击新建，将 ge1-0、ge1-3 加入桥口 bvi0，配置 IP 172.16.11.2/24。

图52 配置接口 IP

(2) 配置静态路由

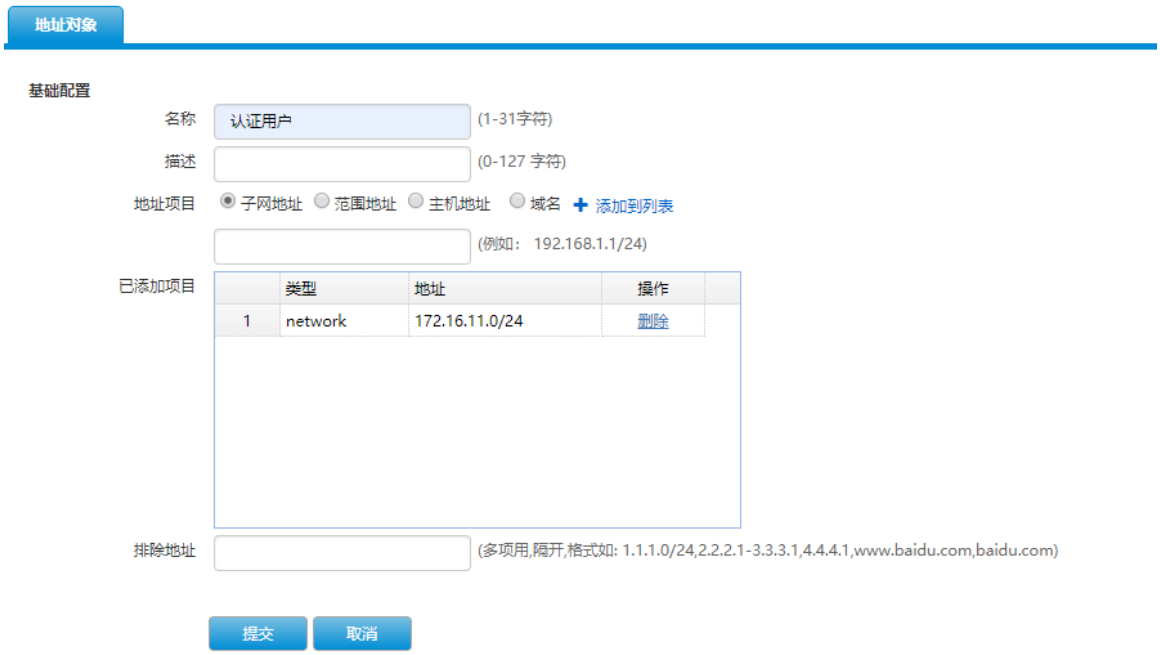
如图 53 所示，进入网络配置>路由管理>静态路由，配置访问外网的默认路由。

图53 配置静态路由

(3) 配置认证用户地址对象

如图 54 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,点击<提交>。

图54 配置认证用户地址对象



(4) 申请并导入 license

如图 55 所示，进入“系统管理 > 系统维护 > 授权管理 ”，点击<导入许可证>。

图55 导入 license

(5) 配置 DNS

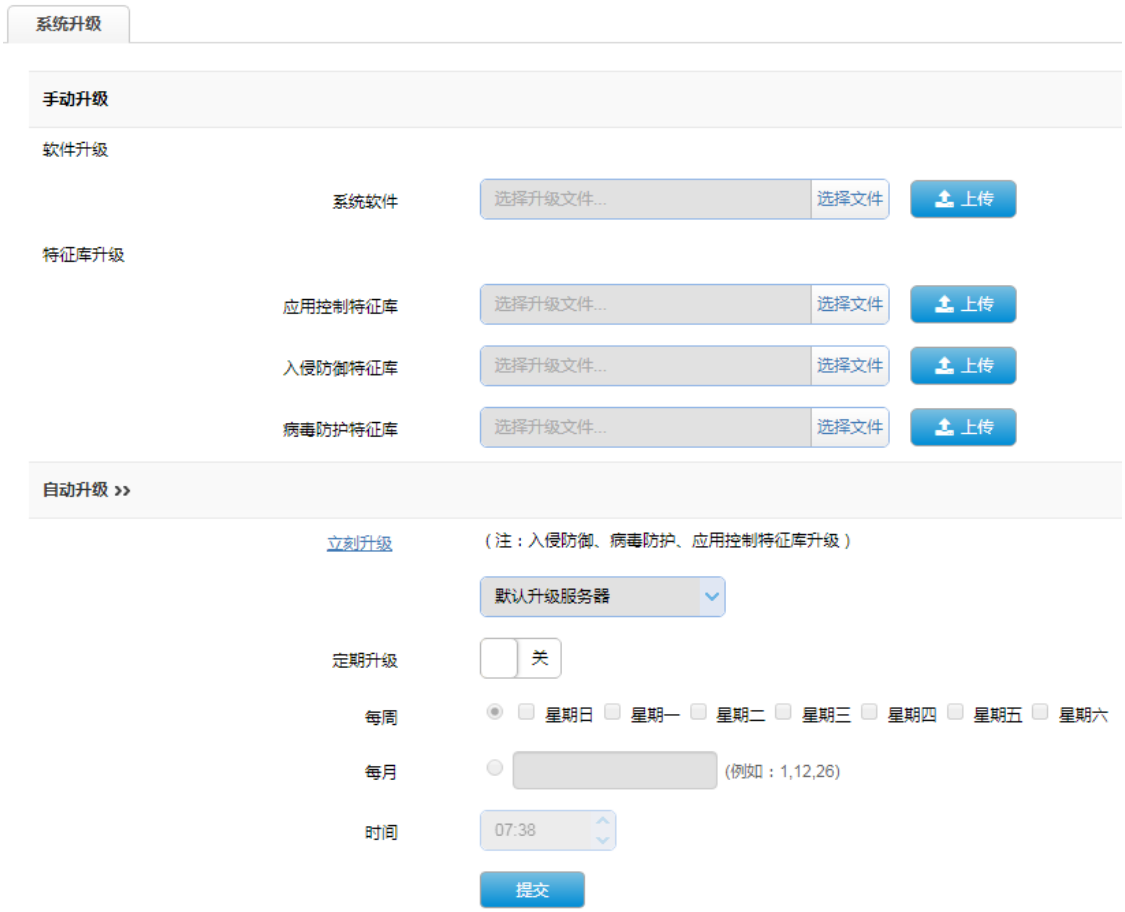
如图 56 所示，进入“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图56 配置 DNS

(6) 升级特征库

如图 57 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图57 升级特征库



(7) 配置用户识别范围

如图 58 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图58 用户识别范围

(8)　配置地址探测对象

如图 59 所示，进入策略配置>对象管理>地址对象>地址探测，点击<新建>按钮创建探测地址对象。

图59 用户识别范围

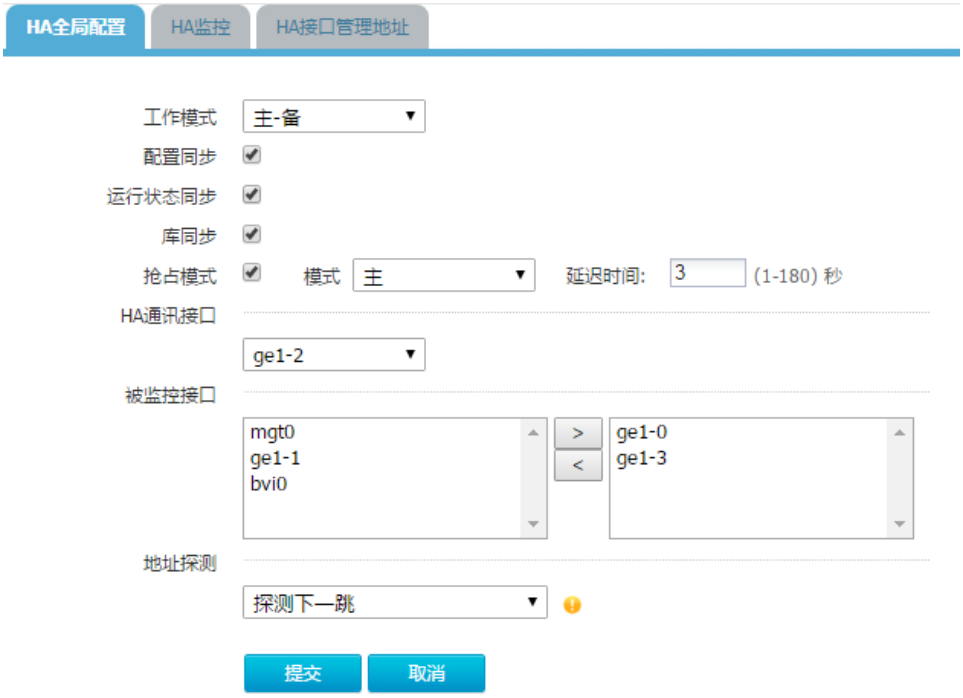
说明

地址探测支持 ping、TCP、DNS 三种方式。

(9)　配置 HA 全局配置

如图 60 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图60 HA 全局配置



说明

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。设备 B 会发送免费 ARP 更新下联交换机的 MAC 表项，用户数据会被转发到设备 B 进行处理。监控接口都为 UP 状态时，设备 A 会抢占为主，转发数据。
- 地址探测：地址探测失败后，设备 A 的 HA 状态变为备，业务切换到设备 B。当探测地址恢复后，设备 A 会重新抢占为主进行数据转发。

(10) 添加本地认证用户

如图 61 所示，进入“用户管理> 用户组织结构 ”页面，点击新建，创建用户账号 test。

图61 添加认证用户

(11) 配置本地 web 认证参数

如图 62 所示，进入“用户管理 > 认证管理 > 认证方式 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图62 配置本地 web 认证参数

(12) 配置认证策略

如图 63 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图63 认证策略页面

2. 设备 B 配置

在配置其它策略前，先保证设备 A 和设备 B 均开启了 HA 主备配置，设备 B 只需要做 HA 全局配置，设备 A 上的所有其它配置都会自动同步给设备 B，不需要人为配置。

(1) 配置 HA 全局配置

如图 64 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图64 HA 全局配置

2.4.5 配置注意事项

- HA 透明桥模式组网需要在 ha-config 模式下配置 fdb refresh enable，当发生 HA 状态切换时，由主切换为备的设备需要 up/down 一次桥接口中的成员接口，以促使上下游交换机刷新接口的 MAC 转发表，将流量同步切换到新的主设备上，只有 HA 桥模式需要开启此命令。
- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主备模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用接口主地址发包，但是发生状态切换变成备状态后，地址探测就会用管理地址发包了，如果不配置管理 IP，会导致原来的主设备永远不能重新变成主设备，即使新的主设备停止服务了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA 主状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

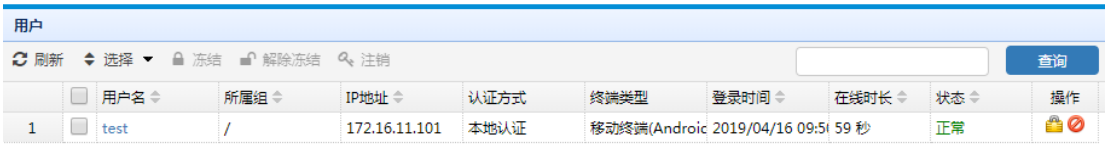
2.4.6 验证配置

1. 查看设备 B 的配置，发现设备 A 上的所有配置都实时同步给了设备 B。

2. 172.16.11.0/24 网段过设备 A 进行认证上网，在线用户会同步给设备 B，当设备 A 挂掉后，用户仍然可以通过设备 B 正常上网，不会断网，也不需要重新认证。

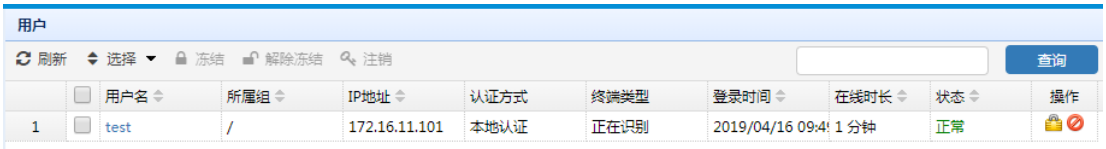
如图 65 所示，设备 A 在线用户。

图65 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。设备 A 恢复后，用户再次切回设备 A 上网。

图66 设备 B 在线用户



3 HA 主备功能使用限制及注意事项

- HA 主备邻居为什么建立不起来时请检查以下内容：

  两台设备必须型号一致，板卡一致。

  两台设备的序列号要求不一致。序列号一致，建不起来邻居。

  查看心跳线接口状态是否正常。

- HA 主备环境一台设备宕机又恢复后，HA 状态不能不变，没有切换回主状态

  a. 确认发探测包的接口是否配置了管理 IP，HA 主备模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成备状态后，地址探测就会用管理地址发包了。

  b. 确认发探测报文的接口是否配置了源 NAT，如果配置了配置源 NAT，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA 模式下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

4 HA 主备相关原理资料

- **什么是 HA 主备模式**

  主备模式是指实现 HA 的两台设备中， 一台为主设备进行数据转发，一台为备设备，不转发数据，作为主设备的备份。主设备在进行业务的同时， 将配置、流表信息和认证用户信息同

步到对端。当其中一台设备出现故障或链路中断时，另外一台设备作为故障设备的备份，接管原主设备的工作，实现网络业务的无缝切换。

在主备模式下，主备设备之间通过 HA 心跳线同步状态信息。

主备模式支持路由模式和透明模式。

- **HA 心跳报文**

  HA 设备之间用来相互通告设备的 HA 配置和 HA 状态的报文。如果一个设备在规定时间没有收到邻居心跳报文，可以认定 HA 邻居已经失效。

- **HA 管理地址**

  a. 处于备状态的 HA 设备不会参与网络转发，因此无法通过其接口配置的 IP 地址访问。为了解决这一问题，可以在设备上配置管理地址，用作备设备的网络管理。用户可以从外部访问备设备的 telnet 服务和 web 管理界面。

  b. 当处理备状态下时，设备不参与转发，使用管理地址来发探测包。

- **HA 主备状态切换**

  当设备启用 HA 主备模式后，设备进入 init（初始化状态），然后状态置为 master。设备收到对端发来的 keepalive 报文，两端设备协商参数。建立 master 邻居后，靠心跳报文保持邻居关系，并启动定时器。若在定时器（定时器时间为 interval *retry 次数）时间内，未收到心跳报文，则状态置为 master。出现故障的设备状态置为 backup。backup 状态的设备，所有接口不参与报文转发。

- **HA 主备心跳报文间隔**

  缺省情况下，报文间隔时间为 200 毫秒，重试次数为 5 次，可以通过 keepalive <20-1000> retry<3-500> 命令进行修改。

目 录

1 简介

本文档介绍设备的 HA 主主功能典型应用场景配置举例，HA 是 High Availability 缩写，即高可用性，可防止网络中由于单个网关产品的设备故障或链路故障导致网络中断，保证网络服务的连续性和安全强度。

随着网络的快速普及和应用的日益深入，各种增值业务（如 IPTV、视频会议等）得到了广泛部署，网络中断可能影响大量业务、造成重大损失。因此，作为业务承载主体的基础网络，其可靠性日益成为受关注的焦点。

在实际网络中，总避免不了各种非技术因素造成的网络故障和服务中断。因此，提高系统容错能力、提高故障恢复速度、降低故障对业务的影响，是提高系统可靠性的有效途径。

主主模式下设备之间会同步如下内容：

- 运行状态同步：session、fdb、用户状态。（默认关闭）
- 监控接口地址同步：当前设备 HA 状态发生异常后，另一主设备会进行 arp 代理，发送免费 arp，更新用户的 ARP 缓存，应用场景为下联设备为二层设备时。

主主模式下如下内容不会同步：

- 配置不会同步。
- 特征库不会同步。
- HA 全局配置不会同步，两设备都需要单独配置。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。

2.1 组网需求1：HA主主路由模式三层组网

2.1.1 组网需求

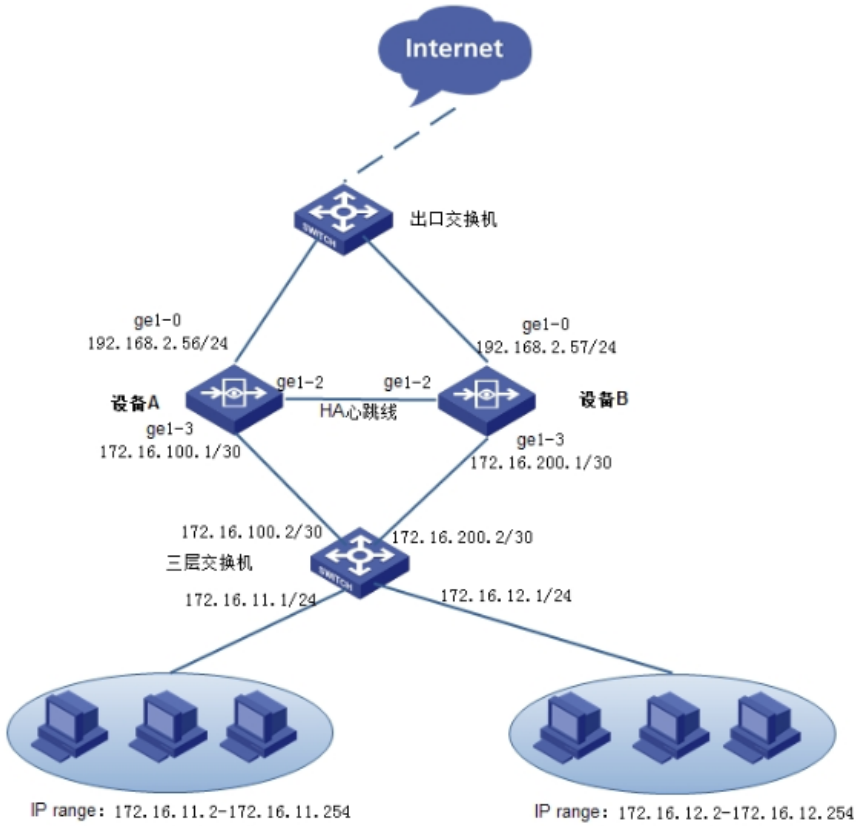
如图 1 所示，某公司内网办公网段 1：IP 地址 172.16.11.0/24，办公网段 2：IP 地址 172.16.12.0/24，其中 172.16.11.1/24 作为办公网段 1 的网关，172.16.12.1/24 作为办公网段 2 的网关。两台设备的：设备 A 和设备 B 工作在路由+NAT 模式，并以 HA 主主模式部署，互为备份，接入网络，两台设备开启本地 web 认证，其中一台设备 A 或 B 挂掉后，已经通过认证上网的用户，仍然能通过另一台备份设备上网，不需要再次认证，具体应用需求如下：

- 办公网段 1：172.16.11.0/24 以设备 A 为主，以设备 B 为备。
- 办公网段 2：172.16.12.0/24 以设备 B 为主，以设备 A 为备。

联动设备为三层交换机或路由器或其它支持策略路由健康检查实现路由备份的设备，因设备选型不一样，配置会不一样，配置不详细列出，配置需求概括如下：

- 172.16.11.0/24 过三层交换机后主链路网关为 172.16.100.1；通过健康检查发现主链路不通后切换到 172.16.200.1 备链路。
- 172.16.12.0/24 过三层交换机后主链路网关为 172.16.200.1；通过健康检查发现主链路不通后切换到 172.16.100.1 备链路。

图1 HA 主主路由模式三层组网图



2.1.2 配置思路

- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 配置 NAT。
- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置地址探测。
- 配置 HA 全局配置，全局配置包含：工作模式、运行状态同步（可选配置）、监控接口地址同步（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

2.1.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

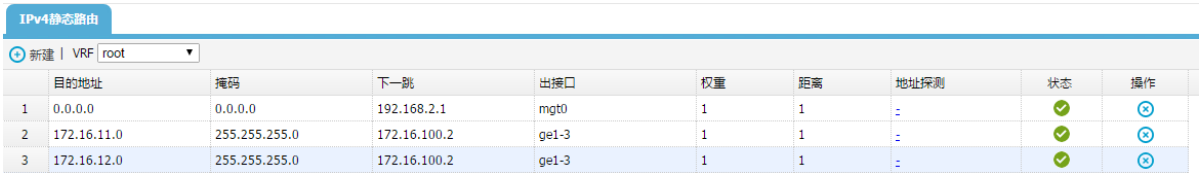
如图 2 所示，进入“网络配置>接口配置”，点击 ge1-0、ge1-3 后的<编辑>按钮，配置 IP 192.168.2.56/24、172.16.100.1/30。

图2 配置接口 IP

(2)　配置静态路由

如图 3 所示，进入“网络配置>路由管理>静态路由”，配置访问外网的默认路由及内网认证用户网段 172.16.11.0/24,172.16.12.0/24 路由。

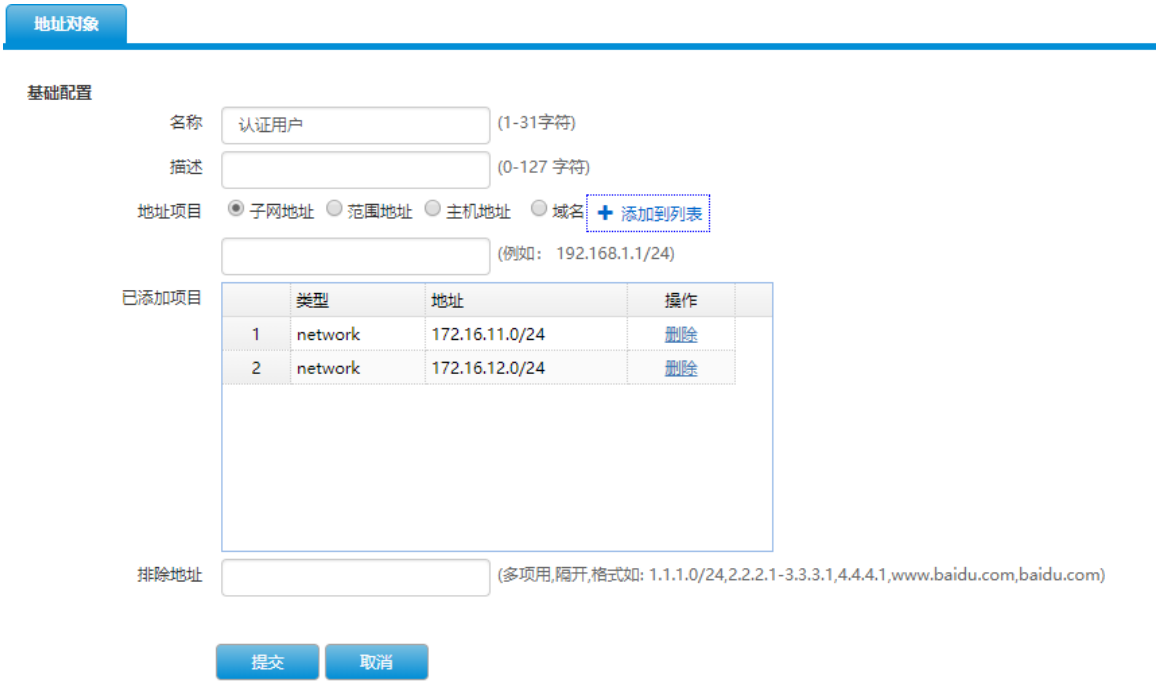
图3 配置静态路由



(3)　配置认证用户地址对象

如图 4 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,172.16.12.0/24，点击<提交>。

图4 配置认证用户地址对象



(4)　配置源 NAT

如图 5 所示，进入“网络配置 > NAT 转换策略 > 源 NAT ”，新建 NAT 策略配置。

图5 配置源 NAT

(5)　申请并导入 license

如图 6 所示，进入“系统管理 > 系统维护 > 授权管理 ”，点击<导入许可证>。

图6 导入 license

(6) 配置 DNS

如图 7 所示，进入“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图7 配置 DNS

(7) 升级特征库

如图 8 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图8 升级特征库

(8) 配置用户识别范围

如图 9 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图9 用户识别范围

(9)　配置地址探测对象

如图 10 所示，进入“策略配置>对象管理>地址对象>地址探测”，点击<新建>按钮创建探测地址对象。

图10 用户识别范围

说明：地址探测支持 ping、TCP、DNS 三种方式。

(10) 配置 HA 全局配置

如图 11 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图11 HA 全局配置

说明：

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- 监控接口地址同步在下联设备为二层设备时开启。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。下联设备检测到主链路不通后，将路由切换到备用链路即可。设备 B 会继续处理设备 A 之前承载的业务，保证业务不中断。监控接口都为 UP 状态时，HA 状态会恢复。
- 地址探测：地址探测失败后，设备 A 的 HA 状态会发生变化，业务切换到设备 B。建议下联联动设备和设备 A 都检查同一个地址，避免设备 A 状态变化后，下联设备路由没有同步切换导致断网的现象出现。

(11) 添加本地认证用户

如图 12 所示，进入“用户管理> 用户组织结构”页面，点击新建选择<用户>，创建用户账号 test。

图12 添加认证用户

(12) 配置本地 web 认证参数

如图 13 所示，进入“用户管理 > 认证管理 > 认证设置 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图13 配置本地 web 认证参数

(13) 配置本地 web 认证策略

如图 14 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图14 认证策略页面

2. 设备 B 配置

所有配置按照拓扑图参照设备 A 的配置步骤和配置方法进行配置即可。

2.1.5 配置注意事项

- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- 如果开启地址探测功能，下联设备健康检查地址要与 HA 设备健康检查地址保持一致。
- HA 主主模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成 master(N)状态后，地址探测就会用管理地址发包了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA master(N)状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

2.1.6 验证配置

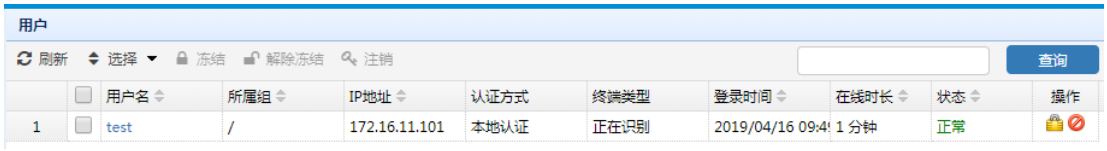
1. 172.16.11.0/24 网段过设备 A 进行认证上网，在线用户会同步给设备 B，当设备 A 挂掉后，用户仍然可以通过设备 B 正常上网，不会断网，也不需要重新认证。

如图 15 所示，设备 A 在线用户。

图15 设备 A 在线用户

将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。设备 A 恢复后，用户再次切回设备 A 上网。

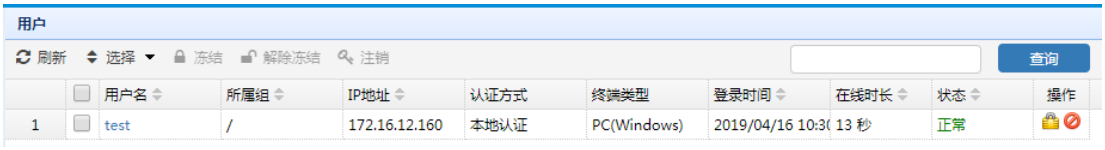
图16 设备 B 在线用户



2. 使用相同的方法验证 172.16.12.0/24 网段的认证效果。用户过设备 B 进行认证上网，在线用户会同步给设备 A，当设备 B 挂掉后，用户仍然可以通过设备 A 正常上网，不会断网，也不需要重新认证。

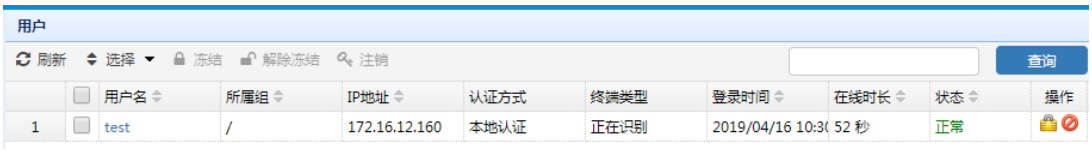
如图 17 所示，设备 A 在线用户。

图17 设备 A 在线用户



将设备 B 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。当设备 B 恢复后，用户再次切回设备 B 上网。

图18 设备 B 在线用户



2.2 组网需求2：HA主主路由模式二层组网

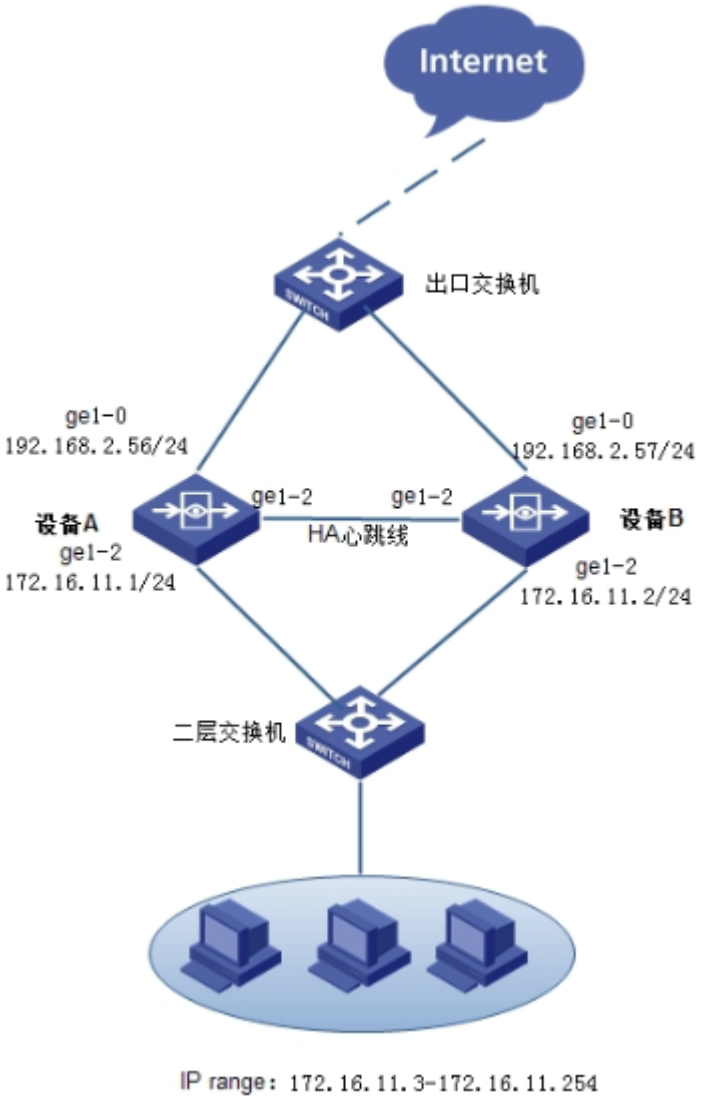
2.2.1 组网需求

如图 19 所示，某公司内网办公网段：IP 地址 172.16.11.0/24 其中 172.16.11.1/24 作为办公网段的网关，172.16.11.2/24 作为办公网段的备用网关。两台设备的：设备 A 和设备 B 工作在路由+NAT 模式，并以 HA 主主模式部署，互为备份，接入网络，两台设备开启本地 web 认证，其中一台设备 A 或 B 挂掉后，已经通过认证上网的用户，仍然能通过另一台备份设备上网，不需要再次认证，具体应用需求如下：

- 办公网段部分用户将网关设置成 172.16.11.1，部分用户将网关设置成 172.16.11.2，当设备 A 故障后，设备 B 会发免费 arp 更新用户 ARP 缓存，原经设备 A 上网的用户会将数据目的 MAC 更改成设备 B 接口 ge1-2 的 MAC 进行上网，当设备 A 恢复后，该部分用户会重新切回设备 A 上网。

该场景下联动设备为二层交换机，只需要保证所有接口在同一个 vlan 即可。

图19 HA 主主路由模式二层组网图



2.2.2 配置思路

- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 配置 NAT。
- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置地址探测。
- 配置 HA 全局配置，全局配置包含：工作模式、运行状态同步（可选配置）、监控接口地址同步（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。

- 配置本地 web 认证策略。
- 验证效果。

2.2.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

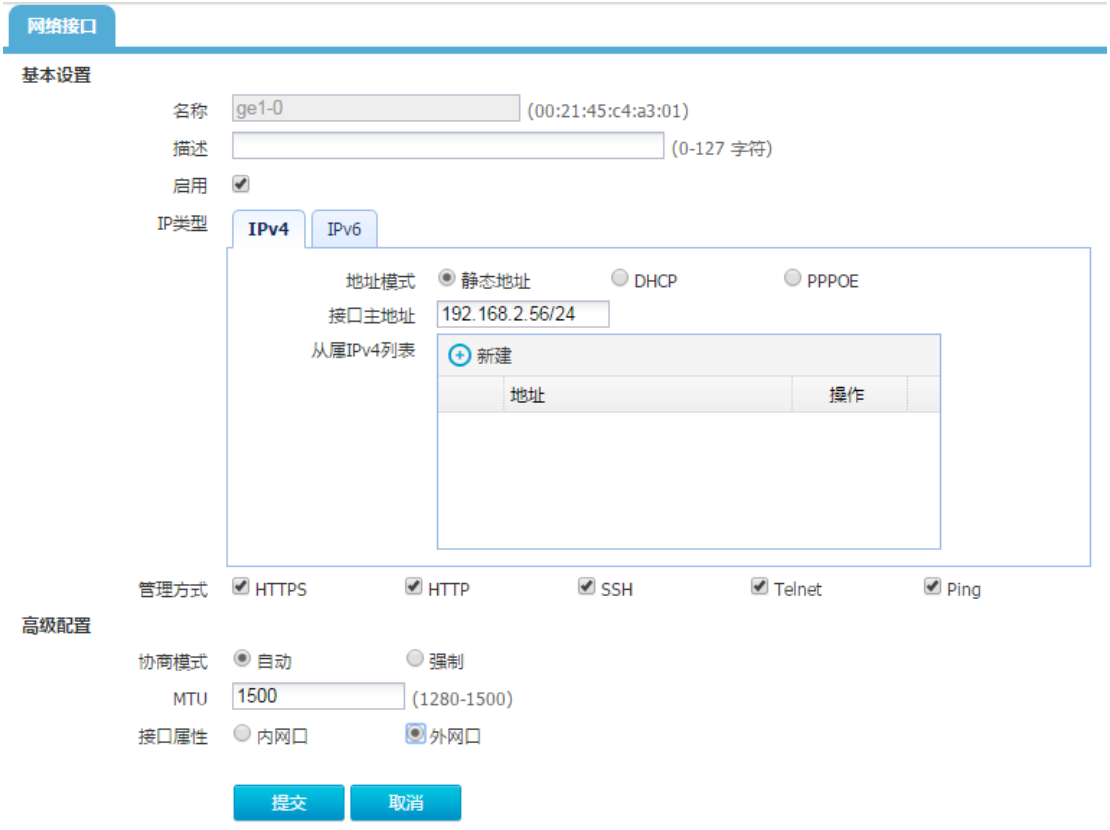
2.2.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 20 所示，进入网络配置>接口配置，点击 ge1-0、ge1-3 后的<编辑>按钮，配置 IP 192.168.2.56/24、172.16.11.1/24。

图20 配置接口 IP



(2)　配置静态路由

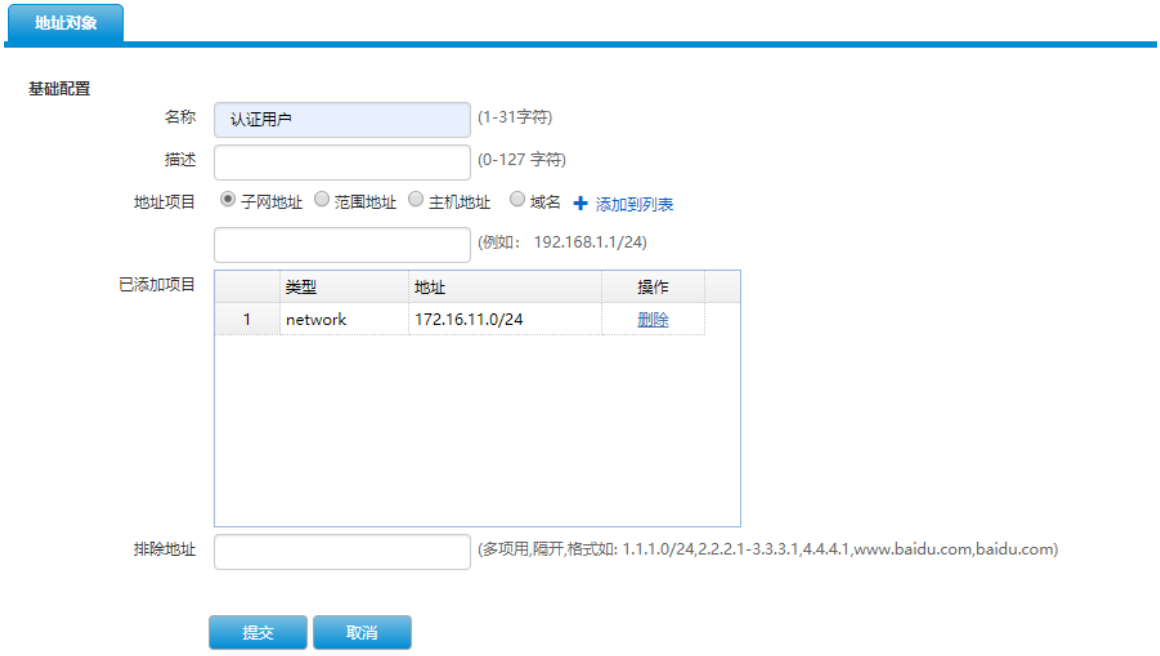
如图 21 所示，进入网络配置>路由管理>静态路由，配置访问外网的默认路由。

图21 配置静态路由

(3)　配置认证用户地址对象

如图 22 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

图22 配置认证用户地址对象



(4) 配置源 NAT

如图 23 所示，进入“网络配置 > NAT 转换策略 > 源 NAT ”，新建 NAT 策略配置。

图23 配置源 NAT

(5) 申请并导入 license

如图 24 所示，进入“系统管理 > 系统维护 > 授权管理 ”，点击<导入许可证>。

图24 导入 license

(6)　配置 DNS

如图 25 所示，进入“网络配置 > 基础网络 > DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图25 配置 DNS

(7)　升级特征库

如图 26 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图26 升级特征库

(8) 配置用户识别范围

如图 27 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图27 用户识别范围

(9)　配置地址探测对象

如图 28 所示，进入策略配置>对象管理>地址对象>地址探测，点击<新建>按钮创建探测地址对象。

图28 用户识别范围

说明：地址探测支持 ping、TCP、DNS 三种方式。

(10) 配置 HA 全局配置

如图 29 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图29 HA 全局配置

说明：

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- 监控接口地址同步在下联设备为二层设备时开启。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。下联设备检测到主链路不通后，将路由切换到备用链路即可。设备 B 会继续处理设备 A 之前承载的业务，保证业务不中断。监控接口都为 UP 状态时，HA 状态会恢复。
- 地址探测：地址探测失败后，设备 A 的 HA 状态会发生变化，业务切换到设备 B。

(11) 添加本地认证用户

如图 30 所示，进入“用户管理> 用户组织结构”页面，点击新建，创建用户账号 test。

图30 添加认证用户

(12) 配置本地 web 认证参数

如图 31 所示，进入“用户管理 > 认证管理 > 认证设置 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图31 配置本地 web 认证参数

(13) 配置本地 web 认证策略

如图 32 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图32 认证策略页面

2. 设备 B 配置

所有配置请按照拓扑图参照设备 A 的配置步骤和配置方法进行配置即可。

2.2.5 配置注意事项

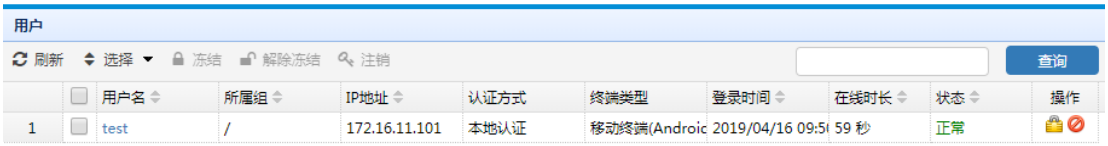
- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主主模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成 master(N)状态后，地址探测就会用管理地址发包了。
- 开启地址探测功能后，在配置源 NAT 时，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA master(N)状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

2.2.6 验证配置

1. 过设备 A 进行认证上网的用户，在线用户会同步给设备 B，当设备 A 挂掉后，用户会切换到设备 B 正常上网，不会断网，也不需要重新认证。

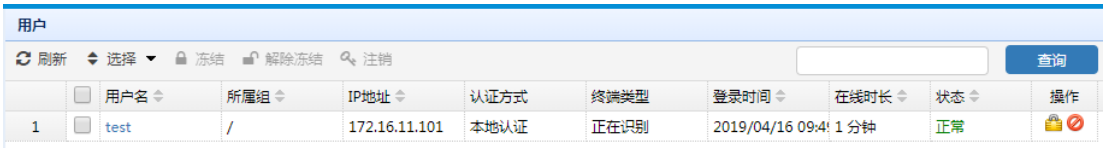
如图 33 所示，设备 A 在线用户。

图33 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。

图34 设备 B 在线用户



2.3 组网需求3：HA主主透明桥模式三层组网

2.3.1 组网需求

如图 35 所示，某公司内网办公网段 1：IP 地址 172.16.11.0/24，办公网段 2：IP 地址 172.16.12.0/24，其中 172.16.11.1/24 作为办公网段 1 的网关，172.16.12.1/24 作为办公网段 2 的网关。两台设备的：设备 A 和设备 B 工作在透明桥模式，并以 HA 主主模式部署，互为备份，接入网络，两台设备开启本地 web 认证，其中一台设备 A 或 B 挂掉后，已经通过认证上网的用户，仍然能通过另一台备份设备上网，不需要再次认证，具体应用需求如下：

- 办公网段 1：172.16.11.0/24 以设备 A 为主，以设备 B 为备。
- 办公网段 2：172.16.12.0/24 以设备 B 为主，以设备 A 为备。

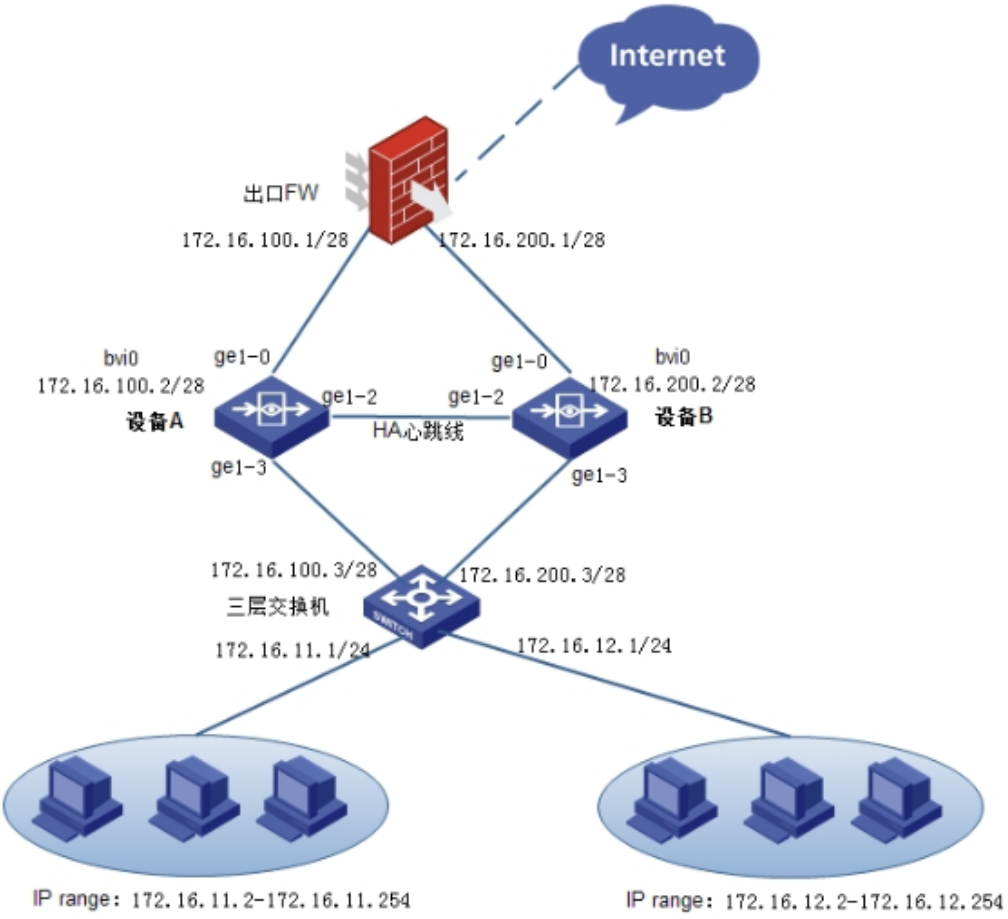
下联联动设备为三层交换机或路由器或其它支持策略路由健康检查实现路由备份的设备，因设备选型不一样，配置会不一样，配置不详细列出，配置需求概括如下：

- 172.16.11.0/24 过三层交换机后主链路网关为 172.16.100.1；通过健康检查发现主链路不通后切换到 172.16.200.1 备链路。
- 172.16.12.0/24 过三层交换机后主链路网关为 172.16.200.1；通过健康检查发现主链路不通后切换到 172.16.100.1 备链路。

上联联动设备为出口 FW，支持策略路由健康检查实现路由备份的功能，因设备选型不一样，配置会不一样，配置不详细列出，主要目的是实现用户数据来回路径保持一致，配置需求概括如下：

- 172.16.11.0/24 的回应数据主链路下一跳为 172.16.100.2；通过健康检查发现主链路不通后切换到 172.16.200.3 备链路。
- 172.16.12.0/24 的回应数据主链路下一跳为 172.16.200.2；通过健康检查发现主链路不通后切换到 172.16.100.3 备链路。

图35 HA 主主路由模式三层组网图



2.3.2 配置思路

- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。

- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置地址探测。
- 配置 HA 全局配置，全局配置包含：工作模式、运行状态同步（可选配置）、监控接口地址同步（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

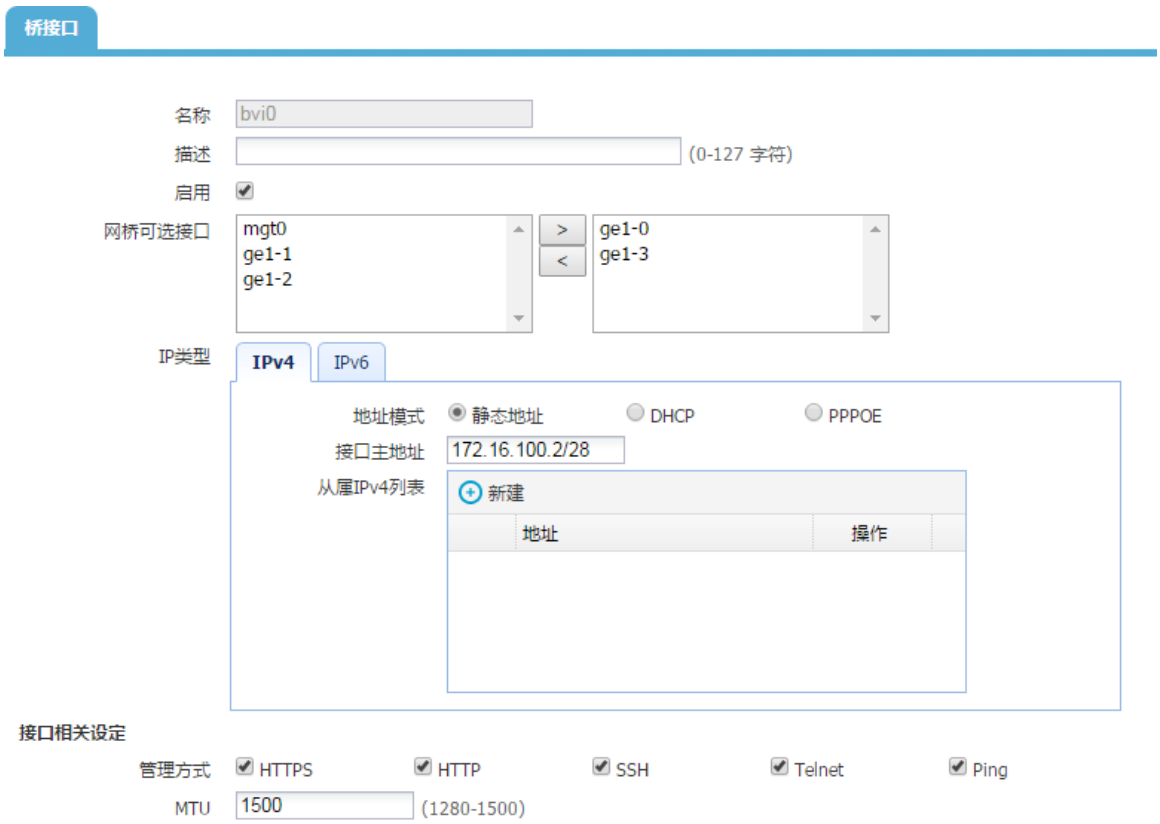
2.3.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 36 所示，进入网络配置>接口配置，在<网桥接口>下点击新建将 ge1-0、ge1-3 添加到桥接口 bvi0 中，并配置 IP 172.16.100.2/28。

图36 配置接口 IP



(2)　配置静态路由

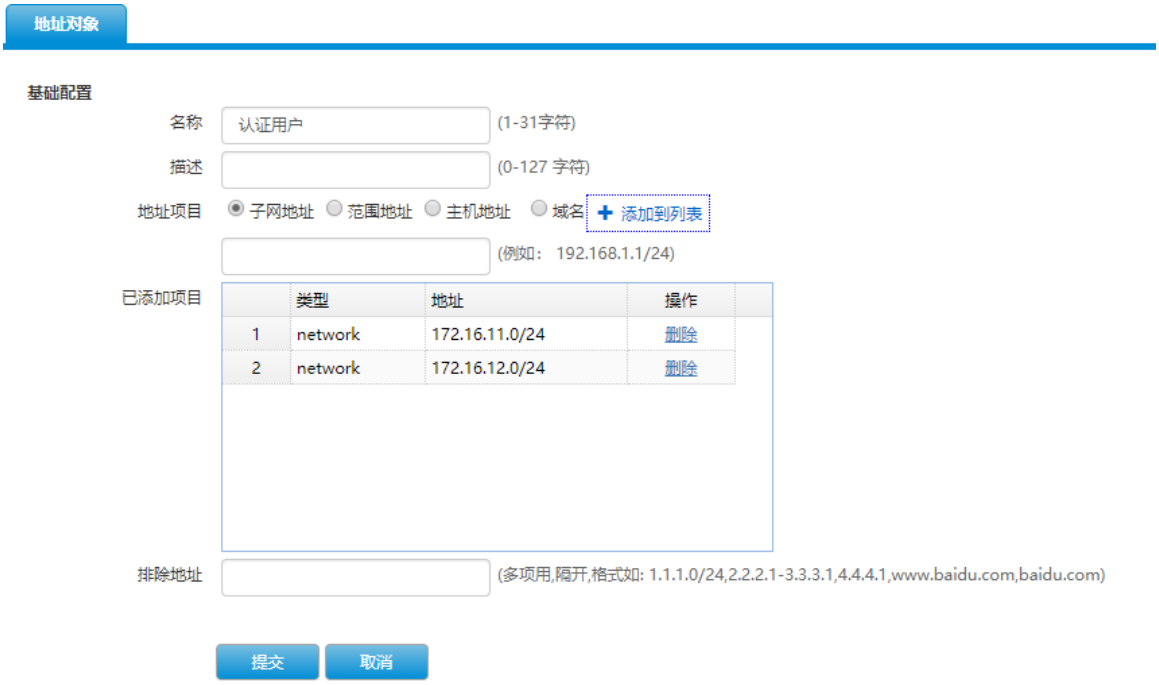
如图 37 所示，进入网络配置>路由管理>静态路由，配置访问外网的默认路由及内网认证用户网段 172.16.11.0/24,172.16.12.0/24 路由。

图37 配置静态路由

(3)　配置认证用户地址对象

如图 38 所示，进入策略配置>对象管理>地址对象>IPv4 地址对象，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24,172.16.12.0/24，点击<提交>。

图38 配置认证用户地址对象



(4)　申请并导入 license

如图 39 所示，进入“系统管理 > 系统维护 > 授权管理”，点击<导入许可证>。

图39 导入 license

(5) 配置 DNS

如图 40 所示，进入“网络配置> DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图40 配置 DNS

(6) 升级特征库

如图 41 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图41 升级特征库

(7) 配置用户识别范围

如图 42 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图42 用户识别范围

(8)　配置地址探测对象

如图 43 所示，进入“策略配置>对象管理>地址对象>地址探测”，点击<新建>按钮创建探测地址对象。

图43 用户识别范围

说明：地址探测支持 ping、TCP、DNS 三种方式。

(9)　配置 HA 全局配置

如图 44 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图44 HA 全局配置

说明：

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- 监控接口地址同步在该场景下不需要开启。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。下联设备检测到主链路不通后，将路由切换到备用链路即可。设备 B 会继续处理设备 A 之前承载的业务，保证业务不中断。监控接口都为 UP 状态时，HA 状态会恢复。
- 地址探测：地址探测失败后，设备 A 的 HA 状态会发生变化，业务切换到设备 B。建议下联联动设备和设备 A 都检查同一个地址，避免设备 A 状态变化后，下联设备路由没有同步切换导致断网的现象出现。

(10) 添加本地认证用户

如图 45 所示，进入“用户管理> 用户 ”页面，点击新建，创建用户账号 test。

图45 添加认证用户

(11) 配置本地 web 认证参数

如图 46 所示，进入“用户管理 > 认证管理 > 认证设置 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图46 配置本地 web 认证参数

(12) 配置本地 web 认证策略

如图 47 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图47 认证策略页面

2. 设备 B 配置

所有配置请根据拓扑图参照设备 A 的配置步骤和配置方法完成配置即可。

2.3.5 配置注意事项

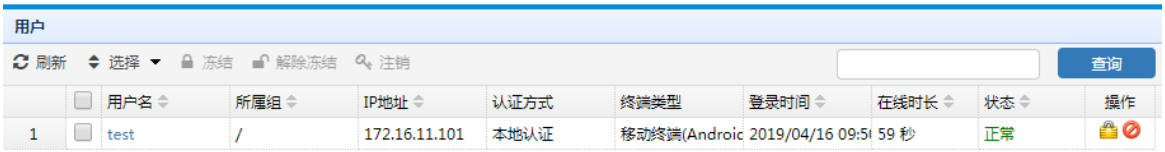
- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主主模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成 master(N)状态后，地址探测就会用管理地址发包了。

2.3.6 验证配置

1. 172.16.11.0/24 网段过设备 A 进行认证上网，在线用户会同步给设备 B，当设备 A 挂掉后，用户仍然可以通过设备 B 正常上网，不会断网，也不需要重新认证。

如图 48 所示，设备 A 在线用户。

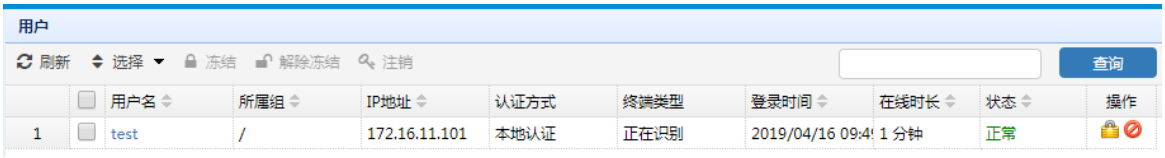
图48 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。设备 A 恢复后，用户再次切回设备 A 上网。

如图 49 所示，设备 B 在线用户。

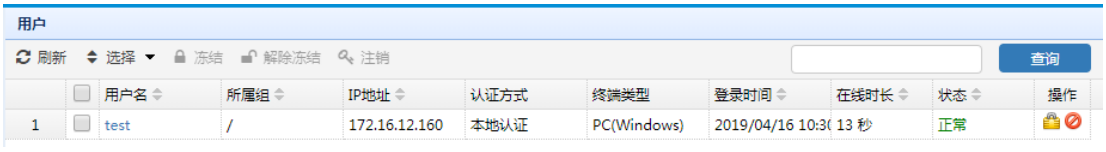
图49 设备 B 在线用户



2. 使用相同的方法验证 172.16.12.0/24 网段的认证效果。用户过设备 B 进行认证上网，在线用户会同步给设备 A，当设备 B 挂掉后，用户仍然可以通过设备 A 正常上网，不会断网，也不需要重新认证。

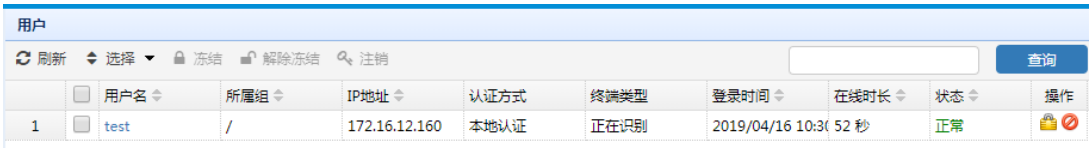
如图 50 所示，设备 A 在线用户。

图50 设备 A 在线用户



将设备 B 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。当设备 B 恢复后，用户再次切回设备 B 上网。

图51 设备 B 在线用户



2.4 组网需求4：HA主主透明桥模式二层组网

2.4.1 组网需求

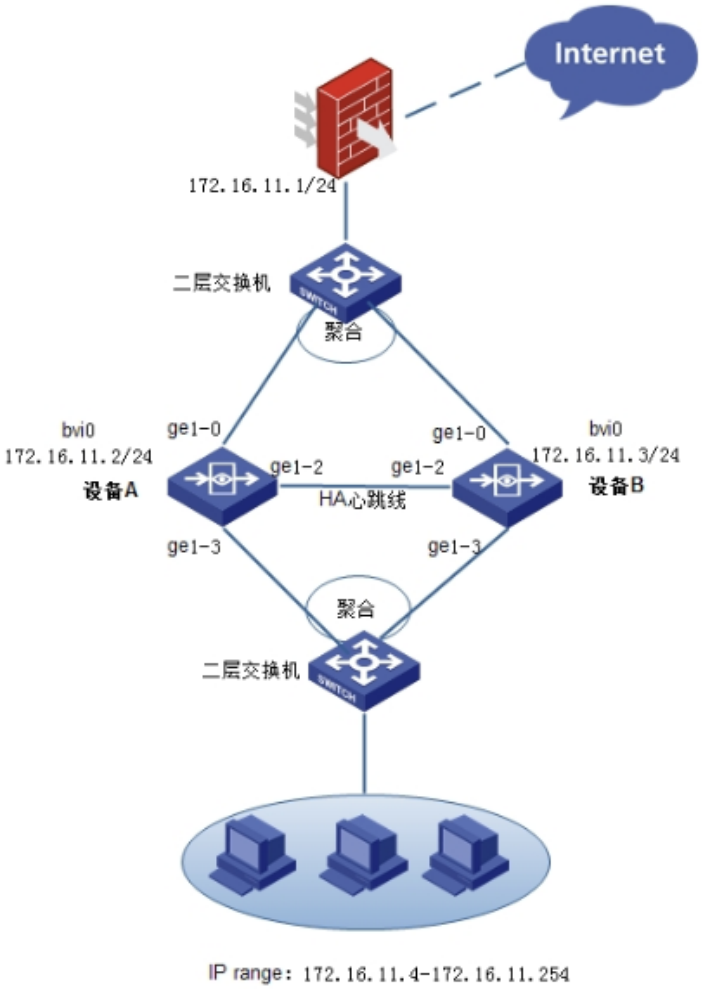
如图 52 所示，某公司内网办公网段：IP 地址 172.16.11.0/24 其中 172.16.11.1/24 作为办公网段的网关。两台设备的：设备 A 和设备 B 工作在透明桥模式，并以 HA 主主模式部署，互为备份，接入网络，两台设备开启本地 web 认证，其中一台设备 A 或 B 挂掉后，已经通过认证上网的用户，仍然能通过另一台备份设备上网，不需要再次认证，具体应用需求如下：

- 办公网段部分用户将网关设置成 172.16.11.1，两台设备透明串接在两台二层交换机中间，转发二层交换机过来的用户流量。

该场景下联动设备为二层交换机，配置需求如下：

- 两台二层交换机之间的两条链路进行聚合，聚合链路算法建议基于源 IP 进行 hash，保证同一个用户的流量走同一条链路。

图52 HA 主主路由模式三层组网图



2.4.2 配置思路

- 配置接口地址。
- 配置路由。
- 配置认证用户地址对象。
- 申请并导入 license 授权。
- 配置 DNS。
- 升级特征库。
- 配置地址探测。
- 配置 HA 全局配置，全局配置包含：工作模式、运行状态同步（可选配置）、监控接口地址同步（可选配置）、HA 通讯接口、被监控接口（可选配置）、地址探测（可选配置）。
- 添加本地认证用户。
- 配置本地 web 认证策略。
- 验证效果。

2.4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

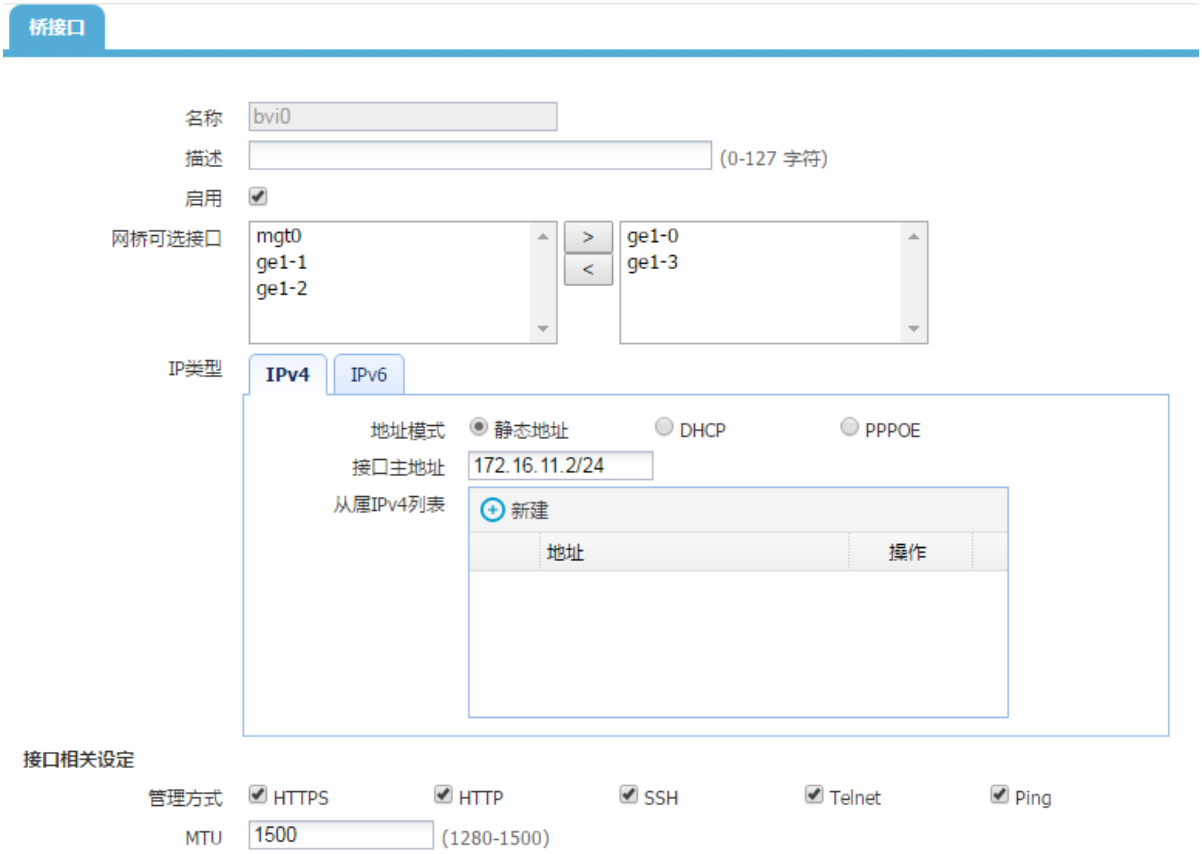
2.4.4 配置步骤

1. 设备 A 配置

(1) 配置接口地址

如图 53 所示，进入“网络配置>接口配置”，在<网桥接口>下点击新建将 ge1-0、ge1-3 添加到桥接口 bvi0 中，并配置 IP 172.16.100.2/28。

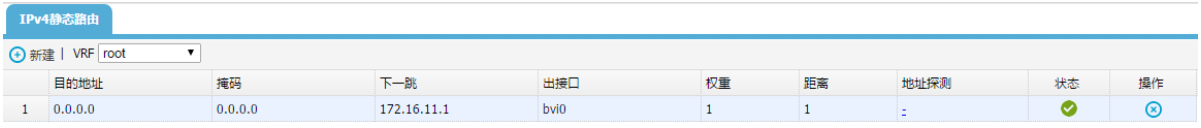
图53 配置接口 IP



(2) 配置静态路由

如图 54 所示，进入“网络配置>路由管理>静态路由”，配置访问外网的默认路由。

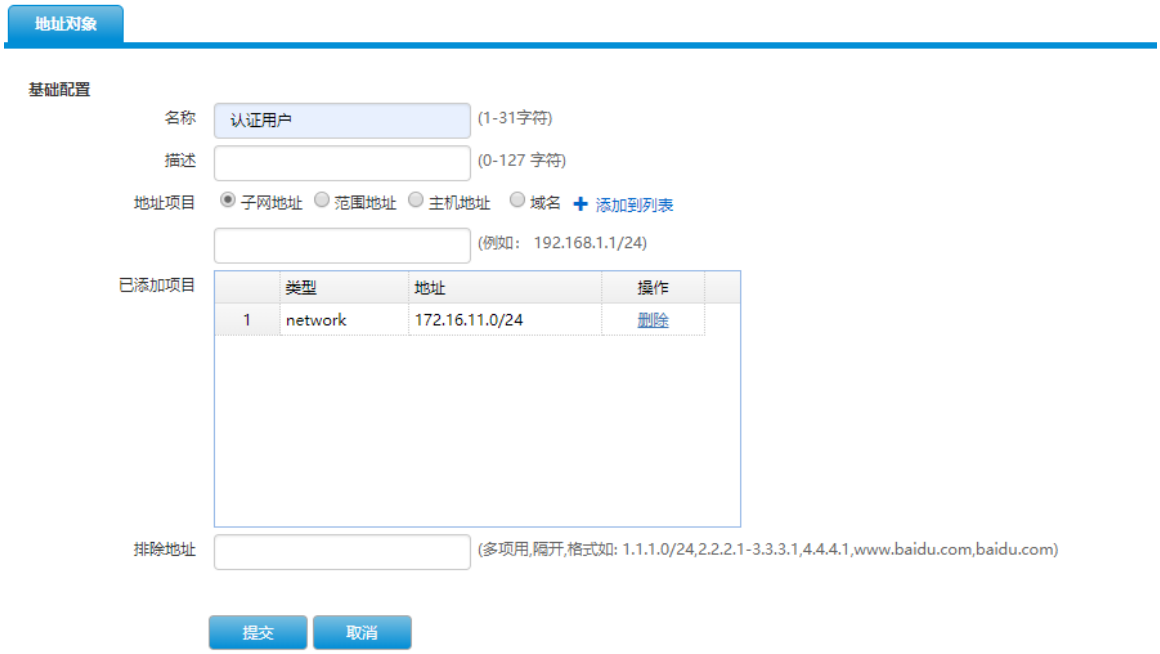
图54 配置静态路由



(3) 配置认证用户地址对象

如图 55 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

图55 配置认证用户地址对象



(4) 申请并导入 license

如图 56 所示，进入“系统管理 > 系统维护 > 授权管理”，点击<导入许可证>。

图56 导入 license

(5) 配置 DNS

如图 57 所示，进入“网络配置> DNS 服务 > DNS 服务器”，配置 DNS 地址，用于升级特征库。

图57 配置 DNS

(6) 升级特征库

如图 58 所示，进入“系统管理 > 系统维护 > 系统升级”，点击立即升级，完成特征库在线自动升级。

图58 升级特征库

(7) 配置用户识别范围

如图 59 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“认证用户”，识别模式选择“强制模式”，提交配置。

图59 用户识别范围

(8) 配置地址探测对象

如图 60 所示，进入“策略配置>对象管理>地址对象>地址探测”，点击<新建>按钮创建探测地址对象。

图60 用户识别范围

说明：地址探测支持 ping、TCP、DNS 三种方式。

(9) 配置 HA 全局配置

如图 61 所示，进入“系统管理 > 系统设定 > 高可用性 > HA 全局配置”页面，进行配置。

图61 HA 全局配置

说明：

- 运行状态同步开启后，会同步 session、fdb、用户等信息。
- 监控接口地址同步在该场景下不需要开启。
- HA 通讯接口用于设备之间交互状态报文、心跳报文、同步运行状态信息。
- 被监控接口：被监控接口中任一接口 down 后，设备 A 的 HA 状态会发生变化，设备 A 不再转发数据。下联设备检测到主链路不通后，将路由切换到备用链路即可。设备 B 会继续处理设备 A 之前承载的业务，保证业务不中断。监控接口都为 UP 状态时，HA 状态会恢复。
- 地址探测：地址探测失败后，设备 A 的 HA 状态会发生变化，业务切换到设备 B。

(10) 添加本地认证用户

如图 62 所示，进入“用户管理> 用户组织结构”页面，点击新建，创建用户账号 test。

图62 添加认证用户

(11) 配置本地 web 认证参数

如图 63 所示，进入“用户管理 > 认证管理 > 认证设置 > 本地 web 认证”页面，没有特殊要求所有配置默认即可。

图63 配置本地 web 认证参数

(12) 配置本地 web 认证策略

如图 64 所示，进入“用户管理 > 认证管理 > 认证策略”页面，选择新建认证策略，按图完成配置。

图64 认证策略页面

2. 设备 B 配置

所有配置请根据拓扑图参照设备 A 的配置步骤和配置方法进行配置即可。

2.4.5 配置注意事项

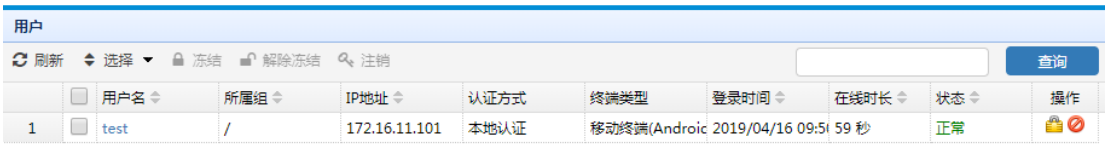
- 用户识别范围要设置成内网用户网段，模式选择强制模式。
- HA 主主模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成 master(N)状态后，地址探测就会用管理地址发包了。

2.4.6 验证配置

1. 过设备 A 进行认证上网的用户，在线用户会同步给设备 B，当设备 A 挂掉后，用户会切换到设备 B 正常上网，不会断网，也不需要重新认证。

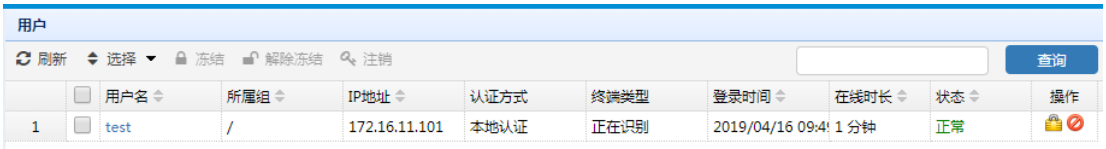
如图 65 所示，设备 A 在线用户。

图65 设备 A 在线用户



将设备 A 重启或 down 监控接口，或探测地址变为不可达，用户仍然可以正常上网。

图66 设备 B 在线用户



3 HA 主主功能使用限制及注意事项

- HA 主主邻居为什么建立不起来时请检查以下内容：

  两台设备必须型号一致，板卡一致。

  两台设备的序列号要求不一致。序列号一致建不起来邻居。

  查看心跳线接口状态是否正常。
- HA 主主环境一台设备宕机后 HA 状态仍然为 master(N)状态，不能转发业务时请检查以下内容：

  a. 确认发探测包的接口是否配置了管理 IP，HA 主主模式下，如果开启地址探测，探测接口需要配置管理 IP，在主状态下地址探测是用主地址发包，但是发生状态切换变成 master(N)状态后，地址探测就会用管理地址发包了。

  b. 确认发探测报文的接口是否配置了源 NAT，如果配置了配置源 NAT，要将管理 IP 的地址排除，避免管理地址过出接口时做源 NAT 导致探测报文发不出去，因为在 HA master(N)

状态下，探测报文源地址为管理 IP 时才会发送，否则会丢包处理，源 NAT 会改变探测报文源地址。

- HA 主主场景，内网用户流量过一台主设备去访问另一台主设备的外网接口时访问不了

  确认 HA 主主是否开启了源 NAT，因为 HA 主设备会同步流给对端主设备，当访问数据到对端主设备外网接口后，在建流时会出现反向流跟已同步过来的流冲突导致丢包。规避方法为 1、不开源 NAT；2、内网用户访问另一台 HA 主设备的内网接口 IP 即可。

4 HA 主主相关原理资料

- **什么是 HA 主主模式**

  主主模式是指实现 HA 的两台设备中， 两台均为主设备。主设备在进行业务的同时， 将流表信息和认证用户信息同步到对端。当其中一台设备出现故障或链路中断时，另外一台设备作为故障设备的备份，接管原主设备的工作，实现网络业务的无缝切换。

  在主主模式下，两台设备均工作，转发流量。主主设备之间通过 HA 心跳线同步状态信息

  主主模式支持路由模式和透明模式。

- **HA 心跳报文**

  HA 设备之间用来相互通告设备的 HA 配置和 HA 状态的报文。如果一个设备在规定时间没有收到邻居心跳报文，可以认定 HA 邻居已经失效。

- **HA 管理地址**

  a. 处于备状态的 HA 设备不会参与网络转发，因此无法通过其接口配置的 IP 地址访问。为了解决这一问题，可以在设备上配置管理地址，用作备设备的网络管理。用户可以从外部访问备设备的 telnet 服务和 web 管理界面。

  b. 当处理备状态下时，设备不参与转发，使用管理地址来发探测包。

- **HA 主主状态切换**

  当设备启用 HA 主主模式后，设备进入 init（初始化状态），然后状态置为 master。设备收到对端发来的 keepalive 报文，两端设备协商参数。建立 master 邻居后，靠心跳报文保持邻居关系，并启动定时器。若在定时器（定时器时间为 interval *retry 次数）时间内，未收到心跳报文，则状态置为 master（A）。出现故障的设备状态置为 master（N）。master（N）状态的设备，监控接口不参与报文转发。

- **HA 主主监控地址同步**

  两台设备均配置监控接口，并开启监控接口地址同步，当其中一台设备的接口 down 掉后，另一台设备的对应接口将对端地址代理，代理地址置为 active，并发送免费 arp 更新用户 arp 缓存，此接口参与出现故障设备的业务转发。

- **HA 主主心跳报文间隔**

  缺省情况下，报文间隔时间为 200 毫秒，重试次数为 5 次，可以通过 keepalive <20-1000> retry<3-500> 命令进行修改。

目录

1 简介

端口镜像（port Mirroring）功能是网络设备上常用的功能，将一个或多个端口的数据流量复制到某一个指定端口来实现对网络的监控。在不影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。

端口镜像功能是对网络流量监控的一个有效的安全手段，对监控流量进行分析和安全性的检查，同时也能及时的在网络发生故障时进行准确的定位。端口镜像功能简单地说就是将被监控流量镜像到监控端口，以便对被监控流量进行故障定位、流量分析、流量备份等，监控端口一般直接与监控主机等相连。端口镜像功能能够将进出网络的所有数据包，供安装了监控软件的管理服务器抓取数据。而企业出于信息安全、保护公司机密的需要，也迫切需要网络中有一个端口能提供这种实时监控功能。在企业中用端口镜像功能，可以很好的对企业内部的网络数据进行监控管理，在网络出现故障的时候，可以做到很好地故障定位。

本模块功能具有如下功能点：

- 支持纯物理接口的端口镜像。
- 支持入流量镜像/出流量镜像/双向流量镜像。
- 支持纯端口镜像，不支持 ACL 镜像。
- 支持一个接口流量镜像到一个或多个监控接口。
- 支持多个接口流量镜像到一个或多个监控接口。
- 支持配置的最大端口镜像规则数量为 8 条。
- 支持保护功能，当设备 packet buffer 数量使用率超过 3/4 时不再进行流量镜像。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解端口镜像特性。

3 使用限制

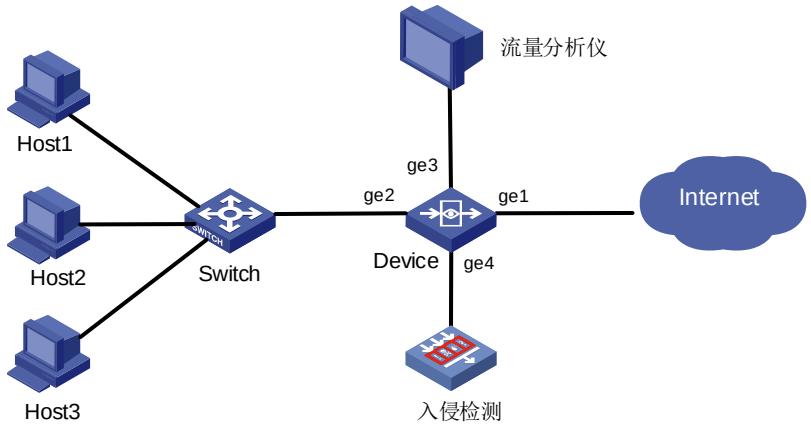
- 接口已经作为镜像规则源接口时不可再配置为其它规则的监控接口。
- 接口已经作为镜像规则监控接口时不可再配置为其它规则的源接口。
- 源接口和监控接口不能是同一个物理接口，要么配置为源接口，要么配置为监控接口，不能同时配置。
- 管理口以及旁路接口不可配置为监控接口。
- 在线业务口不可配置为监控接口（在线业务口即为现网在跑正常业务的物理接口）。
- 端口镜像规则数量规格为 8 条。

4 配置举例

4.1 组网需求

如图 1 所示用户有两台监控分析设备，功能不同，一台是专用流量分析仪，另一台是 IDS 设备。用户希望能对设备上去往和来自 Internet 的流量同时进行流量综合分析和入侵检测。

图1 组网图



4.2 配置思路

按照组网图组网。

(1) 登录 Web 网管。

(2) 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与流量分析仪所连接口。

(3) 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与 IDS 设备所连接口。

4.3 使用版本

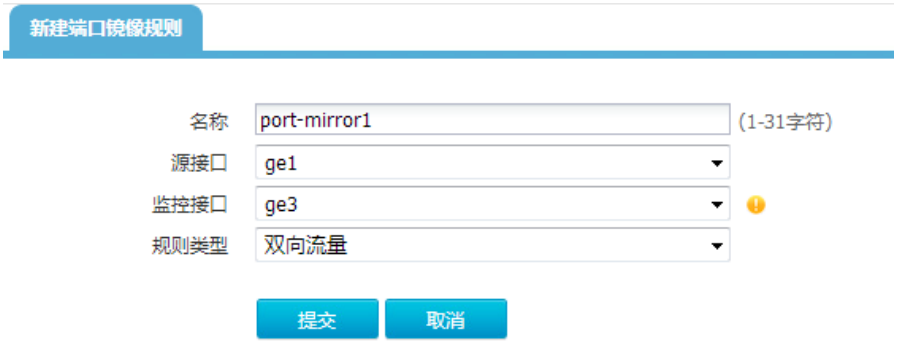
本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

1. 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与流量分析仪所连接口

如图 2 所示，进入“网络配置>基础网络>端口镜像”，新建端口镜像规则 port-mirror1，源端口为 ge1，监控接口为 ge3，规则类型为双向流量，点击<提交>按钮。

图2 新建端口镜像规则 port-mirror1



2. 新建端口镜像规则，将设备连接 Internet 接口流量镜像到设备与 IDS 设备所连接口

如图 3 所示，进入“网络配置>基础网络>端口镜像”，新建端口镜像规则 port-mirror2,源端口为 ge1，监控接口为 ge4，规则类型为双向流量，点击<提交>按钮。

图3 新建端口镜像规则 port-mirror2

3. 配置完成后效果图

如图 4 所示，配置完成后效果如下图。

图4 端口镜像配置效果图

4.5 验证配置

(1) 在设备查看接口流量大小，如下图所示，ge3、ge4 接口发送的流量大小等于 ge1 接口接收和发送流量之和。

	名称	链路状态	属性	工作速率	双工模式	IP地址	IPv6地址	接收速率	发送速率	接收总包数	接收总字节数	发送总包数	发送总字节数	MAC地址
3	ge1	up	-	1000	full	211.136.100.1/24		529.60 Mbps	21.82 Mbps	3653944	5324240611	3645742	219321696	00:01:7a:c4:ca:a7
4	ge2	up	-	1000	full	172.16.1.1/24		21.82 Mbps	529.60 Mbps	3646255	219352476	3654205	5324283897	00:01:7a:c4:ca:a8
5	ge3	up	-	1000	full			0 bps	551.42 Mbps	0	0	7299757	5543613396	00:01:7a:c4:ca:a9
6	ge4	up	-	1000	full			0 bps	551.42 Mbps	0	0	7299794	5543644696	00:01:7a:c4:ca:aa

(2) 用户在两台监控分析设备上可以同时收到去往和来自 Internet 的流量，镜像功能生效。这样，用户就可以对去往和来自 Internet 的流量分别进行综合分析和入侵检测了。

目录

1 简介

DDNS 是对域名绑定的 IP 地址进行动态更新，解决网络中已注册域名的服务器的 IP 地址是动态变化的，服务器公网 IP 变更时，导致 DNS 域名服务器所绑定的该服务器的 IP 地址已经过时，用户通过域名方式无法正常访问该服务器的相关服务。设备开启 DDNS 功能后，通过更新报文把动态 IP 地址信息发送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析；保证网络可以通过此域名正常访问到服务器。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 DDNS 特性。

3 使用限制

- 需先配置 DNS 服务器（若公网接口地址模式为 DHCP 或 PPPoe 且配置更新 DNS 功能，设备可自动获取 DNS 服务器地址，可无需再手工配置 DNS 服务器），保证设备能够正常对域名进行解析。
- 目前服务商只支持花生壳，支持最多 10 个账户同时使用。
- 由于花生壳服务器限制，无法对账户下某个特定域名进行更新，目前支持更新此账户名下的所有绑定的域名。

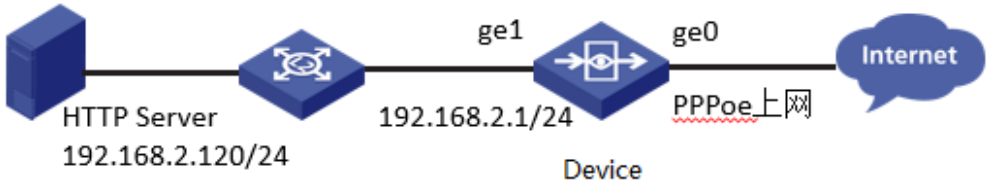
4 配置举例

4.1 组网需求

如下图所示，有一条公网 PPPOE 线路 WLAN 接口，内网服务器提供 HTTP 服务；具体应用需求如下：

- DDNS 实现域名 IP 动态绑定。
- 目的 NAT 实现对内网服务器进行地址映射。
- 在 WLAN 接口公网 IP 变化的情况下，仍可通过域名方式正常访问内网 HTTP 服务。

图1 DDNS 组网图



4.2 配置思路

按照组网图组网。

(1) 配置 DNS 服务器。

(2) 启用 DDNS 功能，配置动态域名服务 DDNS。

(3) 配置目的 NAT，将动态域名映射到内网服务器。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

1. 配置 dns 服务器，保证设备能够正常进行域名解析

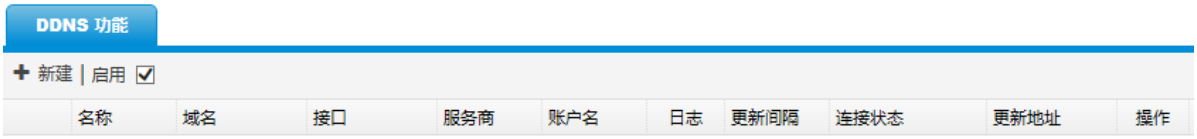
如图 2 所示，进入“网络配置>基础网络>DNS 服务>DNS 服务器”，配置 DNS 服务器为 114.114.114.114，点击<提交>。

图2 配置 dns 服务器

2. 配置 DDNS 功能

如图 3 所示，进入 “网络配置>基础网络>DDNS 服务”。勾选启用选项，点击确定。

图3 启用 DDNS 功能

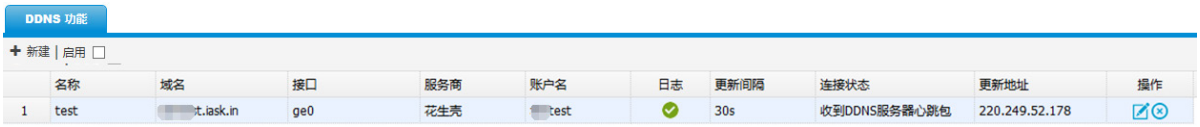


如图 4 所示，进入 “网络配置>基础网络>DDNS 服务”。点击<新建>，配置名称为 test，域名为 ***test.iask.in，接口为 ge0，服务商为花生壳，更新间隔 30，点击<提交>

图4 配置动态域名服务 DDNS

如图 5 所示，创建成功设备将与花生壳服务商进行连接，成功后会根据配置的更新间隔发送更新报文进行更新，并显示当前更新的公网 IP 地址

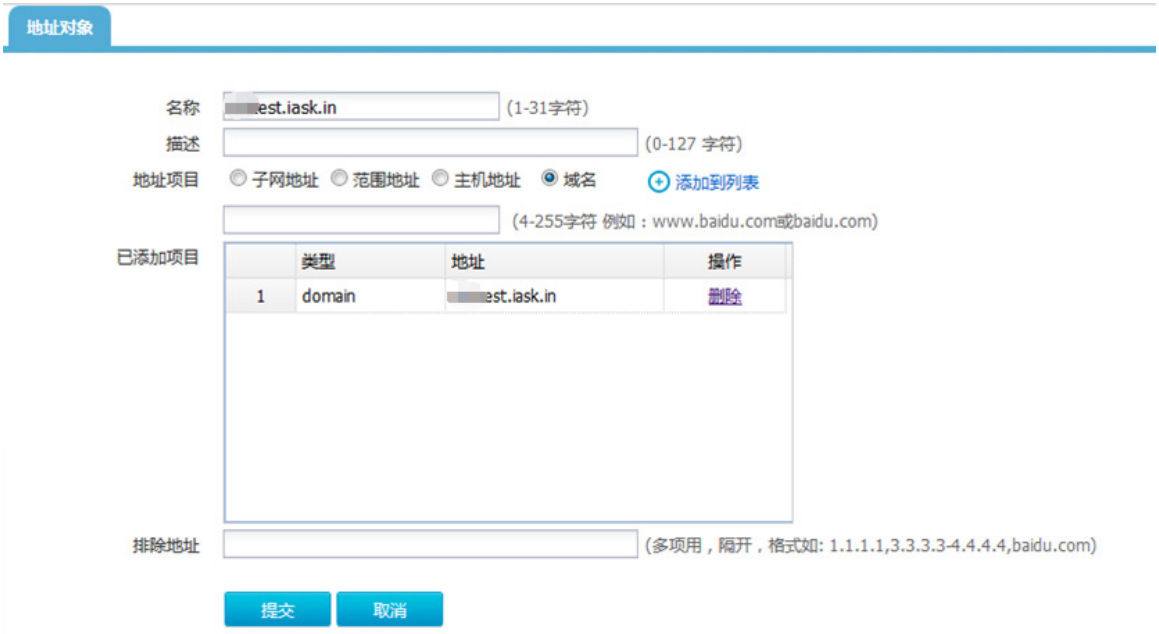
图5 DDNS 功能状态显示



3. 配置目的 NAT，将动态域名映射到内网服务器

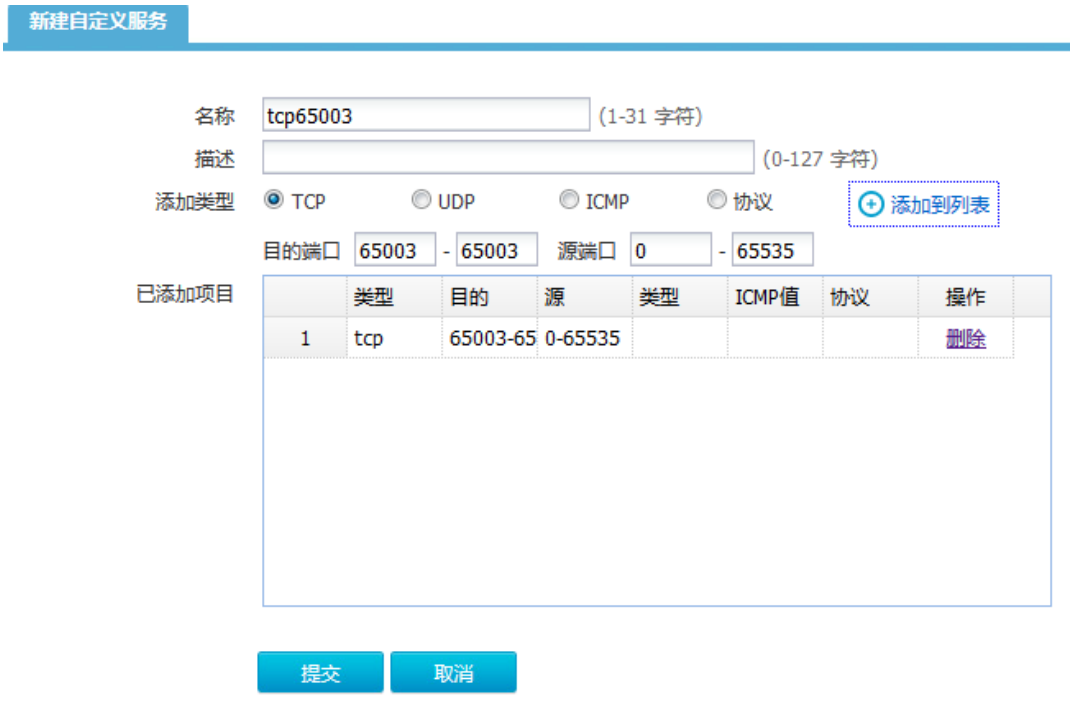
如图 6 所示，进入 “策略配置>对象管理>地址对象>IPv4 地址对象”。点击<新建>，配置域名为 ***test.iask.in ，点击<提交>

图6 配置地址对象



如下图所示，进入“策略配置>对象管理>服务对象>自定义服务”。点击<新建>，配置名称为 tcp65003，目的端口 65003-65003，源端口 0-65535 的自定义服务对象，点击<提交> 。

图7 配置自定义服务



如图 7 所示，进入“策略配置>NAT 转换策略>地址池”。点击<新建>，配置名称为 httpserver，地址池的地址项目为 192.168.2.120，点击<提交>。

图8 配置地址池

如图 9 所示，进入“策略配置>NAT 转换策略>目的 NAT”。点击<新建>，配置源地址为 any，目的地址为地址对象***test.iask.in,服务为自定义服务 tcp65503,接口为 ge0,转换后 IP 为 httpserver，转换后端口为 80，点击<提交>

图9 配置目的 NAT

如图 10 所示，目的 NAT 配置完成后显示

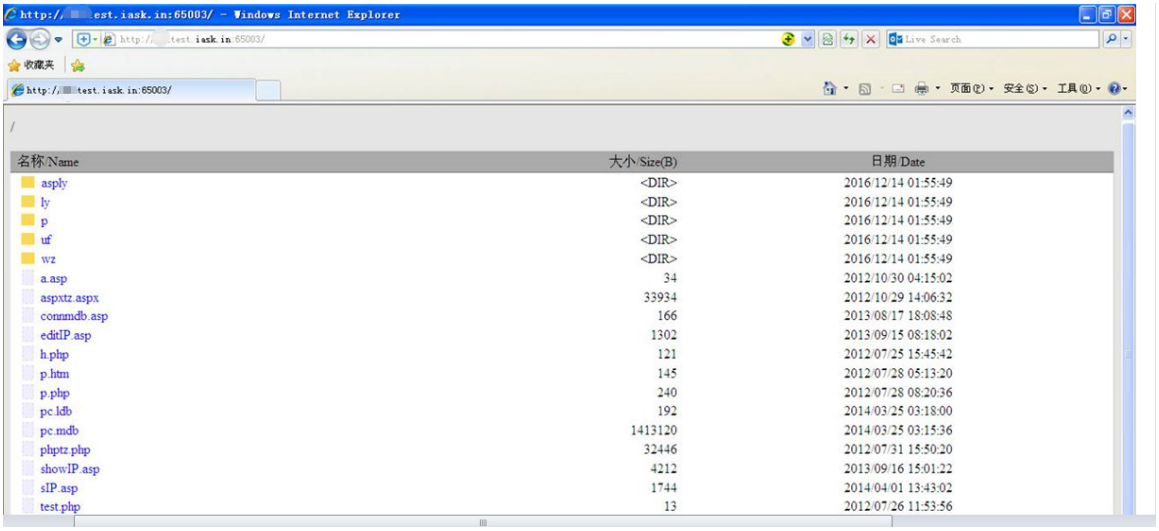
图10 目的 NAT

4.5 验证配置

(1) 验证 DDNS 功能

如图 11 所示，在 Internet 访问 http:// ***test.iask.in:65003，可正常访问内网的 HTTP 服务器，当外网口 IP 地址发生变更后，通过域名访问内网 HTTP 服务器正常。

图11 通过域名访问内网 HTTP 服务器效果图



目 录

1 简介

本文档介绍设备的共享上网监控功能配置举例，在配置前，先了解如下定义：

- 共享用户检测：检测存在多个用户共享一个 IP 或账号上网的行为。
- 共享热点：无线 AP 或 TP-Link 等具备 DHCP 及 NAT 功能，能承载多用户上网的设备。
- 自动阻断：当检测到存在共享上网行为的热点后设备会根据配置的规则阻断用户上网，并推送阻断提示。
- 自动限速：当检测到存在共享上网行为的热点后，设备会根据配置的规则对共享用户进行限速控制。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

- 无线热点可使用 pppoe 拨号、DHCP 或固定 IP 接入网络，本配置举例以手动配置固定 IP 方式进行介绍。

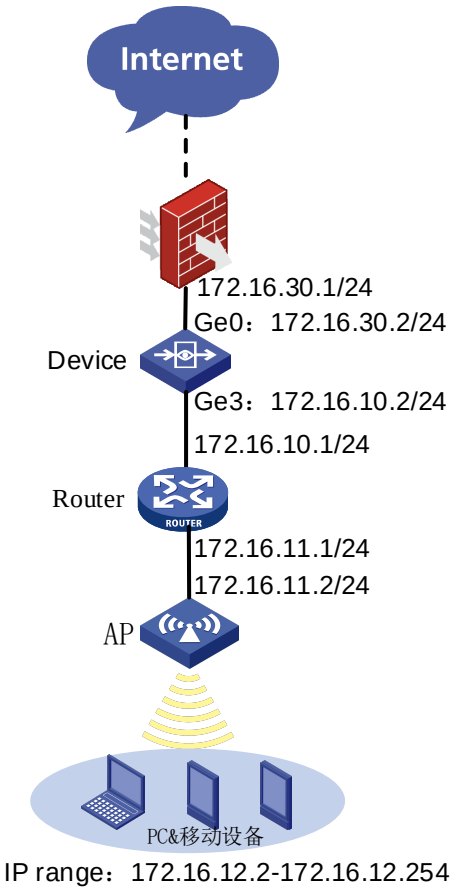
本文档假设您已了解共享上网监控特性。

3 共享上网监控配置举例：阻断惩罚

3.1.1 组网需求

如图 1 所示，某高校给已注册交费的学生开通上网账号，要求一个账号只能允许一个学生使用，禁止一个账号多人共享使用的情况，当发现存在共享上网行为的热点时自动将用户阻断，但允许一台电脑和 1 个移动设备同时接入的情况，使用设备的的 ge0 和 ge3 接口以三层路由模式部署在网络中，设备上联出口 FW，下联三层设备路由器。设备上开启防共享功能，检测共享上网行为并进行阻断和提醒。

图1 防共享组网



3.1.2 配置思路

- 配置设备接口地址及路由。
- 配置共享检测地址对象。
- 配置用户识别范围。
- 配置 IPv4 控制策略默认规则。
- 开启防共享功能。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

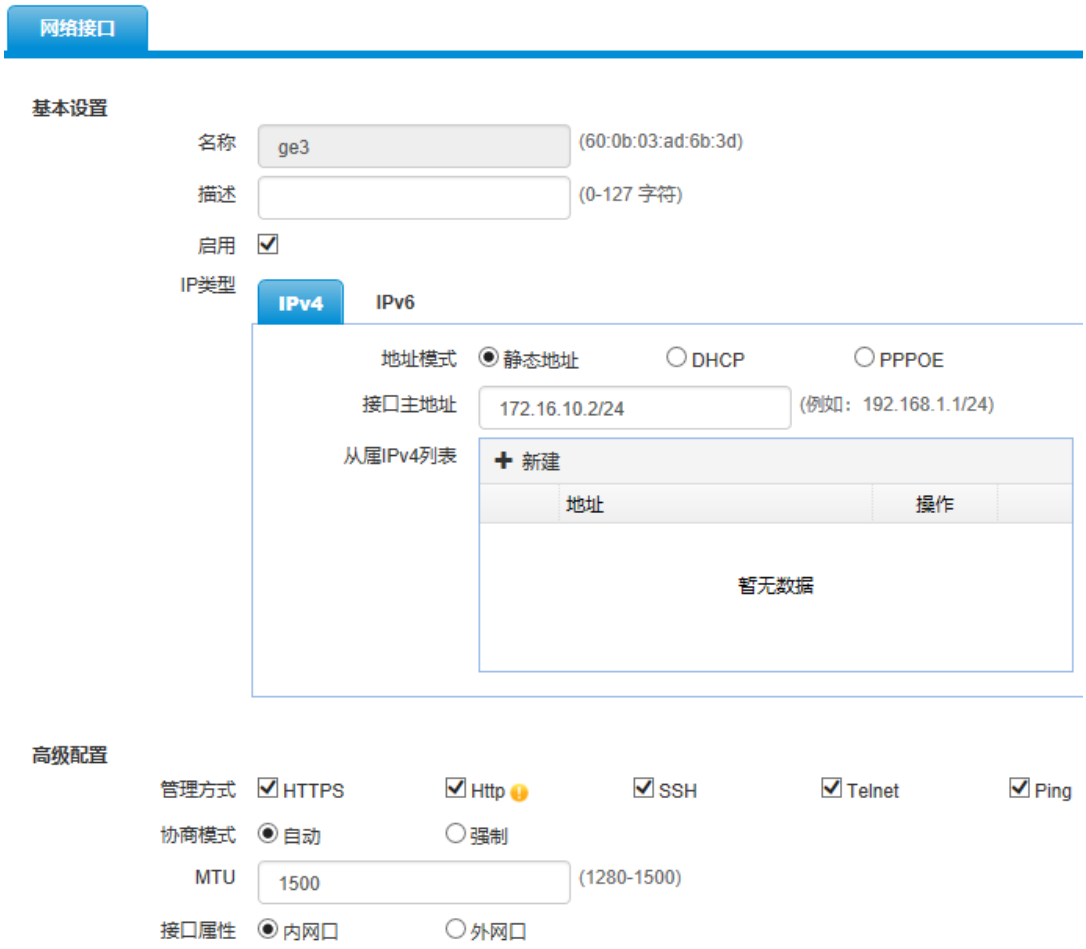
(1) 配置路由接口

如图 2、图 3 所示，进入网络配置>接口配置，点击编辑 ge0、ge3 操作，把 ge0、ge3 的地址分别配置为 172.16.30.2/24、172.16.10.2/24。

图2 配置 ge0 接口


网络接口
基本设置
名称
ge0
(60:0b:03:ad:6b:3a)
描述
(0-127 字符)
启用
IP类型
IPv4
IPv6
地址模式
静态地址
DHCP
PPPOE
接口主地址
172.16.30.2/24
(例如：192.168.1.1/24)
从属IPv4列表
新建
地址
操作
暂无数据
高级配置
管理方式
HTTPS
Http
SSH
Telnet
Ping
协商模式
自动
强制
MTU
1500
(1280-1500)
接口属性
内网口
外网口

图3 配置 ge3 接口



(2) 配置静态路由

如图 4 配置访问外网的默认路由及去往内网用户网段 172.16.11.0/24,172.16.12.0/24 路由。

图4 配置静态路由

	目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	操作
1	0.0.0.0	0.0.0.0	172.16.30.1	ge0	1	1	-		
2	172.16.11.0	255.255.255.0	172.16.10.1	ge3	1	1	-		
3	172.16.12.0	255.255.255.0	172.16.10.1	ge3	1	1	-		

(3) 配置防共享用户地址对象

如图 5 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建防共享用户地址对象，设置地址为 172.16.11.0/24，点击<提交>。

图5 配置防共享用户地址对象

(4) 配置用户识别范围

如图 6 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“防共享用户”，其它配置默认，提交配置。

图6 用户识别范围

(5)　修改 IPv4 控制策略默认规则

如图 7 所示，进入“策略配置>IPv4 控制策略”，选择默认规则为允许。

图7 修改默认规则

(6)　开启防共享功能

如图 8 所示，进入“策略配置 > 共享接入管理 > 共享接入配置”页面，配置防共享参数。

图8 防共享配置

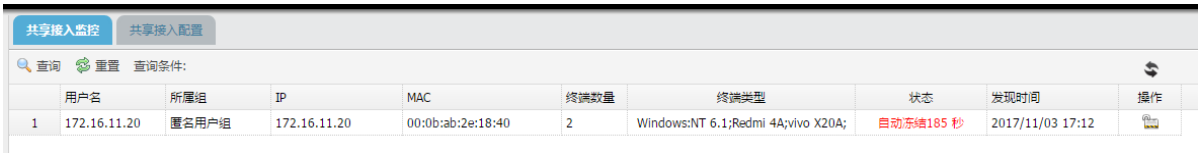
3.1.5 配置注意事项

- 无线热点开启 NAT 功能，开启 DHCP，配置地址池范围为 172.16.12.2/24~172.16.12.254/24。无线热点使用固定 IP 或拨号上网。
- 共享接入用户 NAT 后网段必须在用户识别范围中，否则会导致共享接入检测不到共享用户。

3.1.6 验证配置

如图 9 所示，某学生使用 1 台 PC 和 1 个移动终端访问网络，检测到共享上网行为，上网被阻断，并收到阻断提醒。

图9 共享接入监控状态冻结



如图 10 所示， 设备向终端推送阻断提示

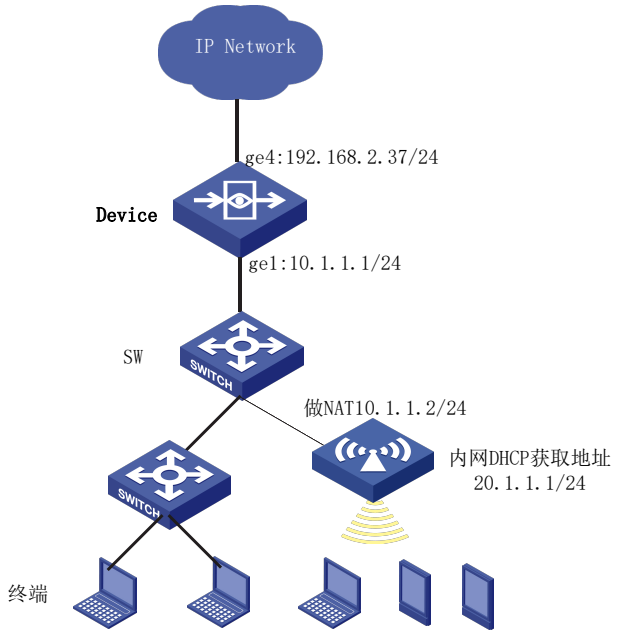
图10 阻断提示

4 共享上网监控功能配置举例：限速惩罚

4.1.1 组网需求

如图 11 所示，某企业网络内网用户通过设备访问外网，但是部分内网用户私接路由器访问外网，导致出口带宽严重不够，影响企业对外提供的一些业务，现需对私接路由器的用户进行检测并对检测到的共享用户进行限速惩罚。

图11 共享上网监控组网



4.1.2 配置思路

- 配置设备接口地址、路由、NAT。
- 配置内网用户地址对象。
- 配置用户识别范围。
- 配置 IPv4 控制策略默认规则。
- 配置限速惩罚通道。
- 开启防共享功能。

4.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.1.4 配置步骤

(1) 配置路由接口

如图 12 所示，进入“网络配置>接口配置>物理接口”，点击编辑 ge1、ge4 操作，把 ge1、ge4 的地址分别配置为 10.1.1.1/24、192.168.2.37/24。

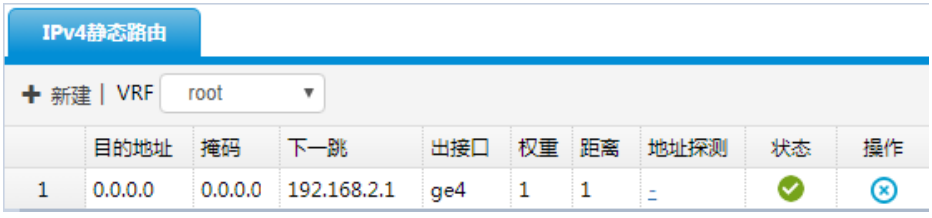
图12 接口地址配置

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0		90.90.1.37/24		00:21:45:3f:de:9a	route	full	100	up		
2	ge1		10.1.1.1/24		00:21:45:3f:de:9b	route	full	100	up		
3	ge2				00:21:45:3f:de:9c	route	full	1000	down		
4	ge3				00:21:45:3f:de:9d	route	full	1000	up		
5	ge4		192.168.2.37/24		00:21:45:3f:de:9e	route	full	100	up		

(2) 配置静态路由

如图 13 所示，进入“网络管理>路由>静态路由”，配置一条访问外网的默认路由。

图13 配置静态路由



(3) 配置源 NAT

如图 14 所示，进入“策略配置>NAT 转换策略>源 NAT”，新建一条源 NAT，使内网用户正常访问外网。

图14 源 NAT 配置

(4) 配置内网用户地址对象

如图 15 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建认证用户地址对象，设置地址为 10.1.1.0/24，点击<提交>。

图15 内网用户地址对象

(5) 配置用户识别范围

如图 16 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“10.1.1.0”，其它配置默认，提交配置。

图16 用户识别范围

(6)　修改 IPv4 控制策略默认规则

如图 17 所示，进入“策略配置>IPv4 控制策略”，选择默认规则为允许。

图17 修改默认规则

(7)　配置限速惩罚通道

如图 18 所示，进入“策略配置>流量控制策略>流量控制”，新建一条“惩罚通道”，配置惩罚通道参数。

图18 惩罚通道

(8)　开启共享上网监控功能

如图 19 所示，进入“策略配置 > 共享接入管理 > 共享接入配置”页面，配置共享接入配置参数。

图19 共享接入配置

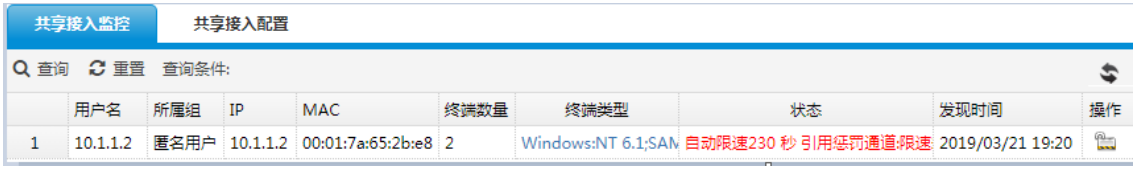
4.1.5 配置注意事项

- 无线热点开启 NAT 功能，开启 DHCP，配置地址池范围为 20.1.1.10-20.1.1.50。无线热点使用固定 IP 或拨号上网。
- 共享接入用户 NAT 后网段必须在用户识别范围中，否则会导致共享接入检测不到共享用户。

4.1.6 验证配置

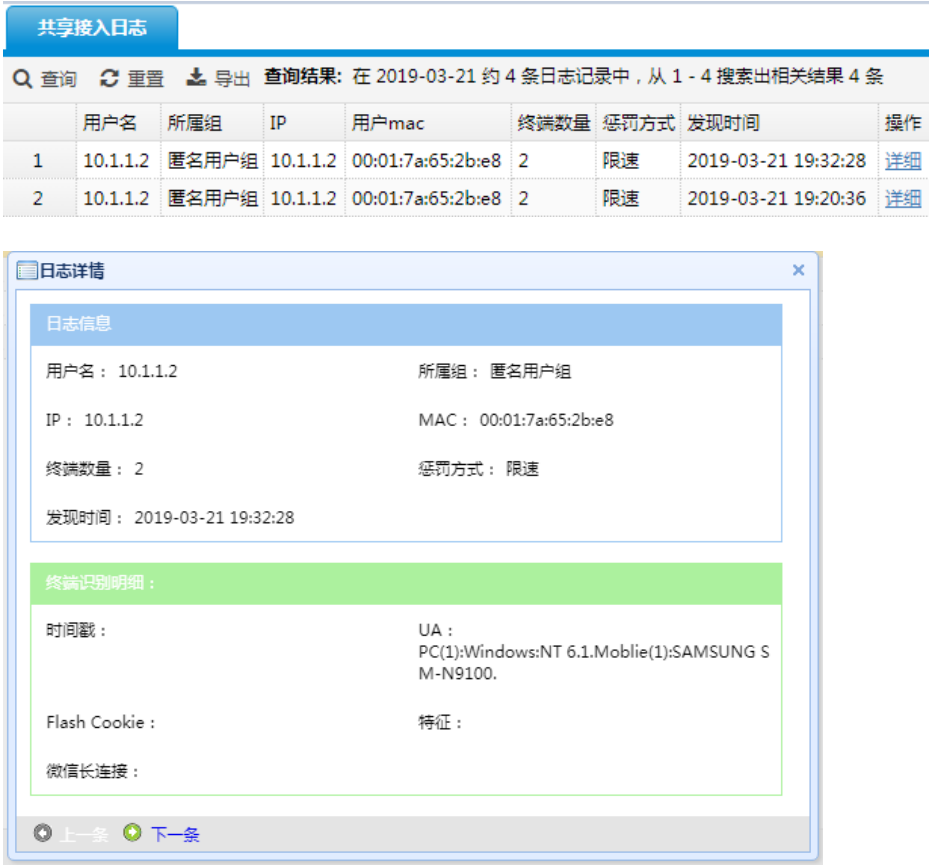
如图 20 所示，某用户使用 1 台 PC 和 1 个移动终端访问网络，能检测到共享上网行为，自动被限速惩罚。

图20 共享接入监控状态被限速惩罚



如图 21 所示， 可以在共享接入日志上查看到终端被限速惩罚的日志信息，点击<详细>可查看到终端识别明细信息。

图21 共享接入限速日志



5 防共享说明

移动终端识别方式包含：

- 基于时间戳识别技术
- 基于 UA 识别技术
- 基于微信长连接识别技术
- 基于应用特征识别技术

PC 终端识别方式包含：

- 基于 webRTC+flash cookie 识别技术
- 基于 UA 识别技术
- 基于应用特征识别技术
- 基于微信长连接识别技术

目录

1 简介

本文档介绍设备的 APP 动态缓存配置举例。

APP 动态缓存介绍：

- 自学习型缓存服务器是一种用来缓冲 Internet 数据的软件或服务器设备。它是这样实现其功能的，接受来自人们需要下载的目标（object）的请求并适当地处理这些请求。也就是说，如果一个人想下载一 web 页面，他请求自学习型缓存服务器为他取得这个页面。缓存服务器随之连接到远程服务器（比如：http：// nlanr.net/）并向这个页面发出请求。然后，缓存服务器不仅显式地聚集数据到客户端机器，而且同时复制一份保存在服务器设备上。当下一次有人需要同一页面时，缓存服务器就可以简单地从磁盘中读到它，那样数据立即就会传输到客户机上，从而加快访问速度，节省了网络带宽。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 APP 动态缓存的特性。

3 使用限制

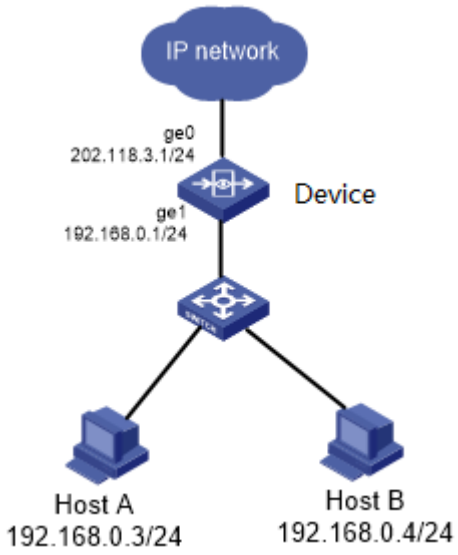
当设备的磁盘空间大于缓存的 APP 文件，APP 动态缓存功能可以正常缓存成功。

4 配置举例

4.1 组网需求

如图 1 所示，某公司内网办公网段 IP 地址为 192.168.0.0/24。使用设备的的 ge1（192.168.0.1）口连接内网设备，ge0 （202.118.3.1/24）口连接外网，在设备开启 APP 动态缓存功能。

图1 APP 动态缓存功能组网图



4.2 配置思路

- 配置 DNS 服务器。
- 新建 APP 动态缓存的域名。
- 测试用户通过设备下载 app 应用。

4.3 使用版本

本举例是在 E6442 上进行配置和验证。

4.4 配置注意事项

- 域名长度 4-255 字符，字符只能是数字，字母，'-'，每一级域名长度不超过 63 个字符，最后一级 2-6 个字符。
- APP 动态缓存的域名规格是 8 条。
- 必须开启 DNS 服务器，设置的 DNS 地址要能正常解析域名，必须保证在设备上能 ping 通动态缓存配置的域名地址。

4.5 配置步骤

4.5.1 配置设备

1. 配置 DNS 服务器

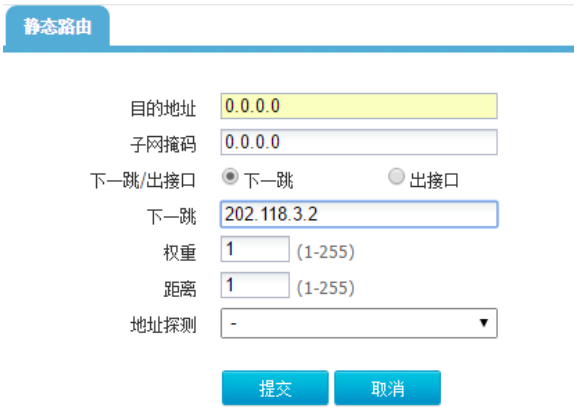
如图 2 所示，在设备上进入“网络配置>基础网络>DNS 服务>DNS 服务器”，启用 DNS 代理，并配置 DNS 地址。

图2 配置 DNS 服务器

2. 配置默认路由

如图 3 所示，在设备上进入“网络配置>路由管理>静态路由”，点击<新建>，配置一条默认路由。

图3 配置默认路由



3. 配置出接口的源 nat

如图 4 所示，在设备上进入“策略配置>NAT 转换策略>源 NAT”，点击<新建>，配置一个源 NAT。

图4 配置出接口源 nat

4. 配置 APP 动态域名缓存

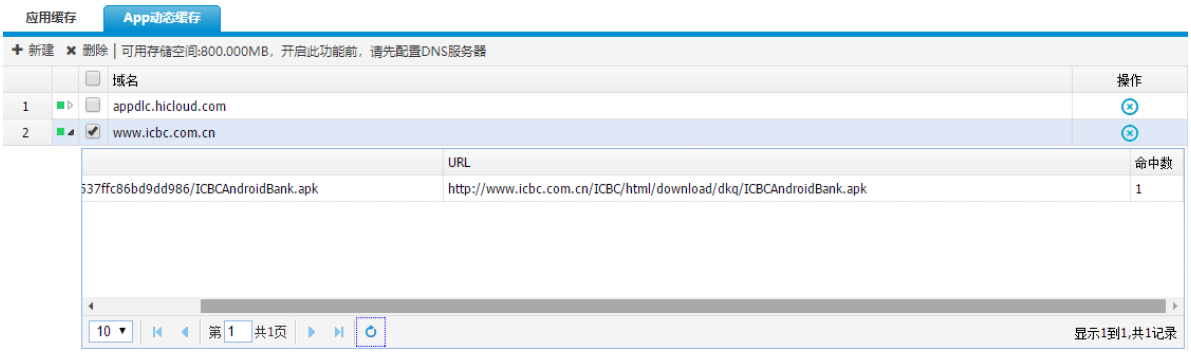
如图 5 所示，在设备上进入“网网络配置>基础网络>应用缓存>APP 动态缓存”，点击<新建>，配置一个动态缓存域名。

图5 配置 APP 动态缓存域名

4.6 验证配置

测试用户 HOSTA 和用户 HOSTB，通过访问如下 URL 下载 app：（http://www.icbc.com.cn/ICBC/html/download/dkq/ICBCAndroidBank.apk），查看 APP 动态缓存的下载文件名，下载文件的 URL，命中数，验证是否生效，如图 6 所示。

图6 验证配置



4.7 配置文件

```
Host:WD-D# display running-config!
user-policy app-local-cache host appdlc.hicloud.com
user-policy app-local-cache host www.icbc.com.cn
Host:WD-D#
```

目录

1 简介

DNS-DNAT 的功能主要是在链路负载均衡策略的接口上设置 DNS 服务器的地址，同时在 DNS 的 request 的出接口上，我们将用户的 DNS 目的地址更换为接口上的 DNS 服务器的 ip 地址，从而保证从该链路上返回来的 ip 地址为该运营商提供的服务。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解链路负载均衡的特性和 DNS-dnat 的特性。

3 使用限制

配置的主备 DNS 可以正常解析 www.baidu.com，DNS 流量经过设备转换成出口的 DNS 地址转发出去。

4 配置举例

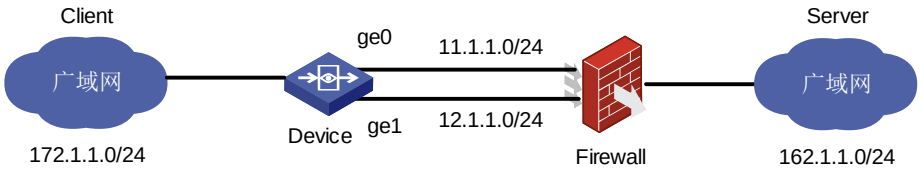
4.1 组网需求

如图 1 所示，某公司内网办公网段 IP 地址为 172.1.1.0/24。使用设备的的 ge4-3 口连接内网设备，ge4-3 网关地址 172.1.1.1/24，在设备开启链路负载均衡功能，出接口 ge0 内网 ip：11.1.1.2/24，出接口 ge1 内网 ip：12.1.1.2/24，具体应用需求如下：

- 将设备的配置两个负载均衡出接口，分别为出接口 ge0，ge1，负载均衡的两个出接口分别配置 DNS-DNAT 功能。

  配置负载均衡策略，负载均衡策略选择按照权重进行负载均衡，匹配条件为默认，添加两个出接口分别为出接口 ge0，ge1。

图1 链路负载均衡功能组网图（DNS-dnat 功能在负载均衡出接口上添加配置）



4.2 配置思路

- 配置链路负载均衡前，先配置链路负载均衡出接口，添加 DNS-DNAT 功能。
- 为每个链路负载出接口添加健康检查策略，保证可以及时监控链路状态。

- 链路负载均衡策略添加相应的链路出接口，保证命中策略的流量能够按照选中接口进行转发。

4.3 使用版本

本举例是在 E6442 上进行配置和验证。

4.4 配置注意事项

- DNS-DNAT 的默认 dns 健康检查地址是 www.baidu.com。
- DNS 使用主备 DNS 地址进行探测，10s 一次，如果三次探测不成功，设备认为 DNS 地址不可用。
- 如果设备配置的主备 DNS 地址均正常可用，默认使用主 DNS 地址，当主 DNS 地址不可用，再使用备 DNS 地址。

4.5 配置步骤

4.5.1 配置设备

1. 配置地址对象

如图 2 所示，进入“策略配置>对象管理>地址对象> IPv4 地址对象”，点击<新建>，IP 地址配置为 172.1.1.0/24 创建办公网段地址对象，点击<提交>.。

图2 登录 Web 网管

2. 配置默认路由

如图 3 所示，在设备上进入“网络配置>路由管理>静态路由”，点击<新建>，配置两条默认路由。

图3 配置默认路由

3. 配置出接口的源 nat

如图 4 所示，在设备上进入“策略配置>NAT 转换策略>源 NAT”，点击<新建>，配置两个源 NAT。

图4 配置源 nat

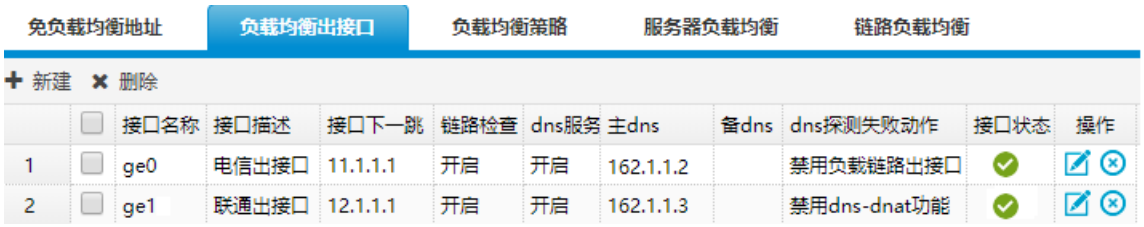
4. 配置负载均衡出接口（2 个出接口）

如图 5、图 6 所示，在设备上进入“策略配置>负载均衡策略>负载均衡出接口”，点击<新建>，配置两个负载均衡出接口。

图5 电信出接口（出接口添加 DNS-dnat 功能）

图6 联通出接口（出接口添加 DNS-dnat 功能）

图7 负载均衡出接口



5. 配置负载均衡策略

图8 负载均衡策略

4.6 验证配置

(1) 验证电信用户的 DNS 流量从电信链路发送出去。

如图 9 所示，观察所有从 ge0 发出去的 DNS 流量，DNS 地址都转换成 162.1.1.2（ge0 做了出接口源 nat）。

图9 观察从 ge0 发送数据流

```
Protocol:  UDP State:Complete    PolicyID:1       VrfId:0
           Status: 0x006aa1ba                      FastCode: 0x8000037f
           UserName: 172.1.1.55                    AppName: dns
           Expire: 00:01:04                        Existed: 00:00:01
           Source Dir: 172.1.1.55:19757      >     200.1.1.2:53          PKTS 1
           Reply  Dir: 162.1.1.2:53          >     11.1.1.2:19757        PKTS 1
           This connection has SRC_NAT DST_NAT
Protocol:  UDP State:Complete    PolicyID:1       VrfId:0
           Status: 0x006aa1ba                      FastCode: 0x8000037f
           UserName: 172.1.1.94                    AppName: dns
           Expire: 00:01:04                        Existed: 00:00:01
           Source Dir: 172.1.1.94:19796      >     200.1.1.2:53          PKTS 1
           Reply  Dir: 162.1.1.2:53          >     11.1.1.2:19796        PKTS 1
           This connection has SRC_NAT DST_NAT
```

(2) 验证联通用户的 DNS 流量从电信链路发送出去

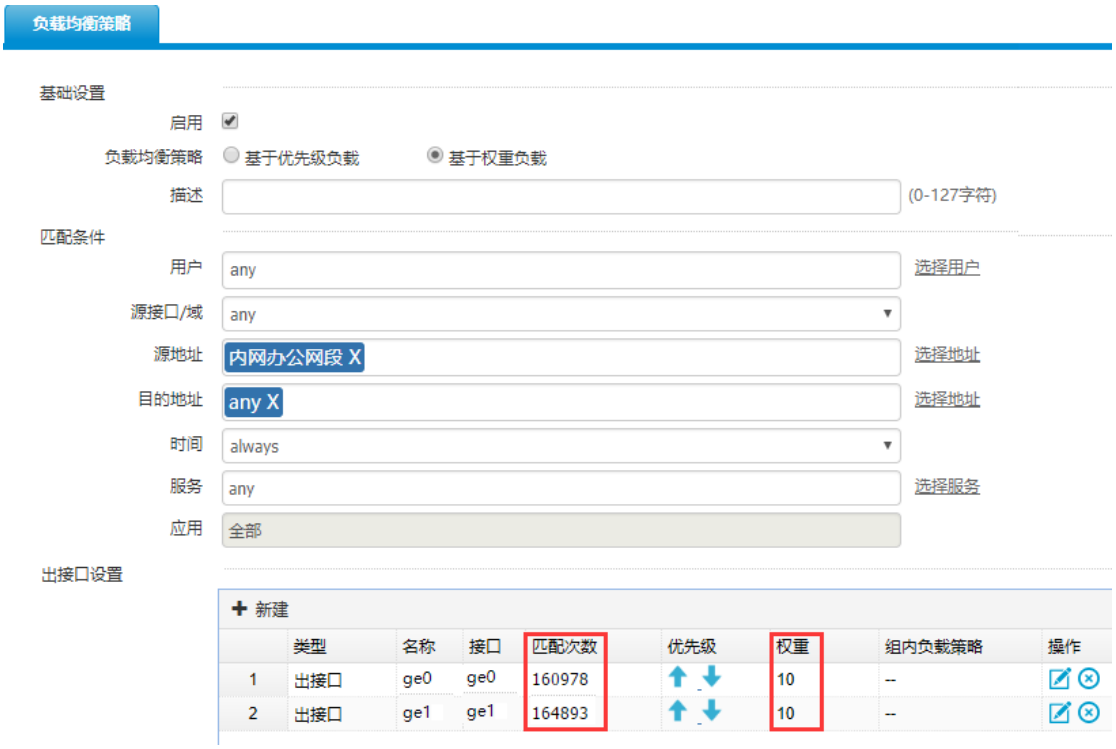
如图 10 所示，观察所有从 ge1 发出去的 DNS 流量，DNS 地址都转换成 162.1.1.3（ge1 做了出接口源 nat）

图10 观察从 ge1 发送数据流

```
Protocol:  UDP State:Complete    PolicyID:1       VrfId:0
           Status: 0x006aa1ba                      FastCode: 0x8000037f
           UserName: 172.1.1.77                    AppName: dns
           Expire: 00:01:03                        Existed: 00:00:02
           Source Dir: 172.1.1.77:19679      >     200.1.1.2:53          PKTS 1
           Reply  Dir: 162.1.1.3:53          >     12.1.1.2:19679        PKTS 1
           This connection has SRC_NAT DST_NAT
Protocol:  UDP State:Complete    PolicyID:1       VrfId:0
           Status: 0x006aa1ba                      FastCode: 0x8000037f
           UserName: 172.1.1.67                    AppName: dns
           Expire: 00:01:03                        Existed: 00:00:02
           Source Dir: 172.1.1.67:19669      >     200.1.1.2:53          PKTS 1
           Reply  Dir: 162.1.1.3:53          >     12.1.1.2:19669        PKTS 1
           This connection has SRC_NAT DST_NAT
```

(3) 验证经过负载均衡的 DNS 流量以 1：1 的比例从 ge0 和 ge1 发出去

图11 验证经过负载均衡的 DNS 流量



4.7 配置文件

```
Host:WD-D# display running-config lb-policy
!
lb-policy wans interface ge0
 description 电信出接口
 next-hop 11.1.1.1
 dns server enable
 monitor dns-dnat
 dns server manual 162.1.1.2  （DNS 健康检查）
 monitor enable
 monitor 11 ping 11.1.1.1 10 10
lb-policy wans interface ge1
 description 联通出接口
 next-hop 12.1.1.1
 dns server enable
 no monitor dns-dnat
 dns server manual 162.1.1.3 （DNS  健康检查）
 monitor enable
 monitor 12 ping 12.1.1.1 10 10
!
lb-policy any 内网办公网段 any any any any always 1
 mode weight-ratio
 out-interface ge0 10
```

```
 out-interface ge1 10
!!
Host:WD-D#
```

目 录

1 简介

内网用户使用域名访问内网服务器时，需要配置 DNAT 和 SNAT 来解决从内网服务器回包的问题，这样的配置易用性较差。所以将 DNAT 功能增加一个发布服务器配置项，简化操作，实现配置灵活性配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 DNAT 发布服务器功能特性。

2 使用限制

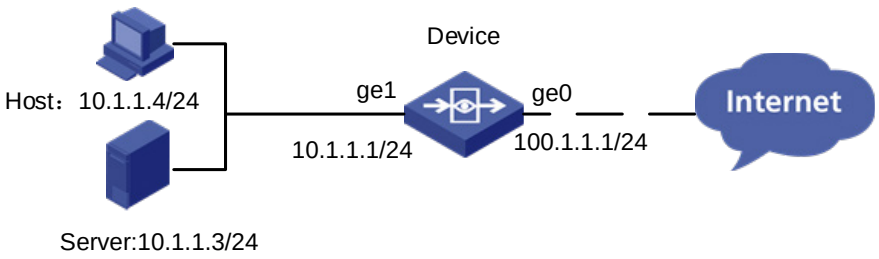
对于接口配置，有如下规格要求：目的 NAT 规则的接口需配置为外网口属性，内网用户所连接口需配置为内网口属性。

3 配置举例

3.1 组网需求

如图 1 所示，内网口地址为 10.1.1.1/24，外网口地址为 100.1.1.1/24，内网服务器 10.1.1.3 提供 web 服务，映射公网地址 100.1.1.3 对外提供服务，内网用户通过 100.1.1.3 公网地址访问内网服务器时，需要在 ge1 口配置一条 DNAT 映射和一条 SNAT 映射才能够正常访问，现只需在外接口提供对外映射的 DNAT 上开启一下发布路由器功能，即可实现内网用户通过外网地址对内网服务器的访问，无需再配置其它 DNAT 和 SNAT。

图1 DNAT 发布服务器组网图



3.2 配置思路

按照组网图组网。

(1) 登录 Web 网管

(2) 配置接口地址

(3) 配置地址对象

(4) 配置地址池

(5) 配置目的 NAT 并开启发布服务器功能

(6) 配置 IPV4 策略

3.3 使用版本

本举例是在 R6611P01 版本上进行配置和验证的。

3.4 配置步骤

1. 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击<操作>按钮，配置外网口 ge0 地址为 100.1.1.1/24，内网口 ge1 地址为 10.1.1.1/24。

图2 配置接口地址

2. 配置地址对象

如图 3所示，进入“策略配置>对象管理>地址对象>IPV4 地址对象”，点击<新建>。配置地址对象名称为“公网地址”，地址项目选择“主机地址”：“100.1.1.3”，点击“添加到列表”，点击提交。

图3 配置地址对象

3. 配置地址池

如图 4 所示，进入“策略配置>NAT 转换策略>地址池”，点击<新建>配置地址池名称为“web-server”，地址项目配置：“10.1.1.3-10.1.1.3”，点击“添加到列表”，配置完成后点击提交。

图4 配置地址池

4. 配置目的 NAT 并开启发布服务器功能

如图 5 所示，进入“策略配置>NAT 转换策略>目的 NAT”，点击<新建>配置地址池源地址为“any”，目的地址为：“公网地址”，转换类型为：“地址映射”，转换后 IP 为“web-server”，开启发布服务器，配置完成后点击提交。

图5 配置目的 NAT 并开启发布服务器功能

5. 配置 IPV4 策略

如图 6 所示，进入“策略配置>IPv4 控制策略”，点击<新建>，配置一条全通策略点击<提交>。

图6 配置 IPv4 策略

3.5 验证配置

(1) 验证 DNAT 发布服务器功能

内网用户通过 100.1.1.3 的公网地址使用 ping 测试和访问 web 服务，均可正常访问内网服务器 10.1.1.3 提供的服务，在设备查看相关会话信息如下。

```
H3C:WD-D# display ip connection protocol all ip source 10.1.1.4 dest 100.1.1.3 app-name any
matched connection count: 2
Protocol:  TCP State:Complete    PolicyID:-       VrfId:0
           Status: 0x006a61be                      FastCode: 0x00000000
           UserName: 10.1.1.4                      AppName: HTTP_PIC_DOWNLOAD
           Expire: 00:59:54                        Existed: 00:00:06
           Source Dir: 10.1.1.4:52777        >     100.1.1.3:80          PKTS 8
           Reply  Dir: 10.1.1.3:80           >     10.1.1.1:52777        PKTS 11
           This connection has SRC_NAT DST_NAT
Protocol: ICMP State:Complete    PolicyID:-       VrfId:0
           Status: 0x006a41ba                      FastCode: 0x00000000
           UserName: 10.1.1.4                      AppName: ICMP
           Expire: 00:00:03                        Existed: 00:00:14
           Source Dir: 10.1.1.4:-            >     100.1.1.3:-           PKTS 13
           Reply  Dir: 10.1.1.3:-            >     10.1.1.1:-            PKTS 13
           This connection has SRC_NAT DST_NAT

H3C:WD-D#
```

目录

1 简介

本文档介绍设备的 portal 逃生的配置举例。

Portal 逃生介绍：当发生网络问题导致 Portal 服务器不可用时，对于指定用户无需认证仍可上网。

已认证用户：包含设备启动后新认证的在线用户和设备启动前曾经认证过的未在线用户。

全局逃生模式：开始逃生时，所有用户均可上网。

已认证用户逃生模式：开始逃生时，只有已认证用户才可上网。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 portal 逃生的特性。

3 使用限制

(1) 1G 内存设备存储规格为 1000；

(2) 2G 内存设备存储规格为 5000；

(3) 4G 内存设备（含小于 8G 设备）存储规格为 1W；

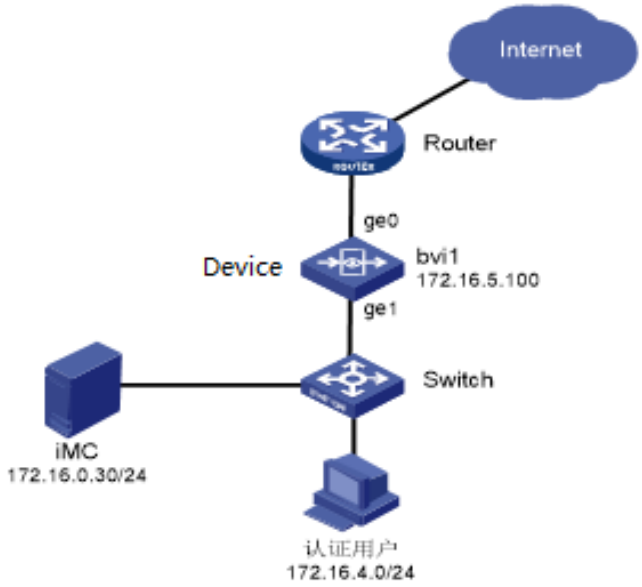
(4) 8G 及超 8G 内存设备规格为 2W。

4 配置举例

4.1 组网需求

如图 1 所示，认证用户网段 IP 地址为 172.16.4.0/24。使用设备的的 ge1 口连接内网设备，ge0 口连接外网，在设备开启 portal 逃生功能。

图1 Portal 逃生功能组网图



4.2 配置思路

- 在设备上配置 iMC 对应的 Radius 服务器。
- 在设备上配置 iMC 对应的 Portal 服务器。
- 在设备上配置地址对象，注意在认证目的地址中排除 iMC 服务器地址和 172.16.0.30。
- 在设备上配置用户策略。
- 配置地址探测。
- 开启 portal 逃生的功能，当地址探测失败时，用户可以正常上网，验证 portal 逃生功能生效。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证。

4.4 配置注意事项

已认证用户逃生，包含设备启动后新认证的在线用户和设备启动前曾经认证过的未在线用户

对于全局逃生模式，要求在逃生时所有用户均可上网、逃生结束后未认证用户均需认证。也就意味着，在逃生期间在线用户不发生变动。

4.5 配置步骤

4.5.1 配置设备

1. 配置 Radius 服务器

如图 2 所示，在设备上进入“用户管理>认证管理>认证服务器”，点击<新建>选择 RADIUS 服务器，配置与 imc 对应的 radius 服务器。

图2 配置 radius 服务器

2. 配置 Portal 服务器

如图 3 所示，在设备上进入“用户管理>认证管理>认证方式> portal sever”，配置 Portal 服务器。

图3 配置 Portal 服务器

3. 配置排除 iMC 服务器地址 172.16.0.30

如图 5 所示，在设备上进入“策略配置>对象管理>地址对象>ipv4 地址对象”，点击<新建>，配置认证用户网段地址为 172.16.4.0/24，配置认证目的地址网段排除 iMC 服务器地址 172.16.0.30。

图4 配置认证用户网段

图5 配置排除 iMC 服务器地址 172.16.0.30

4. 配置 portal 认证用户策略

如图 6 所示，在设备上进入“用户管理>认证管理>认证策略”，点击<新建>，配置 portal 认证用户策略。

图6 配置 portal 认证用户策略

5. 配置地址探测

如图 7 所示，在设备上进入“策略配置>对象管理>地址对象>地址探测”，点击<新建>，配置地址探测。

图7 配置地址探测

6. 配置开启 portal 逃生功能，选择已认证用户逃生模式

如图 8 所示，在设备上进入“用户管理>认证管理>认证方式>portal server>portal 逃生”，点击<新建>，配置开启 portal 逃生功能，选择已认证用户逃生模式。

图8 配置开启 portal 逃生功能，选择已认证用户逃生模式

7. 手动关闭 portal 服务器，查看设备已经认证的服务器是否能正常上网

4.6 验证配置

查看当 portal 逃生的地址探测失败情况下，设备已经认证的服务器能够正常上网，查看从未认证过的设备的用户无法正常上网，如图 9 所示。

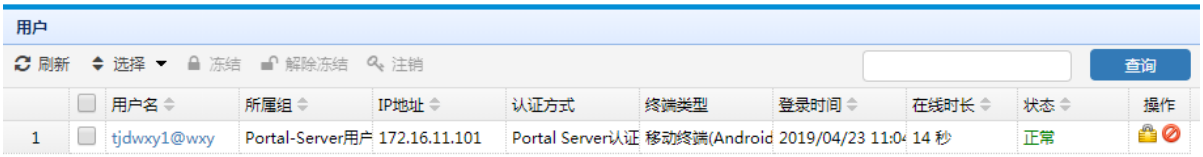
图9　地址探测状态为 down，设备 portal 逃生功能开始生效

设备命令行查看设备存储的已认证用户（当 portal 逃生生效的时候，如果选择已认证用户逃生，包含设备启动后新认证的在线用户和设备启动前曾经认证过的未在线用户均可以正常上网。

图10 查看设备上已认证用户

```
WD-D# display user-authed
#max number can save:5000
#user-authed count:2
user                mac                 online time         alive time          login times
tjdwxy1@wxy         3c:a6:16:1c:72:ae   2019/04/23 11:04    2019/04/23 11:04        1
```

图11 设备已认证用户正常上网，设备未认证用户无法上网



4.7 配置文件

```
Host:WD-D# display running-config!
user-portal-escape mode authed
user-portal-escape track enable
user-portal-escape track portal-server 地址
Host:WD-D#
```

目录

1 简介

本文档介绍设备的应用缓存配置举例。

- 应用缓存的介绍：自学习型缓存服务器是一种用来缓冲 Internet 数据的软件或服务器设备。它是这样实现其功能的，接受来自人们需要下载的目标（object）的请求并适当地处理这些请求。也就是说，如果一个人想下载一 web 页面，他请求自学习型缓存服务器为他取得这个页面。缓存服务器随之连接到远程服务器（比如：http：// nlanr.net/）并向这个页面发出请求。然后，缓存服务器不仅显式地聚集数据到客户端机器，而且同时复制一份保存在服务器设备上。当下一次有人需要同一页面时，缓存服务器就可以简单地从磁盘中读到它，那样数据立即就会传输到客户机上，从而加快访问速度，节省了网络带宽。
- 精确匹配：域名需要完全匹配。
- 精确匹配：路径需要完全匹配。
- 模糊匹配：域名不需要完全匹配。
- 模糊匹配：路径只要是当前下载请求中路径的字串即认为匹配。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解应用缓存的特性。

3 使用限制

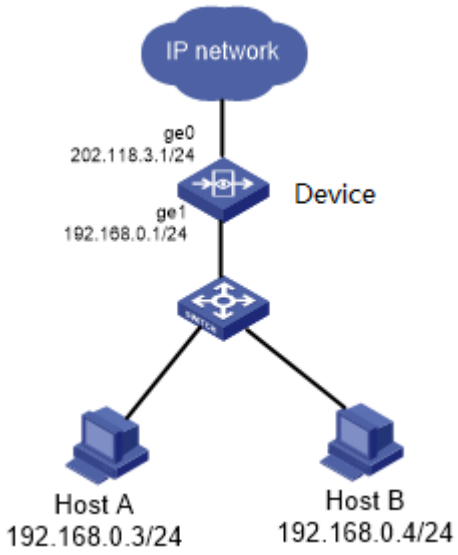
当设备的磁盘空间大于缓存的 APP 文件，应用缓存功能可以正常缓存成功。

4 配置举例

4.1 组网需求

如图 1 所示，某公司内网办公网段 IP 地址为 192.168.0.0/24。使用设备的的 ge1（192.168.0.1）口连接内网设备，ge0 （202.118.3.1/24）口连接外网，在设备开启应用缓存功能。

图1 应用缓存功能组网图



4.2 配置思路

- 新建应用缓存，开启模糊匹配功能。
- 添加 URL，将 app 文件导入设备。
- 测试用户通过设备下载 app 应用。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证。

4.4 配置注意事项

- 域名长度 4-255 字符，字符只能是数字，字母，'-'，每一级域名长度不超过 63 个字符，最后一级 2-6 个字符。
- APP 动态缓存的域名规格是 8 条。

4.5 配置步骤

4.5.1 配置设备

1. 配置默认路由

如图 2 所示，在设备上进入“网络配置>路由管理>静态路由”，点击<新建>，配置一条默认路由。

图2 配置默认路由

2. 配置出接口的源 nat

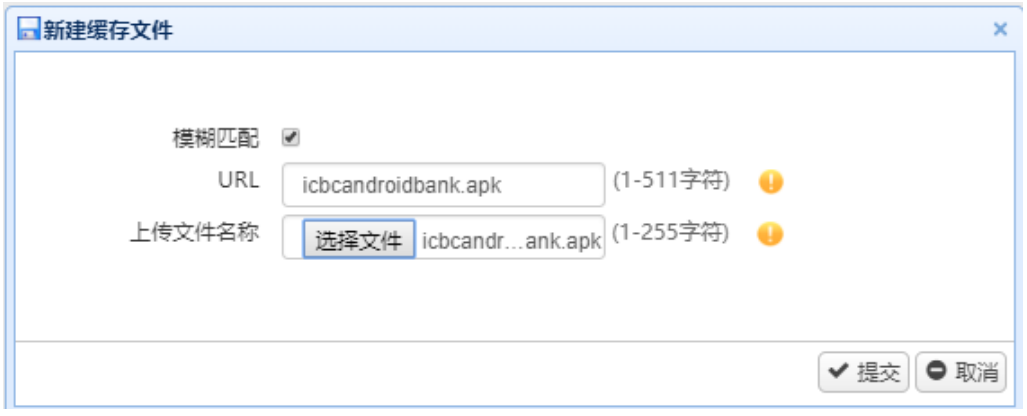
如图 3 所示，在设备上进入“策略配置>NAT 转换策略>源 NAT”，点击<新建>，配置一个源 NAT。

图3 配置出接口源 nat

3. 配置应用缓存文件

如图 4 所示，在设备上进入“网络配置>基础网络>应用缓存”，点击<新建>，配置应用缓存文件。

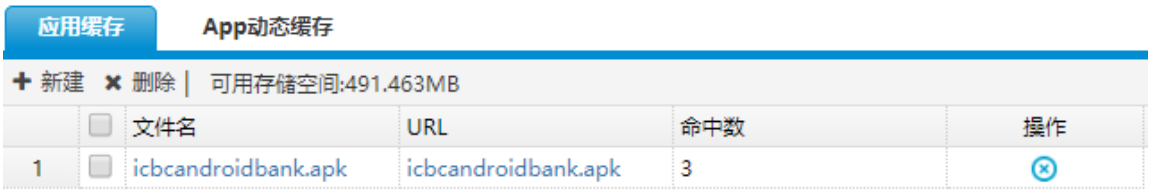
图4 配置应用缓存—模糊匹配功能



4.6 验证配置

测试用户 HOSTA 和用户 HOSTB，通过 URL 下载 app（http://www.icbc.com.cn/ICBC/html/download/dkq/ICBCAndroidBank.apk）查看应用缓存的下载文件名、下载文件的 URL 和命中数，验证是否生效，如图 5 所示。

图5　验证配置



4.7 配置文件

```
Host:WD-D# display running-config!
user-policy app-local-cache fuzzy-match app-path ICBCAndroidBank.apk local-name
ICBCAndroidBank.apk
user-policy app-local-cache host appdlc.hicloud.com
user-policy app-local-cache host www.icbc.com.cn
Host:WD-D#
```

目　录

1 简介

本文档介绍设备的 HTTPS 弹 Portal 功能举例，HTTPS 弹 Portal 是在访问 HTTPS 类型的网站时，查看页面是否会弹 Portal 的配置。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 HTTPS 弹 Portal 特性。

3 使用限制

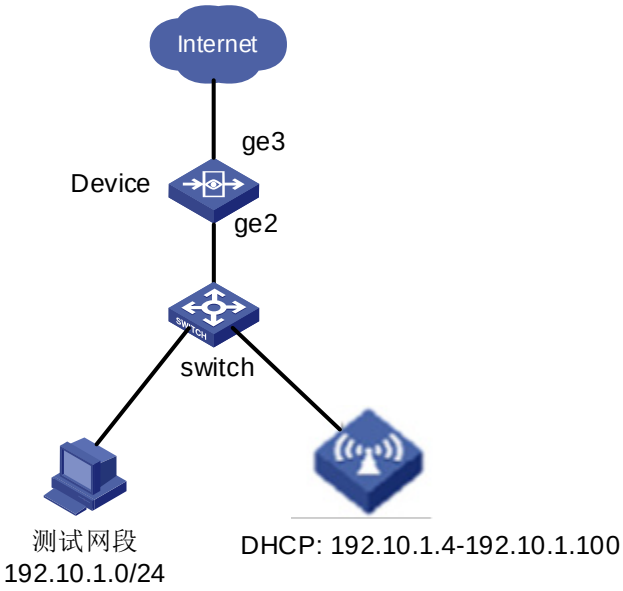
- HTTPS 弹 Portal 对于 HSTS 网站无法弹 Portal。
- IE11 浏览器对于 HTTPS 类型网站无法弹 Portal ,IE11 浏览器有合法证书强制检查，不信任的证书网站不允许用户继续浏览，进行强制保护，导致设备无法对 https 网站弹 portal。
- 网银类网站无法实现 HTTPs 弹 Portal。
- HTTPs 弹 portal 功能默认关闭，使用此功能前需要使用 user-policy https-portal enable 命令开启 https 弹 Portal 功能。

4 配置举例

4.1 组网需求1：HTTPS弹Portal三层组网

如图 1 所示，某公司内网存在测试网段和办公网段，测试网段 IP 地址为 192.10.1.0/24。使用设备的的 ge2 和 ge3 接口路由模式部署在网络中，设备作为出口网关设备，下联交换机。在设备上使用命令 user-policy https-portal enable 启用 HTTPS 弹 Portal 功能。

图1 HTTPS 弹 Portal 组网图



4.2 配置思路

- 在设备上开启 HTTPS 弹 Portal 功能。
- 配置需要认证的地址对象和认证用户。
- 配置本地认证策略。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

HTTPS 弹 Portal 时要保证浏览器可以进行正常的 HTTPS 类型网站的访问。

4.5 配置步骤

4.5.1 开启 HTTPs 弹 portal 功能

如图 2 所示，使用串口或 telnet 进入设备后台，执行命令 user-policy https-portal enable 开启 HTTPs 弹 portal 功能。

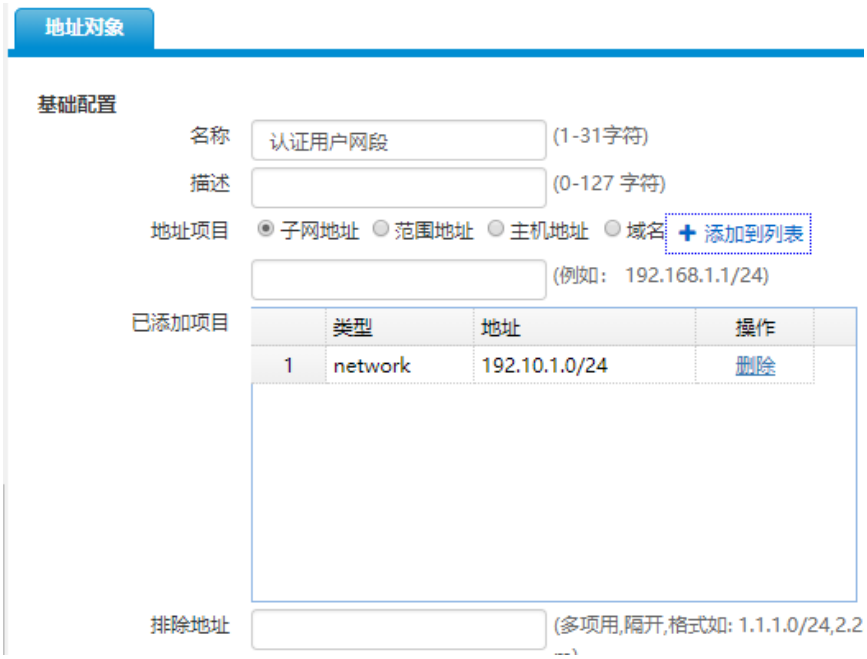
图2 开启 HTTPs 弹 portal 功能

```
Username: admin
Password:
host:WD-D> en
host:WD-D# conf t
host:WD-D(config)# user-policy https-portal enable
host:WD-D(config)#
```

4.5.2 配置认证地址对象

如图 3 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，IP 地址配置为 172.16.10.0/24 创建认证地址网段对象，点击<提交>。

图3 配置认证地址对象



4.5.3 配置本地 web 认证

如图 4 所示，进入“用户管理>认证管理>认证方式>本地 web 认证”，这里按照默认配置，点击<提交>。

图4 配置本地 web 认证

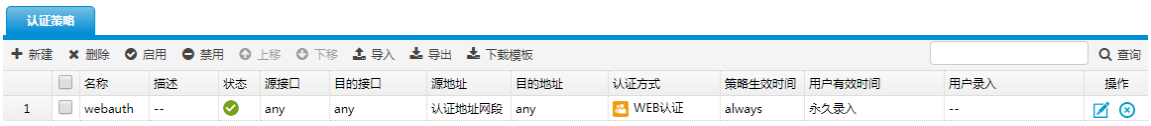
4.5.4 配置本地 web 认证策略

如图 5 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址为地址对象中的认证用户网段，认证方式为 web 认证，点击<提交>。

图5 配置本地 web 认证

如图 6 所示，配置成功的本地 web 认证如下：

图6 本地 web 认证配置成功



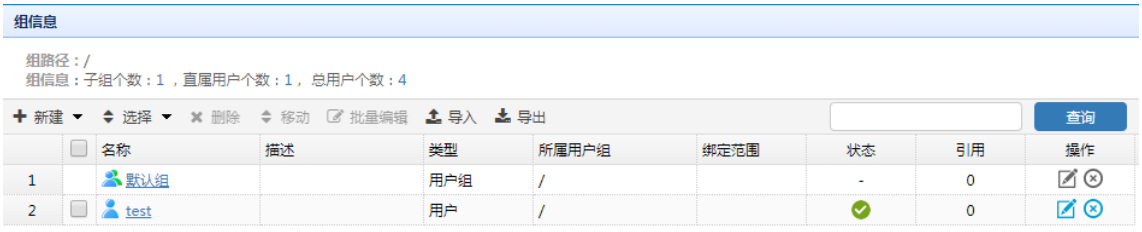
4.5.5 配置认证用户

如图 7 所示，进入“用户管理>用户组织结构”，点击<新建>选择用户，输入用户账号和密码，密码和确认密码保持一致，点击<提交>。

图7 配置认证用户

如图 8 所示，配置成功的用户界面如下：

图8 用户配置成功

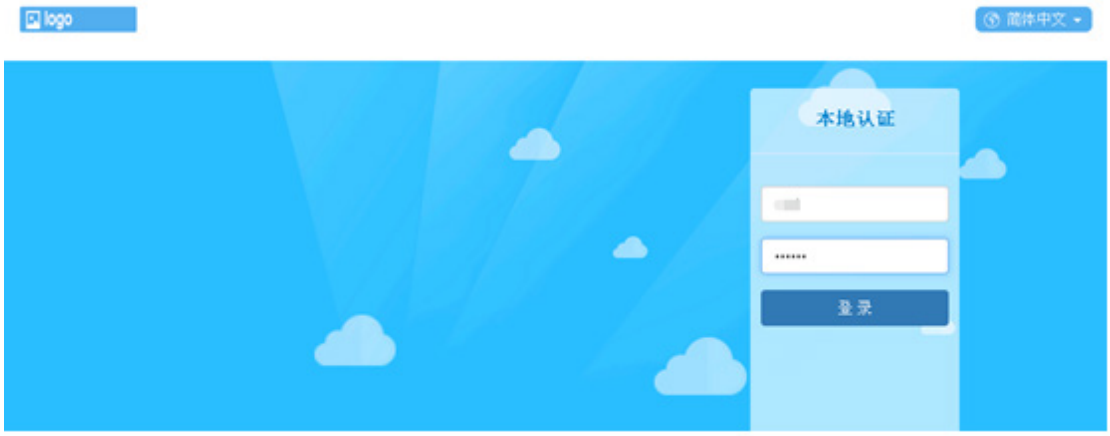


4.5.6 验证配置

1. pc 端重定向方式验证

如图 9 所示，PC 访问 HTTPS 类型的网站，界面会弹出本地认证界面。

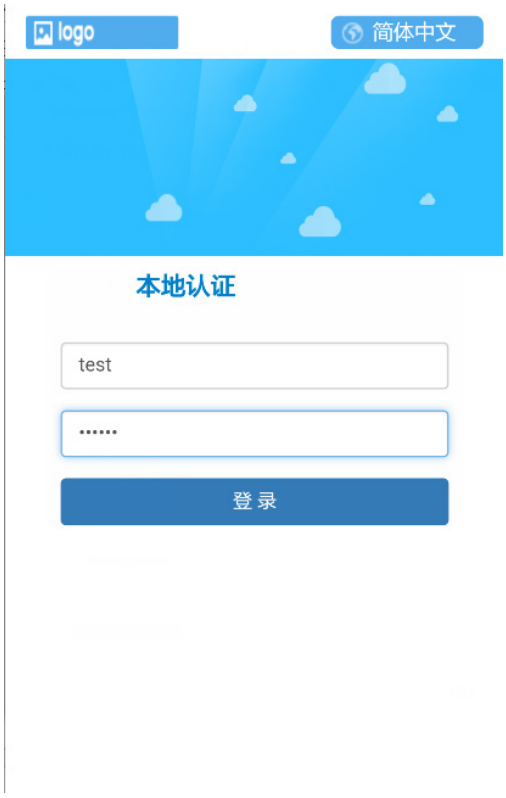
图9 弹出 Portal 认证



2. 移动端重定向方式认证

如图 10 所示，移动端访问 HTTPS 类型网站，浏览器弹出本地认证界面。

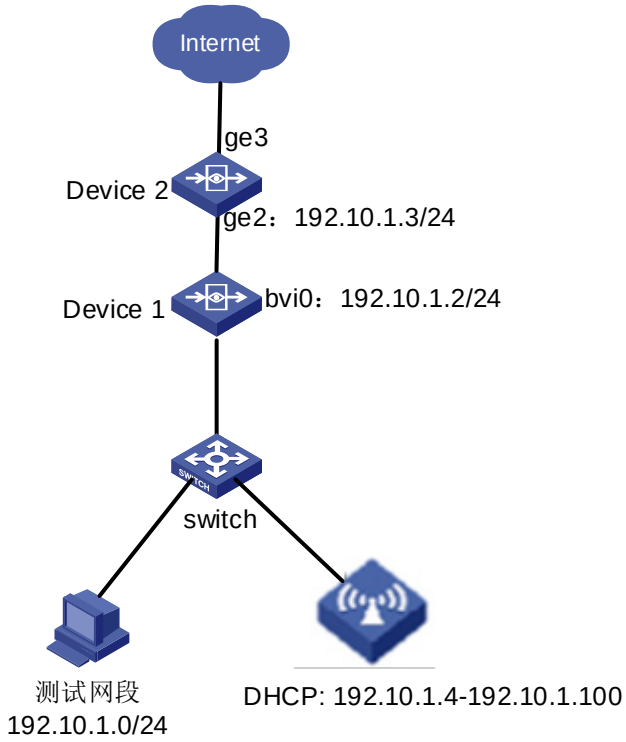
图10 移动端访问网站



4.6 组网需求2：HTTPS弹Portal二层组网

如图 11 所示，某公司内网存在测试网段和办公网段，测试网段 IP 地址为 192.10.1.0/24。使用两台设备的路由模式部署在网络中，设备 2 作为出口网关设备，设备 1 下联交换机，配置桥模式。在设备 1 上使用命令 user-policy https-portal enable 启用 HTTPS 弹 Portal 功能。

图11 HTTPS 弹 Portal 二层组网



4.7 配置思路

- 在设备 1 设备上配置桥模式，并开启 HTTPS 弹 Portal 功能。
- 配置需要认证的地址对象和认证用户。
- 配置本地认证策略。

4.8 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.9 配置注意事项

HTTPS 弹 Portal 时要保证浏览器可以进行正常的 HTTPS 类型网站的访问。

4.10 配置步骤

4.10.1 开启 HTTPs 弹 portal 功能

如图12所示，使用串口或telnet进入设备后台，执行命令user-policy https-portal enable开启HTTPs弹 portal 功能。

图12 开启 HTTPs 弹 portal 功能

```
Username: admin
Password:
host:WD-D> en
host:WD-D# conf t
host:WD-D(config)# user-policy https-portal enable
host:WD-D(config)#
```

4.10.2 配置认证地址对象

如图 13 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，IP 地址配置为 192.10.1.0/24 创建认证地址网段对象，点击<提交>。

图13 配置认证地址对象

4.10.3 配置本地 web 认证

如图 14 所示，进入“用户管理>认证管理>认证方式>本地 web 认证”，这里按照默认配置，点击<提交>。

图14 配置本地 web 认证

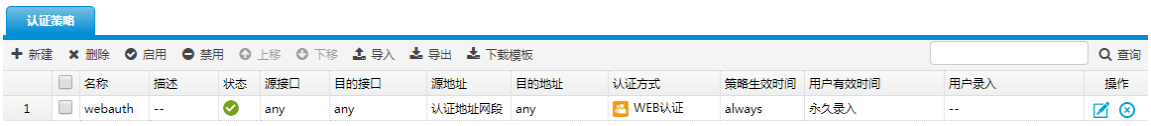
4.10.4 配置本地 web 认证策略

如图 15 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址为地址对象中的认证用户网段，认证方式为 web 认证，点击<提交>。

图15 配置本地 web 认证

如图 16 所示，配置成功的本地 web 认证如下：

图16 本地 web 认证配置成功



4.10.5 配置认证用户

如图 17 所示，进入“用户管理>用户组织结构>用户”，点击<新建>选择用户，输入用户账号和密码，密码和确认密码保持一致，点击<提交>。

图17 配置认证用户

如图 18 所示，配置成功的用户界面如下：

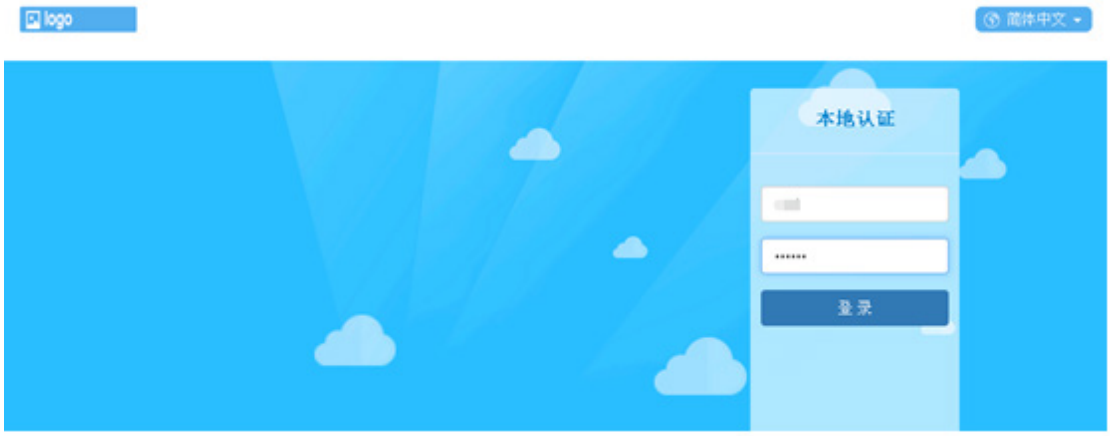
图18 用户配置成功

4.10.6 验证配置

1. pc 端重定向方式验证

如图 19 所示，PC 访问 HTTPS 类型的网站，界面会弹出本地认证界面。

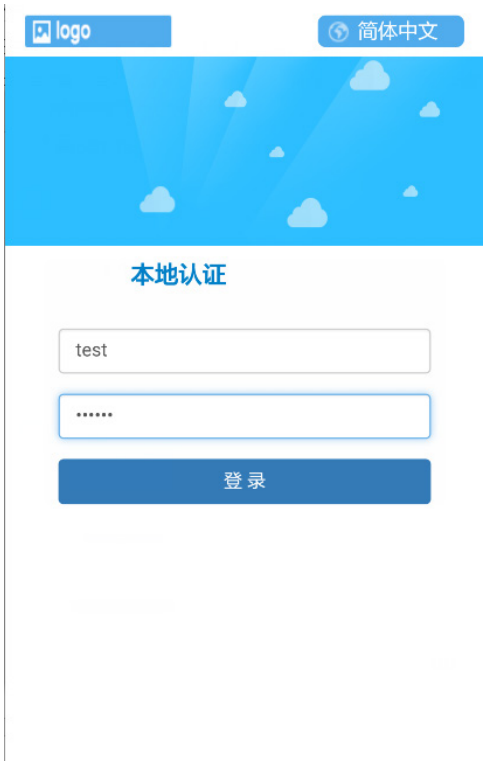
图19 弹出 Portal 认证



2. 移动端重定向方式认证

如图 20 所示，移动端访问 HTTPS 类型网站，浏览器弹出本地认证界面。

图20 移动端访问网站



目 录

1 简介

本文档介绍设备的 IPSEC 备份链路配置举例。支持 IPSEC-VPN 链路备份功能，满足在一条 IPSEC-VPN 链路不通的情况下，启用另一条 IPSEC-VPN 链路。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

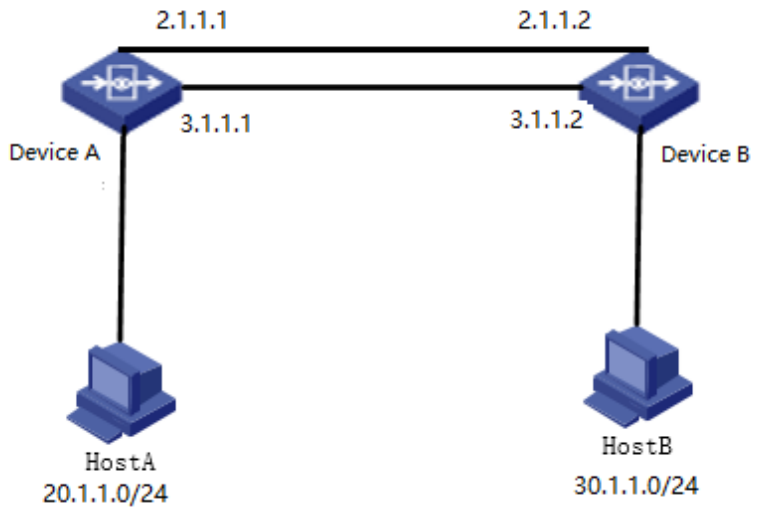
3 VPN 备份链路配置举例

3.1 组网需求：路由模式组网

3.1.1 组网需求

如图 1 所示，某公司内网存在两个网段，IP 地址分别为 20.1.1.0/24 和 30.1.1.0/24。使用两台设备的的对接部署在网络中，在两台设备上启用 VPN 备份链路功能。

图1 VPN 链路备份组网图



3.1.2 配置思路

- 两台设备分别配置主备两条链路。
- 主备链路都正常连接时，备链路断开。
- 主链路断开后，备链路自动连接。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

1. 新建主链路

(1) 新建设备 A 主链路 IKE

如图 2 所示，进入“网络配置>VPN>IPsec-VPN>IPsec 第三方对接”，点击<新建 IKE>。

图2 新建主链路 IKE

(2) 新建设备 A 主链路 ipsec

如图 3 所示，点击<新建 IPSEC>。

图3 新建主链路 IPSEC

2. 新建备链路

(1) 新建设备 A 备链路 IKE

如图 4 所示.，点击<新建 IKE>。

图4 新建备链路 IKE

(2) 新建设备 A 备链路 IPSEC

如图 5 所示，点击<新建 IPSEC>。

图5 新建备链路 IPSEC

3. 新建主备链路 IPSEC 隧道接口

如图 6 所示.，点击<新建 IKE>。

图6 新建备链路 IKE

设备 B 重复上述步骤。

4. 新建两条静态路由

进入“网络配置>路由管理>静态路由”，单击<新建>，如图 7 所示。

图7 新建静态路由

设备 B 重复上述步骤。

3.1.5 配置注意事项

- 在未配置 DPD 检测的情况下，当主链路故障后，需要等待 IPSEC SA 老化，同时需要等待一个切换延迟时间周期后备链路才会发起协商。
- 在配置 DPD 检测的情况下，这样在主链路故障后，等待 DPD 检测周期（DPD 检测失败清除 IPSEC SA 的时间周期）加切换延迟时间后备链路才会发起协商。
- 主备路由切换是通过监控 tunnel 口的 up/down 来实现的，当主链路故障后，主链路对应的 tunnel 口会 down 掉，主链路上配置的路由会自动失效，备链路协商成功后，对应的 tunnel 口会变为 up 状态，对应的路由会变成生效状态，所以配置时分支和中心端设备主链路都必须选择自动连接的方式，备链路必须选择监控链路故障自动连接的方式才能实现。
- 主链路故障检测机制：备链路每 10s 会检测一次主链路的 IPSEC SA 来判断主链路是否正常，当主链路 IPSEC SA 不存在时，就认为主链路故障，在等待切换延迟时间后备链路会发起连接，当主链路恢复后，备链路会自动清掉对应的 IPSEC SA，业务切换到主链路上继续转发。

3.1.6 验证配置

(1) 验证主链路断开后，备份链路自动连接

如图 8 所示，进入“网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec SA”查看，发现连接为备链路。

图8 备链路自动连接

(2) 验证主链路重新连接后，备份链路自动断开连接

如图 9 所示，进入“网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec SA”查看，发现连接为主链路。

图9 主链路恢复连接

IPsec 配置 | IPsec隧道接口 | IKE SA | IPsec SA

		名称	对端网关	本地网关	状态	过期时间/过期流	流量(入/出)	源网络	目的网络	操作
1		主链路	2.1.1.2	2.1.1.1	连接中	0s/0.0KB	0.00kb/0.00kb	20.1.1.0/24	30.1.1.0/24	

目　录

1 简介

本文档介绍设备的伪 portal 抑制举例，伪 portal 抑制是将 Portal 重定向使用 HTTP302 方式改为使用 html-refresh 方式。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

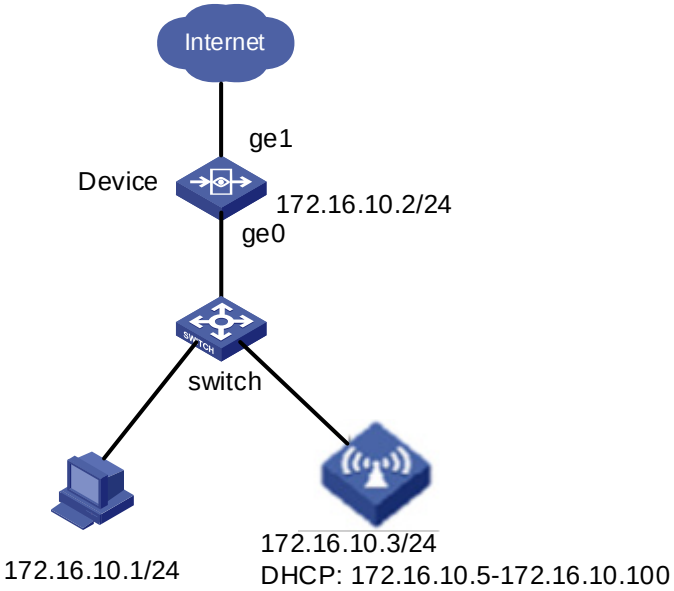
本文档假设您已了解伪 portal 抑制特性。

3 配置举例

3.1 组网需求

如图1所示，某公司内网无线办公网段IP地址172.16.10.0/24，有线办公网段IP地址172.16.10.0/24，AP 上开启 DHCP，地址池为 172.16.10.5-172.16.10.100。

图1 伪 portal 抑制路由模式组网图



3.2 配置思路

- 在设备上更改重定向方式为 refresh。
- 配置本地认证方式的认证策略。
- 配置认证用户的用户名和密码。

3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.4 配置注意事项

- 伪 portal 抑制用的重定向方式为 refresh 方式，先在设备上更改重定向方式为 refresh。
- 设备配置 Web 认证时，允许用户的 TCP 三次握手报文通过，当检测到用户 HTTP 报文时拦截并弹出认证页面。所以，在使用 Web 认证功能时，需要保证终端可以进行正常的 HTTP 访问。

3.5 配置步骤

3.5.1 配置设备

1. 修改重定向方式

如图 2 所示，使用 TELNET/SSH 方式登录设备，默认用户名和密码是 admin/admin，在设备上修改重定向方式为 refresh。

图2 修改重定向方式

```
Host(config)# user-policy redirect-mode html-refresh
Host(config)#
```

输入 display running-config 查看修改结果，如图 3 所示，修改成功的 refresh 重定向如下：。

图3 refresh 重定向修改成功

```
!user-policy
!
user-policy redirect-mode html-refresh
!zone
!
!
```

2. 配置认证地址对象

如图 4 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，IP 地址配置为 172.16.10.0/24 创建认证地址网段对象，点击<提交>。

图4 配置认证地址对象

3. 配置本地 web 认证

如图 5 所示，进入“用户管理>认证管理>认证方式>本地 web 认证”，这里按照默认配置，点击<提交>。

图5 配置本地 web 认证

4. 配置本地 web 认证策略

如图 6 所示，进入“用户管理>认证管理>认证策略”，点击<新建>，源地址为地址对象中的认证地址网段，认证方式为本地 web 认证，点击<提交>。

图6 配置本地 web 认证

如图 7 所示，配置成功的本地 web 认证如下：

图7 本地 web 认证配置成功

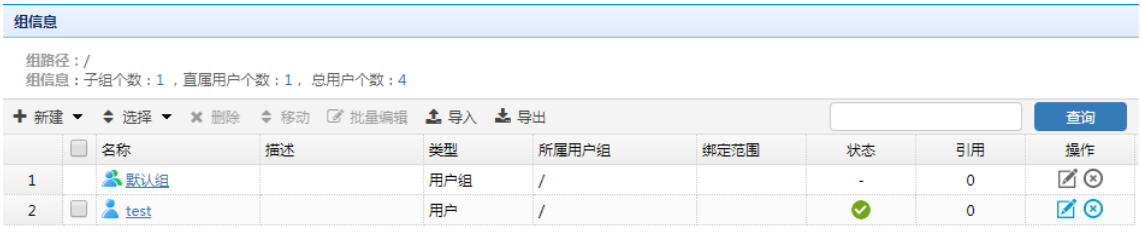
5. 配置认证用户

如图 8 所示，进入“用户管理>用户组织结构”，单击“新建>用户”，输入用户账号和密码，密码和确认密码保持一致，点击<提交>。

图8 配置认证用户

如图 9 所示，配置用户成功的用户界面如下：

图9 用户配置成功



6. 配置文件

!address

!

address 认证用户网段

ip subnet 172.16.10.0/24

!

!user

!

user test

bind-group organization

authenticate local

kTgxl5p34DqlzzT+XZ0R14cv6Qal7urj9YogDjQGHYyVxSLYIpmOxTPwro4b0aN

change-password enable first-log-change-pwd disable!

!

!user-policy

!

!user-policy

!

user-policy redirect-mode html-refresh

user-policy any any 认证地址网段 any always local-webauth enable webauth no-record forever

!zone

!

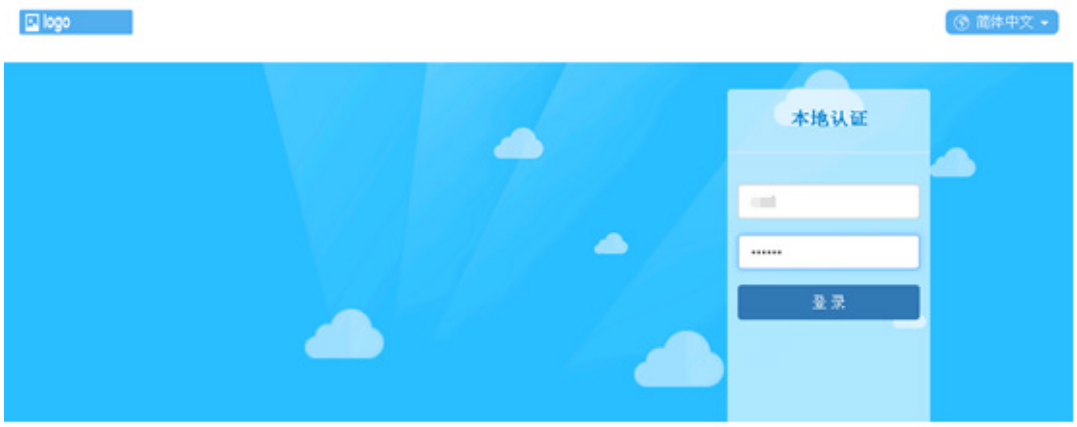
!

3.6 验证配置

(1) pc 端重定向方式验证

如图 10 所示，使用 wireshark 抓包工具，在本地进行抓包。PC 访问网页（以 www.qq.com 为例），弹出认证界面后输入用户名和密码点击<提交>。

图10 进行本地 web 认证

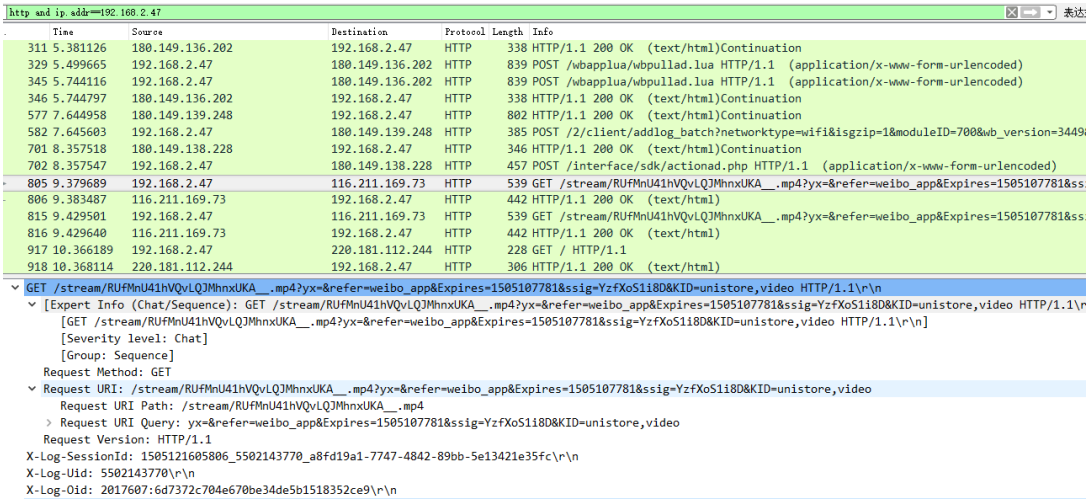


如图 11 所示，在 wireshark 上分析数据包，查看 refresh 重定向方式是否成功。

图11 refresh 重定向方式

如图 12 所示，pc 访问腾讯客户端，在设备上进行抓包。当伪 portal 抑制生效时，界面不会弹出认证界面，打开抓取的报文，过滤条件为 htttp and ip.addr==目的 ip，没有 PC 向设备 portal 地址发起的请求报文，这样表示伪 portal 抑制成功。

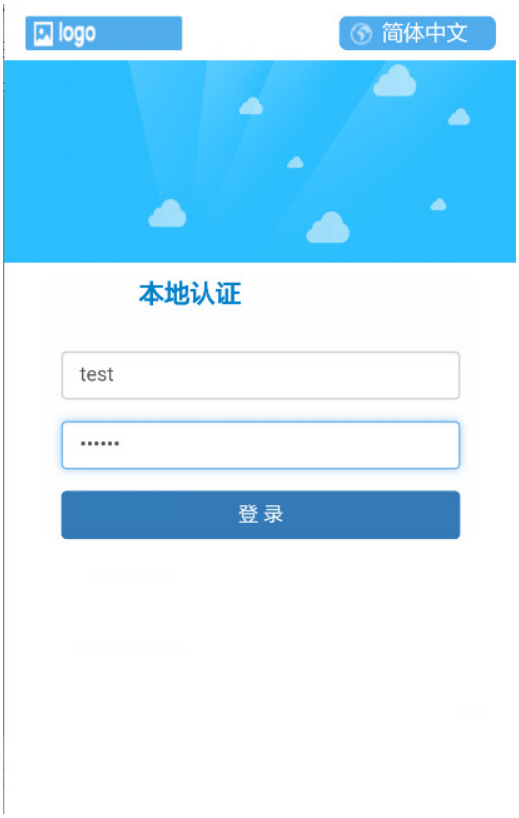
图12 伪 portal 抑制成功



(2) 移动端重定向方式认证

如图 13 所示，在设备上进行抓包。移动端访问应用（以知乎为例），弹出认证界面后输入用户名和密码点击<提交>。

图13 移动端认证

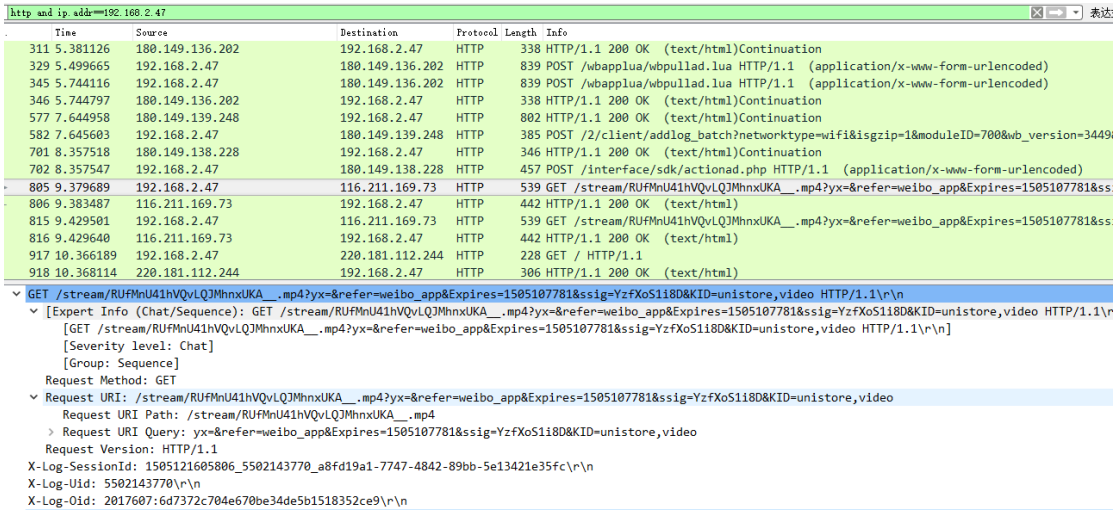


如图 14 所示，打开在设备上抓取的报文，查看 refresh 重定向方式是否成功。

图14 refresh 重定向方式

如图 15 所示，移动终端上访问腾讯客户端，在设备上进行抓包。当伪 portal 抑制生效时，界面不会弹出认证界面，打开抓取的报文，过滤条件为 htttp and ip.addr==目的 ip，没有移动终端向设备 portal 地址发起的请求报文，这样表示伪 portal 抑制成功。

图15 伪 portal 抑制成功



目 录

1 简介

本文档介绍设备的解密策略配置举例，解密策略对通过设备的入接口、源 IP、目的 IP、HTTPS 对象进行访问控制，主要是对使用 SSL 协议传输的流量做审计。支持 HTTPS、邮箱类审计功能，并产生审计日志。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解解密策略特性。

3 使用限制

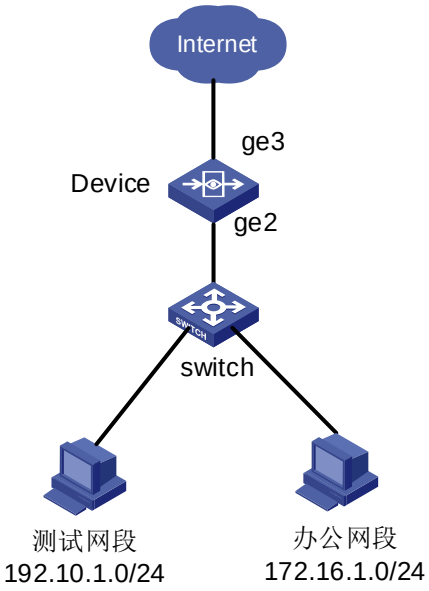
- 当设备 DNS 设置成全局模式时，用户电脑的 DNS 需要指向设备的入接口，以保证 DNS 过设备，解密策略才能生效。若 DNS 不经过设备的话，解密策略不生效。
- HTTPS 解密策略所需证书为 CA 证书。
- 部分邮箱客户端（网易邮箱大师/闪电邮）的 SMTP 是使用的 TLS 加密，TLS 加密不支持解密。
- 部分 HTTPS 站点的客户端会进行证书校验，会显示非安全连接。

4 配置举例

4.1 组网需求

如图 1 所示，某公司内网存在测试网段和办公网段，IP 地址分别为 192.10.1.0/24 和 172.16.10.0/24。使用设备的的 ge2 和 ge3 接口路由模式部署在网络中，设备作为出口网关设备，下联二层交换机。在设上启用解密策略功能。

图1 解密策略路由模式组网图



4.2 配置思路

- 配置需要审计的 HTTPS 对象；
- 生成 CA 证书；
- 导入本地证书；
- 启用 IPV4 审计策略；
- 启用解密策略；
- 引用证书。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- 解密策略用的证书为 CA 证书，先在证书管理>根 CA 配置管理页面生成 CA 证书，再导出证书至 PC 本地。
- DNS 回应报文 IP 地址解析。443 端口的站点（包含网页版邮箱）解密，需首先把站点域名转化为 IP 地址，作为流量过滤条件，只有符合条件的 HTTPS 流量进入解密流程。
- 代理模块需要和客户端建立 SSL 连接，因此需要给客户端安装证书，设备需要支持证书签发功能及导入导出功能，且可以被解密策略引用。解密策略可根据当前导入的证书选择使用哪个证书。

- 邮箱类解密分为网页版邮箱和客户端版邮箱。网页版邮箱内置需要审计的域名对用户不可见，对外通过配置说明文档体现网页版邮箱支持规格。客户端邮箱解密支持 SMTP、POP3、IMAP 协议。有些 SMTP 使用的 TLS 加密不支持审计。
- 如果是网桥模式组网，配置步骤是一致的，需要注意的是网桥接口下一定要配置 IP 地址，并且要保证桥接口 IP 能访问外网。

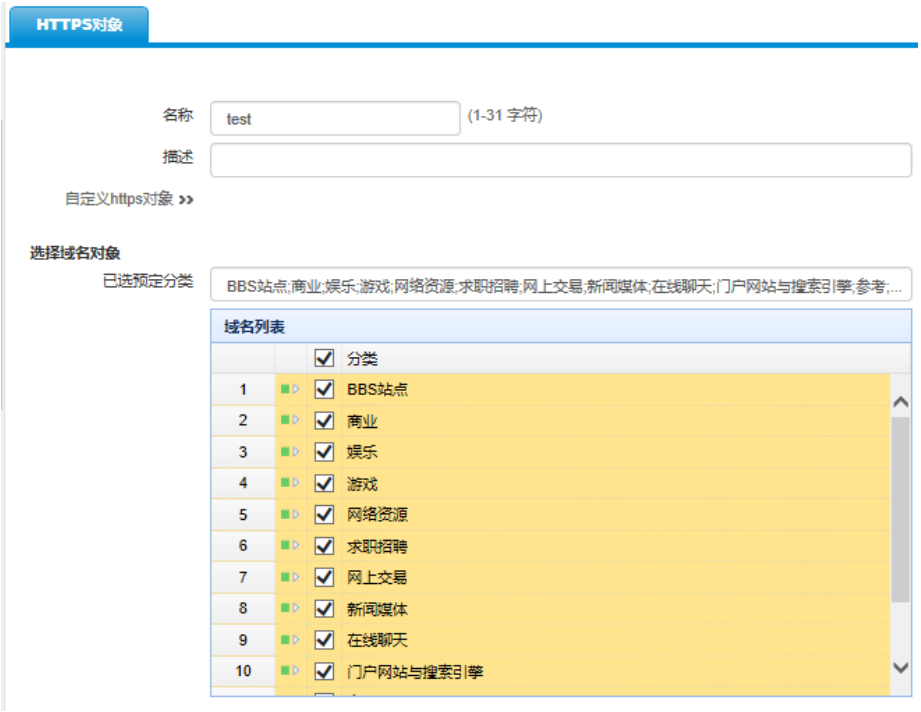
4.5 配置步骤

4.5.1 配置设备

1. 配置 HTTPS 对象

如图 2 所示，进入“策略配置>对象管理>URL 对象>HTTPS 对象”，点击<新建>。

图2 配置 HTTPS 对象



如图 3 所示，创建成功的 HTTPS 对象配置如下：

图3 HTTPS 对象配置成功

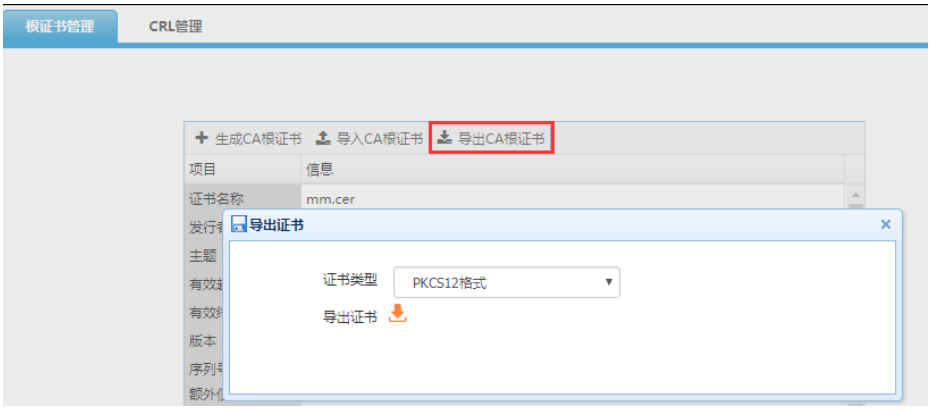
2. 生成 CA 证书

如图 4 所示，进入“策略配置>对象管理>CA 服务器>根 CA 配置管理”，点击<生成 CA 根证书>。

图4 生成 CA 根证书

如图 5 所示，在生成 CA 证书以后，导出证书。.

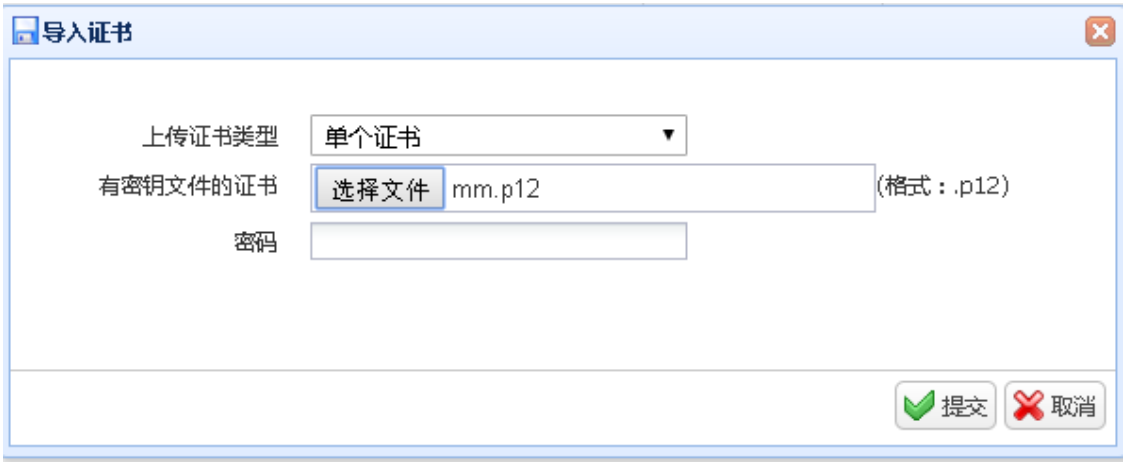
图5 导出 CA 证书



3. 导入本地证书

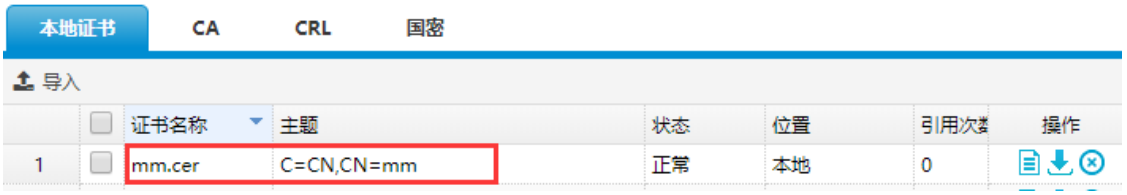
如图 6 所示，进入“策略配置>对象管理>本地证书>证书>本地证书”，点击<导入>，选择之前生成的 CA 证书。

图6 导入证书



如图 7 所示，导入成功的证书如下：

图7 导入证书成功



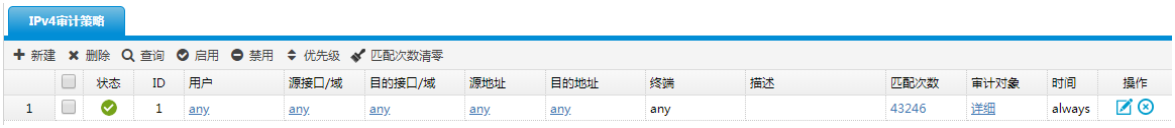
4. 启用 IPV4 审计策略。

如图 8 所示，进入“策略配置>Ipv4 审计策略”，点击<新建>，配置审计策略，选择所有审计对象。

图8 启用 IPV4 审计策略

如图 9 所示，创建成功的 IPV4 审计策略如下：

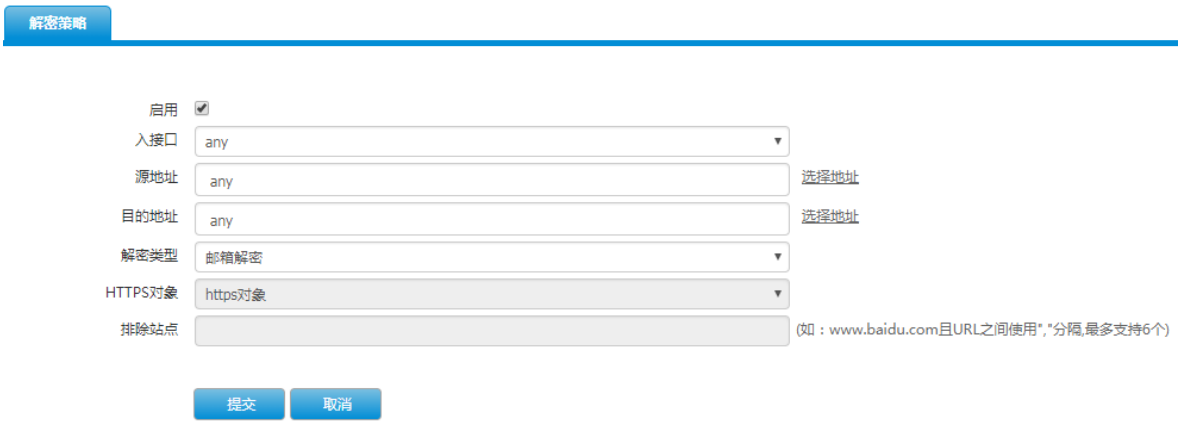
图9 IPV4 审计策略配置成功



5. 启用解密策路，开启站点解密和邮箱解密

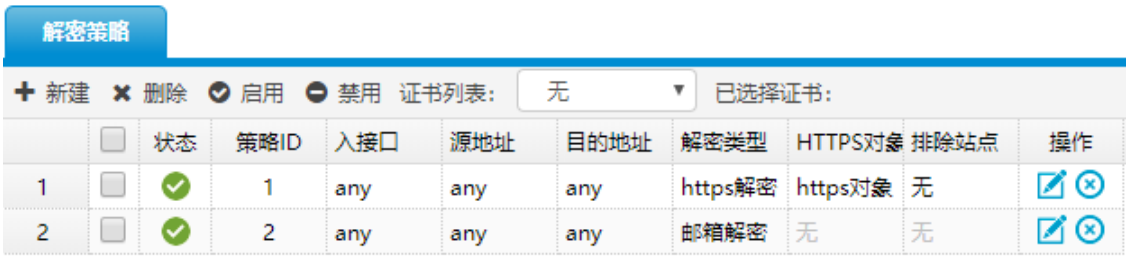
如图 10 所示，进入“策略配置>SSL 解密策略”，点击<新建>，配置解密策略。

图10 启用解密策略



如图 11 所示，创建成功的解密策略配置如下：

图11 解密策略配置成功



6. 引用证书

如图 12 所示，进入“策略配置>SSL 解密策略”，点击<证书列表>，引用生成证书。

图12 引用证书成功

4.6 验证配置

(1) 验证审计日志里的搜索引擎日志。

如图 13 所示，进入“数据中心>日志中心>审计日志>搜索引擎日志”查看，发现已经审计到用户访问百度的搜索引擎内容，并正确地记录了日志。

图13 测试网段搜索引擎日志

(2) 验证审计日志里的邮箱日志。

如图 14 所示，进入“数据中心>日志中心>审计日志>邮件日志”，可以看到办公网段已经被正确记录了所有 SSL 邮箱日志。

图14 办公网段邮件日志

(3) 验证审计日志里的网站访问日志。

如图 15 所示，进入“数据中心>日志中心>审计日志>访问网站日志”查看，发现已经审计到用户访问百度的访问网站内容，并正确地记录了日志。

图15 测试网段访问网站日志

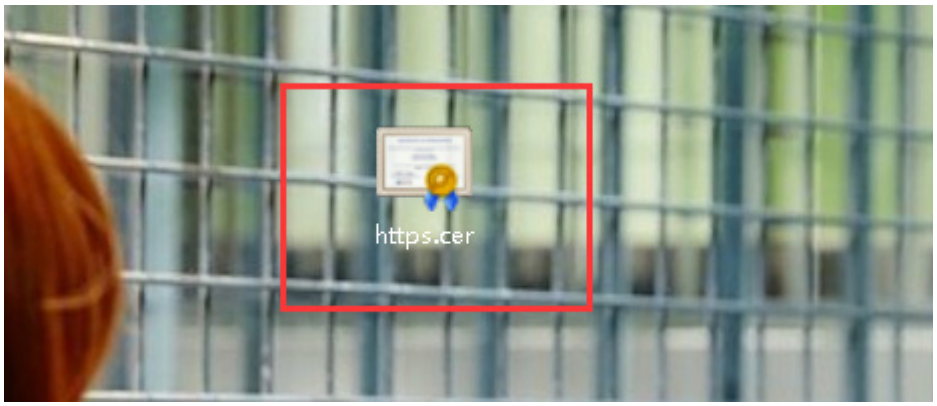
68:91:d0:d0:0b:63	其他	Mr Beam - Laser Cutting for Everybody
00:0c:29:e1:8a:19	门户网站与搜索引擎	百度一下，你就知道
68:91:d0:d0:0b:63	其他	TopMyths
00:0c:29:e1:8a:19	计算机与互联网	Ubuntu Start Page
c4:86:e9:b4:7e:34	娱乐	首页 - 优酷视频
68:91:d0:d0:0b:4d	门户网站与搜索引擎	日历啊 - Yahoo Search Results
68:91:d0:d0:0b:63	其他	Welcome to EXECUTIVE SEARCH WORLDWIDE

5 终端证书导入方法

5.1 PC浏览器证书导入方法

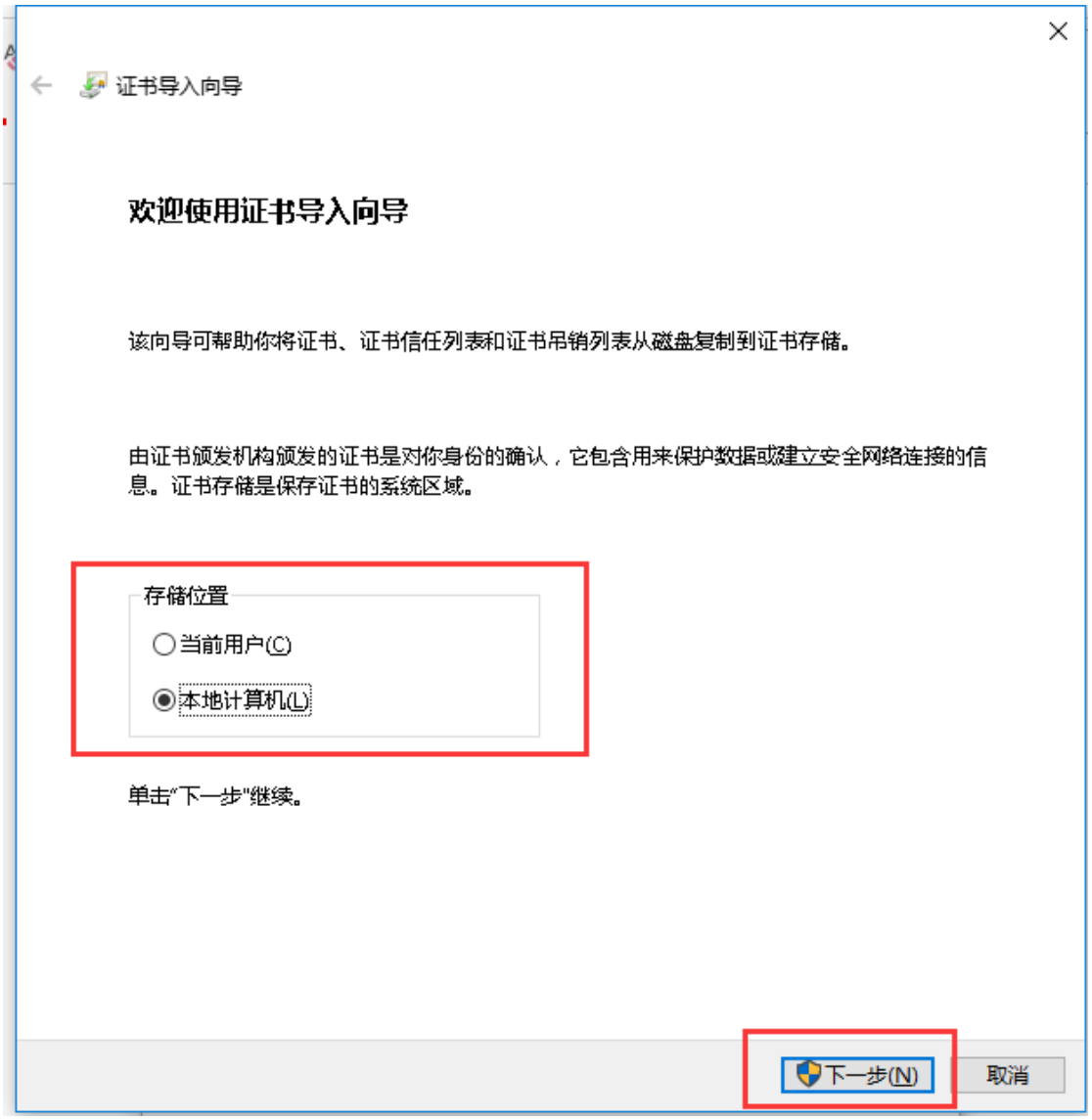
5.1.1 IE/chrome 浏览器证书的导入【适用于除 Firefox 以外的浏览器】

(1) 下载证书【https.cer】到 PC。

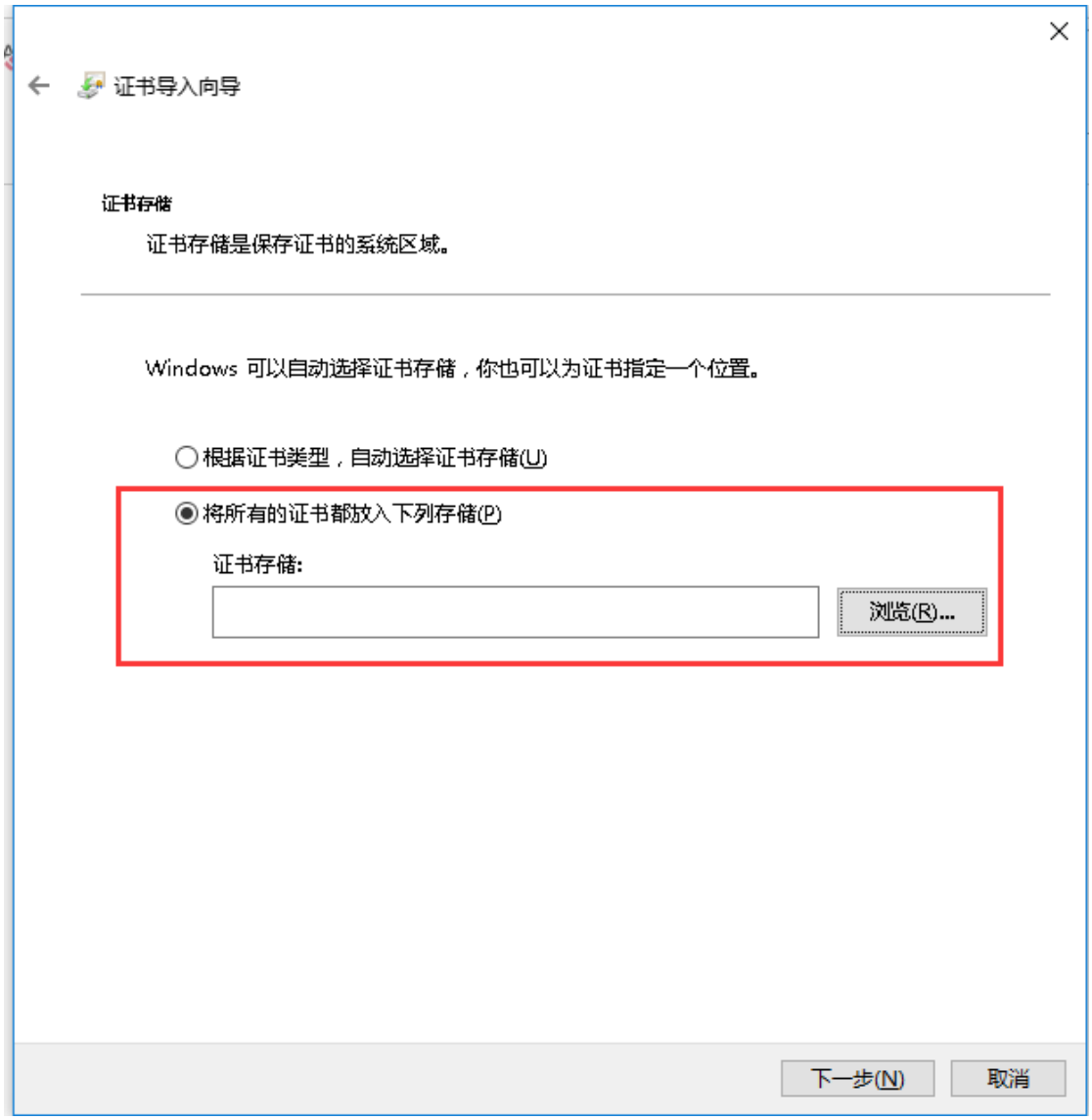


(2) 双击打开证书【https.cer】，选择安装证书。

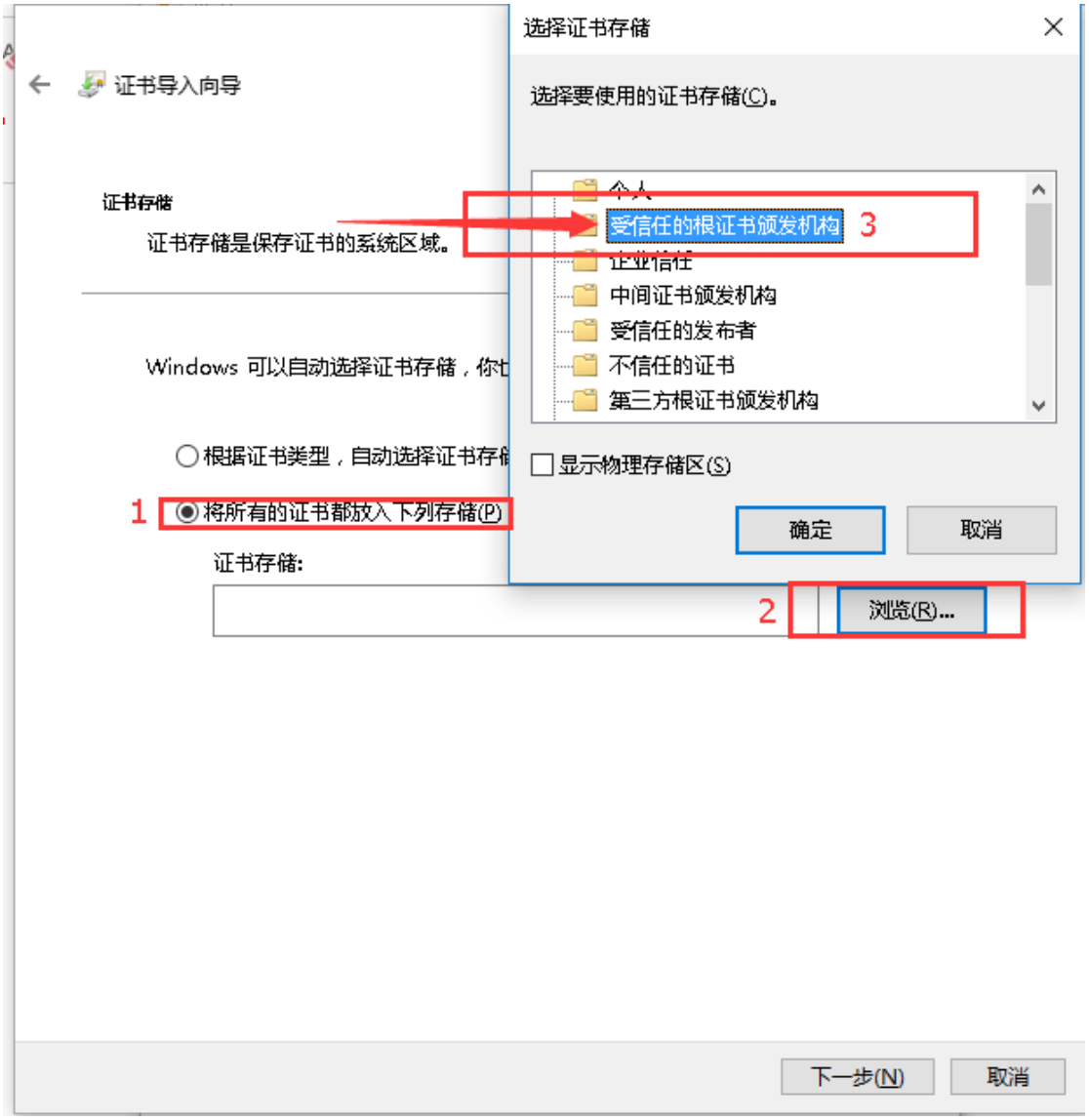
(3) 选择证书存储位置【二者皆可】



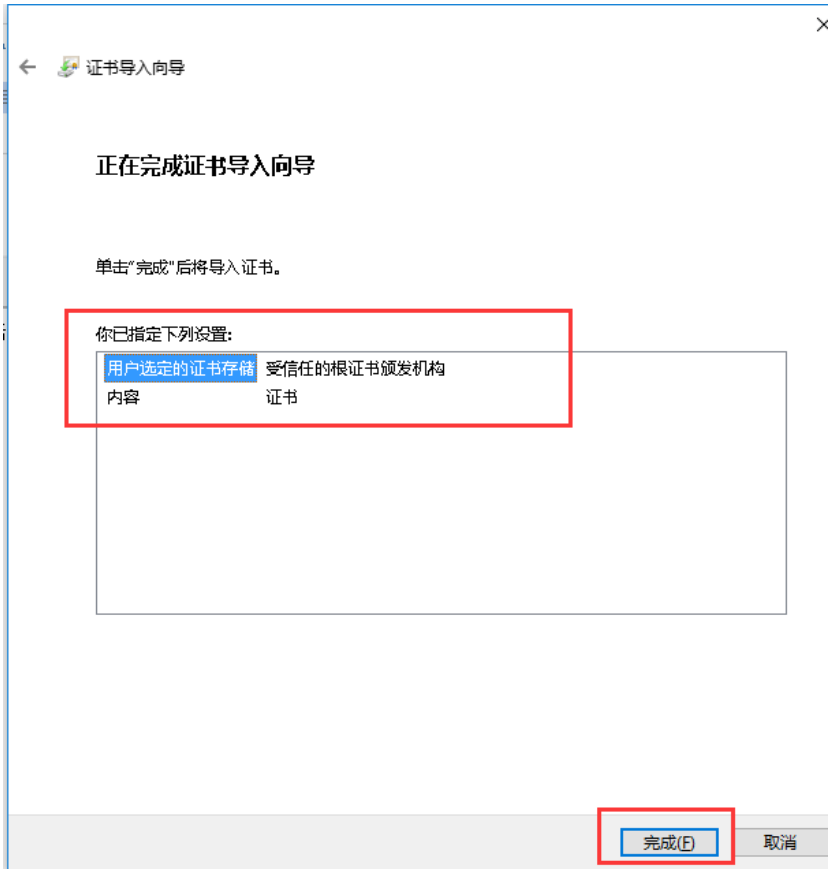
(4) 选择【将所有证书放入下列存储】

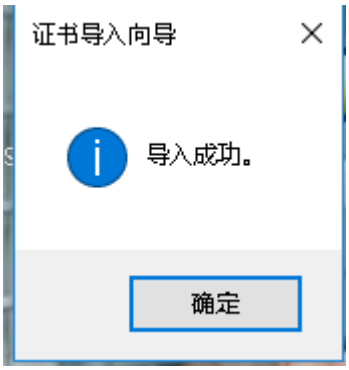


(5) 点击【浏览】选择【受信任的根证书颁发机构】然后【下一步】


证书导入向导
证书存储
证书存储是保存证书的系统区域。
Windows 可以自动选择证书存储，你
根据证书类型，自动选择证书存
1
将所有的证书都放入下列存储(P)
证书存储:
2
浏览(R)...
下一步(N)
取消
选择证书存储
选择要使用的证书存储(C)。
个人
受信任的根证书颁发机构
3
企业信任
中间证书颁发机构
受信任的发布者
不信任的证书
第三方根证书颁发机构
显示物理存储区(S)
确定
取消

(6) 确认信息点击【完成】





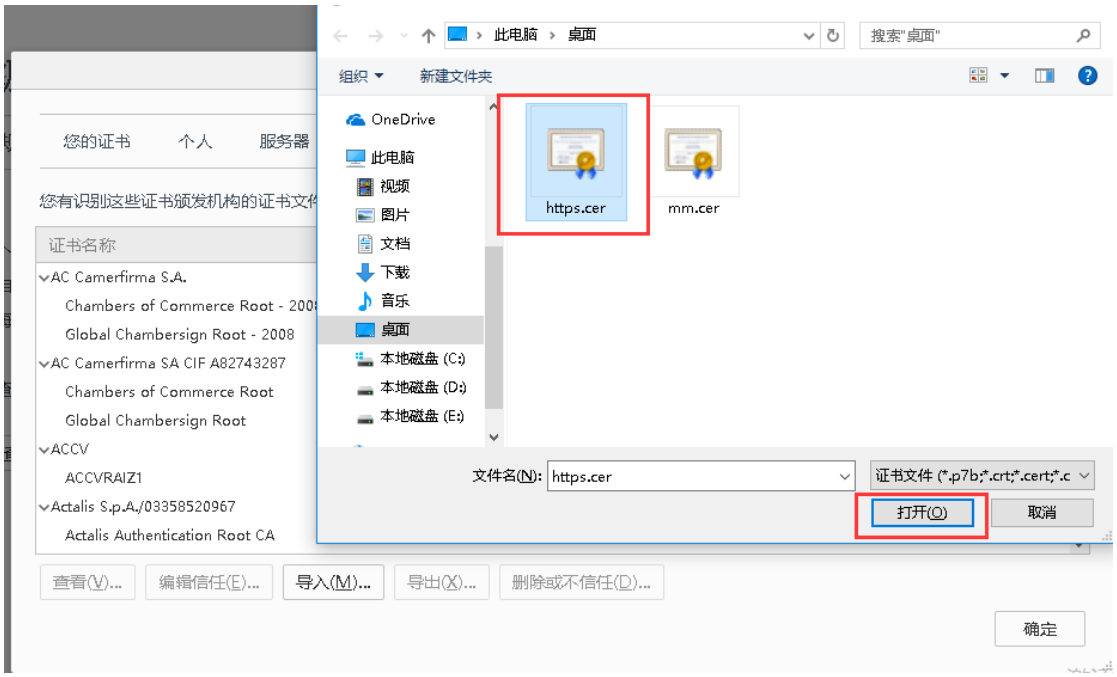
5.1.2 Firefox 浏览器证书的导入

(1) 打开 Firefox 浏览器，选择【选项】

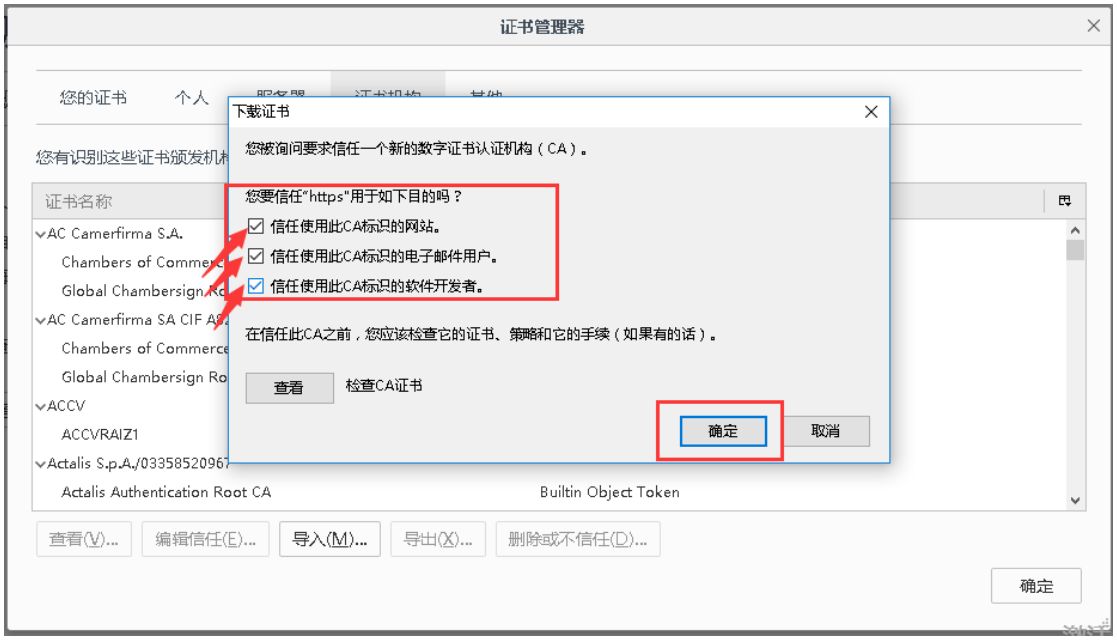
(2)　选择【高级】——【证书】——【查看证书】

(3)　进入【证书机构】——选择【导入】

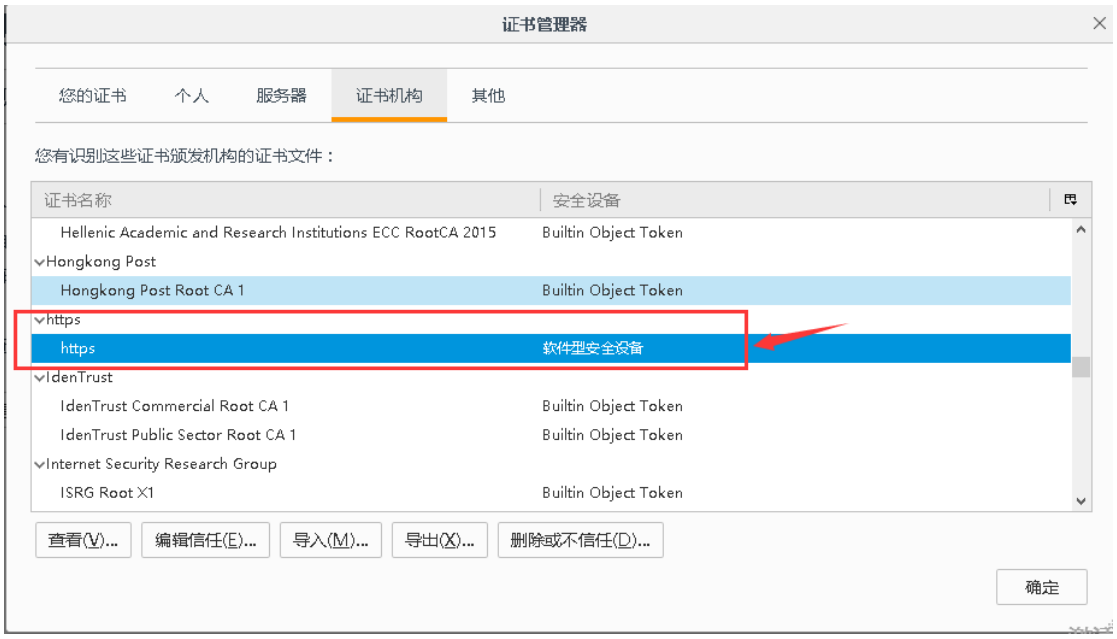
(4)　选择【https.cer】点击【打开】



(5)　【全部勾选三个信任提示】——【确定】



(6)　确认导入的证书点击【确定】



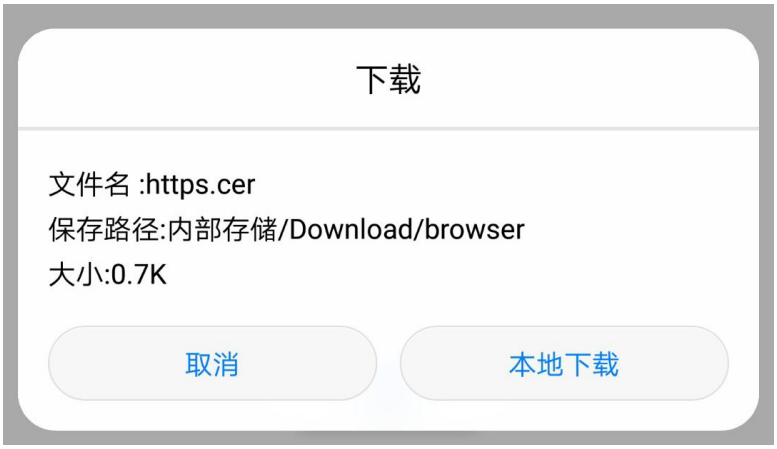
注：浏览器导入证书需要清除缓存以后重新打开浏览器！

5.2 移动终端证书导入方法

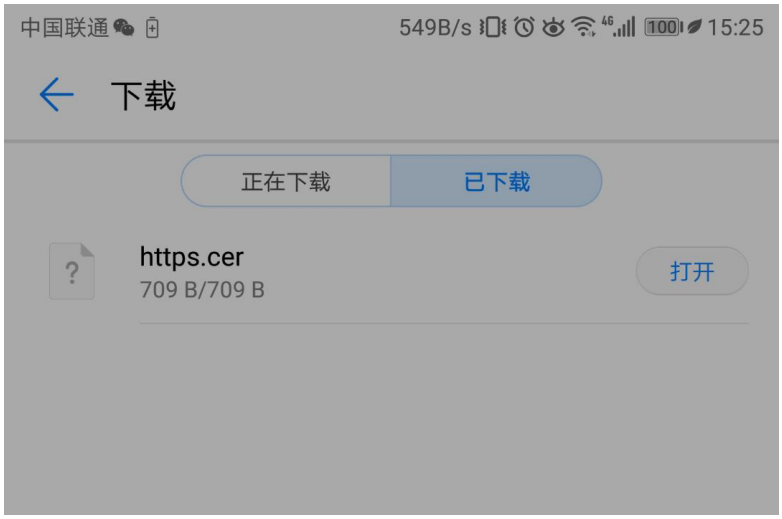
5.2.1 安卓证书导入

(1)　将证书放置 http 网站。

(2) 点击下载证书



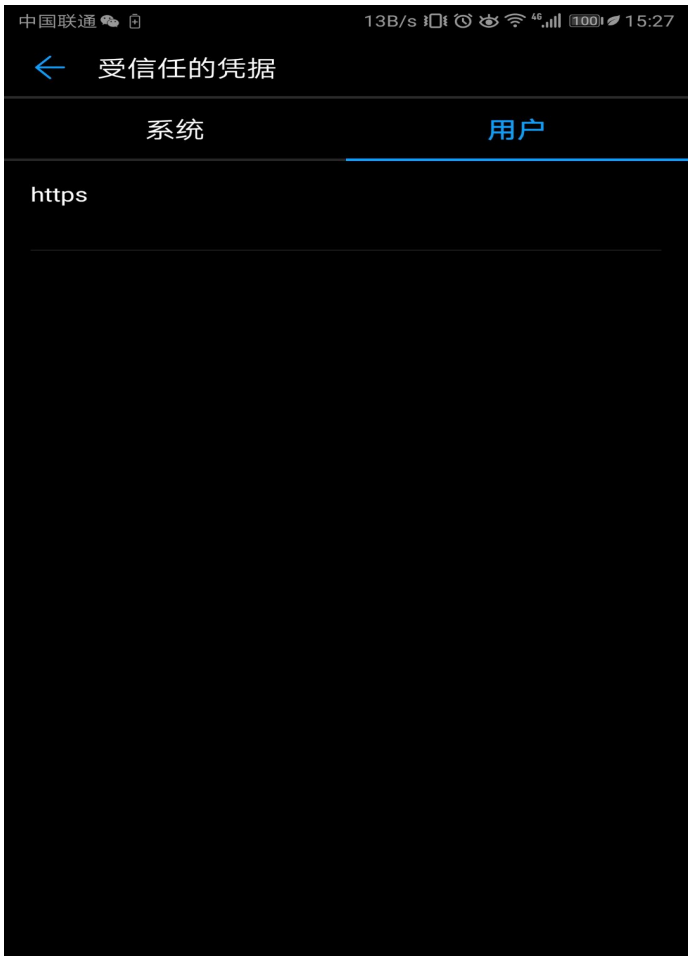
(3) 下载成功后，选择“打开”证书。



(4) 证书安装器会弹出“为证书命名”，并且凭据用途要先选择“WLAN”。

(5) 凭据用途选择“VPN 和应用”再安装一次。

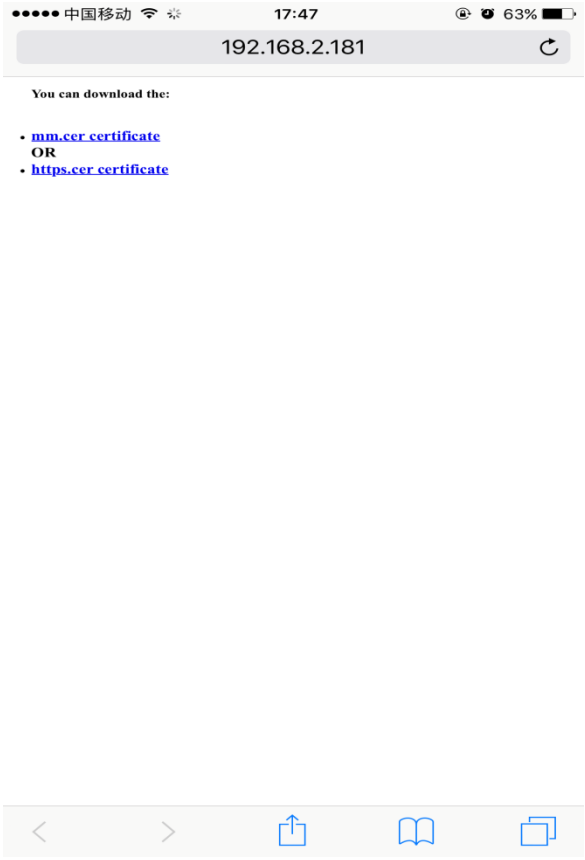
(6)　进入手机“安全与隐私”，选择“受信任的凭据”中“用户”查看证书是否安装成功。



(7) 如果未成功，选择在“安全与隐私”中“从 SD 卡安装证书”，找到证书路径，重复上述步骤安装证书。

5.2.2 苹果 IOS 证书导入

(1) 将证书放置 http 网站。

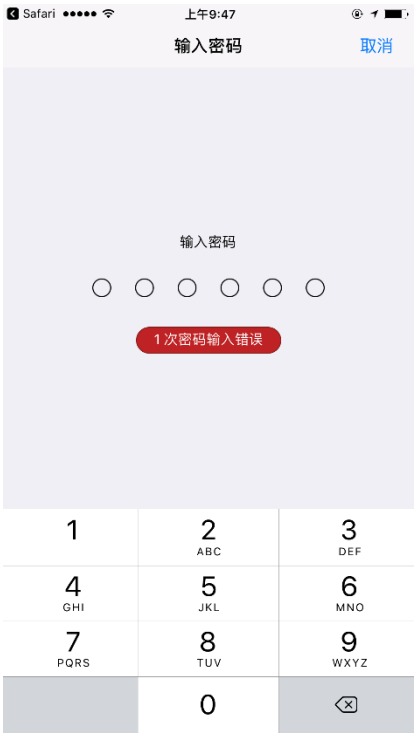

●●●●● 中国移动
17:47
63%
192.168.2.181
You can download the:
mm.cer certificate
OR
https.cer certificate

(2)　点击下载证书

(3)　选择“允许”后，iphone 会直接跳转到安装界面。

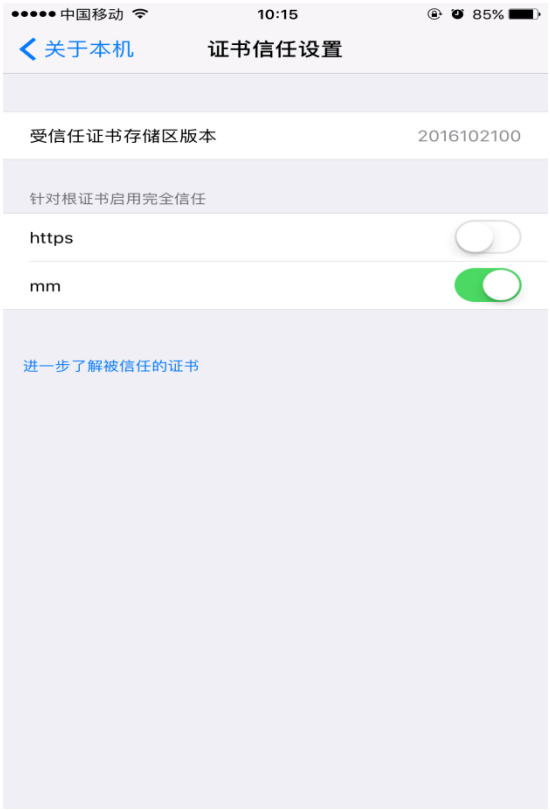
(4) 选择“安装”

对于有些设置了密码的手机，当点击安装后，会跳出以下输入密码的界面，输入自身手机的开机密码即可：



(5)　安装后描述文件显示“已验证”。

(6)　进入“通用”—“关于本机”—“证书信任设置”


●●●●● 中国移动
10:15
85%
关于本机
证书信任设置
受信任证书存储区版本
2016102100
针对根证书启用完全信任
https
mm
进一步了解被信任的证书

(7) 在证书勾选信任。

目 录

1 简介

本文档介绍设备的自定义应用配置举例。自定义应用功能为根据自己定义的规则，标识为自定义的应用。从而方便管理和监控整个网络。

2 配置前提

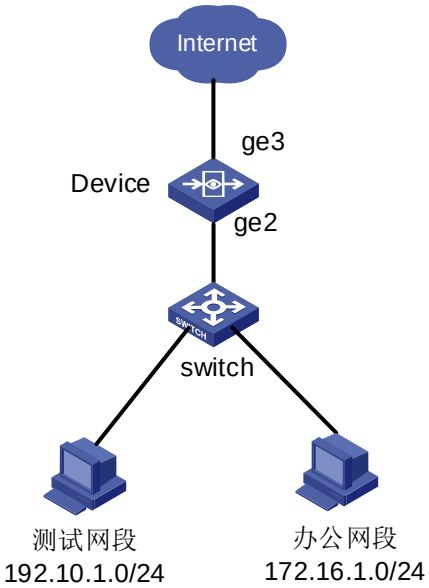
本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 自定义应用配置举例

3.1.1 组网需求

如图 1 所示，某公司内网存在测试网段和办公网段，IP 地址分别为 192.10.1.0/24 和 172.16.10.0/24。使用设备的的 ge2 和 ge3 接口路由模式部署在网络中，设备作为出口网关设备，下联二层交换机。在设备上启用告警功能。

图1 应用自定义路由模式组网图



3.1.2 配置思路

- 配置自定义应用，根据自定义的规则自定义应用。
- 根据自定义规则匹配流量过设备，并且用户在识别范围内。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

1. 新建自定义应用

如图 2 所示，进入“策略配置>对象管理>应用对象>自定义应用”，点击<新建>。

图2 新建自定义应用

如图 3 所示，创建成功的自定义应用如下：

图3 自定义应用配置成功

3.1.5 配置注意事项

- 自定义规则端口、IP、URL 可三选一的填写或者都填写。
- 自定义应用按顺序进行匹配。
- 请尽量使用未被使用的端口进行自定义应用，避免占用其它使用端口流量不识别。
- 用户在设备识别范围内。

3.1.6 验证配置

(1) 验证匹配上自定义应用的流量被识别为自定义应用

如图 4 所示，进入“数据中心>数据分析>会话监控统计>会话监控”查看，发现已经被识别到用户的自定义应用，并正确地记录了会话。

图4 会话监控页面识别到自定义应用

	用户组	源地址	源端口	目的地址	目的端口	协议	类型	应用	发送流量	接收流量	总流量
1	匿名用户组	192.10.1.10	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
2	匿名用户组	192.10.1.8	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
3	匿名用户组	192.10.1.6	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
4	匿名用户组	192.10.1.11	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
5	匿名用户组	192.10.1.2	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
6	匿名用户组	192.10.1.3	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
7	匿名用户组	192.10.1.5	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
8	匿名用户组	192.10.1.9	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
9	匿名用户组	192.10.1.7	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)
10	匿名用户组	192.10.1.4	5335	202.1.1.10	1000	UDP	半连接	AAA	5.17(MB)	0(B)	5.17(MB)

目 录

1 简介

本文档介绍设备的告警功能配置举例。告警功能用于设备超过配置的警告阈值产生的告警日志，并且将日志发送到用户邮箱里。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

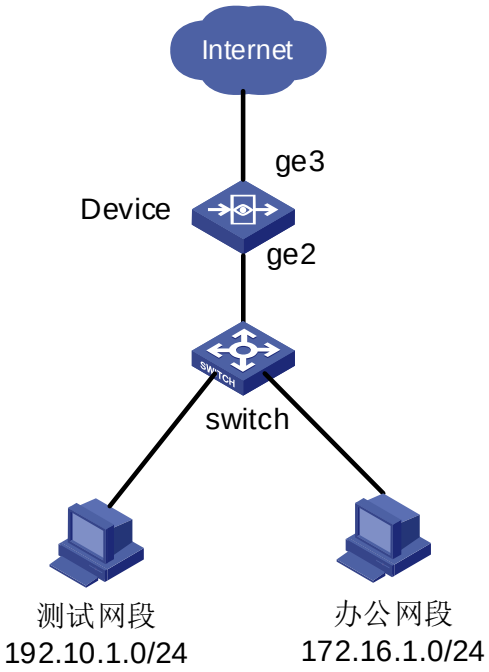
3 告警功能配置举例

3.1 组网需求：路由模式组网

3.1.1 组网需求

如图 1所示，某公司内网存在研发网段和财务网段，IP 地址分别为 192.10.1.0/24 和 172.16.10.0/24。使用设备的的 ge2 和 ge3 接口路由模式部署在网络中，设备作为出口网关设备，下联二层交换机。在设备上启用告警功能。

图1 告警路由模式组网图



3.1.2 配置思路

- 配置告警时间，启用并设置警告项目及其阈值。
- 配置邮箱服务器，产生的日志发送至用户邮箱。
- 配置 DNS 服务器。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

1. 配置告警事件

进入“系统管理>系统维护>系统告警>告警事件”，如图 2 所示，启用并配置告警事件。

图2 配置告警事件

2. 配置邮件服务器

进入“系统管理>系统维护>系统告警>邮件配置”，如图 3 所示，配置邮件服务器。

图3 配置邮件服务器

3. 配置 DNS 服务器

进入“网络配置>基础网络>DNS 服务>DNS 服务器”，如图 4 所示，启用 DNS 代理并填写 DNS 服务器。

图4 配置 DNS 服务器

3.1.5 配置注意事项

- 设备告警事件必须超过设置的阈值才会产生警告日志。
- 开启 DNS 服务器，必须使用域名解析。
- 某些邮箱设定启用 smtp 服务器时，需要授权码进行身份认证，所以密码应该填授权码而不是邮箱密码。

3.1.6 验证配置

1. 测试网段和办公网段大流量、多会话过设备。

设备到达设置的告警阈值，产生告警日志如图 5 所示。

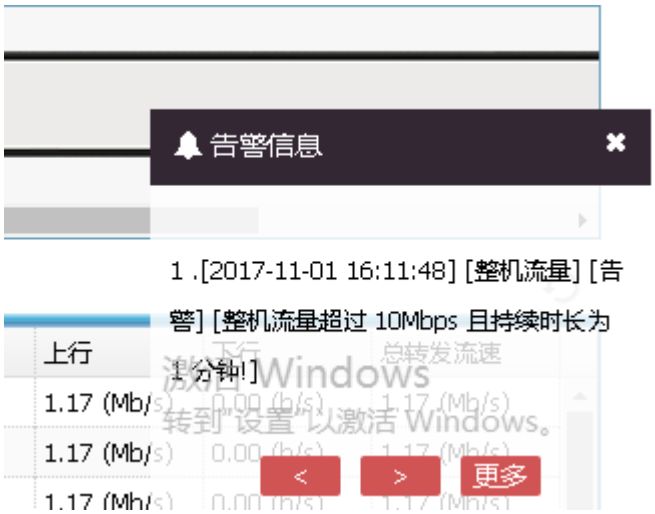
图5 告警日志页面

	时间	告警内容
1	2019-04-23 19:24:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
2	2019-04-23 19:24:36	CPU利用率超过 50% 且持续时长为 1 分钟!
3	2019-04-23 19:23:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
4	2019-04-23 19:23:36	CPU利用率超过 50% 且持续时长为 1 分钟!
5	2019-04-23 19:22:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
6	2019-04-23 19:21:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
7	2019-04-23 19:20:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
8	2019-04-23 19:19:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
9	2019-04-23 19:18:36	整机流量超过 10Mbps 且持续时长为 1 分钟!
10	2019-04-23 19:17:36	整机流量超过 10Mbps 且持续时长为 1 分钟!

2. 2 . 设备首页弹出日志告警。

设备产生告警日志，设备系统首页弹出告警弹窗如图 6 所示。

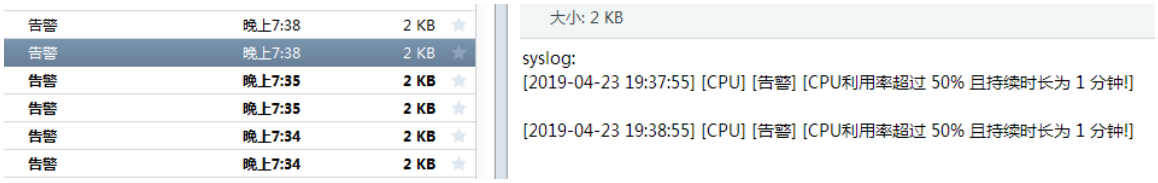
图6 告警弹窗



3. 3 .用户邮箱收到告警日志。

设备产生告警日志，用户邮箱收到告警日志邮件如图 7 所示。

图7 用户邮箱收到告警日志



目 录

1 简介

DNS（Domain Name System，域名系统），因特网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。通过主机名，最终得到该主机名对应的 IP 地址的过程叫做域名解析（或主机名解析）。DNS 协议运行在 UDP 协议之上，使用端口号 53。在网关实现透明代理可以既解决内网用户繁杂的 DNS 服务器设置问题，又可以方便的对服务器进行切换。另外，由于各个 WAN 出口的带宽不通。DNS Proxy 在进行请求转发时需要在各个接口上面进行负载均衡，为了增加 DNS 管理的灵活性，设备提供静态域名和特定域名的定向转发功能。透明代理的规则分为 2 种类型：手工配置和自动链路继承。手工配置是指对于配置有 IP 地址的三层网络接口，需要人为的配置正确的 DNS 服务器地址才能正常域名解析的类型。自动链路继承是指对于配置为 DHCP 或 PPPOE 类型的网络接口，既可以人为配置 DNS 服务器地址也可以从地址服务器端获取 DNS 服务器地址的类型。

本文档介绍设备的 DNS 配置举例，包括域名管理、动态缓存、特定域名解析、DNS 透明代理、DNS 全服务器。

在配置 DNS 前，先了解如下几个定义：

- 域名管理：域名管理也就是之前的静态域名功能，是 DNS 代理常见的功能，实现域名和 IP 地址的固定映射。该映射关系的优先级最高，如果一个 DNS 请求能匹配域名管理，那优先使用域名管理进行 DNS 应答。
- 动态缓存：开启 DNS 功能后，下联 pc 通过访问动态域名和特定域名后设备解析出来形成一个 cache 表项，下次 pc 再次访问这个域名的时候可以直接通过缓存进行域名访问。动态缓存支持开启和关闭。
- 特定域名解析：一些特殊域名使用公共的 DNS 服务器无法解析，需要在特定的 DNS 服务器才能解析域名。例如指定域名 www.baidu.com 和 map.baidu.com 的 DNS 请求必须用 2.2.2.2 的 DNS 服务器进行解析，而其它任何 DNS 服务器都是错误的。
- DNS 透明代理：DNS 透明代理可以为内网用户提供统一无感知的 DNS 解析服务。内网 pc 只需要随便设置一个 DNS 地址，当 pc 访问域名时由网关统一进行 dns 解析。
- DNS 全局代理：全局 DNS 代理开启时，使用全局代理的 DNS 服务器进行域名解析，解析成功，完成应答，并完成统计和形成缓存。下联 pc 需要把 DNS 地址指向网关地址。

本模块功能具有如下功能点：

- 能够根据用户的 DNS 请求，从本地查找 DNS 缓存，然后对用户的请求做出应答。
- 能够向配置的远端 DNS server 请求，然后对用户的请求做出应答。
- 能够支持 DNS 代理服务的策略配置。
- 能够支持 DNS 透明代理域名管理模糊匹配。
- 能够支持 DNS 透明代理特定域名的定向转发。
- 能够支持 DNS 透明代理域名匹配的优先级。
- 能够支持 DNS 透明代理基于权重的转发。
- 能够支持 DNS 透明代理基于优先级的转发。
- 能够支持 DNS 透明代理基于流量的转发。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 DNS 特性。

3 使用限制

- 对于接口配置，有如下规格要求：
  - 必须是配置 IP 的三层接口，最多配置 32 条接口规则。
  - 只允许 PPPOE 和 DHCP 接口配置继承链路，其它接口都配置为手工方式。
  - 接口配置为手工还是继承链路，只看最原始的接口地址类型。配置成功后，切换接口地址类型，DNS 代理方式更改不生效。例，某接口为静态 ip，配置为手工方式。将此接口更改为 DHCP 获取地址，更改为继承链路功能不生效。
- 域名管理支持前缀模糊匹配，最大配置 128 条。
- 特定域名，特定 DNS 解析，域名同样支持前缀模糊匹配，最大配置 128 条，每条提供主备 DNS。
- DNS 透明代理提供基于优先级和权重的选项。
- DNS 缓存按 5 秒进行一次老化处理，最大缓存数 5W 条。
- DNS 请求的并发性能为每秒 1w 条。
- 本机报文不走 DNS 代理流程，只需要在全局 dns 配置一个有效的 DNS 地址（DNS 全局代理可关闭），在设备上就可以 ping 域名。
- 基于流量的 DNS 透明代理服务器需要使用运营商给的 DNS（使用第三方 DNS 解析出来的 DNS 解析报文有可能联通解析出电信的地址导致 DNS 负载流量统计错误）。

4 配置举例

4.1 组网需求

如图 1 所示，一个拥有 100 员工的公司，有一条电信 100M 带宽的 WLAN 接口，一条联通 20M 的 PPPOE 线路 WLAN 接口，需要平衡网络负载，充分利用带宽资源，具体应用需求如下：

(1) 电信 100M，联通 20M PPPOE 拨号上网。

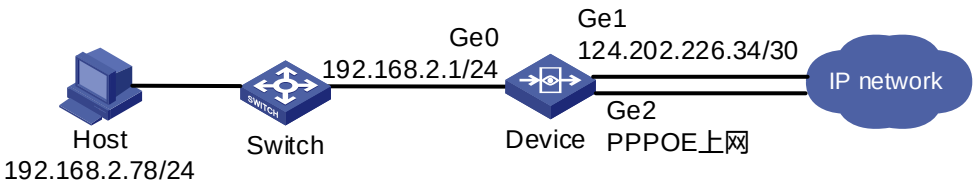
(2) 按照带宽比进行 DNS 负载 100:20。

(3) 内部服务器映射为内网 IP，sapl.123test.com 映射地址 192.168.0.245。

(4) 域名服务器需要特定 DNS 进行解析。例 www.google.com 需要 223.5.5.5 DNS 服务器进行解析。

(5) 开启动态缓存。

图1 DNS 组网图



4.2 配置思路

按照组网图组网。

(1) 开启代理功能，配置基于权重的 DNS 透明代理。

(2) 配置特定域名管理。

(3) 配置特定域名代理。

(4) 开启动态缓存。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

1. 开启 DNS 代理功能，配置基于权重的 DNS 透明代理

如图 2 所示，进入左树“网络配置>基础网络>DNS 服务>DNS 透明代理”，“勾选”启用代理（先新建 DNS 链路才能启用代理功能）。

图2 启用基于权重 DNS 透明代理

如图 3 所示，DNS 透明代理页面，点击<新建>。ge1 接口配置为 DNS 出接口，权重 100，主 DNS 为 114.114.114.114；备 DNS 为 114.114.115.115，点击<提交>。

图3 MGT0 手工 DNS 配置

如图 4 所示，DNS 透明代理页面，点击<新建>。GE2 接口配置为 DNS 出接口，权重 20，DNS 类型继承链路配置，点击<提交>。

图4 GE2-2 继承链路配置

如图 5 所示，创建成功的 DNS 透明代理配置如下：

图5 DNS 透明代理配置效果

2. 配置静态域名

如图 6 所示，进入左树“网络配置>基础网络>DNS 服务>域名管理”。点击<新建>，配置域名为 sapl.123test.com,IP 映射为 192.168.0.245 点击<提交>。

图6 配置静态域名

如图 7 所示，创建成功后的域名管理配置如下：

图7 静态域名配置效果

3. 配置特定域名解析

如图 8 所示，进入左树“网络配置>基础网络>DNS 服务>特定域名解析”。点击<新建>，配置域名为 www.google.com ，主 DNS 为 223.5.5.5 点击<提交>。

图8 配置特定域名解析

如图 9 所示，创建成功后的特定域名解析配置如下：

图9 特定域名解析配置效果

4. 开启动态缓存

如图 10 所示，进入左树“网络配置>基础网络>DNS 服务>动态缓存”。勾选“启用”。

图10 启用动态缓存

4.5 验证配置

(1) 验证 DNS 透明代理功能

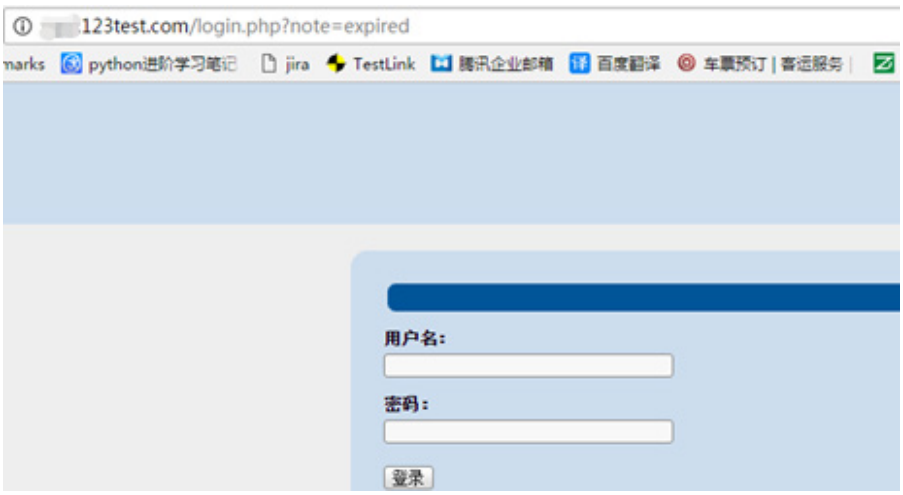
如图 11 所示，访问 www.baidu.com，设备响应主机的 DNS 请求，最终可正常打开百度的主页。

图11 DNS 透明代理效果图

(2) 验证域名管理

如图 12 所示，访问***.123test.com，设备直接匹配域名管理，访问内网服务器。

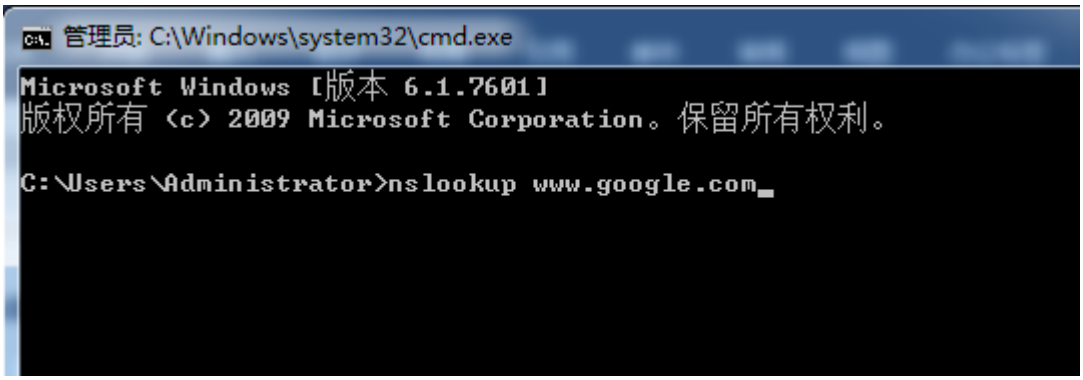
图12 静态域名效果图



(3) 验证特定域名代理

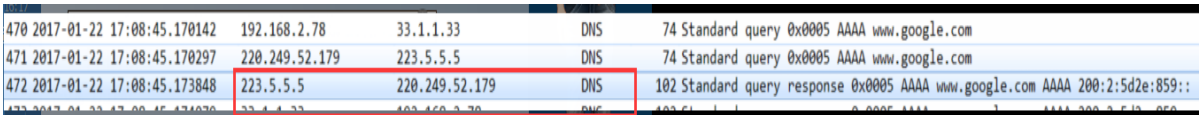
如图 13 所示，在 PC 打开 cmd，nslookup www.google.com。

图13 PC 端 CMD 下 nslookup www.google.com



在设备抓包，接口选择 any，目的端口 53 抓包。如图 14 所示，服务器进行解析的。

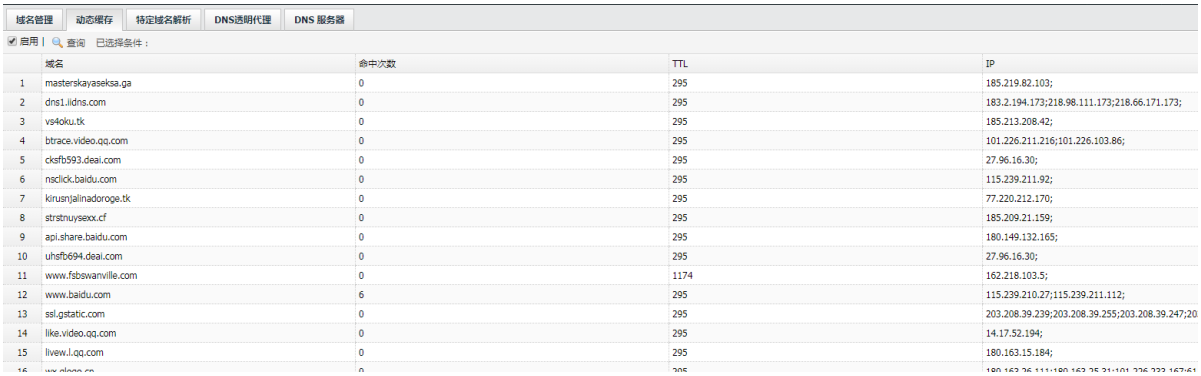
图14 抓包查看特定域名效果图



(4) 验证动态缓存

如图 15 所示，访问各种域名，DNS 解析成功后形成缓存。

图15 动态缓存效果图



	域名	命中次数	TTL	IP
1	masterskayaseksa.ga	0	295	185.219.82.103;
2	dns1.lidns.com	0	295	183.2.194.173;218.98.111.173;218.66.171.173;
3	vs4oku.tk	0	295	185.213.208.42;
4	btrace.video.qq.com	0	295	101.226.211.216;101.226.103.86;
5	cksfb593.deai.com	0	295	27.96.16.30;
6	nsclick.baidu.com	0	295	115.239.211.92;
7	kirusnjalinadoroge.tk	0	295	77.220.212.170;
8	strstnuysexx.cf	0	295	185.209.21.159;
9	api.share.baidu.com	0	295	180.149.132.165;
10	uhsfb694.deai.com	0	295	27.96.16.30;
11	www.fsbswanville.com	0	1174	162.218.103.5;
12	www.baidu.com	6	295	115.239.210.27;115.239.211.112;
13	ssl.gstatic.com	0	295	203.208.39.239;203.208.39.255;203.208.39.247;20
14	like.video.qq.com	0	295	14.17.52.194;
15	livew.l.qq.com	0	295	180.163.15.184;

目 录

1 简介

内网用户使用域名解析的公网 IP 地址访问内网服务器时，需要配置 DNAT 和 SNAT 来解决从内网服务器回包的问题，这样的配置易用性较差。所以添加 DNS 映射功能，直接将服务器解析成私网地址发送给内网用户，用户采用私网地址同内网服务器直接通信。

本文档假设您已了解 DNS 映射功能特性。

2 使用限制

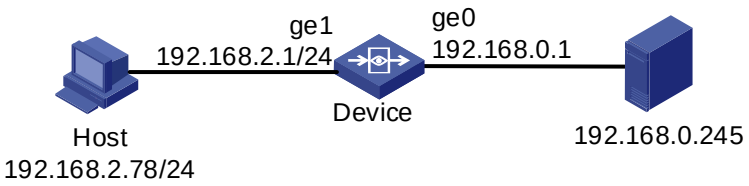
无。

3 配置举例

3.1 组网需求

如图 1 所示，内网服务器 192.168.0.245 对外提供服务，对应的域名地址为***.123test.com，外网 DNS 服务器上域名***.123test.com 绑定的是内网服务器 192.168.0.245 对外映射的公网 IP，现内网用户通过域名***.123test.com 访问内网服务器的服务，只需在 DNS 域名管理开启 DNS 映射，即可实现内网用户通过域名对内网服务器的访问，无此在配置其它 DNAT 和 SNAT。

图1 DNS 映射测试组网图



3.2 配置思路

按照组网图组网。

(1) 配置接口地址。

(2) 新建域名并开启 DNS 映射。

3.3 使用版本

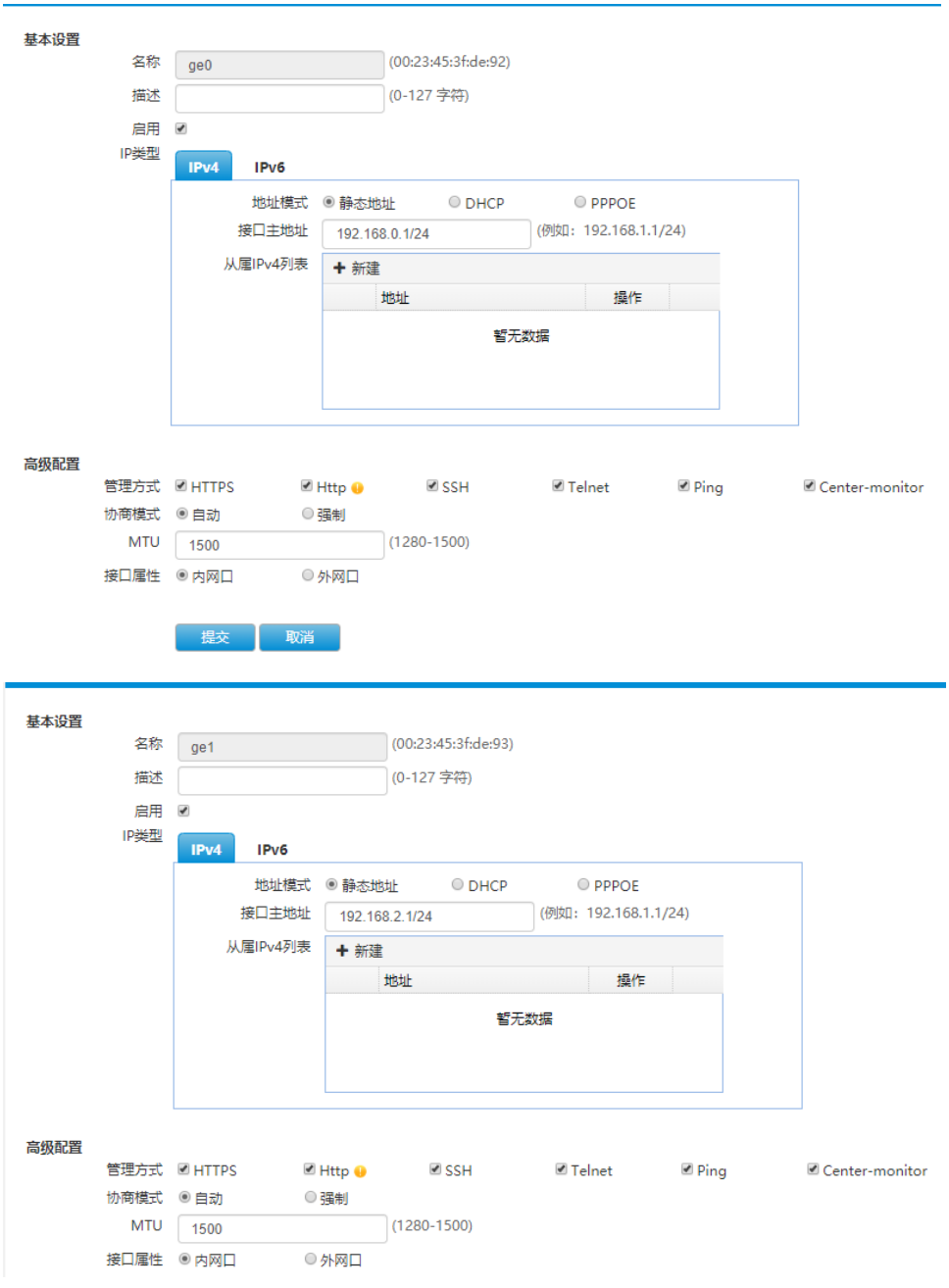
本举例是在 E6442 版本上进行配置和验证的。

3.4 配置步骤

1. 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击<操作>按钮，配置外网口 ge0 地址为 192.168.0.1/24，内网口 ge1 地址为 192.168.2.1/24。

图2 配置接口地址



2. 新建域名并开启 DNS 映射

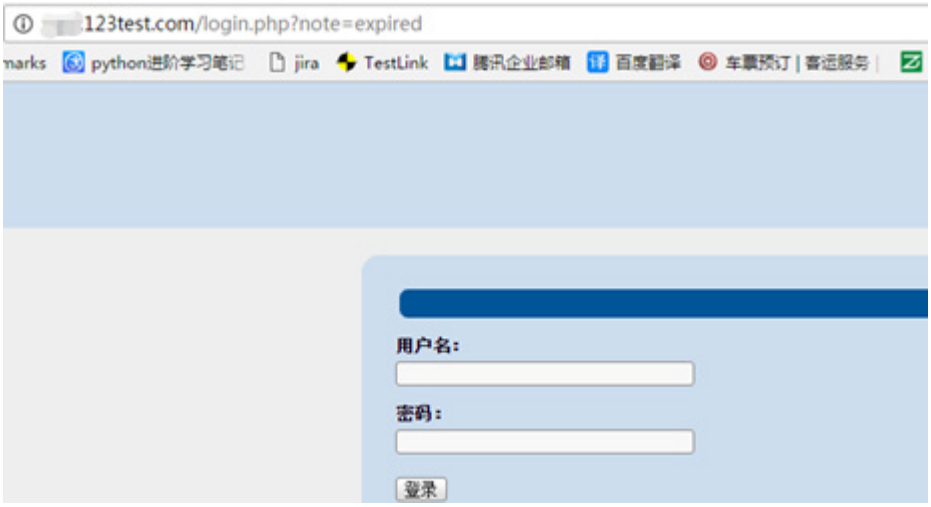
如图 3 所示，进入“网络配置>基础网络>DNS 服务>域名管理”，点击<新建>。配置域名管理并开启 DNS 映射，点击提交。

图3 新建域名并开启 DNS 映射

3.5 验证配置

(1) 验证 DNS 映射功能

内网用户通过域名***.123test.com 可直接访问内网服务器上 192.168.0.243 上提供的 web 服务。



目 录

1 IPsec 快速配置简介

由于连锁酒店分支机构众多，IPSEC VPN 业务的部署和维护非常复杂，给管理员的工作带来非常大的挑战：“VPN 业务多变，管理复杂”，现有标准 IPSEC VPN 的配置比较繁琐，组网变化带来的配置改动比较大。因此急需提供一种易用性更好，配置更简洁的解决方案。IPSEC 快速配置就是在这样的场景下应运而生的。

按照以往 VPN 的配置，一个分支上线会有很多相关配置，步骤较多，且在隧道显示上也不太友好，主要表现在如下几个方面：

- 每个分支上线都需要创建 IKE、IPsec 和对应的 tunnel 口，然后在 tunnel 口配置感兴趣流，和对应的 tunnel 路由。中心端有多少个 IP，分支端就需要创建多少个 IKE、IPsec 和 tunnel 口及 tunnel 路由。当走 IPsec 隧道的网段发生变化时，我们需要同步修改对应的感兴趣流和 tunnel 路由。当分支特别多的时候，对于管理员来说是一项非常巨大且繁琐的工作，很容易出现配置错误，不好排查。
- 在 web 页面查看各隧道的流量和状态时，每个隧道只能显示本端 IP 和对端 IP，却不知道这条隧道对应的哪个分支，需要根据分支和 IP 的对应关系，才能知道属于哪个分支。且一个分支的多个感兴趣流会显示多个 SA，无法聚合，显得比较杂乱，不便查看。
- 如果一个分支的私有网段和另一个分支的私有网段有冲突，如，都使用了 192.168.10.1/24 网段，则后上线的分支需要做 NAT，转换为另外一个不冲突的网段才能正常工作。这个 NAT 配置需要绑定对应的隧道口，以明确只有过隧道的流量才需要转换。如果隧道口有变动，则相应的 NAT 配置也需要做对应变动。

鉴于以上配置上的繁琐和显示上的不友好，我们要做出改进，优化连锁酒店的 IPSEC VPN 管理工作，尽可能地使 VPN 配置自动化，简单化，甚至是傻瓜化，做到“快速上线、动态适应、部署简单”。

针对以上目标，IPsec 快速配置具体的改进措施如下：

- 隐藏 IKE/IPsec/tunnel 口的创建过程。

  管理员只需配置本端分支名称，对端 IP 和预共享密钥。后台根据这些配置，自动生成对应的 IKE、IPsec 和 tunnel 口，其它相关参数均使用内置的默认参数。
- 感兴趣流不再配置，tunnel 路由不再配置。

  管理员只需要配置本端的保护网段，即需要走 IPsec 的源网段。对端也是如此。当两端建立起 IKE 后，交互各自的保护网段，形成感兴趣流，同时以对端的保护网段为目的网段，生成对应的 tunnel 路由。
- 支持多线路备份。

  高优先级线路断开后，无缝切换到低优先级的线路；当高优先级线路恢复后，再切换回高优先级线路。
- NAT 规则不再配置。

  管理员只需要配置哪些源网段转换为哪些目的网段。后台会自动生成对应的 NAT 规则。
- 隧道状态展示优化。

  页面显示隧道状态时，以分支名称为 key，一条记录聚合显示该分支相关隧道的信息，便于查看，支持搜索。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解快速 IPsec 特性。

3 使用限制

(1) 快速 vpn 模板不允许手动修改。

(2) 默认主模式，不支持 DNAT。

(3) 感兴趣流保护接口只保护主地址，不支持从地址。

(4) 网段映射：一对一 NAT 映射，源网段和映射后网段掩码必须一致，按照 IP 的顺序进行一对一映射，（例如映射前 ip 为 192.168.1.100；那么映射后就是 172.16.21.100）。

(5) 网段映射：最多支持 32 个网段映射。

(6) 分支端：线路 IP，设置线路对应的 IP，线路 IP 必须在对端网关 IP 中。

4 创建 IPsec 快速配置

4.1 配置概述

IPsec 配置的推荐步骤如下表所示。

表1 IPsec 快速配置的推荐步骤

配置任务	说明	详细配置
节点基本信息配置	必选	4.2
保护网段配置	必选	4.3
高级选项配置（选路策略、网段映射）	可选	4.4

4.2 节点基本信息配置

在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 快速配置”，进入 IPsec 快速配置的显示页面，如图 1、图 2、图 3 所示。

图1 IPsec 快速配置分支节点显示页面

图2 IPsec 快速配置新建对端网关显示页面

图3 IPsec 快速配置中心节点显示页面

页面的详细说明如表 2 所示。

表2 IPsec 快速配置显示页面的详细说明

项目	说明
名称	节点的IPSEC名称，多隧道时聚合隧道的名称显示成该名称
节点位置	包含分支节点、中心节点两种类型
新建对端网关	分支对端中心节点IP配置，多隧道时配置多个IP，IP最多配置4个，每配置一个IP就会自动生成一套IKE、IPSEC、tunnel的配置
本端IP配置	中心节点与分支对接的接口IP配置，多个接口配置多个IP，最多配置4个IP，每配置一个IP就会自动生成一套IKE、IPSEC、tunnel的配置
预共享密钥	用于分支和中心之间验证对端身份（长度为6-39个字符）

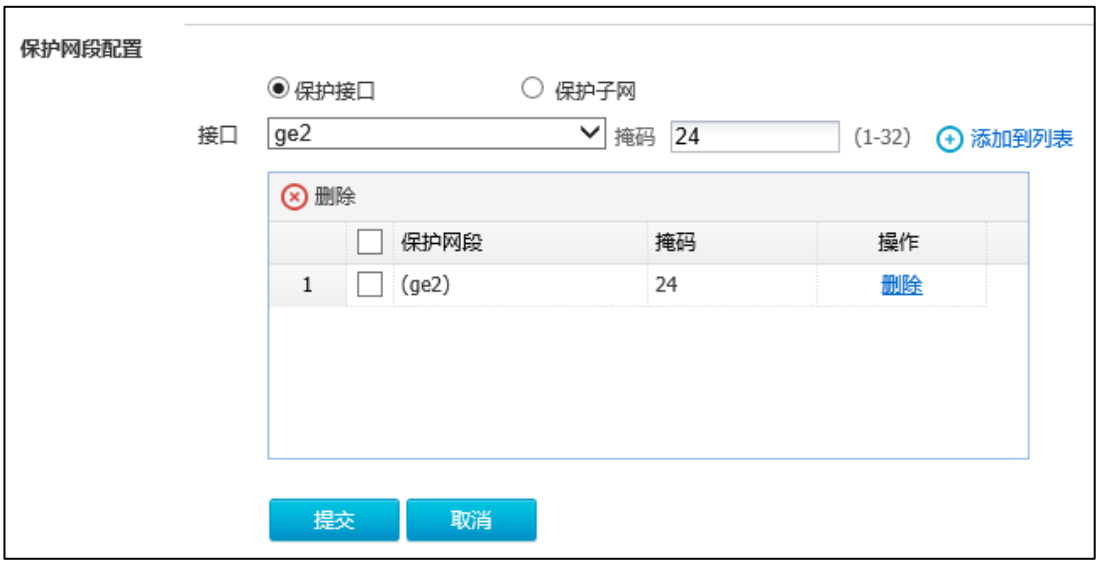
4.3 保护网段配置

在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 快速配置”，进入 IPsec 保护网段的显示页面，单击<保护接口>按钮，在接口列表中选择<接口 >并设置掩码，或者单击<保护子网>按钮，设置保护网段和掩码，如图 4 所示。

图4 IPsec 保护子网配置页面

点击左侧<保护接口>按钮可以保护接口配置选项，如图 5 所示。

图5 IPsec 协商策略详细配置页面



页面的详细说明如表 3 所示。

表3 IPsec 保护网段配置的详细说明

项目	说明
保护接口	自动根据保护接口IP及掩码生成保护网段，该网段会自动传递给对端网关，对端网关根据此保护网段自动生成相应tunnel口的路由
保护子网	该网段会自动传递给对端网关，对端网关根据此保护网段自动生成相应tunnel口的路由

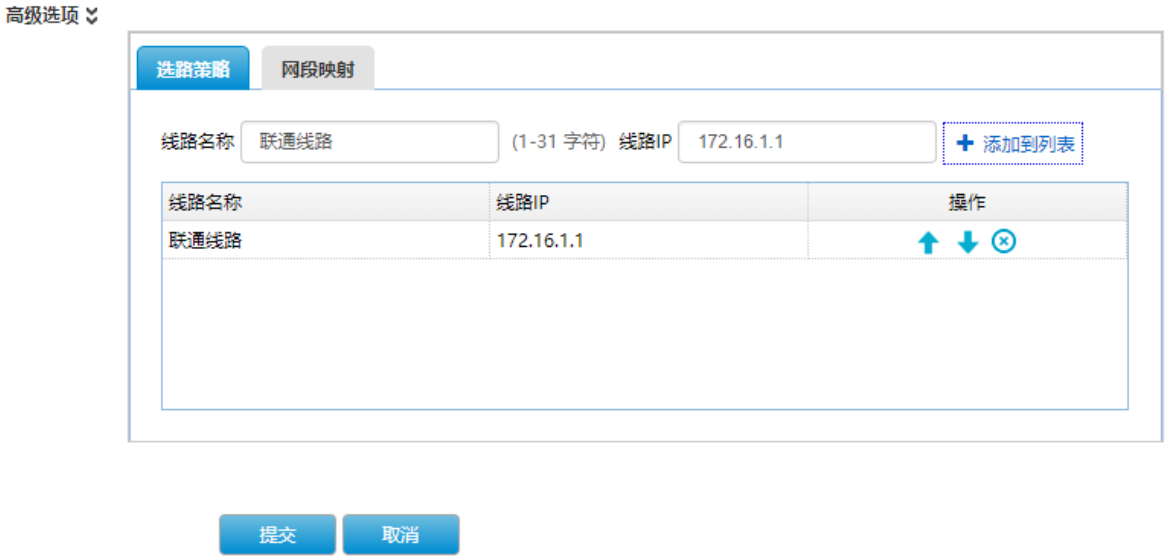
输入完毕后，点击<添加到列表>，点击<提交>按钮，应用配置。

在 IPsec 保护网段列表中，点击保护网段右侧的<删除>按钮，可以删除对应的保护网段，或者选中多个条目，点击左上角的<删除>按钮，批量删除多个保护网段的配置。

4.4 高级选项配置

在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 快速配置”，节点类型选择<分支节点>，单击对端网关<新建>按钮，进入分支节点“高级选项配置”。如图 6 所示。

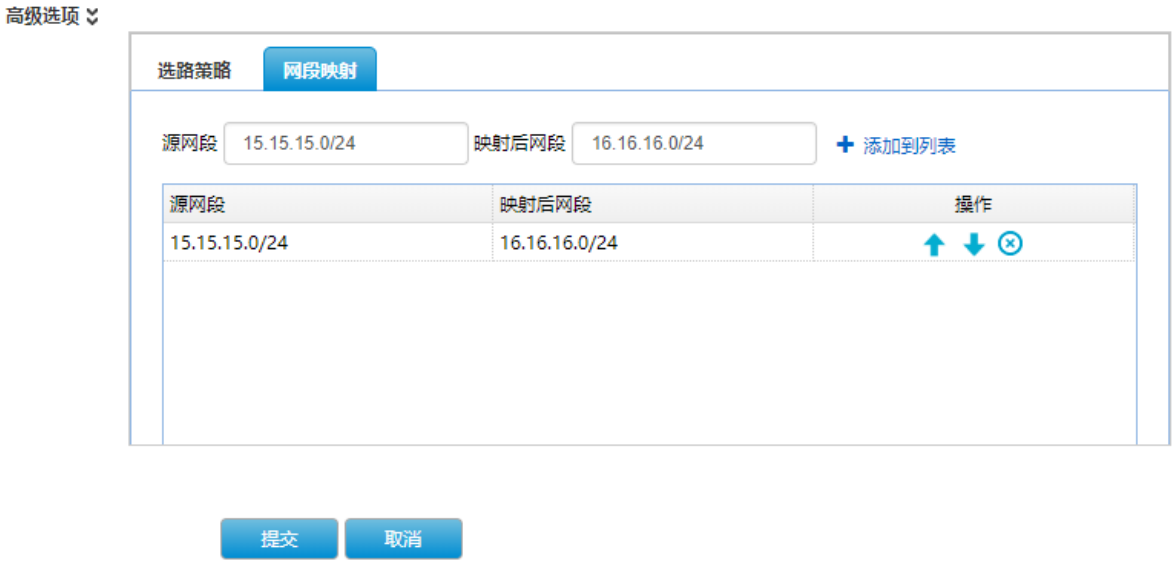
图6 IPsec 分支节点高级选项选路策略配置页面



输入线路名称、线路 IP，点击<添加到列表>，点击<提交>应用配置。

点击右侧<网段映射>，进入高级选项-网段映射配置页面，如图 7 所示。

图7 IPsec 分支节点高级选项网段映射配置页面



输入源网段、映射后网段，点击<添加到列表>，点击<提交>应用配置。

页面的详细说明如表 4 所示。

表4 IPsec 高级选项的详细说明

项目	说明
选路策略	选路策略中的线路顺序决定了不同隧道的路由优先级，规格支持配置4条线路
线路名称	设置线路名称
线路IP	设置线路对应的IP，线路IP必须在对端网关IP中
网段映射	一对一NAT映射，源网段和映射后网段掩码必须一致，按照IP的顺序进行一对一映射，最多支持32个网段映射
源网段	映射前源网段
映射后网段	映射后目的网段，在对端网关看到的保护网段是映射后网段

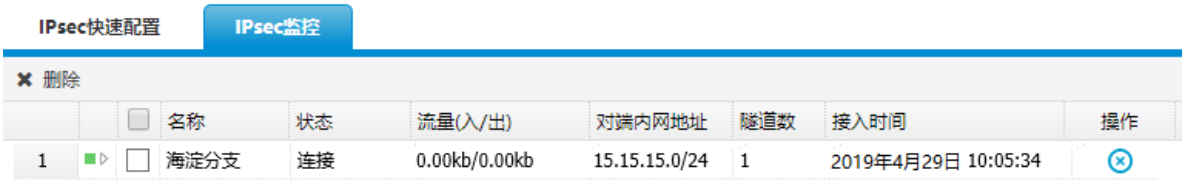
说明：中心节点高线选项配置只有网段映射，没有选路策略，选路策略只需在分支节点配置，分支节点配置的选路策略会自动同步给中心节点。

4.5 IPsec状态监控

4.5.1 查看 IPsec 监控

在导航栏中选择“网络配置>VPN>IPsec-VPN 快速配置>IPsec 监控”，进入 IPsec 监控显示页面。页面中显示了已经新建的 IPsec 聚合隧道。如图 8、图 9 所示。

图8 IPsec 监控显示页面



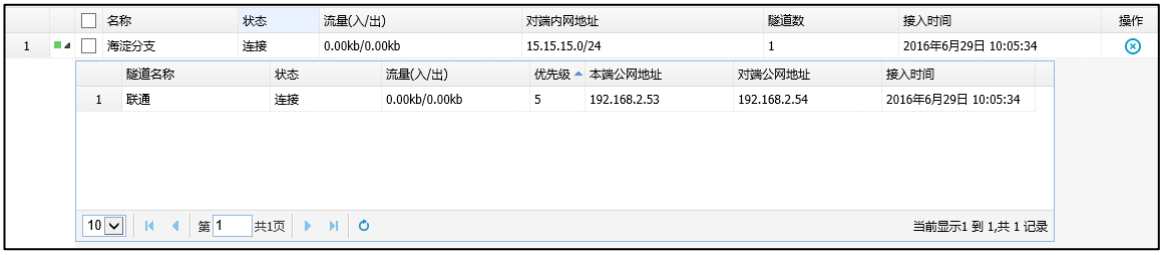
页面的详细说明如表 5 所示。

表5 IPsec 监控显示页面的详细说明

项目	说明
名称	对端IPSEC名称
状态	IPSEC SA状态
流量（入/出）	聚合隧道的双向总流量
对端内网地址	对端保护网段
隧道数	分支与中心设备之间建立的隧道数量计数
接入时间	隧道建立时间
操作	点击 可删除聚合隧道

点击聚合隧道左侧的 按钮，可以展开显示各隧道的详细情况，如图 9 所示。

图9 展开显示隧道情况



页面的详细说明如表 6 所示。

表6 IPsec 监控显示页面的详细说明

项目	说明
隧道名称	隧道名称，显示为分支端配置的选路策略中的线路名称
状态	隧道IPSEC SA状态
流量（入/出）	隧道的双向流量统计
优先级	隧道优先级，多隧道备份时流量优先走优先级数值小的隧道，其它隧道做备份
隧道数	分支与中心设备之间建立的隧道数量计数

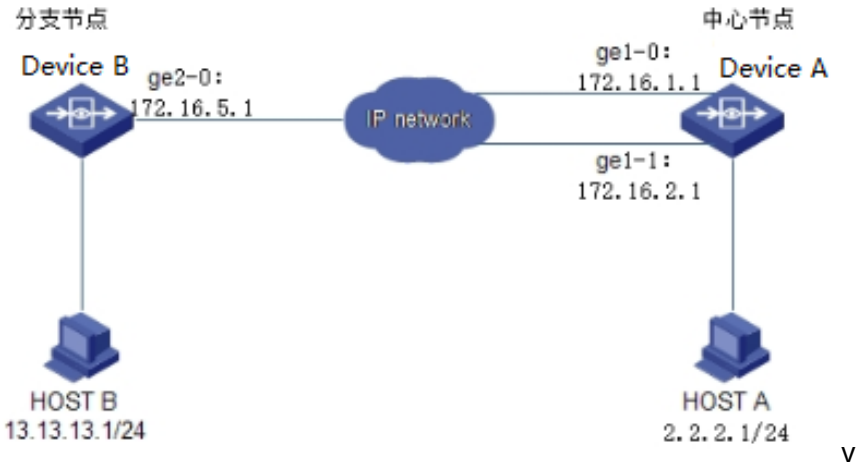
项目	说明
本端公网地址	隧道本端的公网地址
对端公网地址	隧道对端的公网地址
接入时间	隧道建立时间

5 IPsec 快速配置举例

5.1 组网需求

如图 10 所示，在设备 A 和设备 B 之间建立两个安全隧道，对 Host A 代表的子网（2.2.2.0/24）与 Host B 代表的子网（13.13.13.0/24）之间的数据流进行安全保护，同时实现隧道备份。

图10 IPsec 举例组网图



v

5.2 配置思路

按照组网图组网。

(1) 中心设备 IPsec 快速配置。

(2) 分支设备 IPsec 快速配置。

(3) 分支端选路策略配置。

5.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

5.4 配置步骤

5.4.1 配置设备

(1) 中心设备 IPsec 快速配置

对设备设备 A 的 IPsec 配置如图 11 所示。

图11 中心端 IPsec 快速配置

(2) 分支设备 IPsec 快速配置

对设备设备 B 的 IPsec 快速配置如图 12、图 13 所示。

图12 分支端 IPsec 快速配置

图13 分支端设备选路策略配置

5.5 验证配置

在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 快速配置> IPsec 监控”，查看隧道建立状态，如图 14、图 15 所示。

图14 设备 A 的 IPsec 监控

图15 设备 B 的 IPsec 监控

目 录

1 简介

IPsec 用于保护敏感信息在 Internet 上传输的安全性。它在网络层对 IP 数据包进行加密和认证。IPsec 提供了以下网络安全服务，这些安全服务是可选的，通常情况下，本地安全策略决定了采用以下安全服务的一种或多种：

- 数据的机密性：IPsec 的发送方对发给对端的数据进行加密。
- 数据的完整性：IPsec 的接收方对接收到的数据进行验证以保证数据在传送的过程中没有被修改。
- 数据来源的认证：IPsec 接收方验证数据的起源。
- 抗重播：IPsec 的接收方可以检测到重播的 IP 包并且丢弃。

使用 IPsec 可以避免数据包的监听、修改和欺骗，数据可以在不安全的公共网络环境下安全的传输，IPsec 的典型运用是构建 VPN。IPsec 使用“封装安全载荷（ESP）”或者“鉴别头（AH）”证明数据的起源地、保障数据的完整性以及防止相同数据包的不断重播；使用 ESP 保障数据的机密性。密钥管理协议称为 ISAKMP，根据安全策略数据库（SPDB）随 IPsec 使用，用来协商安全联盟（SA）并动态的管理安全联盟数据库。

相关术语解释：

- 鉴别头（AH）：用于验证数据包的安全协议。
- 封装安全有效载荷（ESP）：用于加密和验证数据包的安全协议；可与 AH 配合工作也可以单独工作。
- 加密算法：ESP 所使用的加密算法。
- 验证算法：AH 或 ESP 用来验证对方的验证算法。
- 密钥管理：密钥管理的一组方案，其中 IKE（Internet 密钥交换协议）是缺省的密钥自动交换协议。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 IPsec 特性。

3 使用限制

(1) 当使用 FQDN、U-FQDN 时，只能在野蛮模式下使用，主模式不支持。

(2) 当使用证书认证时，ID 类型不可配置，只能使用它内部默认的 ASN1DN 类型，这是与证书认证配套使用的 ID 类型。

(3) ID 在 IKE 协商中有校验对端身份的作用，我们设备只有响应方会校验，主动方不校验。

(4) 在野蛮模式下，还可以根据对端 ID 选用不同的 IKE 来与对端协商。主模式则不可以，因为主模式的 ID 是在最后两个交互报文发送的，而野蛮模式则在第一个报文中发送。

(5) 目前我们支持配置的 ID 类型为 FQDN/UFQDN 和 IP 地址等类型。

(6) 其中 FQDN 是域名，U-FQDN 是用户邮箱格式，但厂商实现的时候，也并不对这些格式进行校验，因此一般都是字符串。

(7) IPsec 使用数字证书验证注意事项：

a. IPSec 的校验都是在响应端做的。

b. 本端设备会使用所有的本地 CA 证书对对端设备配置的用户证书进行校验，所以只要对端设备上有本端设备上 IPsec 配置的用户证书的 CA 证书就会验证通过，连接成功，和 IPsec 中配置的 CA 证书无关。

c. 当使用数字证书对接时，需要在本地证书处导入 CRL。自动更新 CRL 必须是请求发起方的才行，才能把吊销证书的序列号同步过来，IPsec 才能做校验。

d. 用户证书撤销了之后，应该在 CA 服务器—根 CA 配置管理——CRL 管理，导出 CRL，然后把 CRL 导入本地证书的 CRL 到才能和用户证书做校验。

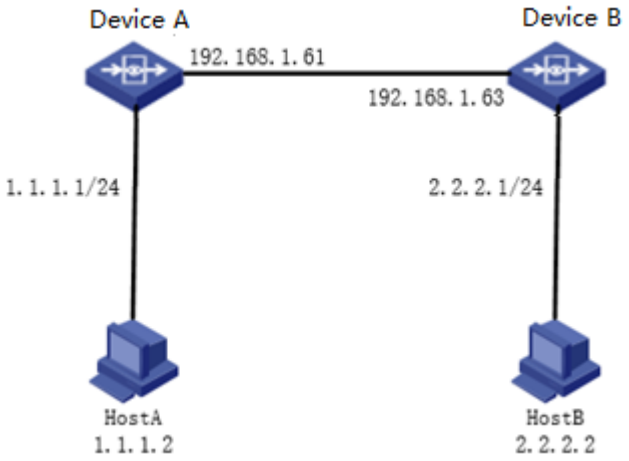
e. 已撤销的证书，证书本身是证明不了自己已撤销。从 CRL 路径中获取 revoke-list，然后获取证书的序列号，看该证书的序列号是否在 revoke-list 中，如果在，则校验失败。即该证书无效。

4 商密 IPsec 配置举例

4.1 组网需求

如图 1 所示，在设备 A 和设备 B 之间使用商密标准建立一个安全隧道，对 Host A 代表的子网（1.1.1.0/24）与 Host B 代表的子网（2.2.2.0/24）之间的数据流进行安全保护。

图1 IPsec 组网图



4.2 配置思路

(1) 按照组网图组网。

(2) 新建 IKE 协商。

(3) 配置 IPsec 协商策略。

(4) 新建所需地址对象。

(5) 新建 IPsec 安全策略。

(6) 新建 IPsec 隧道。

(7) 配置静态路由。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

(1) 新建 IKE 协商：在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 第三方对接”，进入 IPsec 的显示页面，新建 IKE

对设备 A 的 IKE 配置如图 2 所示。

图2 设备 AIKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

对设备 B 的 IKE 配置如图 3 所示。

图3 设备 B 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

(2) 配置 IPsec 协商策略：在导航栏中选择“网络配置 > VPN > IPsec-VPN > Ipsec 第三方对接”，进入 IPsec 协商策略的显示页面，选择要创建 IPsec 的 IKE，然后单击<新建 IPsec>，或者点击对应 IPsec 的右侧<编辑>按钮，进入 IPsec 协商策略的配置页面。

对设备 A 的 IPsec 协商策略配置如图 4 所示。

图4 设备 A 的 IPsec 协商策略配置

对设备 B 的 IPsec 协商策略配置如图 5 所示。

图5 设备 B 的 IPsec 协商策略配置

(3) 新建所需地址对象配置如图 6 所示。

图6 地址对象配置

(4) 新建 IPSec 安全策略配置如图 7 所示。

图7　设备 A 的 IPv4 控制策略配置信息

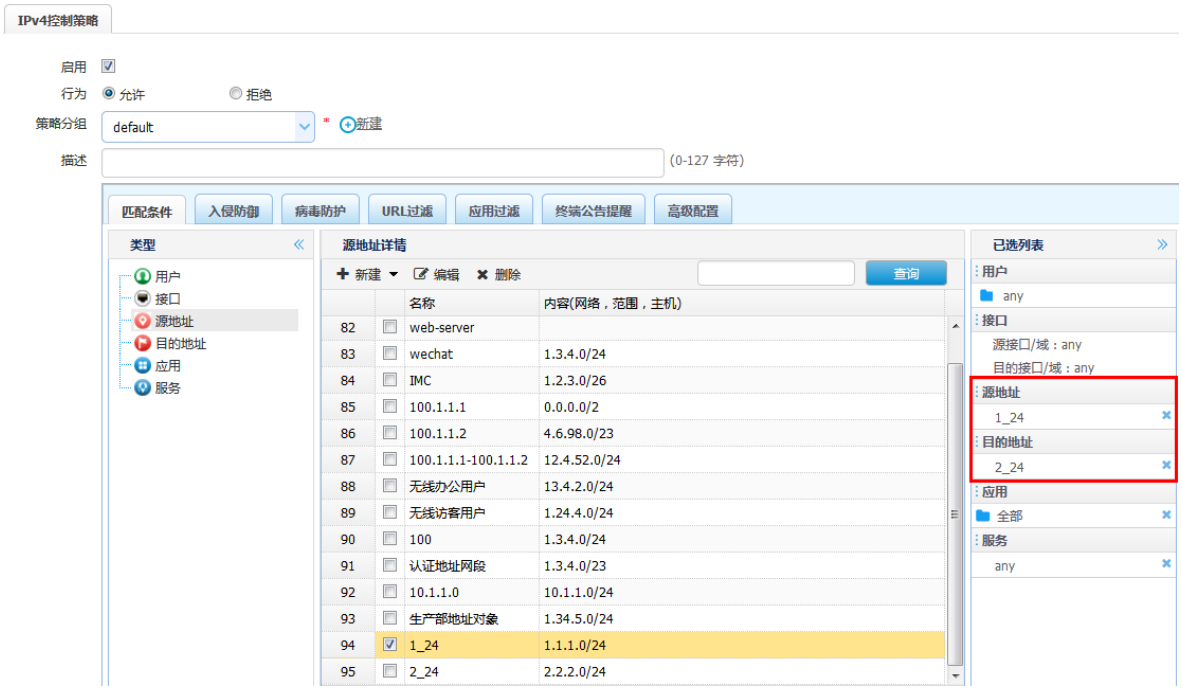
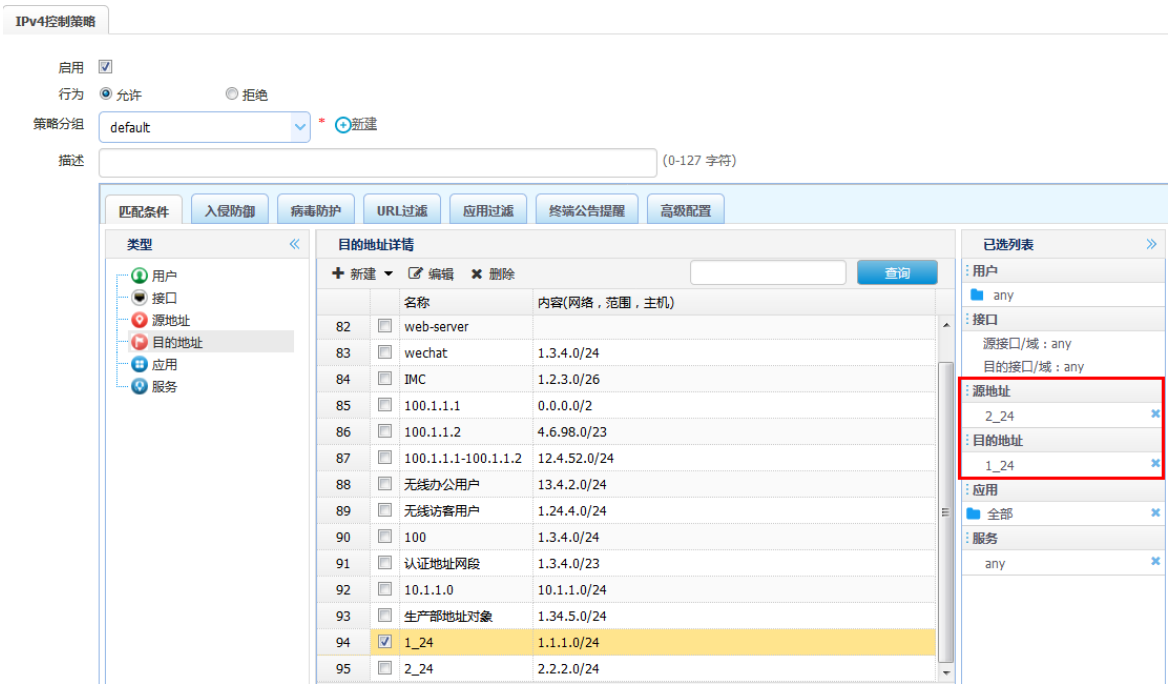


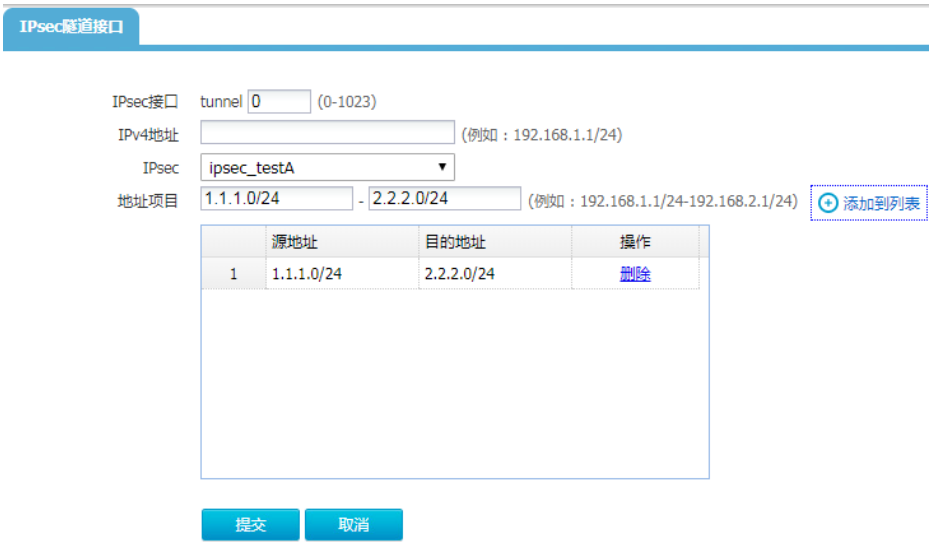
图8　设备 B 的 IPv4 控制策略配置信息配置如图 8 所示。



(5)　新建 IPSEC 隧道接口

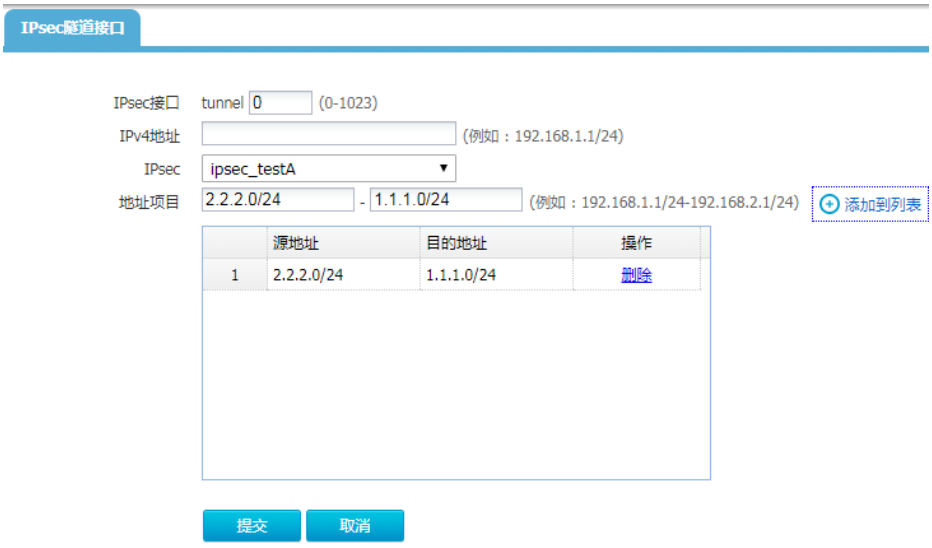
对设备 A 的隧道接口配置如图 9 所示。

图9 设备 A 的隧道接口配置



对设备 B 的隧道接口如图 10 所示。

图10 设备 B 的隧道接口配置



(6) 配置静态路由

需要将感兴趣流的路由指向 tunnel 口，配置如图 11 所示。

图11 设备 A 静态路由配置

图12 设备 B 静态路由配置

4.5 验证配置

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 第三方对接 > IPsec SA ”，查看 IPsec SA。

图13 设备 A 的 IPsec SA

IPsec 配置 | IPsec隧道接口 | IKE SA | IPsec SA

		名称	对端网关	本地网关	状态	过期时间/过期流	流量(入/出)	源网络	目的网络	操作
1		IPsec_test	192.168.1.63	192.168.1.61	连接	0s/0.0KB	0.00kb/0.00kb	1.1.1.0/24	2.2.2.0/24	

图14 设备 B 的 IPsec SA

IPsec 配置 | IPsec隧道接口 | IKE SA | IPsec SA

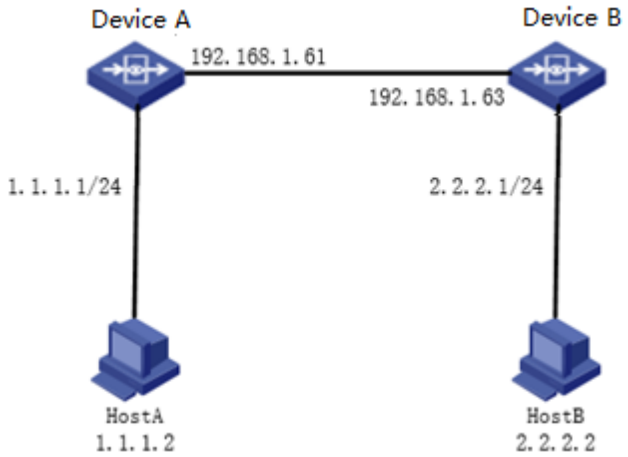
		名称	对端网关	本地网关	状态	过期时间/过期流:	流量(入/出)	源网络	目的网络	操作
1		IPsec_test	192.168.1.61	192.168.1.63	连接中	0s/0.0KB	0.00kb/0.00kb	1.1.1.0/24	2.2.2.0/24	

5 国密 IPsec 配置举例

5.1 组网需求

如图 15 所示，在设备 A 和设备 B 之间使用国密标准建立一个安全隧道，对 Host A 代表的子网（1.1.1.0/24）与 Host B 代表的子网（2.2.2.0/24）之间的数据流进行安全保护。

图15 IPsec 组网图



v

5.2 配置思路

(1) 按照组网图组网。

(2) 导入国密 CA 证书

(3) 导入国密用户证书

(4) 新建 IKE 协商

(5) 配置 IPsec 协商策略

(6) 新建所需地址对象

(7) 新建 IPsec 安全策略

(8) 新建 IPsec 隧道

(9) 配置静态路由

5.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

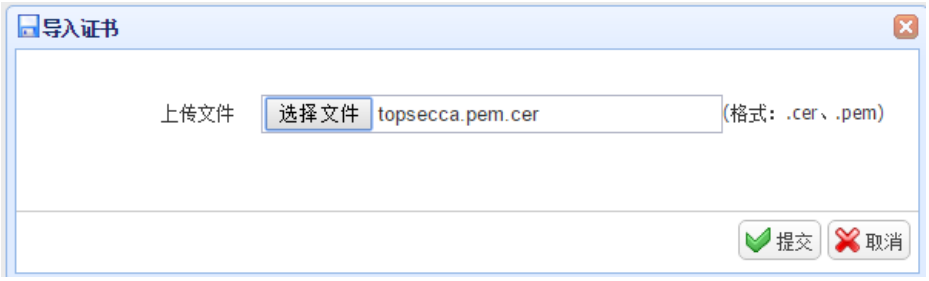
5.4 配置步骤

(1) 导入国密 CA 证书

注：国密证书需要向国密局申请，本案例中的国密证书是已申请下来的。

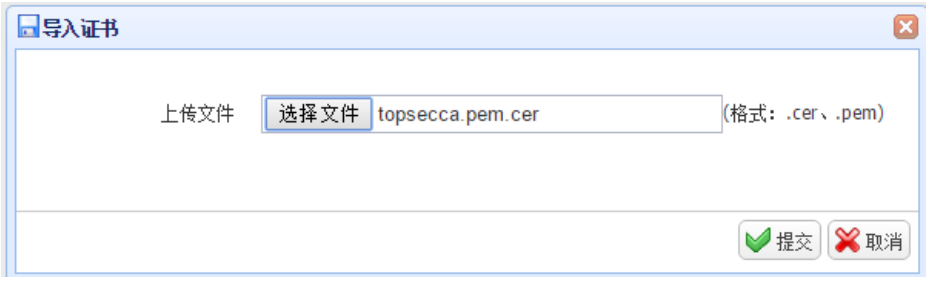
设备 A：进入策略配置>对象管理>本地证书>证书>CA，点击导入。配置如图 16 所示。

图16 设备 A 导入国密 CA 证书



设备 B：进入策略配置>对象管理>本地证书>证书>CA，点击导入。配置如图 17 所示。

图17 设备 B 导入国密 CA 证书



(2) 导入国密用户证书

设备 A：进入策略配置>对象管理>本地证书>证书>国密，点击导入。上传证书类型选择证书秘钥分离。配置如图 18 所示。

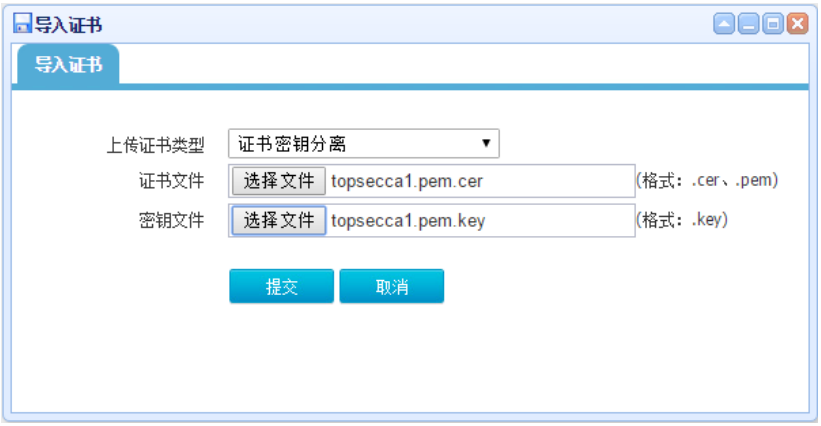
图18 设备 A 导入本端国密用户证书

图19 设备 A 导入对端国密用户证书

设备 B：进入策略配置>对象管理>本地证书>证书>国密，点击导入。上传证书类型选择证书秘钥分离。配置如图 20 所示。

图20 设备 B 导入本端国密用户证书

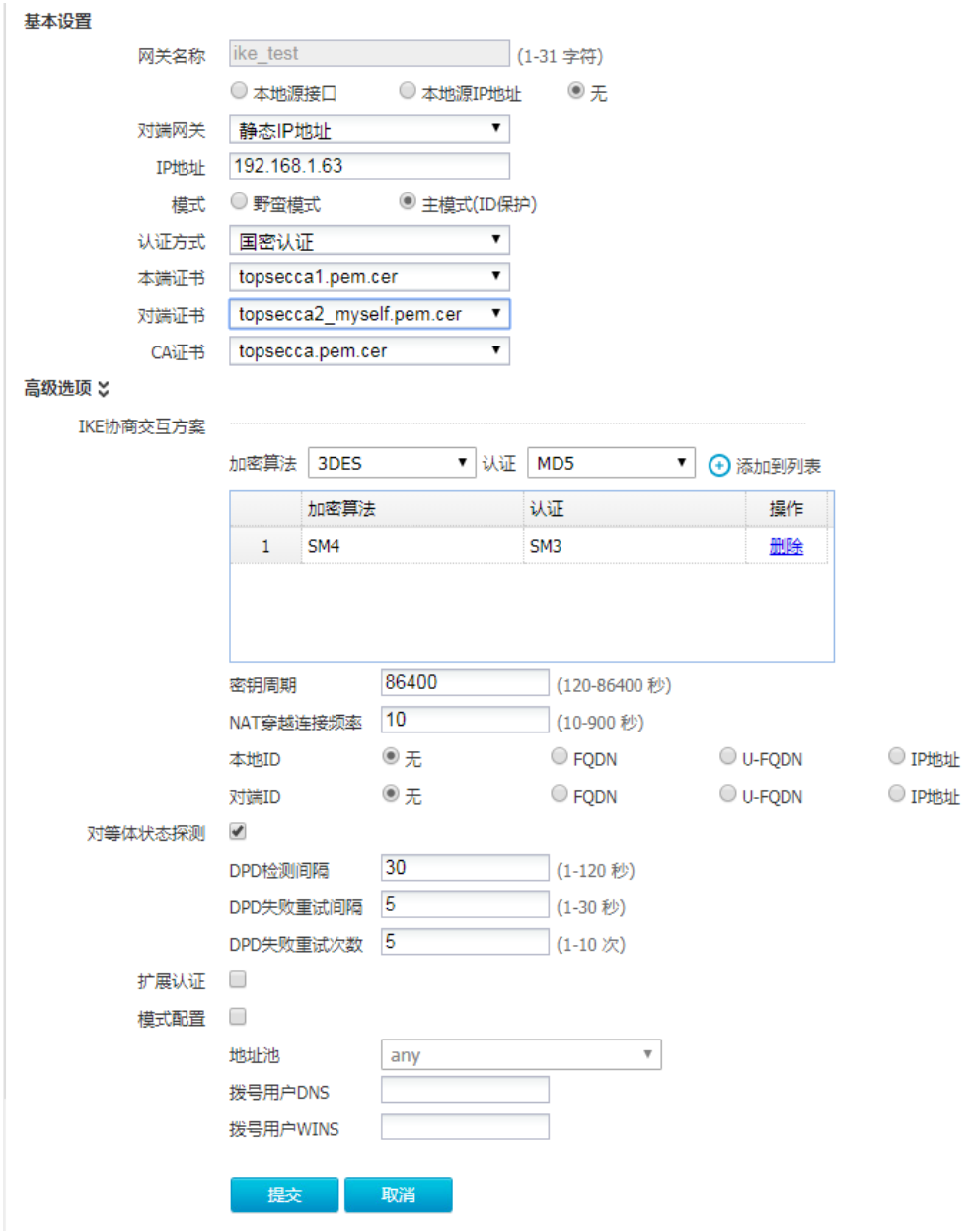
图21 设备 B 导入对端国密用户证书



(3) 新建 IKE 协商：在导航栏中选择“网络配置>VPN>IPsec-VPN>IPsec 第三方对接”，进入 IPsec 的显示页面，新建 IKE

对设备 A 的 IKE 配置如图 22 所示。

图22 设备 A 的 IKE 配置



注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

对设备 B 的 IKE 配置如图 23 所示。

图23 设备 B 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

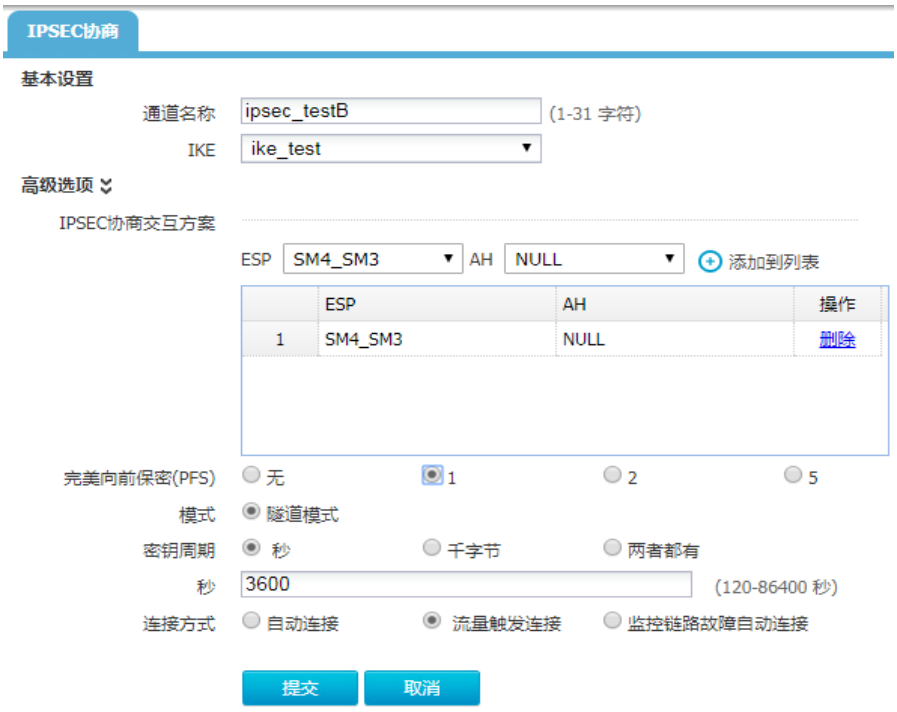
(4) 配置 IPsec 协商策略：在导航栏中选择“网络配置 > VPN > IPsec-VPN > Ipsec 第三方对接”，进入 IPsec 协商策略的显示页面，选择要创建 IPsec 的 IKE，然后单击<新建 IPsec>，或者点击对应 IPsec 的右侧<编辑>按钮，进入 IPsec 协商策略的配置页面。

对设备设备 A 的 IPsec 协商策略配置如图 24 所示。

图24 设备 A 的 IPsec 协商策略配置

对设备 B 的 IPsec 协商策略配置如图 25 所示。

图25 设备 B 的 IPsec 协商策略配置



(5) 新建所需地址对象配置如下图 26 所示。

图26 地址对象配置

		名称	内容(网络，范围，主机)	排除地址	描述	引用	操作
1		any	0.0.0.0/0		任何地址	8	
2		private	10.0.0.0/8,172.16.0.0/12,192.168.0.0/16		私有地址	1	
3		ChinaUnicom	1.2.2.0/24,1.4.4.0/24,1.8.0.0/16,...		中国联通	0	
4		ChinaTelecom	1.0.1.0/24,1.0.2.0/23,1.0.8.0/21,...		中国电信	0	
5		ChinaEducation	1.51.0.0/20,1.51.16.0/20,1.51.128.0/20,..		教育网	0	
6		ChinaMobile	36.128.0.0/12,36.144.0.0/14,36.148.0.0/		中国移动	0	
7	☐	认证用户	172.16.11.0/24			0	
8	☐	SRC1	192.168.1.0/24			0	
9	☐	SRC2	192.168.2.0/24			0	
10	☐	1_24	1.1.1.0/24			0	
11	☐	2_24	2.2.2.0/24			0	

(6) 新建 IPSec 的 IPv4 控制策略，配置如图 27 所示。

图27 设备 A 的配置信息

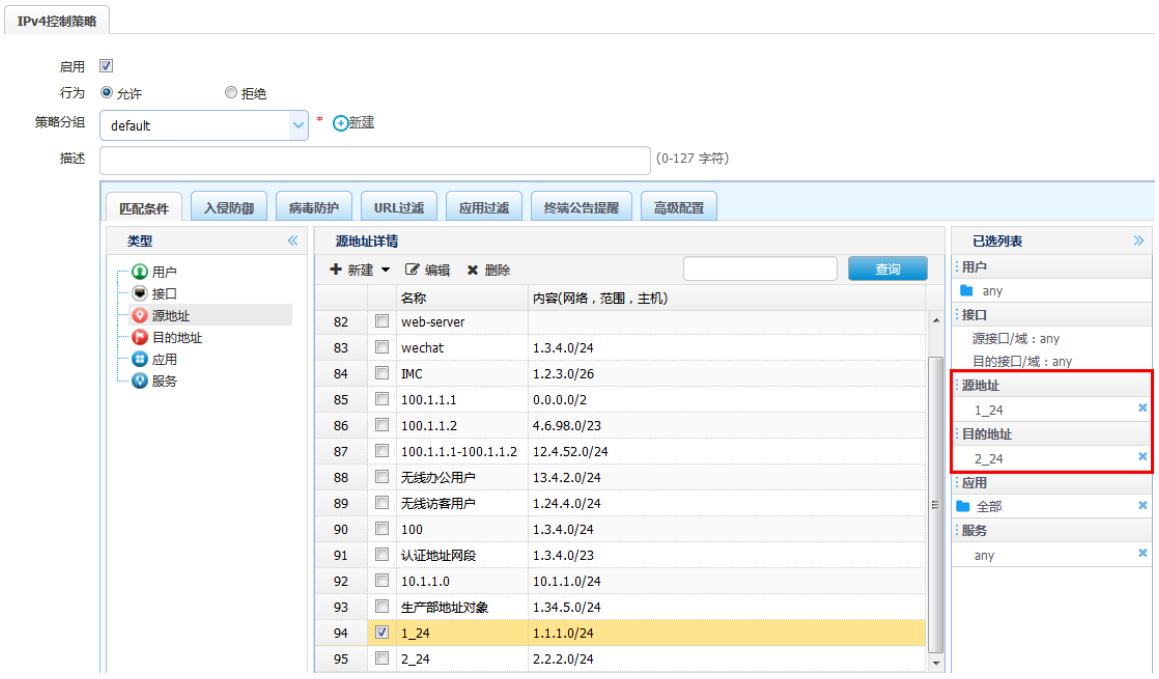
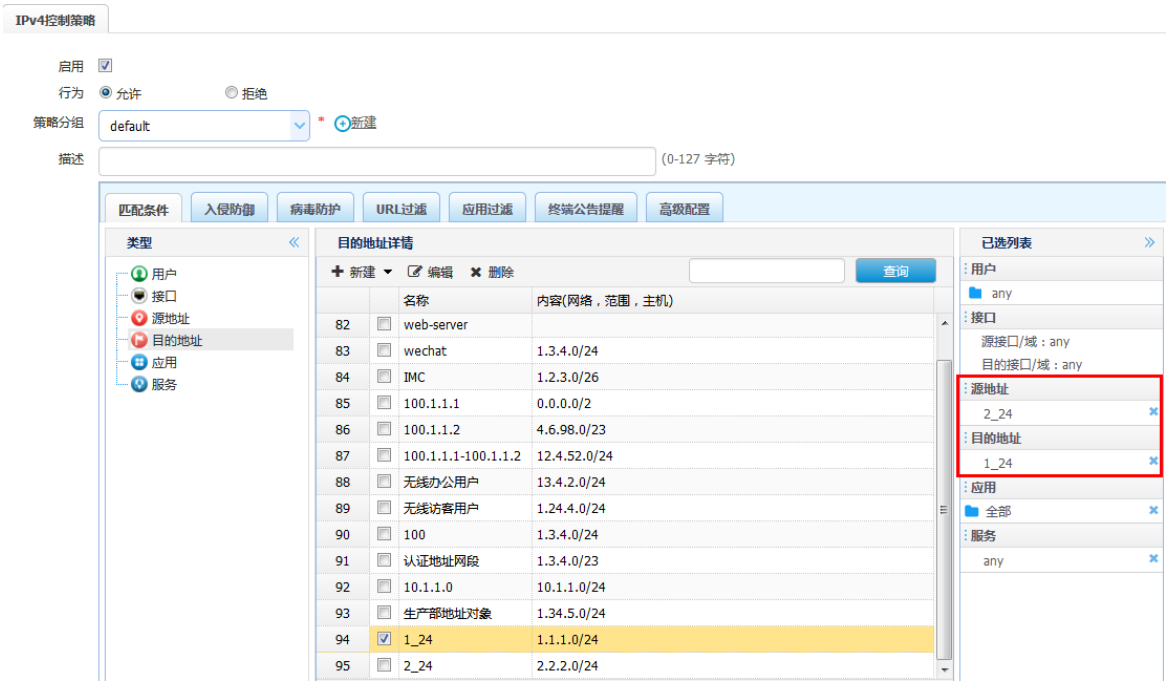


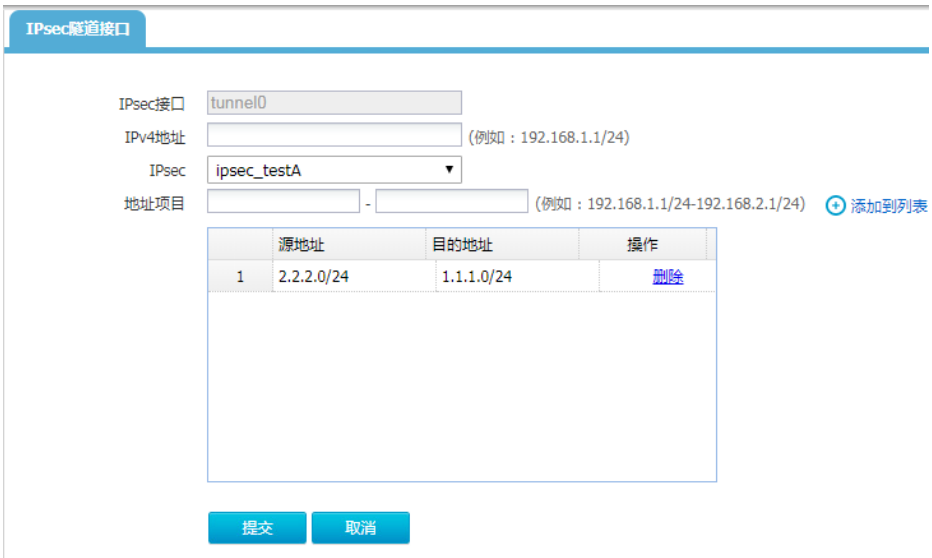
图28 设备 B 的配置信息



(7) 新建 IPSEC 隧道接口配置。

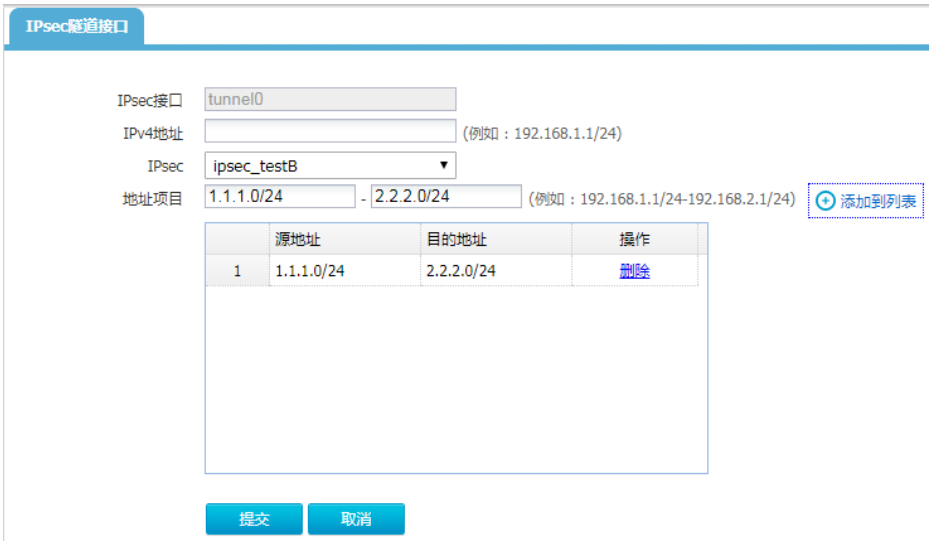
对设备 A 的隧道接口如图 29 所示。

图29 设备 A 的隧道接口配置



对设备 B 的隧道接口如下图 30 所示。

图30 设备 B 的隧道接口配置



(8) 配置静态路由

需要将感兴趣流的路由指向 tunnel 口。

图31 设备 A 静态路由配置

出接口配置方式：

图32 设备 B 静态路由配置

出接口配置方式：

5.4.2 验证配置结果

在导航栏中选择“网络配置 > VPN > IPsec-VPN > IPsec 第三方对接 > IPsec SA”，查看 IPsec SA。

图33 设备 A 的 IPsec SA

图34 设备 B 的 IPsec SA

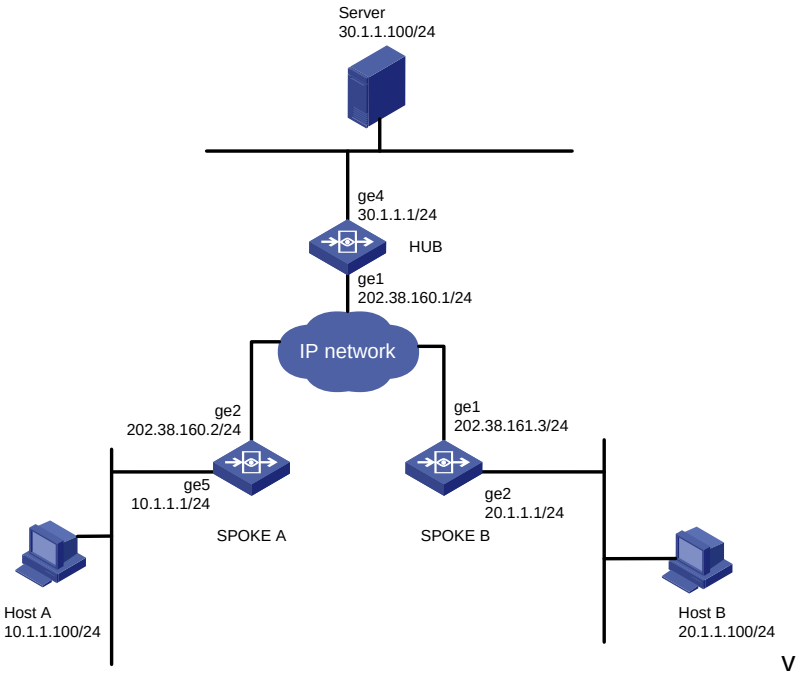
6 HuB-Spoke 组网 IPsec 配置举例

6.1 组网需求

如图 35 所示，公司总部需要与两个分支建立 IPsec，保证分支可以和总部内网互通，并且在设备 A 和设备 B 之间通过总部的 IPsec 也可以互通。总部公网 IP 为固定地址（202.38.160.1），两分支出

口 IP 为动态地址.需要对总部 Sever 子网（30.1.1.1/24）,分支 Host A 的子网（10.1.1.1/24）与分支 Host B 的子网（20.1.1.0/24）之间的数据流进行安全保护。

图35 IPsec 组网图



6.2 配置思路

(1) 按照组网图组网。

(2) 配置路由模式以及接口，使设备可以访问外网；

(3) 配置 IKE；

(4) 配置 IPsec；

(5) 配置地址对象

(6) 配置 Tunnel 口；

(7) 配置路由使 Tunnel 口互通；

(8) 配置安全策略；

(9) 查看 IPSEC SA 是否协商成功。

6.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

6.4 配置步骤

(1) 配置路由模式，使 3 台设备能够访问外网（基本访问外网的配置不再截图）。

(2) 配置 IKE

配置 HUB 的 IKE，进入网络配置>VPN>IPsec-VPN>Ipsec 第三方对接，点击新建，选择新建 IKE。配置如图 36 所示。

图36 HUB-Spoke 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

配置 SPOKE A 的 IKE，进入网络配置>VPN>IPsec-VPN>Ipsec 第三方对接，点击新建，选择新建 IKE。如下图 37 所示。

图37 SPOKE A 的 IKE 配置

注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

在 SPOKE_B 上配置与 SPOKE_A 协商参数一致的 IKE，对端网关配置静态 IP 地址：202.38.160.1。

(3) 配置 IPsec 协商策略

配置 HUB 的 IPSec，进入网络配置>VPN>IPsec-VPN>Ipsec 第三方对接，点击新建，选择新建 IPsec 协商策略配置如图 38 所示。

图38 HUB 的 IPSec 协商策略配置

配置 SPOKE A 的 IPSec，进入网络配置>VPN>IPsec-VPN>Ipsec 第三方对接，点击新建，选择新建 IPsec。配置如图 39 所示。

图39 SPOKE A 的 IPSec 协商策略配置

在 SPOKE B 上配置与设备 A 协商参数一致的 IPSec(分支端的 ipsec 配置自动连接，中心端的不配置自动连接)。

(4)　新建所需地址对象配置如下图 40 所示。

图40 设备地址对象配置

在 Spoke A、Spoke B 上也配置同样的地址对象。

(5) HUB 上配置安全策略，进入策略配置>IPv4 控制策略，将默认规则设置为允许。配置如图 41 所示。

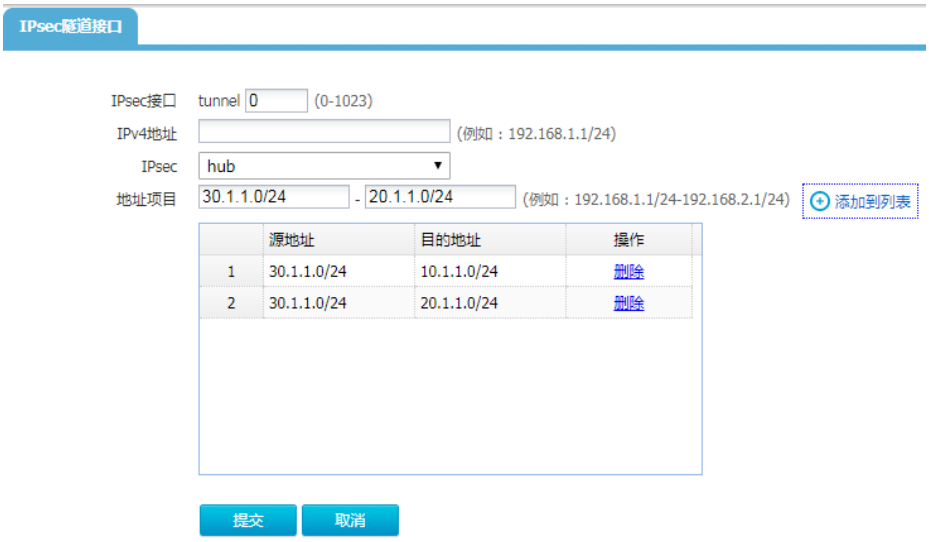
图41 设备 A 的配置信息

Spoke A、Spoke B 上配置相同的全通策略。

(6) 新建 IPSEC 隧道接口

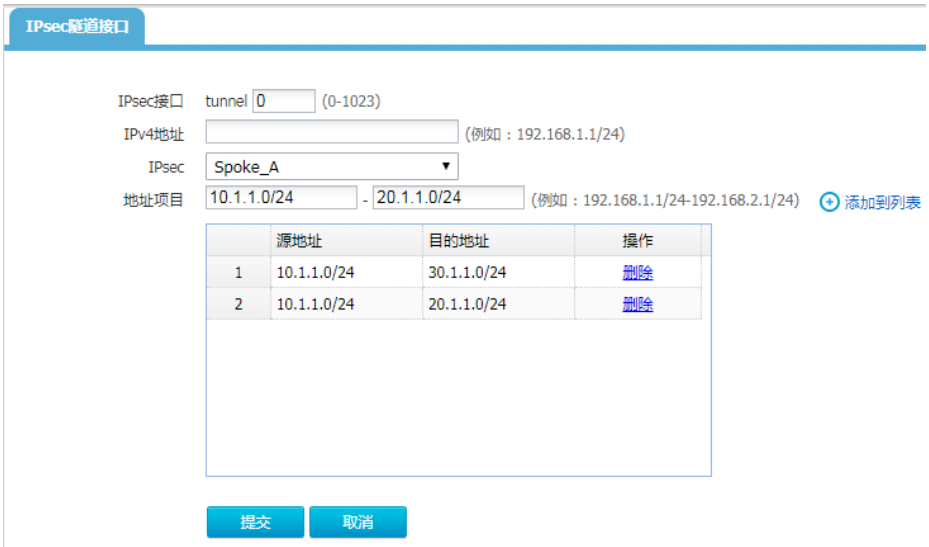
配置 HUB 的 Tunnel 口，进入网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 隧道接口，点击新建。配置如图 42 所示。

图42 HUB 的 Tunnel 口配置



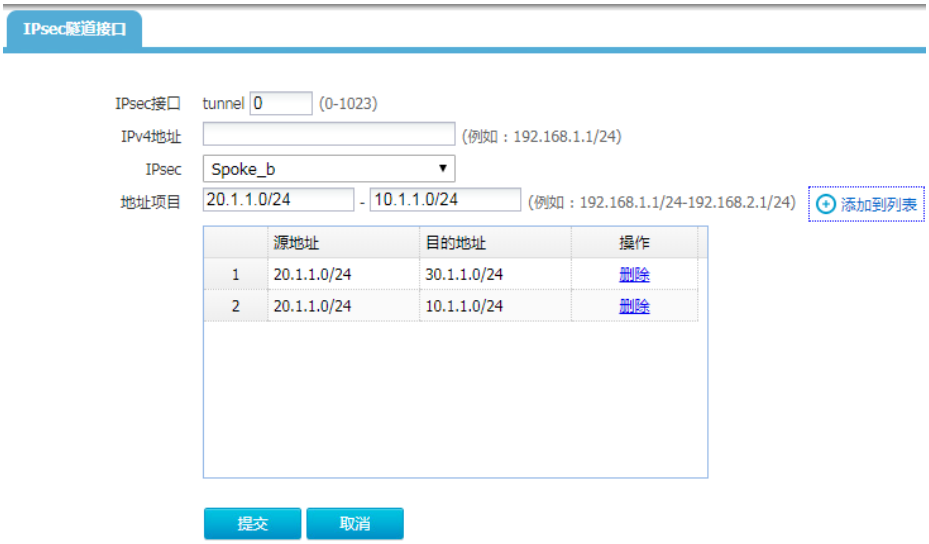
配置 Spoke A 的 Tunnel 口，进入网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 隧道接口，点击新建。如下图 43 所示。

图43 Spoke A 的 Tunnel 口配置



配置 Spoke B 的 Tunnel 口，进入网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 隧道接口，点击新建。如图 44 所示。

图44 SpokeB 的 Tunnel 口配置



(7) 配置路由使 Tunnel 口互通

配置 hub 为路由模式，进入网络配置>路由管理>静态路由，点击新建。配置如图 45 所示。

图45 hub 静态路由配置

配置 Spoke_A 为路由模式，进入网络配置>路由管理>静态路由，点击新建。配置如图 46 所示。

图46 Spoke_A 路由配置。

配置 Spoke_B 为路由模式，进入网络配置>路由管理>静态路由，点击新建。配置如图 47 所示。

图47 Spoke_B 路由配置

(8) 查看 IPSec 是否协商成功

HUB：进入“网络配置>VPN>IPsec-VPN>IPSEC 第三方对接”，查看 IKE SA 和 IPsec SA 如图 48 所示。

图48 Spoke 设备 SA 状态

Spoke A：进入“网络配置>VPN>IPsec-VPN>IPSEC 第三方对接”，如图 49 所示。

图49 Spoke A 设备 SA 状态

Spoke B：进入“网络配置>VPN>IPsec-VPN>IPSEC 第三方对接”，如图 50 所示。

图50 Spoke B 设备 SA 状态

6.4.2 验证配置结果

PC 访问 Server：Host A ping Host BPsec SA。

图51 设备 A 的 IPsec SA

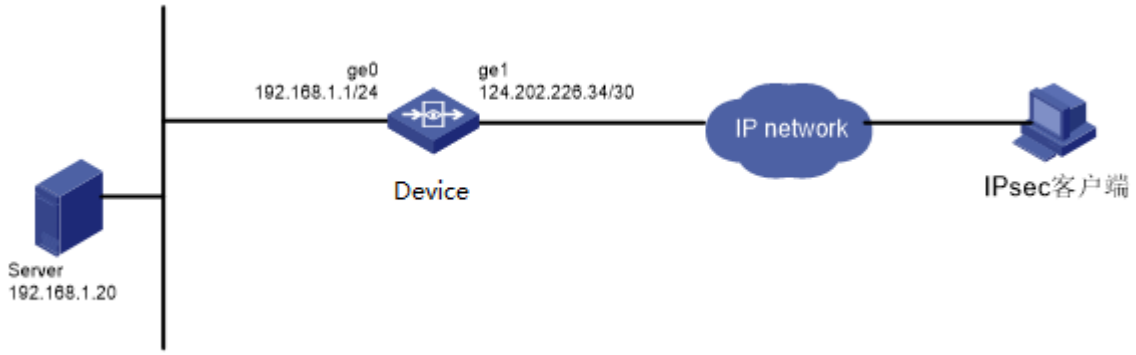
```
HOST# dis ip connection protocol icmp ip source any dest any app-name any
Protocol:ICMP State:Complete        PolicyID:-            VrfId:0
              UserName: 10.1.1.100                  AppName: ICMP
              Expire: 00:00:03                      Existed: 00:00:24
              Source Dir: 10.1.1.100:8          >   20.1.1.100:0
              Reply  Dir: 20.1.1.100:0          >   10.1.1.100:0

HOST# dis ip connection protocol tcp ip source 10.1.1.100 dest any app-name any
Protocol:TCP  State:Complete        PolicyID:-            VrfId:0
              UserName: 10.1.1.100                  AppName: FTP
              Expire: 00:59:32                      Existed: 00:00:32
              Source Dir: 10.1.1.100:3417       >   30.1.1.100:21
              Reply  Dir: 30.1.1.100:21         >   10.1.1.100:3417
```

7 客户端接入 IPsec 配置举例

7.1 组网需求

如图 52 所示，由于公司业务扩大，在外办公人员较多，为了方便在外人员能够及时的访问到公司内部资料。在公司出口搭建 remote IPsec 建立一个安全隧道，对 IPsec 客户端的子网（172.16.190.1/24）与 Server 的子网（192.168.1.0/24）之间的数据流进行安全保护。

图52 IPsec 组网图



7.2 配置思路

按照组网图组网。配置接口 ip，路由以及 NAT，使内网 pc 可以访问外网（基本配置不再赘述）。

(1) 配置 IPsec IKE

(2) 配置 IPSec VPN

(3) 配置本地用户

(4) 配置 IPSec 隧道接口

(5) 配置路由

(6) 配置策略

(7) 配置客户端

7.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

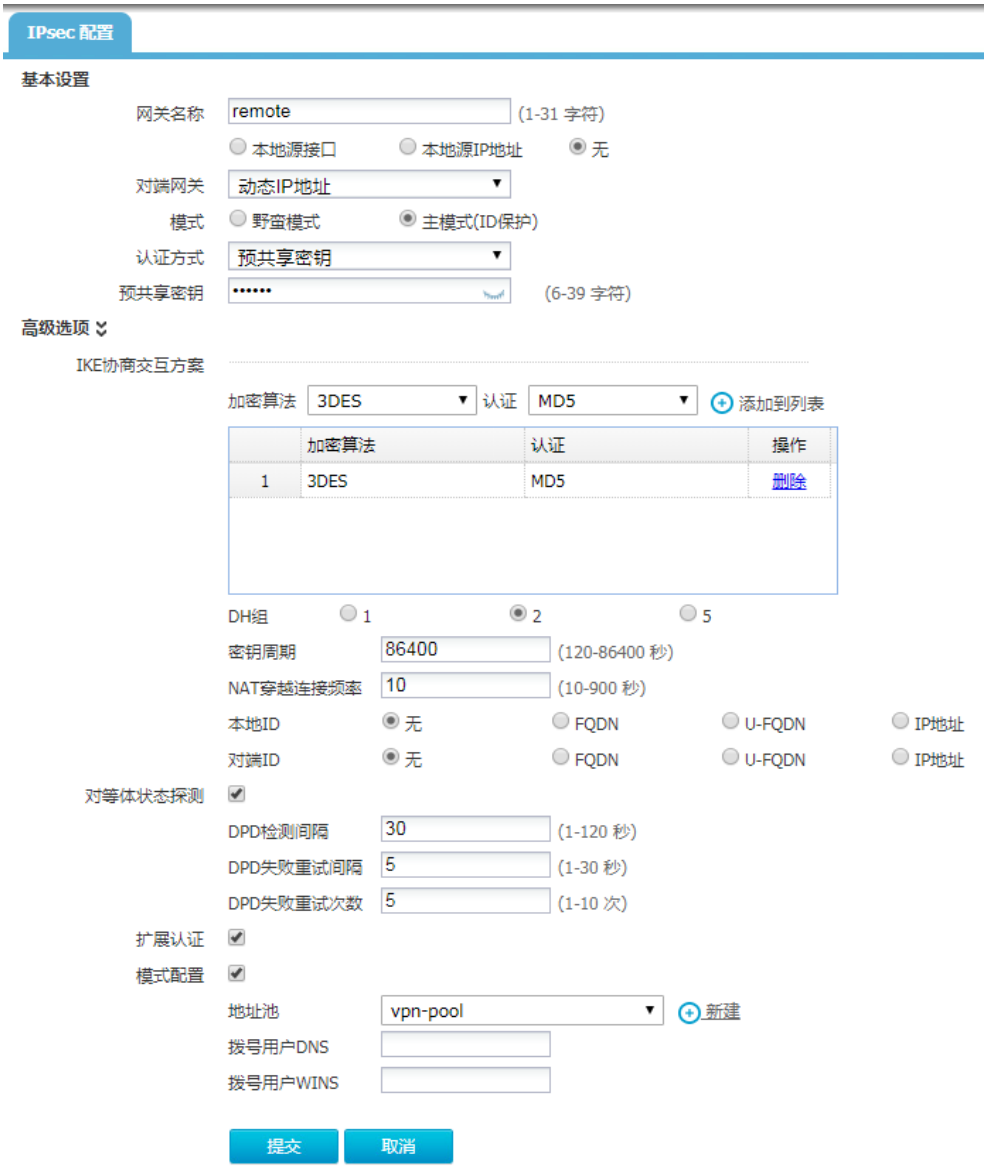
7.4 配置步骤

7.4.1 配置设备

(1) 新建 IKE 协商：进入网络配置>VPN>IPsec-VPN>IPsec 第三方对接>IPsec 配置，点击新建，选择新建 IKE。

对设备 A 的 IKE 配置如图 53 示。

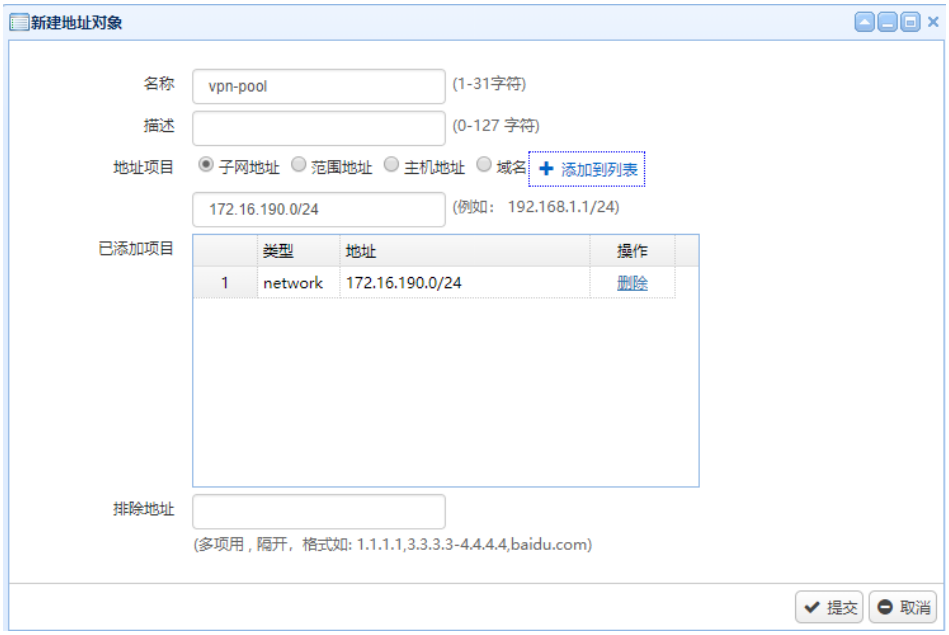
图53 设备 A 的 IKE 配置



注意：如果本端有多个出口可以到达对端，则必须指定本地源 IP 或本地源接口。

地址池，点击新建，配置分配给客户端的子网。配置如图 54 所示。

图54 Remote vpn 地址池配置



(2) 配置 IPsec 协商策略

对设备 A 的 IPsec 协商策略配置如下图 55 所示。

图55 设备 A 的 IPsec 协商策略配置

(3) 配置本地用户

进入用户管理>用户组织结构，点击新建用户。密码为 123456。配置如图 56 所示。

图56 新建本地用户配置

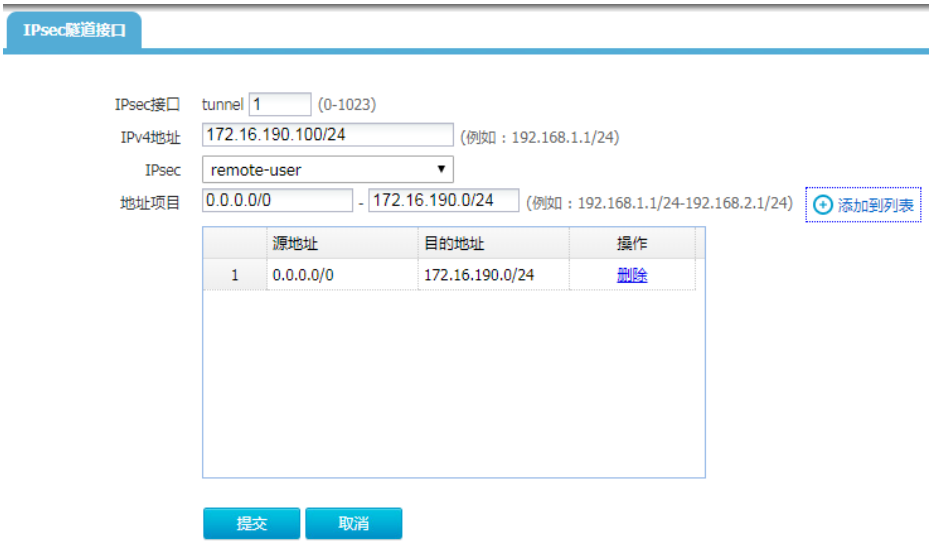
(4) 进入策略配置>IPv4 控制策略，将默认规则修改为允许，配置如图 57 所示。

图57 设备 A 的配置信息

(5) 新建 IPSEC 隧道接口

进入网络配置>VPN>IPsec-VPN>Ipsec 第三方对接>IPSec 隧道接口，点击新建。配置如图 58 所示。

图58 隧道接口配置



(6) 配置静态路由

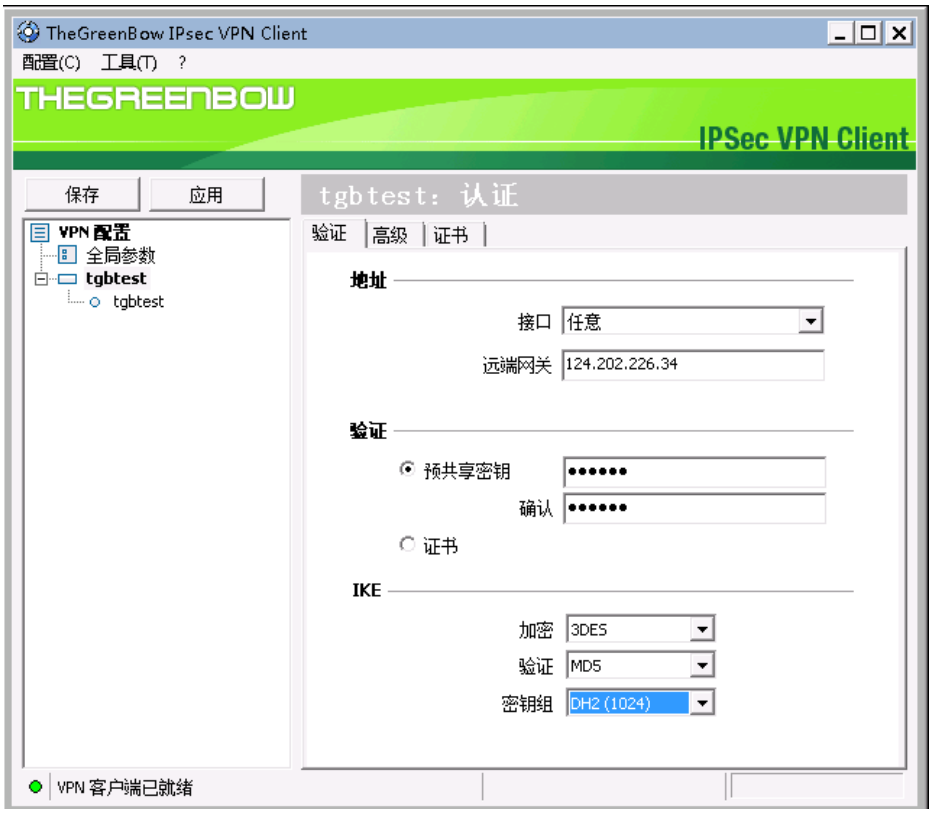
进入网络配置>路由管理>静态路由，点击新建。配置如图 59 所示。

图59 静态路由配置

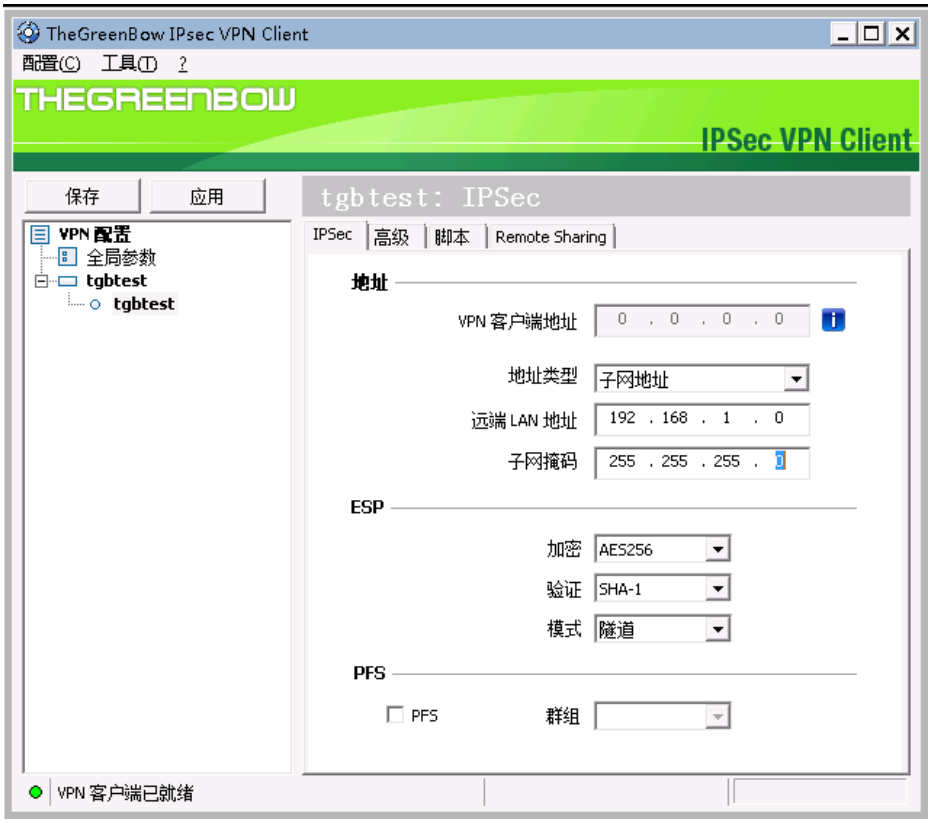
(7) PC 客户端配置（vpn 客户端使用的开源 TheGreenBow IPsec VPN Client）

PC 安装好 IPSec VPN 客户端，新建一条隧道，网关 ip 地址为 124.202.226.34，远端子网配置想要访问的子网（设置为 192.168.1.0/24），认证方式：与共享密钥；密钥：123456，选择扩展认证，点设置，用户名为 test，密码默认为 123456。配置如图 60 所示。

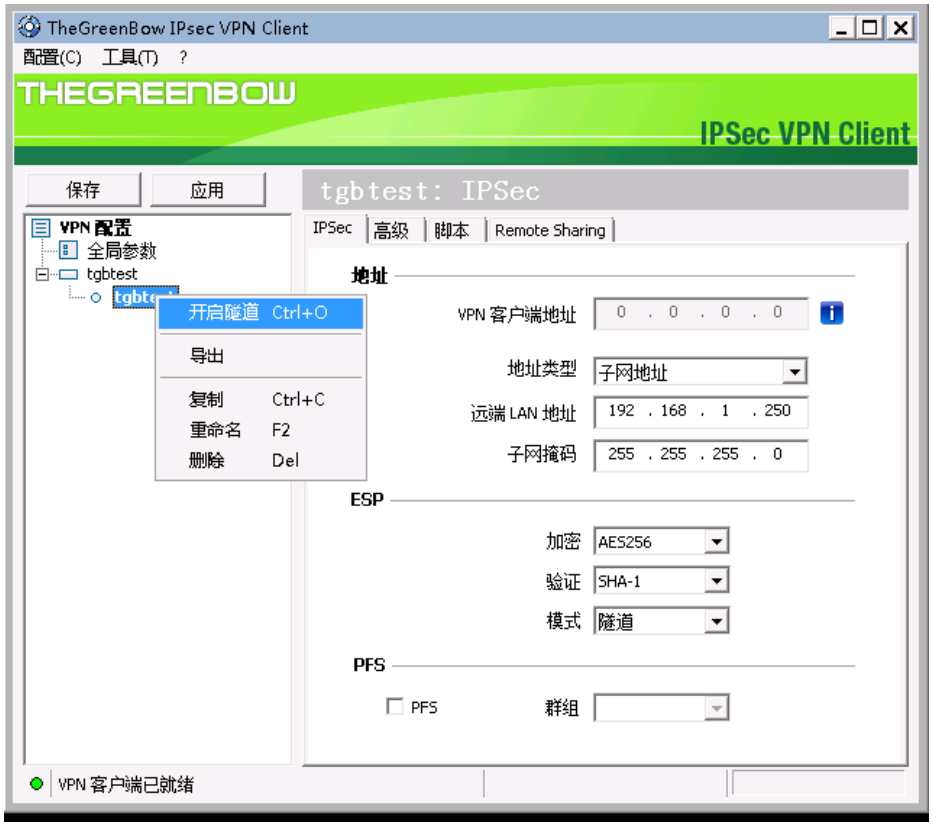
图60 TheGreenBow IPsec VPN Client 配置

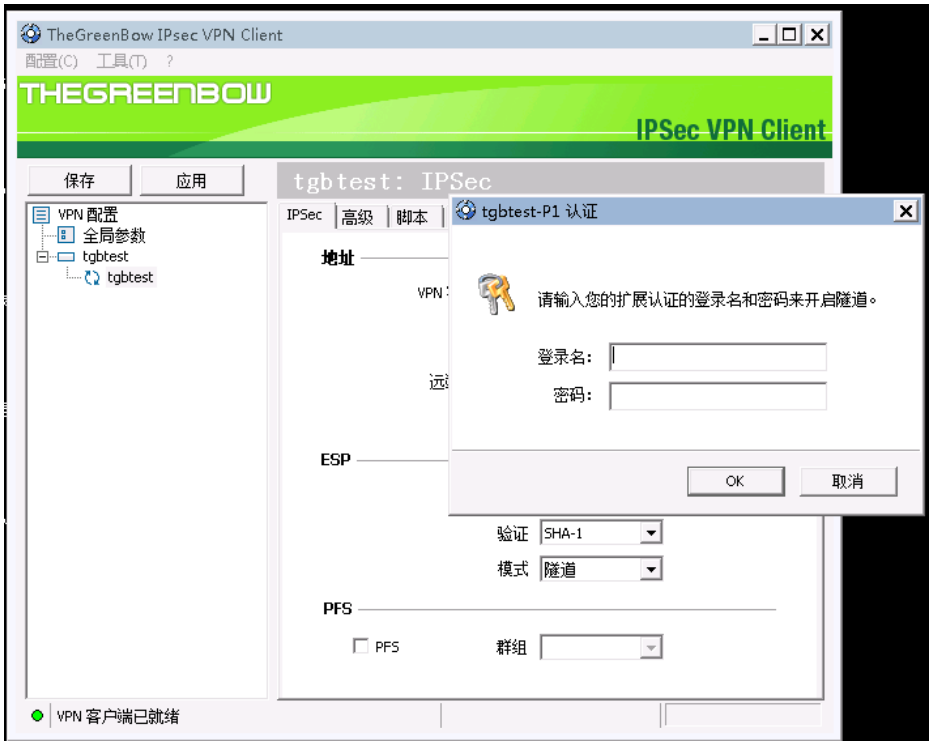


点高级，网关 VPN 的协商模式为主模式，具体参数与网关 IPSec VPN 的参数一致。



提交后，在二阶段 tgbtest 鼠标右键开启隧道出现认证页面输入用户名密码点击 ok，详见下图。


TheGreenBow IPsec VPN Client
配置(C) 工具(T) ?
THEGREENBOW
IPSec VPN Client
保存
应用
tgbtest: IPSec
VPN 配置
全局参数
tgbtest
tgbtest
开启隧道 Ctrl+O
导出
复制 Ctrl+C
重命名 F2
删除 Del
IPSec
高级
脚本
Remote Sharing
地址
VPN 客户端地址
0 . 0 . 0 . 0
地址类型
子网地址
远端 LAN 地址
192 . 168 . 1 . 250
子网掩码
255 . 255 . 255 . 0
ESP
加密
AES256
验证
SHA-1
模式
隧道
PFS
PFS
群组
VPN 客户端已就绪


TheGreenBow IPsec VPN Client
配置(C) 工具(T) ?
THEGREENBOW
IPSec VPN Client
保存
应用
tgbtest: IPSec
VPN 配置
全局参数
tgbtest
tgbtest
IPSec
高级
脚本
tgbtest-P1 认证
请输入您的扩展认证的登录名和密码来开启隧道。
登录名:
密码:
OK
取消
地址
ESP
验证
SHA-1
模式
隧道
PFS
PFS
群组
VPN 客户端已就绪


tgbtest
隧道已开启。

7.5 验证配置

连接成功后，分配的 ip 地址为 172.16.190.0/24，pc 可以访问公司 server。

目 录

1 简介

许多大中型企业在全国各地都建有分支机构或者办事处，一般在企业总部会部署如 OA 系统、ERP 系统等应用软件，将企业分布在各地的分支机构和办事处与企业总部互联，达到安全地共享数据和软件资源的目的，我们使用 SSLVPN 功能提供远程安全接入，解决其所面临的远程接入、传输保密、用户认证、网络安全防护、访问控制等问题。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 SSL VPN 特性。

3 使用限制

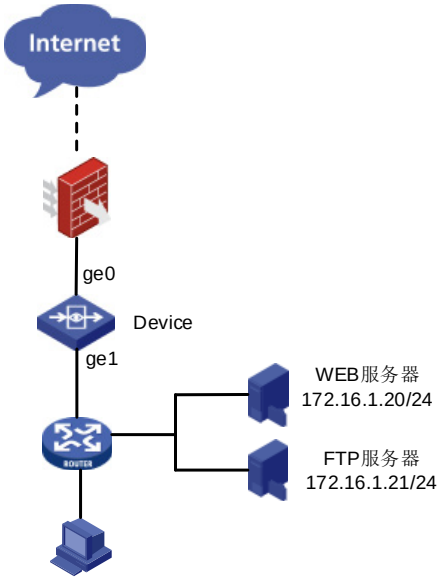
- 第三方用户必须同步到本地，不支持第三方非同步用户登录。
- 不支持苹果 mac 和 ios 系统。

4 配置举例

4.1 组网需求

如图 1 所示，使用设备的 ge0 和 ge1 接口以路由方式部署在网络中。用户希望设备提供 SSL VPN 服务，以供互联网用户通过 SSL VPN 访问内网的 Web 和 FTP 服务器。

图1 SSL VPN 功能配置组网图



4.2 配置思路

(1) 按照组网图组网。
(2) 配置接口。
(3) 配置静态路由。
(4) 配置用户。
(5) 配置 SSL VPN 全局配置。
(6) 配置 SSL VPN 资源。
(7) 配置 SSL VPN 策略

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

1. 配置接口

如图 2 所示，进入“网络配置>接口配置>物理接口”页面，点击“编辑”按钮为 ge0 接口配置 ip 地址，并点击<提交>。

图2 配置接口

2. 配置静态路由

如图 3 所示，进入“网络配置>路由管理>静态路由”页面，点击<新建>按钮，配置一条静态路由：目的网段为服务器的网段：172.16.1.1/24，下一跳为 ge1 对端互联接口地址。

图3 配置静态路由

3. 配置用户

如图 44 所示，进入“用户管理> 用户组织结构>用户”页面，点击<新建>按钮，新建用户“sslvpntest”，并点击<提交>。

图4 配置用户

4. 配置 SSL VPN 全局配置

如图 55 所示，进入“网络配置>VPN>SSL VPN>全局配置”页面，进行 SSL VPN 全局配置，并点击<提交>。

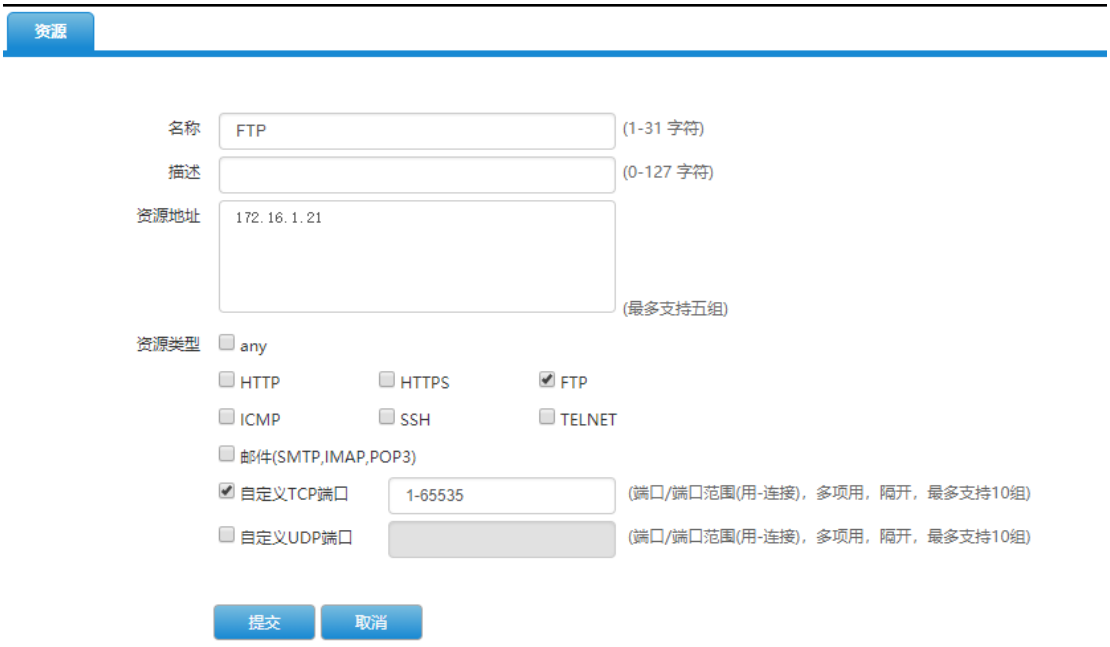
图5 配置全局配置

5. 配置 SSL VPN 资源

如图 66 和图 77 所示，进入“网络配置>VPN>SSL VPN>资源”页面，点击“新建”按钮，进行 SSL VPN 的 web 和 ftp 资源配置，并点击<提交>。

图6 配置 HTTP 资源

图7 配置 ftp 资源



6. 配置 SSL VPN 策略

如图 88 所示，进入“网络配置>VPN>SSL VPN>策略”页面，点击<新建>按钮，进行 sslvpn 的策略配置，并点击<提交>。

图8 策略配置

7. 配置 SSL VPN 在线用户与 IP 绑定

如果选择为 SSL VPN 分配静态 IP，如图 9 所示，进入“网络管理>VPN>SSL VPN>全局配置”页面，点击<全局配置>按钮，取消勾选<登录设定>中“允许多处登录”。

图9 用户 IP 绑定全局设置图

如图 10 所示，进入“网络管理>VPN>SSL VPN>IP 用户绑定”页面，点击<新建>按钮，勾选<启用>，选择绑定用户，输入 SSL VPN 分配地址池中的 IP 地址，设置完毕后，客户端登录 SSL VPN 后，分配 IP 地址为绑定地址。

图10 IP 用户绑定图

4.5 验证配置

(1) 查看 SSL VPN 在线用户

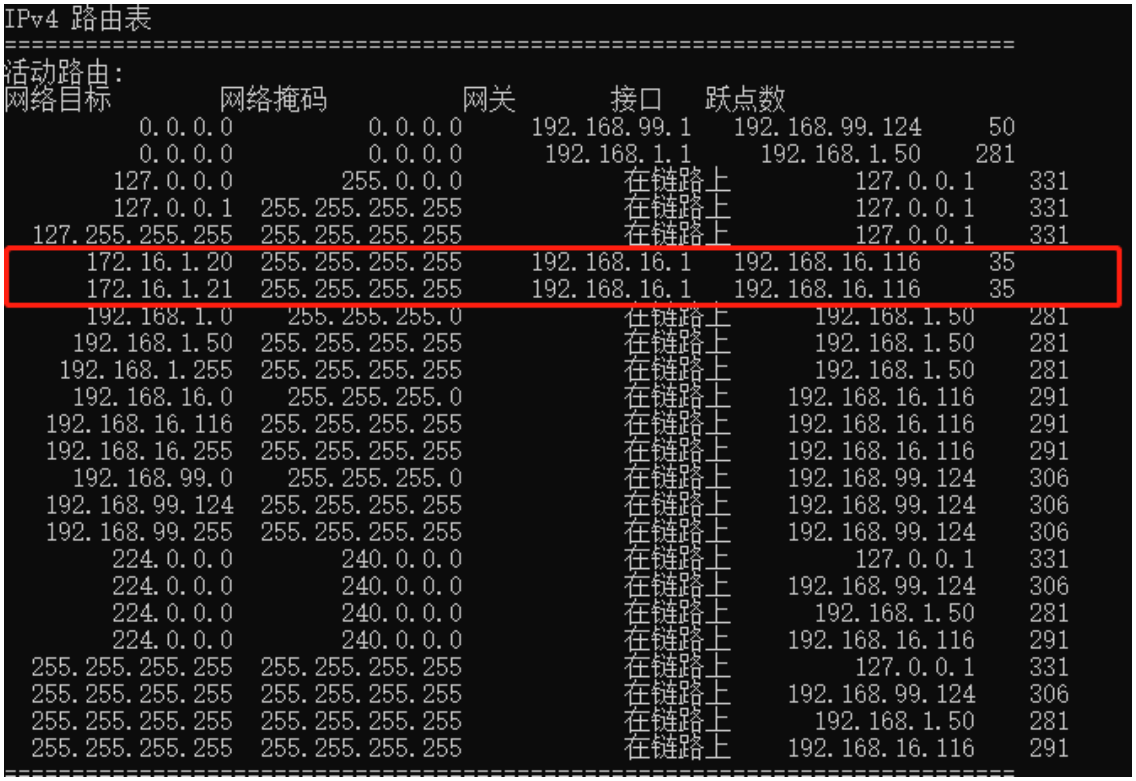
如图 1111 所示，SSL VPN 连接成功后，进入“数据中心>系统监控>SSL VPN 在线用户”页面，查看在线用户。

图11 SSL VPN 在线用户

(2) 查看客户端路由表

如图 122 所示，SSL VPN 连接成功后，查看客户端的路由表，下发了两条路由。

图12 客户端路由表



IPv4 路由表

活动路由：

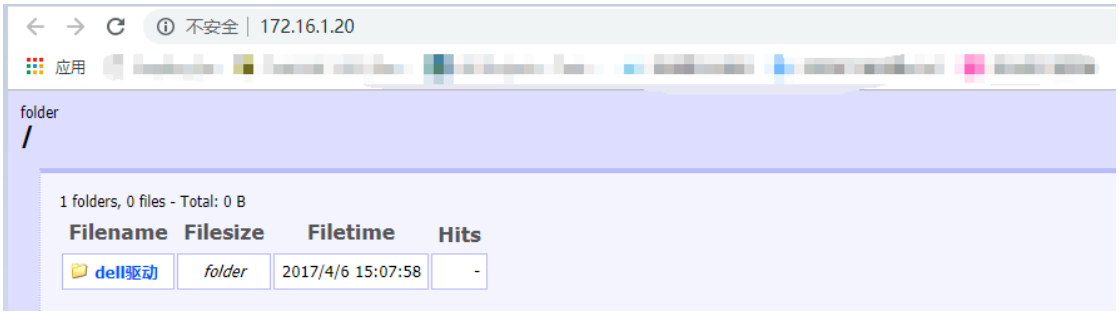
网络目标	网络掩码	网关	接口	跃点数
0.0.0.0	0.0.0.0	192.168.99.1	192.168.99.124	50
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.50	281
127.0.0.0	255.0.0.0	在链路上	127.0.0.1	331
127.0.0.1	255.255.255.255	在链路上	127.0.0.1	331
127.255.255.255	255.255.255.255	在链路上	127.0.0.1	331
172.16.1.20	255.255.255.255	192.168.16.1	192.168.16.116	35
172.16.1.21	255.255.255.255	192.168.16.1	192.168.16.116	35
192.168.1.0	255.255.255.0	在链路上	192.168.1.50	281
192.168.1.50	255.255.255.255	在链路上	192.168.1.50	281
192.168.1.255	255.255.255.255	在链路上	192.168.1.50	281
192.168.16.0	255.255.255.0	在链路上	192.168.16.116	291
192.168.16.116	255.255.255.255	在链路上	192.168.16.116	291
192.168.16.255	255.255.255.255	在链路上	192.168.16.116	291
192.168.99.0	255.255.255.0	在链路上	192.168.99.124	306
192.168.99.124	255.255.255.255	在链路上	192.168.99.124	306
192.168.99.255	255.255.255.255	在链路上	192.168.99.124	306
224.0.0.0	240.0.0.0	在链路上	127.0.0.1	331
224.0.0.0	240.0.0.0	在链路上	192.168.99.124	306
224.0.0.0	240.0.0.0	在链路上	192.168.1.50	281
224.0.0.0	240.0.0.0	在链路上	192.168.16.116	291
255.255.255.255	255.255.255.255	在链路上	127.0.0.1	331
255.255.255.255	255.255.255.255	在链路上	192.168.99.124	306
255.255.255.255	255.255.255.255	在链路上	192.168.1.50	281
255.255.255.255	255.255.255.255	在链路上	192.168.16.116	291

(3) 访问 SSL VPN 资源

SSL VPN 连接成功后，访问内网的 FTP 和 HTTP 资源，能够访问成功，如图 133 和图 144 所示。

图13 访问 FTP 资源

图14 访问 HTTP 资源



目 录

1 简介

广告推送是一种在用户使用浏览器上网的同时，网络设备强制浏览器打开特定的广告窗口的方法。按某种规则给用户浏览器弹出一个广告页面，以达到广告推广或者提示用户的目的。

本文档介绍设备的广告设置配置举例，包括广告对象和广告策略。

本模块功能具有如下功能点：

- 一个网页支持在多个位置显示广告（例如左下、左上、右下、右上）。
- 每个广告位置支持轮播形式展示多张图片广告（最多 4 张）。
- 第三方广告信息只需配置广告 URL，显示效果视服务器而定。

通过菜单“策略配置 > 广告推送策略”，新建广告对象，进入如下图所示页面。在该页面上，可以新建广告对象和查看已经配置的广告对象信息。这些信息的详细说明如图 1 所示。

图1 广告对象配置页面

表1 广告对象显示信息说明

标题项	说明
广告名称	广告对象名称
广告描述	广告进行描述，不会在弹出广告页面显示
广告类型	可选本地自定义广告和第三方广告，默认显示本地自定义广告
设备管理IP	广告对象里的管理IP必须保证可以和下联终端互通，否则开启广告后网页无法打开
位置	广告图片展示的位置，默认右下角，可以选择右下角、右上角、左下角、左上角
广告图片	上传图片后在本地广告里面引用的弹出图片，最多可以展示4张，每张图片默认展示3秒，加上1秒缓冲。例如4张图片4*3+1=13秒

标题项	说明
图片描述	广告图片可以添加描述信息范围（0-31字符）
图片URL	当广告图片展示时点击图片的链接URL
广告对象选择文件按钮	上传本地广告图片使用
广告对象开始上传按钮	广告图片配置完成后上传使用
广告对象已存在按钮	上传图片后可以查看上传图片
第三方广告URL	第三方广告需要配合第三方广告服务器使用，除了serverip需要填写外其它参数为动态参数，如果用户URL里输入了参数，且参数后边是<>，说明该参数用户需要，且底层根据实际数据流的信息给参数赋值，但是如果URL里输入了参数，参数等号后边是直接的值，是需要用户直接配置下来的，底层根据用户的配置信息来组织js
提交按钮	所有参数配置完成后，点击提交生效
取消按钮	所有参数配置完成后，点击取消按钮后，不会生效

图2 广告策略配置页面

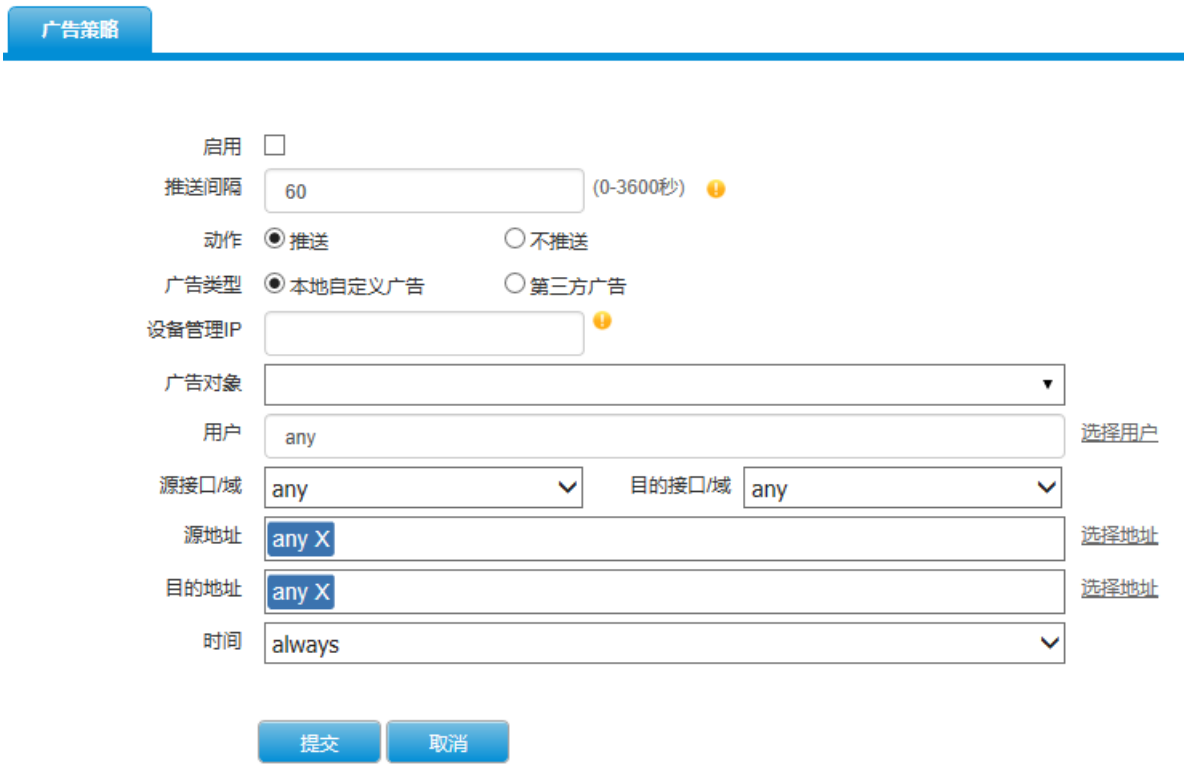


表2 广告策略显示信息说明

标题项	说明
广告策略开关	广告策略使能开关
推送间隔	范围60-3600秒，针对单个用户弹出广告间隔设置（同一用户在一定间隔内不会重复弹送广告）

标题项	说明
动作	推送和不推送。默认推送，当广告策略启用且选择了不推送后，该策略不生效，继续匹配下一跳广告策略
广告类型	可选本地自定义广告和第三方广告，默认显示本地自定义广告。当选择好广告类型后，广告对象不能交叉引用
广告策略里设备管理IP	设备管理IP为选配项可为空，若配置优先使用配置IP，否则使用报文入接口IP，两者均为获取到则不弹广告；配置管理IP务必保证用户可达，否则无法加载原始页面
广告对象	策略使用的广告对象
用户	匹配广告策略的用户
源接口/域	流量入接口/域
目的接口/域	流量出接口/域
源地址	匹配广告策略的源地址对象
目的地址	匹配广告策略的目的地址对象
时间	策略生效时间
提交按钮	所有参数配置完成后，点击提交生效
取消按钮	所有参数配置完成后，点击取消按钮后，不会生效

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解广告设置特性。

3 使用限制

(1) 广告服务对象配置支持 16 条。

(2) 广告策略配置支持 16 条。

(3) 一条广告策略可引用 1-3 个广告对象。

(4) 本地广告对象最多支持 4 张图片。

(5) 命令行不支持图片导入，不支持图片 ha。

(6) 策略中引用的广告对象必须种类相同，不可第三方及本地同时引用。

(7) 被引用的广告对象不可修改类型。

(8) 命令行不支持新建广告对象。只能修改一些参数，图片不支持修改，命令行主要做配置恢复。

(9) 图片格式目前支持 jpg、png，不支持动态图片上传 gif,不支持 bmp 格式图片。

(10) 一条策略里三组图片，如果图片位置一样的话，pc 访问页面广告覆盖显示。

(11) 广告对象里的设备 ip 不通的情况下广告图片无法加载；策略里地址对象不通导致 web 页面打不开。

(12) 域名白名单模糊匹配（使用简单的字符串匹配）。配 xw.qq.com 访问 www.xw.qq.com 这才是包含关系。

(13) 手机广告对象弹出只有置中与广告对象上下左右不一致。，广告对象位置信息只针对 PC 端生效，移动端全屏显示。

(14) 广告推送如果跨网段推送广告。需要在下联用户的入接口开启 http 服务（推送模板需要基于设备的一些 js 库，需走设备入接口 http 服务）。

(15) 手机端 UC 浏览器需要关闭广告过滤推送的广告才能显示。

(16) 腾讯微博和新浪微博内置了域名白名单不会弹送广告。

(17) 某些网站安全检查走的是云加速，存在 302 跳转导致无法打开。开启云加速功能后无法抓到第一个 GET 包，目前手机 qq 浏览器需关闭“云加速”后才能够弹出广告。

(18) 163 和 126 邮箱页面和广告模板存在兼容问题。

4 配置举例

4.1 组网需求

如图 3 所示，在公司出口网关开启广告设置，推送公司的一些活动或者提示用户一些信息。具体应用需求如下：

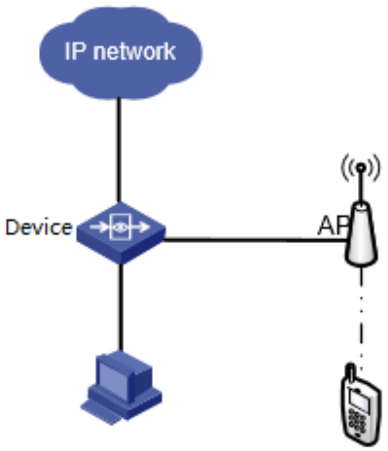
(1) 将来自 192.168.1.0/24 PC 终端弹出广告推送。

(2) 将来自 192.168.2.0/24 无线 AP 上网的手机客户弹出广告推广。

(3) 需要把 www.qq.com 网站放到白名单，不推送广告。

(4) 领导的 IP 需要放到白名单不推送广告。

图3 广告设置配置案例组网图



4.2 配置思路

按照组网图组网。

(1) 配置安全策略

(2) 创建广告对象

(3) 创建广告策略

(4) 配置终端

(5) 配置无线 AP

(6) 配置域名白名单

(7) 配置源地址组白名单

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

4.4.1 配置设备

1. 配置安全策略

通过菜单“策略配置>IPv4 控制策略”，将默认规则修改为允许，如图 4 所示的页面。

图4 IPv4 控制策略配置

2. 创建广告对象

通过菜单“策略配置>广告推送策略”，新建广告对象，进入如图 5 所示页面。配置广告设置（本地自定义广告推送），添加描述信息、自定义广告图片、配置推送 URL，点击提交。

图5 本地广告对象配置

3. 创建广告策略

通过菜单“策略配置>广告推送策略>广告策略”，新建广告策略，进入如图 6 所示页面。配置广告策略设置（本地自定义广告推送），广告对象、用户、接口、地址和时间，点击提交。

图6 广告策略配置

4. 配置终端

配置下联 pc 上网 ip。

图7 配置 PC 地址

5. 配置无线 AP

6. 配置域名白名单

广告白名单仅支持在命令行下进行配置。

排除 www.qq.com 网站，不让推送广告。

```
host(config)# http hijack whitelist host www.qq.com
```

此时再次访问 www.qq.com 页面不再推送广告。

7. 配置源地址组白名单

排除一部分源地址，不让推送广告。

(1) 创建地址对象

```
host(config)# address bt-ad
host(config-address)# ip address 192.168.2.218
```

(2) 配置基于源地址组的广告白名单

```
host(config)# http hijack whitelist source-address bt-ad
```

此时源地址 192.168.2.218 的地址再次访问 http 网址页面不再推送广告。

4.5 验证配置

(1) 验证 PC 端广告推送

如图 8 所示，下联 PC 访问 http 网站上网查看效果（多张图片的话有轮播效果）。点击图片跳转到链接网站；点击图片 X 号关闭广告图片。

图8 PC 端广告设置弹出效果

(2) 验证域名管理

如图 9 所示，下联手机客户端通过无线 AP 访问网站上网（http）查看效果。点击图片跳转到链接网站如图 9 所示；点击图片 X 号关闭广告图片。

图9 手机客户端广告设置弹出效果

目 录

1 简介

本文档介绍设备的 AD 域单点登录配置举例。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 使用限制

需将启动脚本放置安全类软件白名单。

不同用户登录同一台域内测试 pc，在线用户只显示一个账号，在线用户只识别第一次登录的账号，避免频繁出现账号切换，目前设备是基于 IP 来识别用户的，无法实现两个 IP 一样账号不一样的用户同时在线。

单点登录用户不支持 HA 主备：

HA 主备单点登录配置支持 HA 同步，但在线用户不支持 HA 同步，如果发生 HA 切换，存在以下两种情形：

- 单点登录失败的用户，不需要认证，自动上线。

新的主设备收到用户心跳报文后（默认 30s 发一次心跳报文），用户会重新上线，但是如果上网流量产生在心跳报文之前，则以 IP 作为用户名直接上线。

- 单点登录失败的用户，继续匹配后续策略。

新的主设备收到用户心跳报文后（默认 30s 发一次心跳报文），用户会重新上线，但是如果上网流量产生在心跳报文之前，则会继续匹配设备上的后续认证策略，如果没有后续认证策略，则会丢弃在收到下个心跳报文之前的 30s 内的所有报文，后续收到心跳报文后则会重新上线。

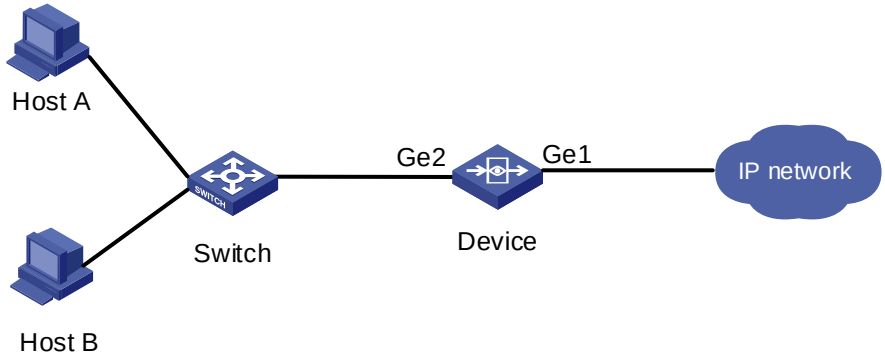
4 配置举例

4.1 组网需求

- HostA 、HostB 均为内网用户，属于 192.168.1.0/24 网段,通过 NAT 的方式访问 Internet。
- GE2 接口 ip ： 192.168.1.1。
- 内网存在 AD 域服务器、已加入 AD 域的 PC。

如图 1 所示。

图1 组网图



4.2 配置思路

AD 域登录成功后，用户自动上线。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

内网服务器存在至少两台同类型的服务器，此处以 http server 为例。

4.5 配置步骤

4.5.1 配置设备

1. 配置认证策略

在导航栏中选择“用户管理>认证管理>认证策略”，进入认证策略的显示页面，如图 2 所示。

图2 认证策略界面

单击<新建>，配置源接口为 GE2，认证方式为单点登录，登录失败的用户选择动作为不需要认证，自动上线。配置时间对象为 always。如图 3 所示。

图3 配置认证策略界面

2. 单点登录配置

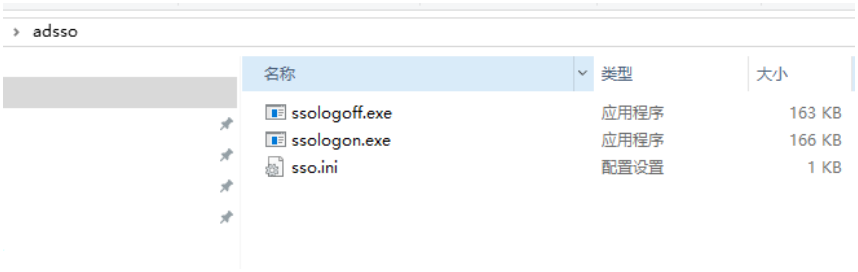
在导航栏中选择“用户管理>认证管理>认证方式>单点登录”，启用单点登录，配置会话密钥（如:123456），如图 4。

图4 单点登录配置界面

3. 单点登录脚本

下载域单点登录程序，并解压，如图 5 所示。

图5 单点登录配置脚本



4. 配置 sso.ini

修改 Gwip 为 GE2 接口 IP，修改 seessionKey 为之前配置的密码，如图 6 所示。

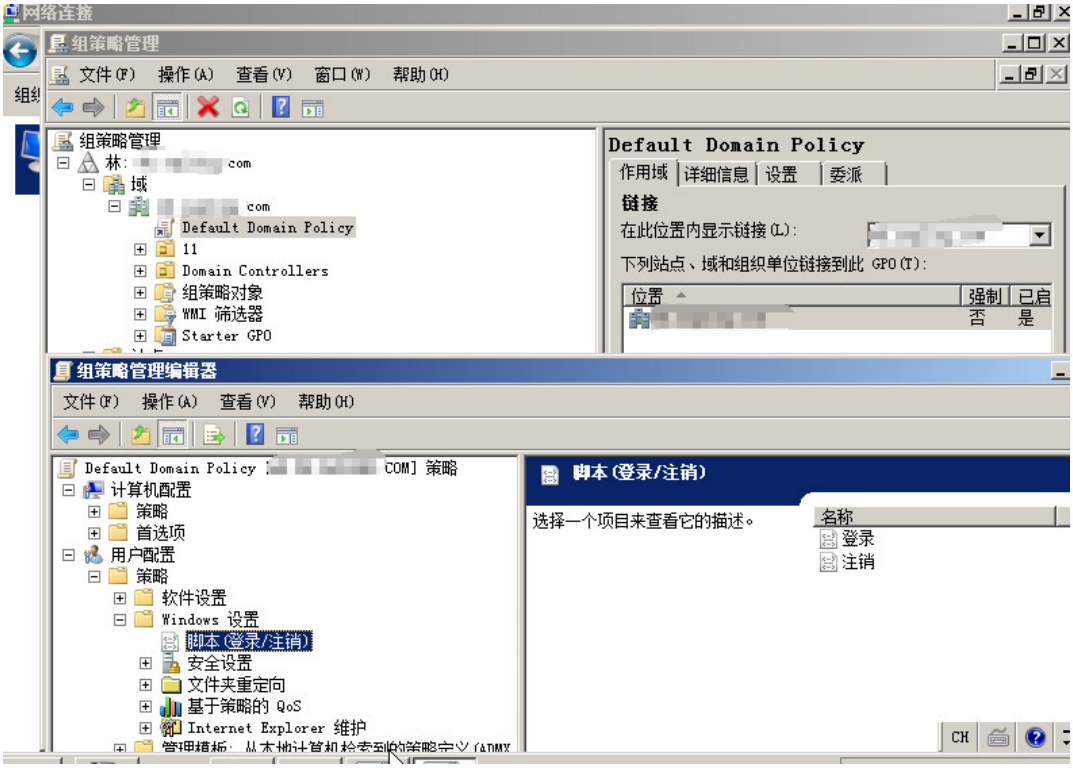
图6 脚本配置界面

```
[SSOCtrl]
EnableHeartBeat = 1
EnableCopyStartup = 1
HeartBeatInterval = 30
LogPath = C:\

[GW1]
GWIP = 192.168.1.1
Port = 6622
SessionKey = 123456
```

5. 登录 AD 域控

进入组策略：AD 域服务器“运行”输入“gpmc.msc”，选择“Default Domian Policy”，选择“用户配置>脚本（登录/注销）”，如图 7 所示。

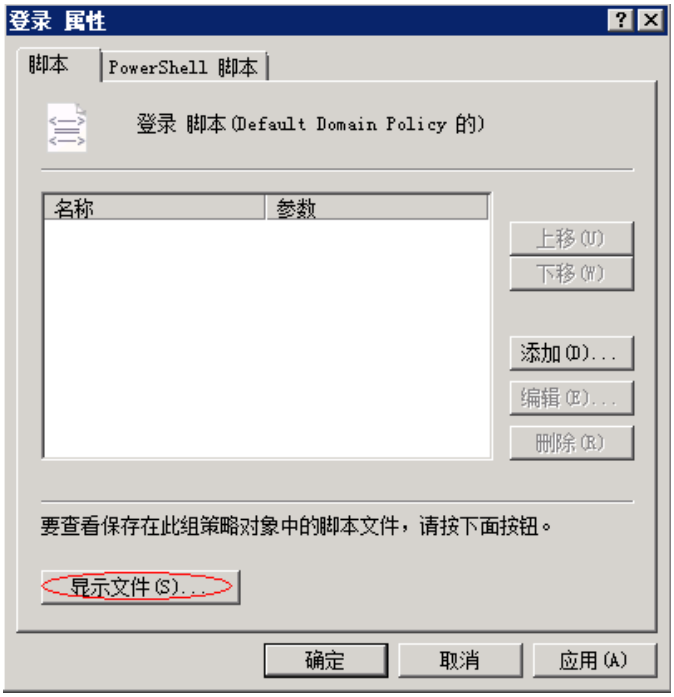
图7 组策略配置界面



6. 导入登录脚本

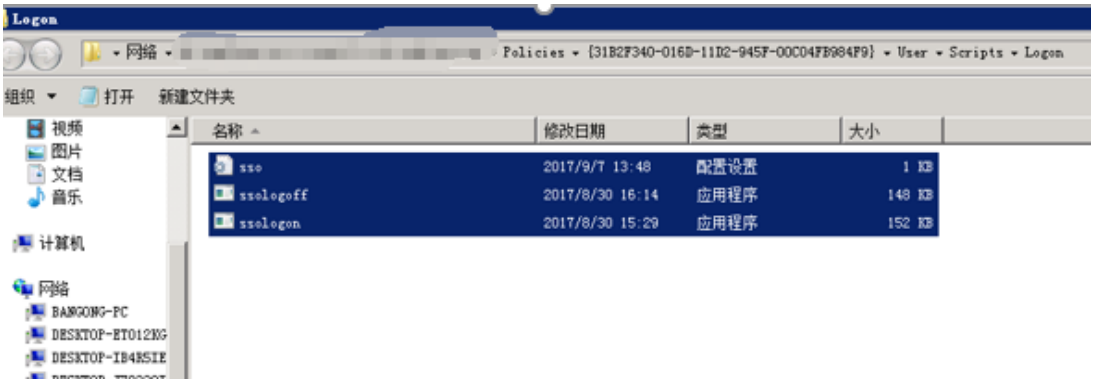
如图 8 所示。

图8 组策略配置界面



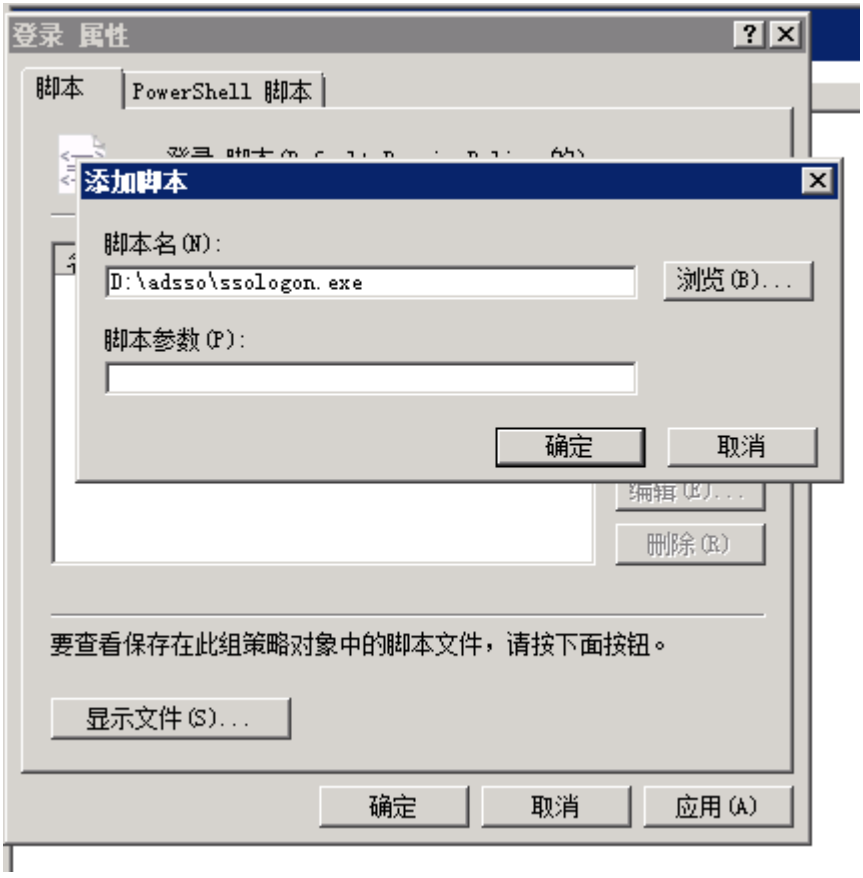
将配置文件及脚本导入到启动目录，如图 9 所示。

图9 组策略脚本配置界面



在图 8 的界面上点击添加，选中登录脚本，并确定即可，如图 10 所示。

图10 组策略脚本配置界面



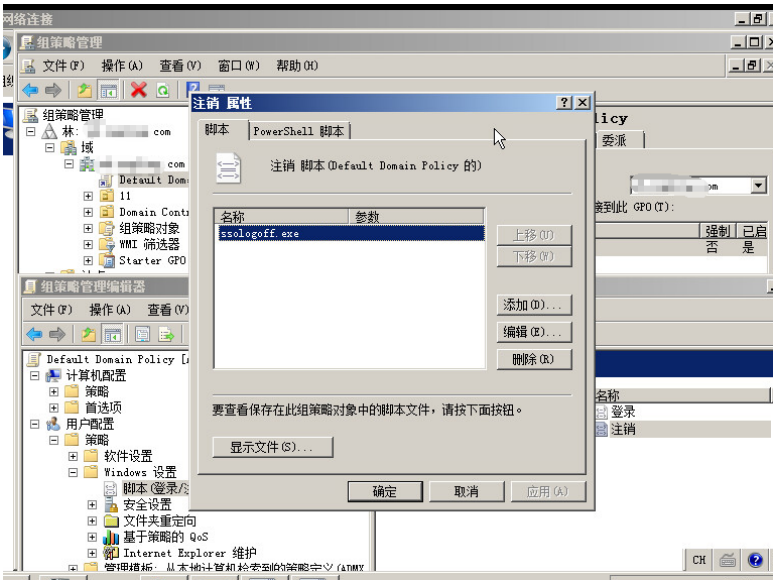
登录脚本导入完成，如图 11 所示。

图11 组策略脚本配置界面

7. 导入注销脚本

如图 12 所示。

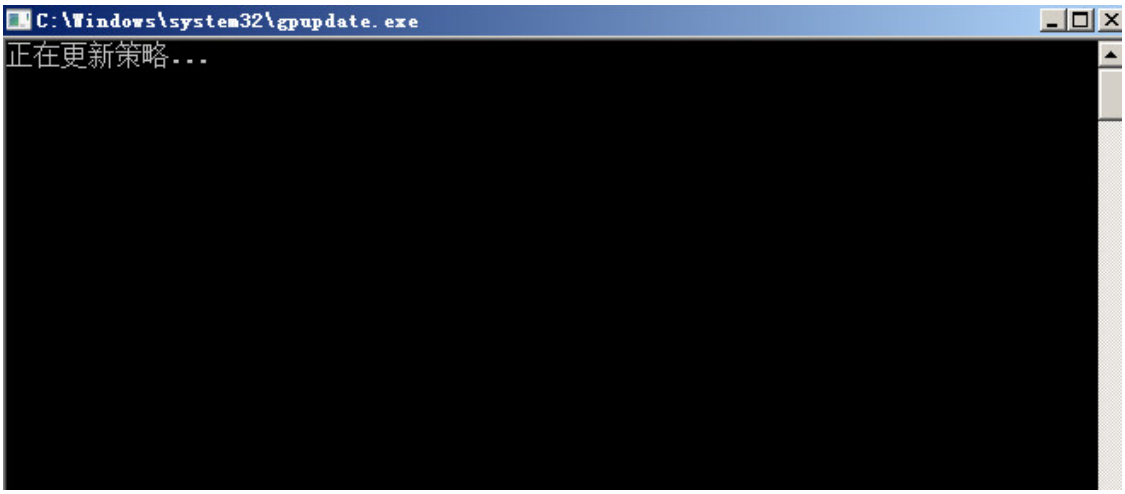
图12 组策略脚本配置界面



8. 组策略更新

通过组策略下发给域用户域控中，运行“gpupdate.exe”，如图 13 所示。

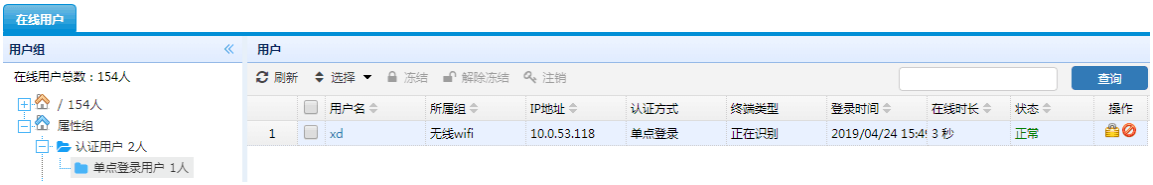
图13 组策略更新界面



4.6 验证效果

如图 14 所示。使用正常加入域的 PC，输入域账号登录，正常进入 PC 桌面后，查看设备在线用户，可以看到域用户已自动上线，可以正常访问网络。

图14 在线用户状态界面



4.7 配置文件

```
!user-group
!
!
!
!user-policy
!
user-policy ge2 any any any always sso-no-authen-ip enable sso no-record forever
!zone
!
!user-sso
!
user-adsso session-key kTgxl5p34DqlzzT+XZ0R14cv6Qal7urj9YogDjQGHYyVxSLYIpmOxTPwro4b0aN
```

5 相关原理资料

- **sso.ini**

  脚本配置文件，用于配置网关地址、会话密钥、心跳报文间隔时间等

  网关地址：设置为设备的地址

  会话密钥：必须与设备上配置的会话密钥一致

  心跳报文间隔时间：默认为 30s，登录脚本会定期向设备发送心跳报文，如果超过 3 次未收到用户的心跳报文，设备会将用户踢下线。使用命令 user-adsso timeouts <1-72>可以修改心跳报文超时下线次数

  其它参数全部默认即可，不需要修改。

- **ssologon.exe**

  登录脚本，域用户登录后，域服务器会将此登录脚本推送到域用户 PC 本地，然后脚本会自动运行，将上线用户的信息发送给设备，设备检查到此登录脚本发送的信息后，会将用户加入在线列表

- **ssologoff.exe**

  注销脚本，当域用户登录后，域服务器会将此注销脚本推送到域用户 PC 本地，当域用户注销后，注销脚本会将用户信息发送给设备，设备检查到此注销脚本发送的信息后，会将用户下线。

目 录

1 简介

随着 internet 的普及，单位和企业的应用系统需要面对越来越多的访问量和数据量，这就对系统的稳定性、可靠性提出了更高的要求，这样就使得单一的网络设备已经不能满足需求了。一些单位和企业则引入了多台服务器并建立服务器集群，但同时它也带来了另外一个问题就是我们如何将服务请求发送到合适的服务器才能使得每台服务器的处理能力得到充分的发挥？由此，SLB 的概念就被引出来了。

SLB 实现了在客户访问多台同时工作的服务器的情况下，即时按需动态检查各个服务器的状态，根据预设的规则将请求分配给最有效率的服务器，实现数据流合理的分配，使每台服务器的处理能力都能得到充分的发挥，提高应用系统的整体性能，改善应用系统的可用性。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 使用限制

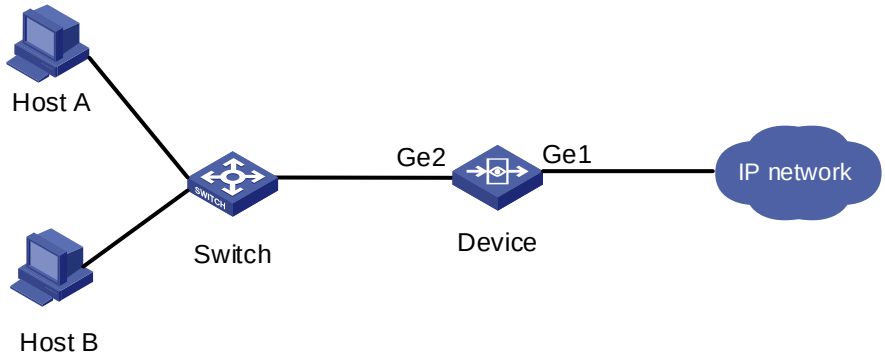
内网需至少存在两个类型一致的服务器。

4 配置举例

4.1 组网需求

如图 1 所示 HostA、HostB 均为内网用户，属于 192.168.1.0/24 网段,通过 NAT 的方式访问 Internet 限制每用户/ip 的上下行速率。

图1 服务器负载均衡组网图



4.2 配置思路

根据负载均衡策略对服务器进行转发。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

4.5 配置步骤

4.5.1 配置设备

1. 新增负载均衡策略

在导航栏中选择“策略配置>负载均衡策略>服务器负载均衡”，单击<新建>按钮，进入服务器负载均衡策略配置页面，如图 2 所示。

图2 服务器负载均衡策略界面

2. 配置策略

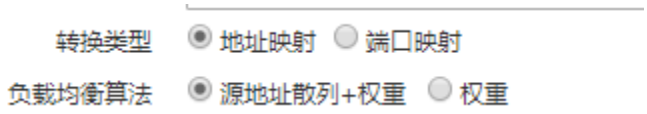
启用策略，配置 ID 为 1 ，源地址为 any，目的地址 any，服务为 http，接口 ge1，如图 3 所示。

图3 服务器负载均衡界面

3. 配置转换类型与算法

配置转换类型为地址映射，配置负载均衡算法为源地址散列，如图 4 所示。

图4 服务器负载均衡界面



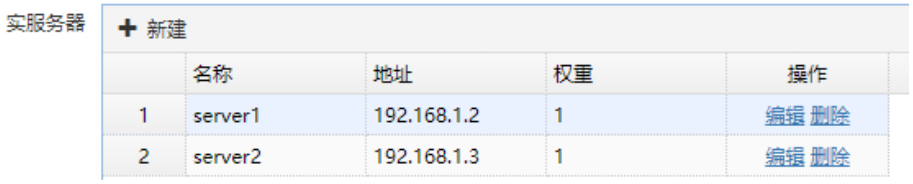
4. 配置实服务器：

新增实服务器：

- 名称：server1 地址 192.168.1.2，权重 1。
- 名称：server2 地址 192.168.1.3，权重 1。

如图 5 所示。

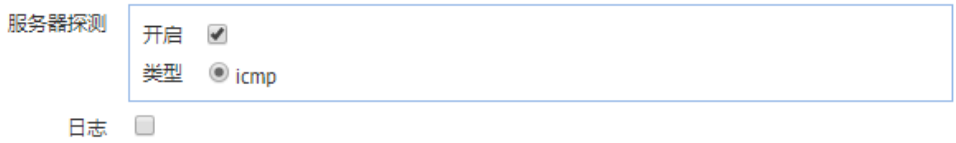
图5 实服务器配置界面



5. 开启服务器探测

类型为 icmp，如图 6。

图6 服务器探测界面



6. 查看策略配置，

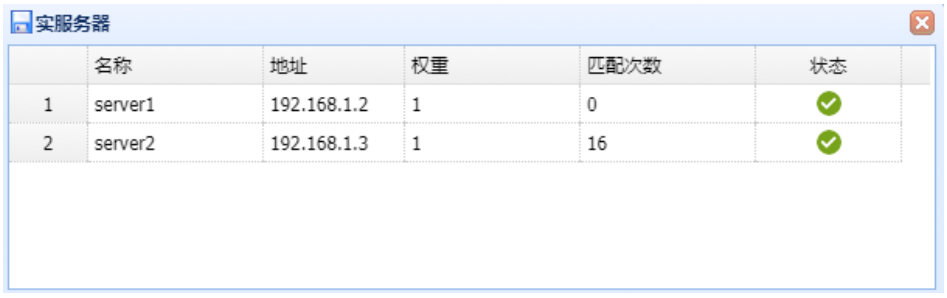
配置完成后查看策略配置，如图 7。

图7 服务器负载均衡界面

4.6 验证效果

Internet 上的 ip1 访问 GE1 的 http 服务：http://192.168.201.92，重复刷新几次，检查实服务器详情，是否仅匹配 server 服务器中的一个，如图 8。

图8 实服务器界面



4.7 配置文件

```
slb 1
 rule ge1 any any http source-addr-hash icmp
 track enable
 real-server server1 192.168.1.2 1
 real-server server2 192.168.1.3 1
!
```

目 录

1 简介

设备的 QOS 支持每 IP QOS，功能开启的时候，在网络出口每条流的每个 IP 都会受到 QOS 的控制。在实际应用中，一个认证用户可能同时存在多个 IP，例如电脑上网，手机上网；如果需要针对每个用户进行限速，那么每 IP 功能就无法满足要求，所以考虑实现每用户限速功能。

2 配置前提

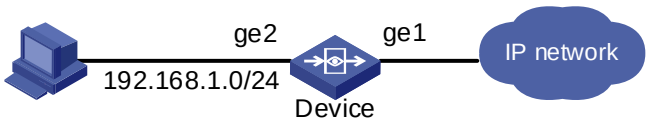
本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

3 配置举例

3.1 组网需求

如图 1 所示 HostA、HostB 均为内网用户，属于 192.168.1.0/24 网段，通过 NAT 的方式访问 Internet 限制每用户/ip 的上下行速率分别为 5M/s。

图1 组网图



3.2 配置思路

- 根据每 ip/用户，配置一个限速的阈值，保证网络的带宽。
- 对流控通道的补充，根据不同的场景，选择用户或者 ip 限速。

3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.4 配置注意事项

- 每 IP/用户 限速最小粒度为 8Kb。
- 每 IP/流控限速需建立在流控通道内。

3.5 配置步骤

3.5.1 配置设备

1. 配置地址对象

如图 2 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，IP 地址配置为 192.168.1.0/24。

图2 新建地址对象

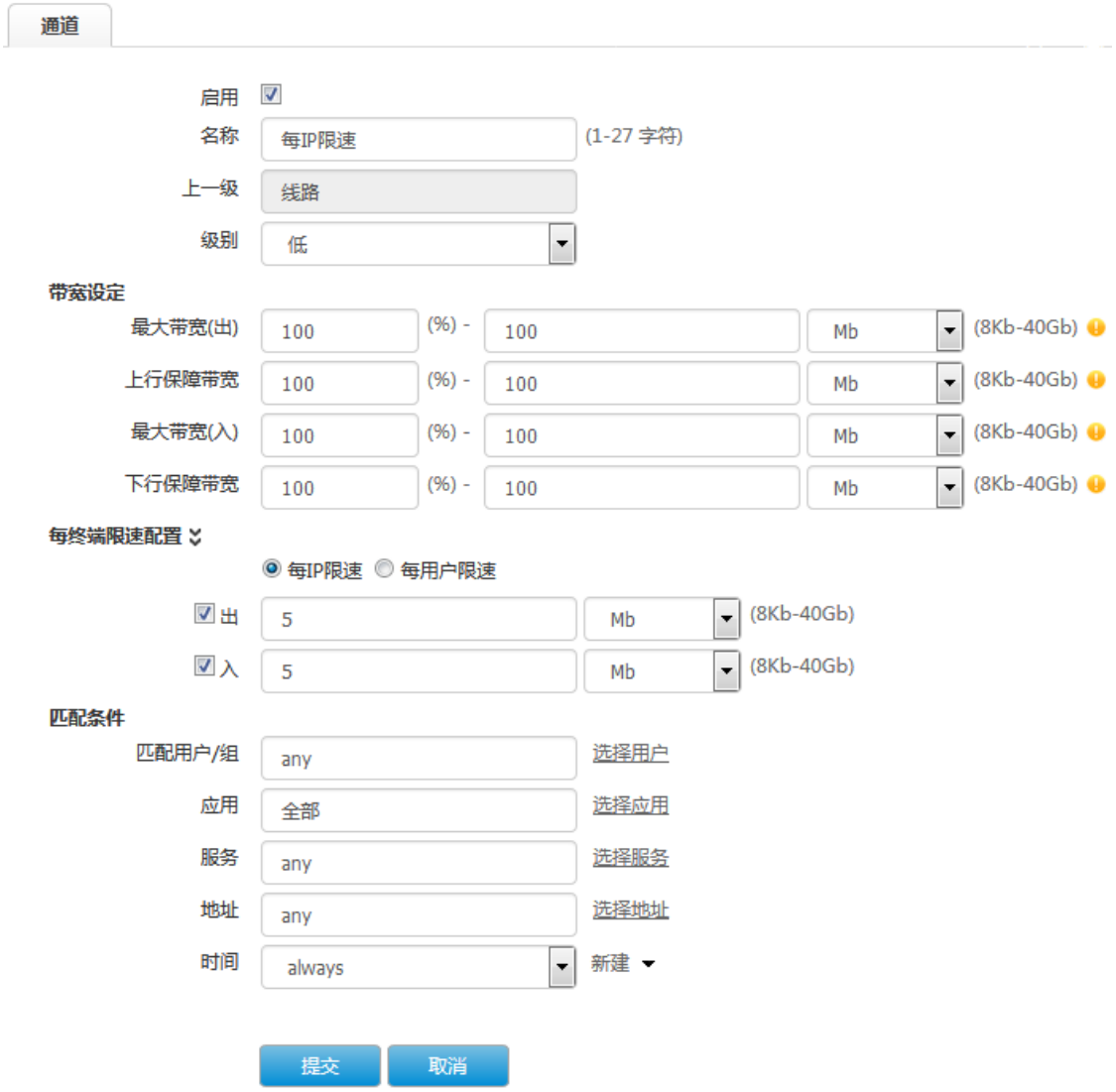
2. 新建线路

在导航栏中选择“策略配置>流量控制策略”，选择“新建>线路”进入新建线路的显示页面，如图 3。

图3 新建线路

选中<线路>，选择“新建>通道”进入“通道”配置页面，新增通道为每 IP 限速；配置流量控制，新建通道“每 ip 限速”，最大带宽 100Mb，上行保证带宽 100Mb、最大带宽入 100Mb、最大带宽出 100Mb。每终端限速配置：选择每 IP 限速　出 5Mb 入 5Mb，如图 4。

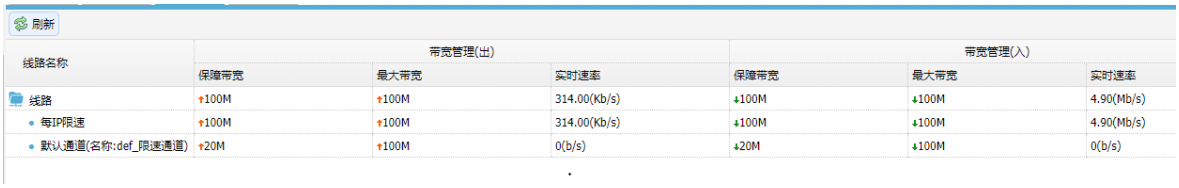
图4 流量控制



3.6 验证效果

下载一个文件，查看速率，如图 5。

图5 验证效果



3.7 配置文件

```
qos-profile line 线路
 limit both
 maxbandwidth ingress 100000
 maxbandwidth egress 100000
 match interface ge1
!
qos-profile channel 每IP限速 parent 线路
 bandwidth ingress 100000
 maxbandwidth ingress 100000
 bandwidth egress 100000
 maxbandwidth egress 100000
 match user any
 match application any
 match service any
 match address any
!
qos-profile channel def_限速通道 parent 线路
!
policy6 default-action permit
```

目 录

1 简介

本文档介绍设备的流量和时长限额举例，包括基于流量的日限额和月限额，基于时长的日限额和月限额。

限额策略具有如下特点：

- 流量限额：支持日限额和月限额。
- 时长限额：支持日限额和月限额 。
- 支持设置惩罚时长。
- 支持提醒：达到限额条件后推送提醒页面提示用户，可以设置只提醒一次或定期提醒。
- 支持惩罚通道限速：基于时长惩罚或一直惩罚。
- 支持禁止上网：基于时长禁止上网或一直禁止上网。
- 支持限额统计：基于 IP 维度和用户账号维度。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

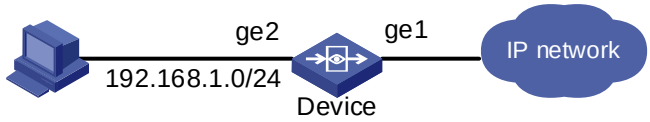
本文档假设您已了解限额策略特性。

3 基于流量的限额策略配置举例

3.1 组网需求

如图 1 所示 HostA、HostB 均为内网用户，属于 192.168.1.0/24 网段,通过 NAT 的方式访问 Internet 限制每用户，每日限额为 500MB，超出限额后，禁止访问网络。

图1 限额策略配置组网图



3.2 配置思路

根据每 ip 分配日限额流量，流量达到限额后对网络进行阻断或添加到惩罚通道进行限速。

3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.4 配置注意事项

3.5 配置步骤

1. 配置地址对象

如图 2 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>，IP 地址配置为 192.168.1.0/24。

图2 配置地址对象

2. 配置基于流量的日限额策略/禁止上网

(1) 新增限额策略

引用源 IP，如图 3 所示，进入“策略配置>用户限额策略”，点击<新建>，“源地址”配置为 192.168.1 网段。

图3 限额策略配置界面

(2) 配置日限额

选择限额类型为流量 日限额，配置 500MB，动作为禁止上网，如图 4、图 5。

图4 限额用户配置界面

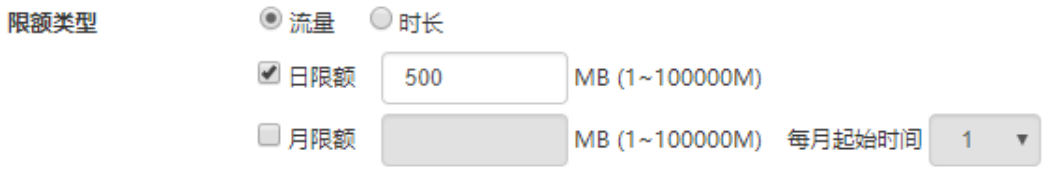


图5 限额策略配置界面

(3) 查看限额状态

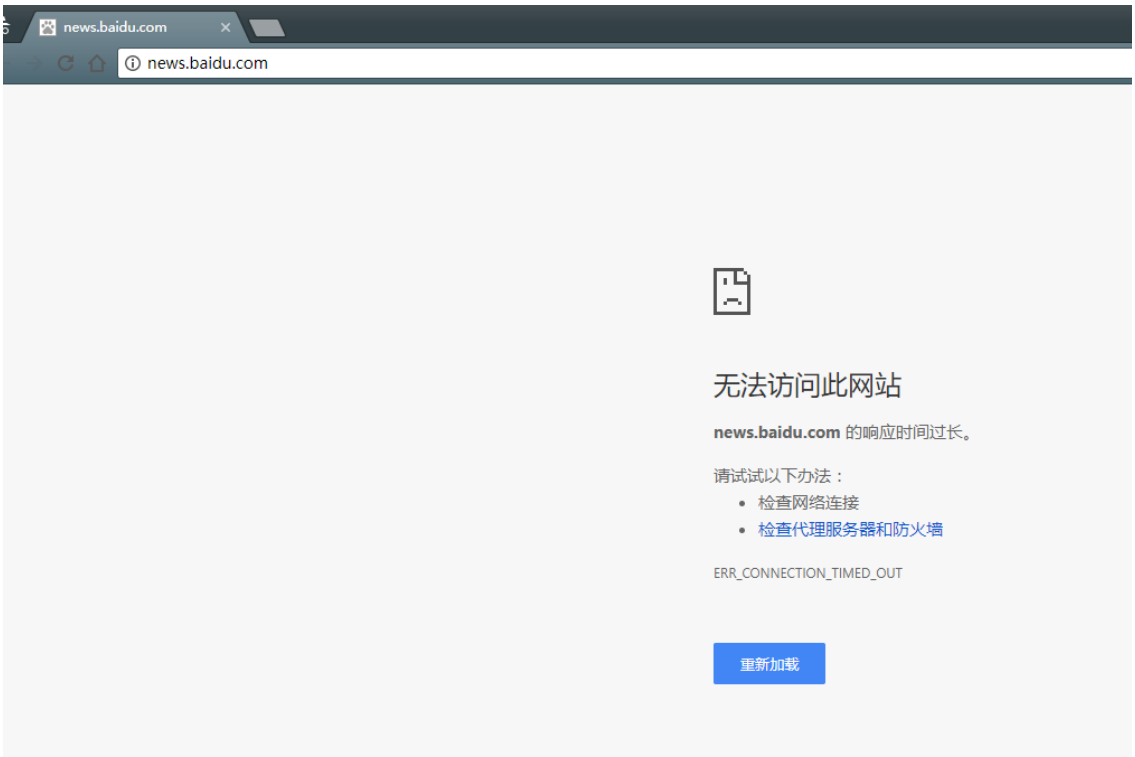
访问 internet 下载一个 500+MB 文件，检查限额状态，如图 6。

图6 限额用户统计界面

(4) 结果检查

访问 http 页面，检查页面是否被禁止，如图 7。

图7 访问外网界面



3. 配置基于流量的日限额策略/惩罚通道

(1) 配置惩罚通道

在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，点击<新建>，选择<惩罚通道>进入配置页面，如图 8 所示。

图8 惩罚通道配置界面

(2) 配置日限额

在导航栏中选择“策略配置>用户限额策略”，配置限额类型为流量/日限额，阈值为 500MB。源 IP 为 192.168.1.0 网段，限额超出处理为添加到惩罚通道，如图 9 所示。

图9 限额策略配置界面

(3) 结果检查

配置完成后，内网 PC 访问外网 internet，如图 10。

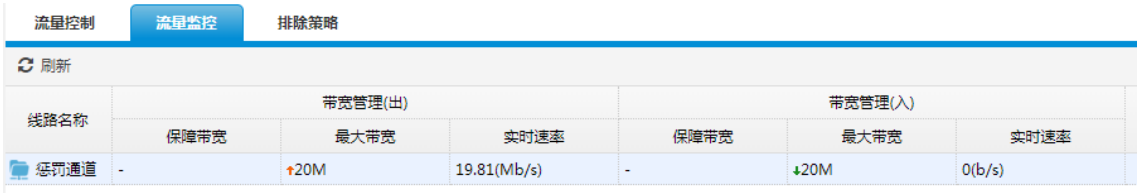
图10 限额用户统计页面

下载 500+MB 数据后,查看限额用户统计状态是否为限速，如图 11。

图11 限额用户统计界面

查看流量监控，流量是否限速为 20Mbps，如图 12。

图12 流量监控页面



4. 配置基于流量的月限额策略/禁止上网

(1) 新增限额策略

进入“策略配置>用户限额策略”，点击<新建>选择限额类型为流量 月限额，配置 500MB，动作为禁止上网，惩罚时间为 10 分钟，如图 13、图 14 所示。

图13 配置月限额策略

(2) 查看限额状态

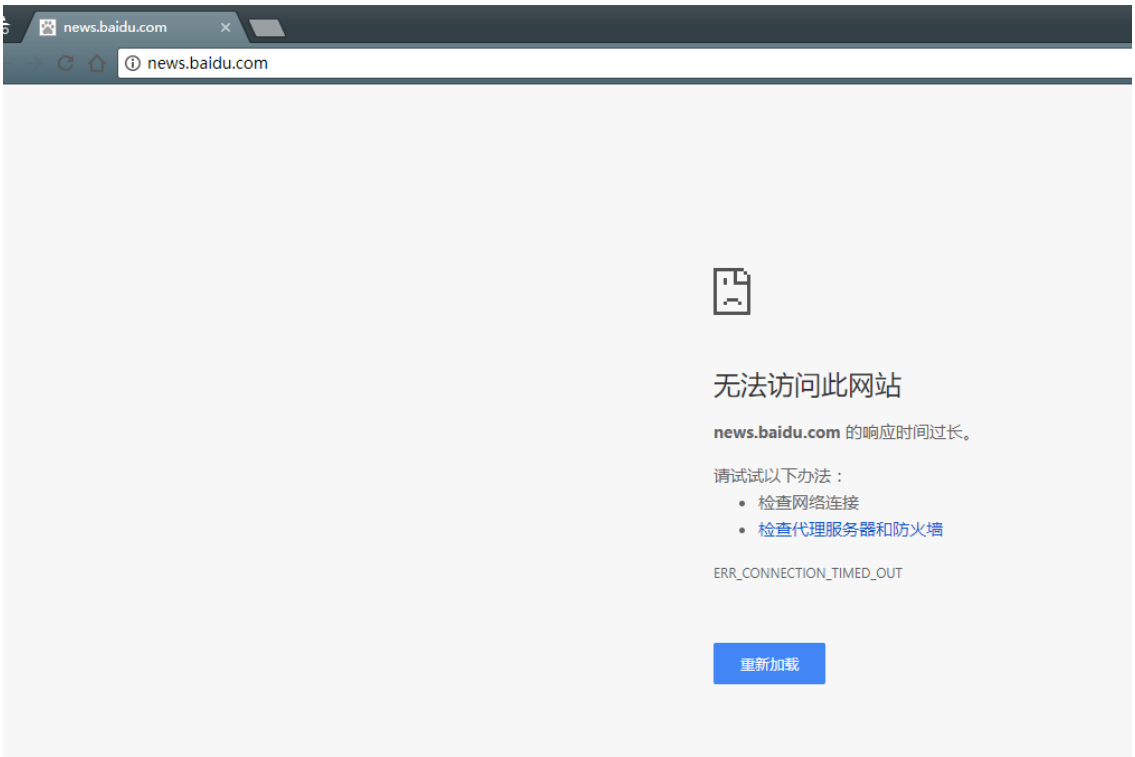
访问 internet 下载一个 500+MB 文件，检查限额状态，如图 14。

图14 查看限额状态

(3) 结果检查

访问 http 页面，检查页面是否被禁止，如图 15。

图15 禁止访问网络



5. 配置基于流量的月限额策略/惩罚通道

(1) 配置惩罚通道

在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，点击<新建>，选择<惩罚通道>进入配置页面，如图 16 所示。

图16 惩罚通道配置界面

(2) 配置月限额

在导航栏中选择“策略配置>用户限额策略”，点击<新建>限额策略，配置限额类型为流量/月限额，阈值为 500MB。限额超出处理为添加到惩罚通道，惩罚时间为 10 分钟，如图 17。

图17 限额策略配置页面

(3) 结果检查

配置完成后，内网 PC 访问外网 internet，如图 18 所示。

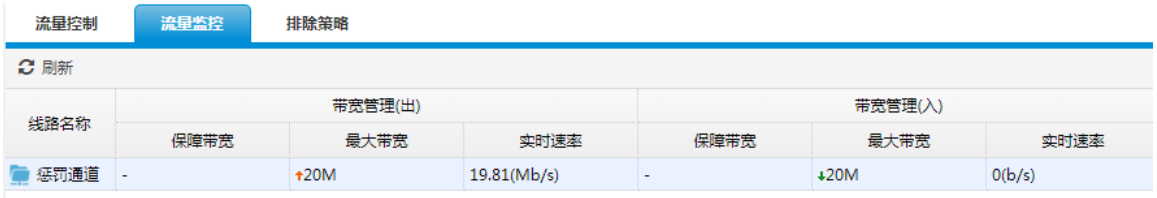
图18 查看限额状态

下载 500+MB 数据后,查看限额用户统计状态是否为限速，如图 19。

图19 查看限额状态

查看流量监控，流量是否限速为 20Mbps，如图 20。

图20 查看状态



10 分钟后检查速率可以正常恢复到之前的速率。

3.6 配置文件

```
interface ge1
 ip address 192.168.201.92/24
 allow access https
 allow access ping
!
interface ge2
 ip address 192.168.1.1/24
 allow access https
 allow access http
!
policy-quota 日流量限额
 enable
```

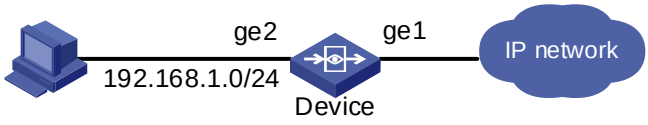
```
 log disable
 schdule always
 match user any
 match application any
 match src-address any
 match dst-address any
 quota mode traffic
 perday enable
 perday bandwidth 500
 notify disable
 punish disable
policy6 default-action permit

policy-quota 日流量限额-流控通道
 enable
 log disable
 schdule always
 match user any
 match application any
 match src-address any
 match dst-address any
 quota mode traffic
 perday enable
 perday bandwidth 500
 notify disable
 punish enable
 punish action limit qos-profile 惩罚通道
 punish interval 0
policy6 default-action permit
!
```

4 基于时长的限额配置举例

4.1 组网需求

如图 21 所示 HostA、HostB 均为内网用户，属于 192.168.1.0/24 网段,通过 NAT 的方式访问 Internet 限制每用户，每日限额为 500MB，超出限额后，禁止访问网络。

图21 限额策略配置组网图



4.2 配置思路

根据每 ip 分配日限额流量，上网时间达到限额后对网络进行阻断或添加到惩罚通道。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

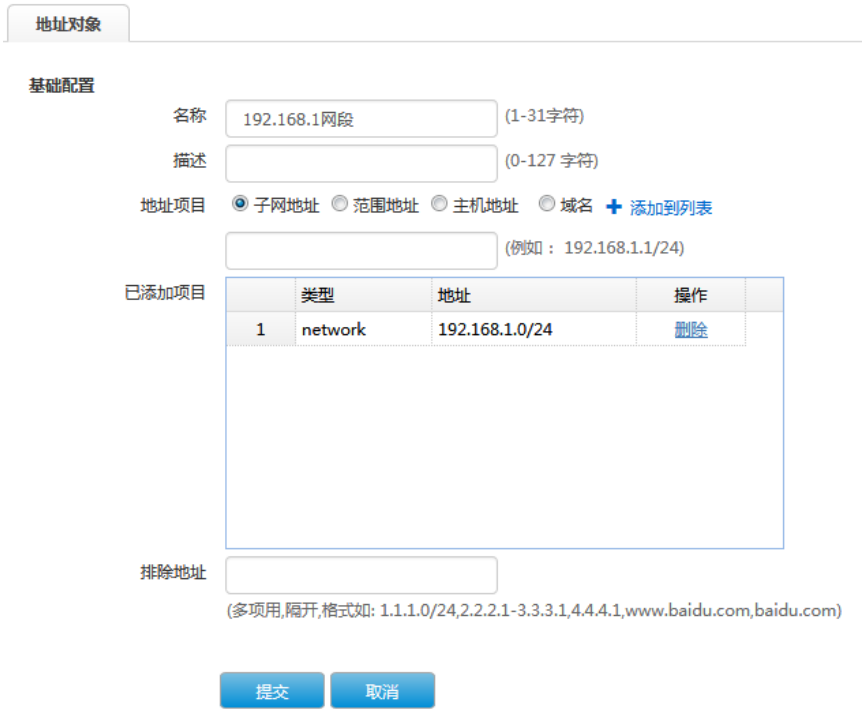
4.5 配置步骤

4.5.1 配置设备

1. 配置地址对象

如图 22 所示，进入“策略配置>对象管理>地址>IPv4 地址对象”，点击<新建>，IP 地址配置为 192.168.1.0/24。

图22 配置地址对象

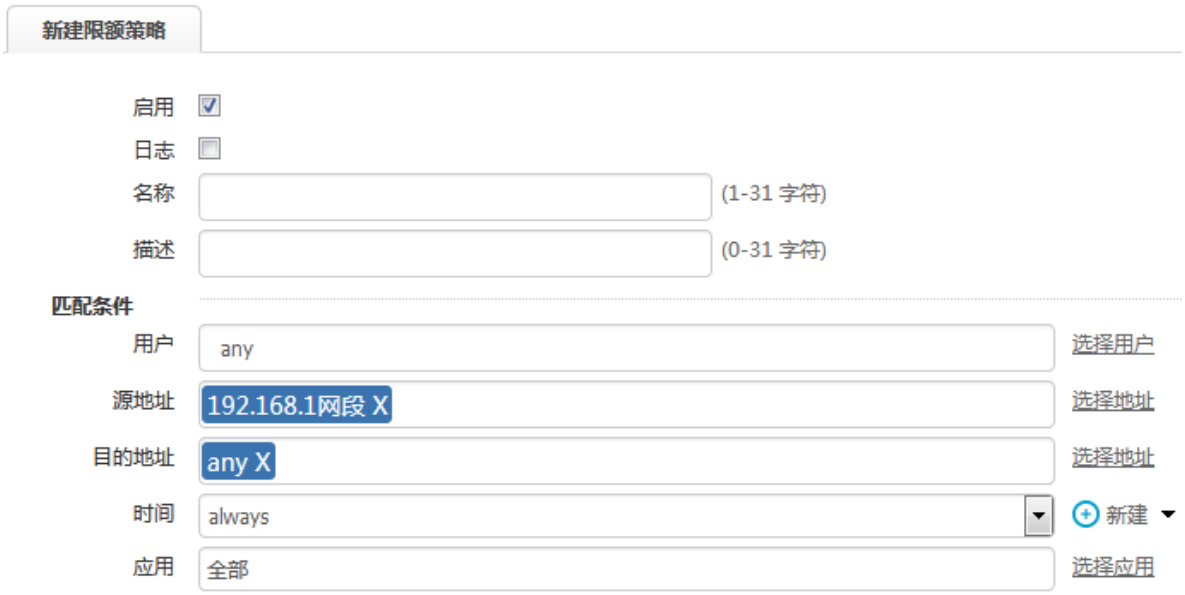


2. 配置基于时长的日限额策略/禁止上网

(1) 新增限额策略

如图 23 所示，进入“策略配置>用户限额策略”，点击<新建>，“源地址”配置为 192.168.1 网段。

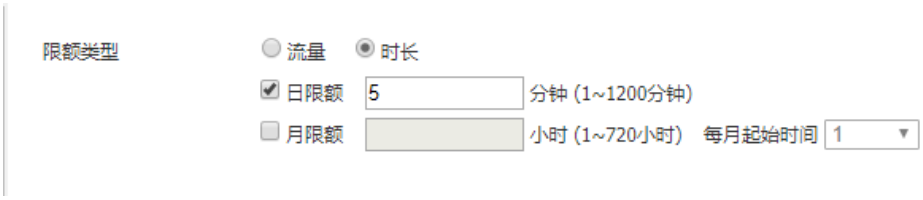
图23 限额策略配置界面



(2) 配置日限额

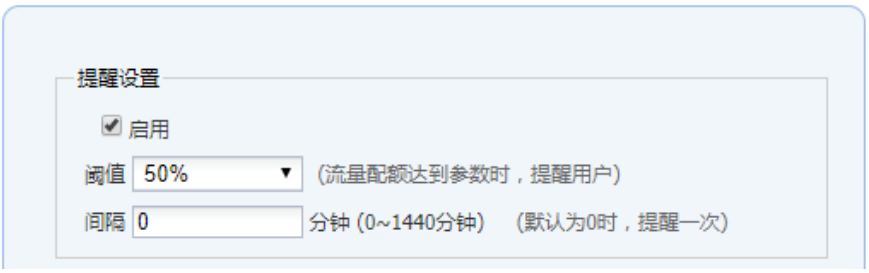
选择限额类型为时长日限额，配置日限额为 5 分钟，如图 24 所示。

图24 限额策略配置界面



配置限额超出处理：开启提醒，阈值为 50%，间隔为 0 分钟，如图 25。

图25 限额策略配置界面



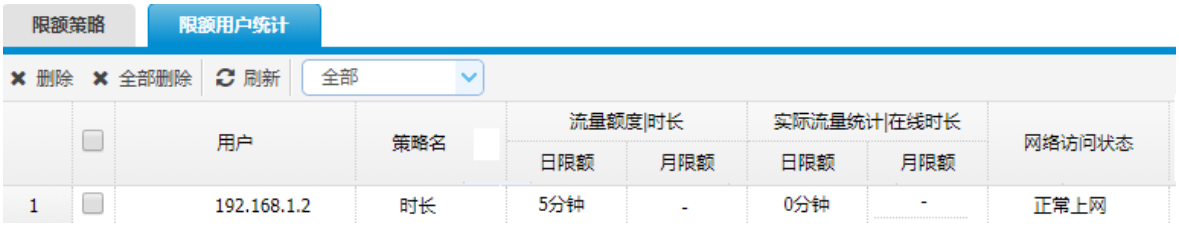
配置惩罚设置，惩罚时长为 5 分钟，动作为禁止上网，如图 26。

图26 限额策略配置界面

(3) 查看限额状态

访问 http 页面，检查限额状态页面，如图 27 。

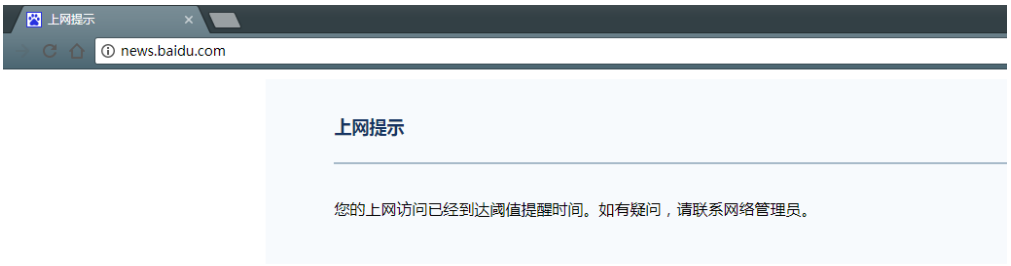
图27 限额用户统计页面



(4) 检查提醒功能

三分钟后访问 http 页面，检查是否弹出提醒页面.如图 28。

图28 访问外网界面



(5) 仅提醒一次验证

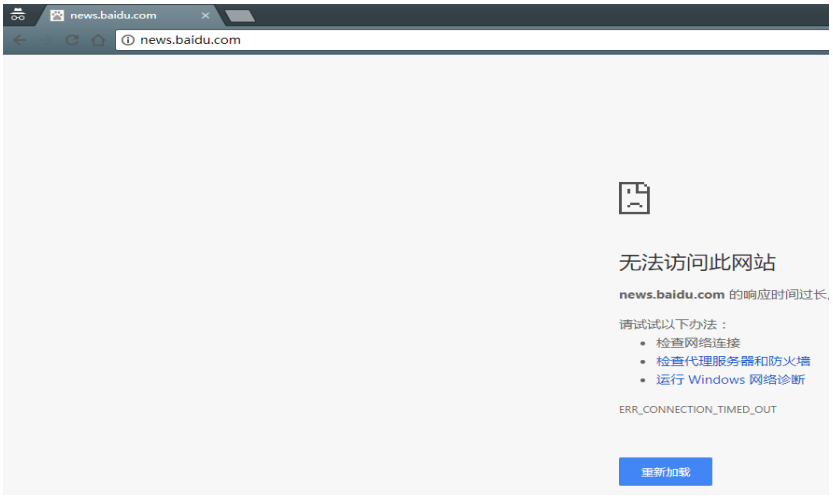
再次访问页面，检查是否正常显示，如图 29。

图29 访问外网界面

(6) 日限额阈值验证

第 5 分钟后，再次访问，检查页面是否被禁止，如图 30。

图30 访问外网界面



(7) 惩罚时间验证

第 10 分钟后（惩罚 5 分钟），重新访问，检查网络是否恢复正常，如图 31。

图31 访问外网界面

3. 配置基于时长的日限额策略/惩罚通道

(1) 新增惩罚通道

配置 惩罚通道，在导航栏中选择“策略配置 > 流量控制策略 > 流量控制”，点击<新建>，选择<惩罚通道>进入配置页面，如图 32 所示。

图32 惩罚通道配置界面

(2) 新增限额策略

在导航栏中选择“策略配置>用户限额策略”， 配置限额类型为时长/日限额，阈值为 5 分钟，源 IP 为 192.168.1.0 网段，限额超出处理为添加到惩罚通道，如图 33 所示。

图33 新增限额策略

(3) 结果检查

配置完成后，内网 PC 访问外网 internet，下载文件，检查是否为限速下载，如图 34。

图34 限额用户统计界面

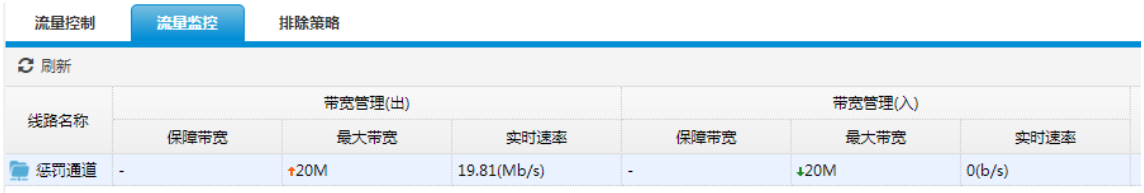
5 分钟后，下载文件，检查限额用户统计，如图 35。

图35 限额用户统计界面

(4) 进入惩罚通道

查看流量监控，流量是否限速为 20Mbps，如图 36。

图36 流量监控界面



4. 配置基于时长的月限额策略/禁止上网

(1) 新增限额策略

引用源 IP，如图 37 所示，进入“策略配置>用户限额策略”，点击<新建>，“源地址”配置为 192.168.1 网段。

图37 限额策略配置界面

(2) 配置月限额

选择限额类型为“时长/月限额”，配置阈值为 1 小时，动作为禁止上网，惩罚时间为 10 分钟，如图 38。

图38 限额策略配置界面

(3) 限额状态检查

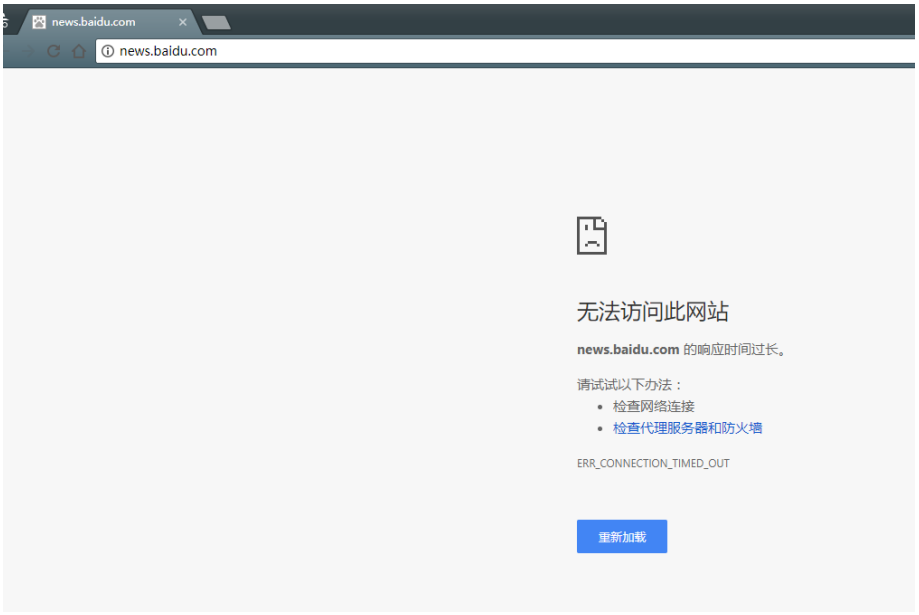
访问 internet，检查限额状态，如图 39。

图39 限额用户统计界面

(4) 时间限额阈值验证

一小时后，访问 http 页面，检查页面是否被禁止，如图 40。

图40 访问外网界面



10 分钟后，再次访问 http 页面，检查是否正常。

5. 配置基于时长的月限额策略/惩罚通道

(1) 新增惩罚通道

配置 惩罚通道，在导航栏中选择“策略配置 > 流量控制策略 > 流量 控制”，点击<新建>，选择<惩罚通道>进入配置页面，如图 41 所示。

图41 惩罚通道的配置

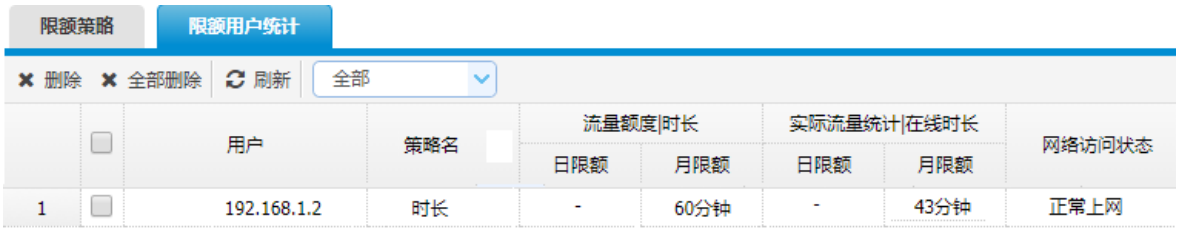
(2) 新增限额策略

在导航栏中选择“策略配置>用户限额策略”，配置限额类型为流量/月限额，阈值为 1 小时，限额超出处理为添加到惩罚通道，惩罚时间为 10 分钟，如图 42。

图42 新增限额策略

(3) 速率检查

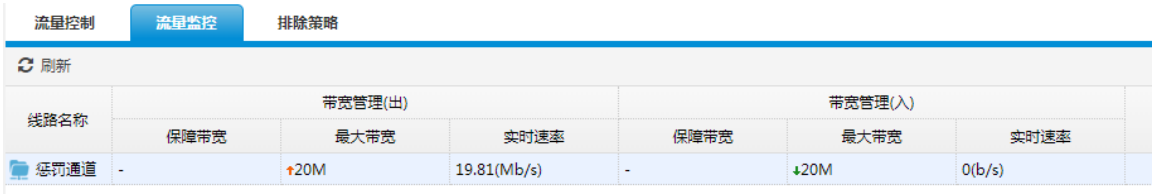
配置完成后，内网 PC 访问外网 internet，下载数据，检查是否为限速。



(4)　限速检查

1 小时后查看流量监控，流量是否限速为 20Mbps，如图 43。

图43 限速检查



10 分钟后检查速率是否恢复限速。

4.6 配置文件

```
interface ge1
 ip address 192.168.201.92/24
 allow access https
 allow access ping
!
interface ge2
 ip address 192.168.1.1/24
 allow access https
 allow access http
!
policy-quota 日流量限额
 enable
 log disable
 schdule always
 match user any
 match application any
 match src-address any
 match dst-address any
 quota mode traffic
 perday enable
 perday bandwidth 500
 notify disable
 punish disable
policy6 default-action permit

policy-quota 日流量限额-流控通道
```

```
 enable
 log disable
 schdule always
 match user any
 match application any
 match src-address any
 match dst-address any
 quota mode traffic
 perday enable
 perday bandwidth 500
 notify disable
 punish enable
 punish action limit qos-profile 惩罚通道
 punish interval 0
policy6 default-action permit
!
```

目 录

1 简介

本文档介绍设备的无线非经功能配置举例，包括厂商、场所、AP、上报周期、应用关系对照表配置。

在配置前，先了解如下几个定义：

- 无线非经：即公共场所无线上网安全管理条例，非经营性互联网信息服务提供者从事非经营性互联网信息服务时，应当遵守国家的有关规定，接受有关部门依法实施的监督管理 。
- 厂商：隶属相关部门授权并遵循指定的标准（协议、应用维度）和一定的行为规则（场所编码规则、经营性质等），对外提供开放接口用来收集指定场所用户上网行为数据平台。
- 场所：经过设备的流量是从哪些场所过来，就填写哪些场所，表明有多少个场所流量经过设备；
- AP：AP 是存在于场所内的，表明该场所内有多少个 AP，这样可以知道具体某个用户是在哪一个场所中的哪一个 AP 使用网络。
- 上报周期：根据对接厂商标准接口文档按一定的周期上报无线非经数据。
- 应用关系对照表：按照对接厂商平台要求，将我司应用转换成其对应的应用 ID 上报至网监平台，以便网监平台显示对应应用名称。

无线非经功能主要目的是将对接厂商需要的数据按照一定的格式要求，采用指定的协议标准上传至网监平台服务器，实现网监对非经营性场所上网用户行为的监控。

无线非经功能主要涉及到三大块，分别为应用识别审计、数据组织及数据上报，即按网监要求的格式对审计到的数据以固定的字段格式上报到网监系统对应的平台上去。

- 应用识别审计：主要是流量经过设备之后能够对其进行分析识别并审计，此块主要与引擎和特征库相关。
- 数据组织：设备上根据识别审计的日志以及日志平台需要上报的内容进行日志过滤及存储入数据库，并按网监要求生成对应的文件。
- 数据上报：设备根据对接厂商要求，在指定目录下获取生成的数据文件，按照网监平台指定的协议进行上报，上报周期可以手动配置。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

在配置前，需要做如下准备：

- 获取参与对接厂商的名称及组织机构代码。
- 本文档假设您已了解无线非经功能特性。

3 无线非经功能配置举例

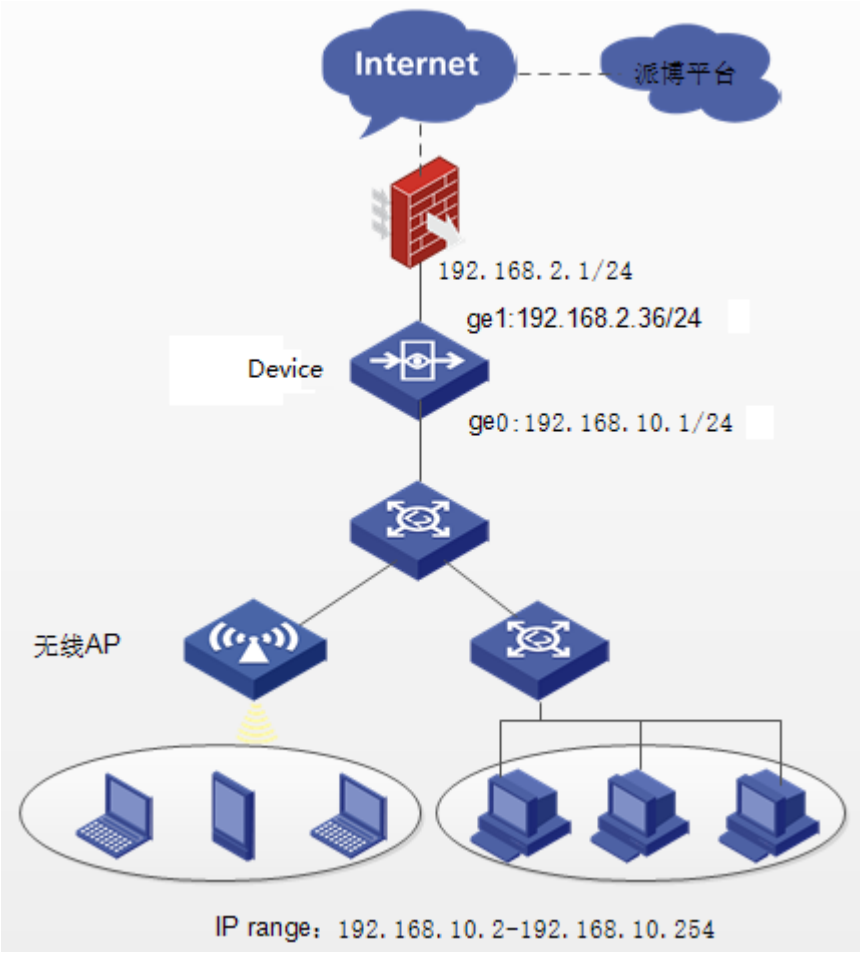
3.1 组网需求1：路由模式组网-派博平台对接

3.1.1 组网需求

如图 1 所示，某公司内网研发部门办公网段 IP 地址 192.168.10.0/24，其中 192.168.10.1/24 作为内网的网关地址。TPLINK 设备上开启 DHCP，地址池为 192.168.10.2/24~192.168.10.254/24。使用设备的的 ge0 和 ge1 接口作为路由模式，设备作为研发部门网关出口设备，上连公司出口防火墙，下连二层交换机。设备的上开启审计、本地认证和无线非经功能。具体应用需求如下：

- 内网用户访问外网时需要通过本地认证。
- 内网用户访问外网的流量通过设备处理上报至派博平台。

图1 路由模式组网



3.1.2 配置思路

- 网络基础配置，配置接口地址、路由、NAT、DNS 等信息。
- 升级特征库。

- 配置 IPv4 审计策略。
- 配置 Web 认证功能，添加认证账号、地址对象等信息。
- 配置无线非经功能，添加厂商、场所、AP 和上报周期等信息。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

1. 网络基础配置

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”页面，点击对应接口后面的操作，进行接口 IPv4 地址配置。

图2 添加接口地址

(2) 配置静态路由

如图 3 所示，进入“网络配置>路由管理>静态路由”页面，点击<新建>添加一条缺省路由。

图3 添加路由

(3) 配置源 NAT

如图 4 所示，进入“策略配置>NAT 转换策略>源 NAT”页面，点击<新建>添加一条源 NAT，使内网地址访问外网做 NAT。

图4 配置源 NAT

(4) 配置 DNS 服务器

如图 5 所示，进入“网络配置>基础网络>DNS 服务>DNS 服务器”页面，勾选“启用 DNS 全局代理”，并配置 DNS 服务器地址，使其设备能够进行域名解析。

图5 配置 DNS 服务器

2. 升级特征库

(1) 升级 license

如图 6 所示，进入“系统管理>系统维护>授权管理”页面，点击<导入许可证>，将 license 文件信息复制到 license 栏点并击提交。

图6 导入许可证

(2) 升级特征库

如图 7 所示，进入“系统管理>系统维护>系统升级”页面，升级应用控制特征库，如果网络较好，可以直接连网点击立即升级，如果网络状况较差，可以将特征库文件下载到本地，进行本地导入升级。

图7 特征库升级

3. 配置 IPv4 审计策略

(1) 添加 IPv4 审计策略

如图 8 所示，进入“策略配置>IPv4 审计策略”页面，点击<新建>IPv4 审计策略，审计对象全选，点击提交。

图8 配置 IPV4 审计策略

4. 配置本地认证

(1) 配置地址对象

如图 9 所示，进入“策略配置>对象管理> 地址对象> IPv4 地址对象”页面，配置需要认证的网段地址，点击<提交>。

图9 配置认证地址对象

(2) 配置认证账号

如图 10 所示，进入“用户管理>用户组织结构”页面，选择新建认证账号，如添加测试认证账号分别为 test1，test2 等。

图10 添加认证账号

(3) 配置本地认证策略

如图 11 所示，进入“用户管理>认证管理>认证策略”页面，点击<新建>创建本地认证策略。

图11 添加本地认证策略

5. 配置无线非经

(1) 添加厂商配置

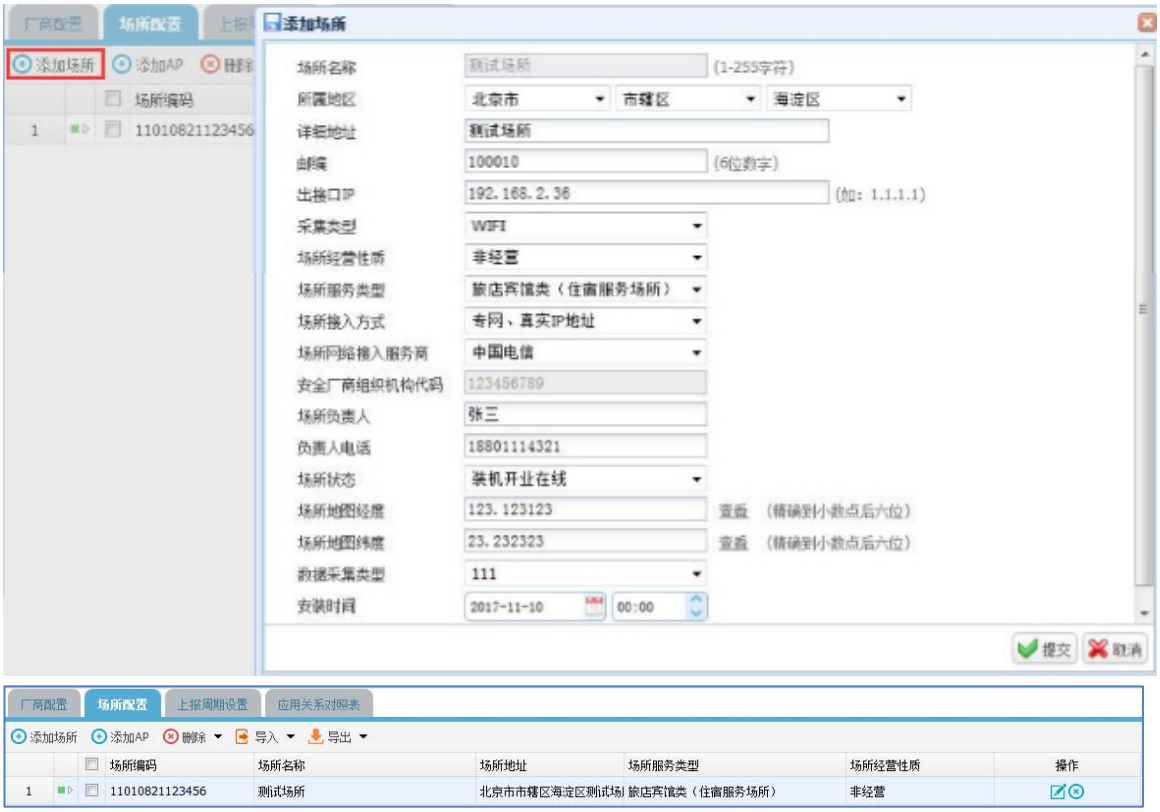
如图 12 所示，进入“系统管理>系统设定>无线非经>厂商配置”页面，对接厂商选择<派博>，其它信息根据要求进行配置，提交配置。

图12 添加厂商配置

(2) 添加场所配置

如图 13 所示，进入“系统管理>系统设定>无线非经>场所配置”页面，点击<添加场所>，将场所信息根据要求进行配置，提交配置。

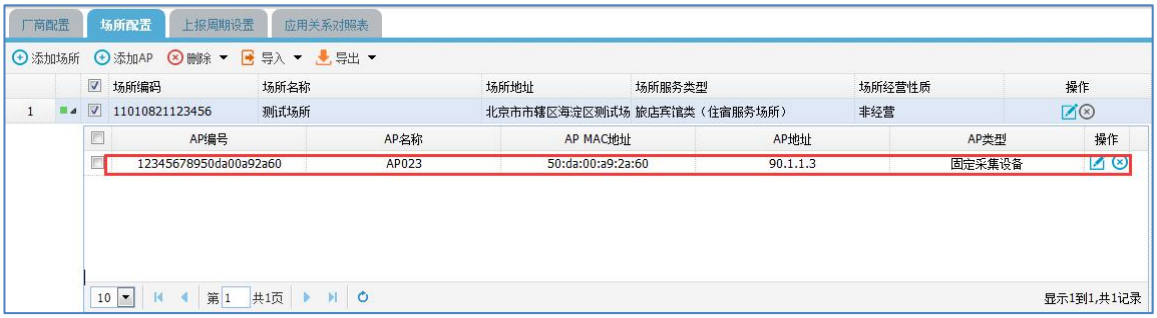
图13 添加场所配置



(3) 添加 AP 配置

如图 14 所示，进入“系统管理>系统设定>无线非经>厂商配置>场所配置”页面，勾选对应场所，并点击<添加 AP>，将 AP 信息根据要求进行配置，提交配置。

图14 添加 AP 配置



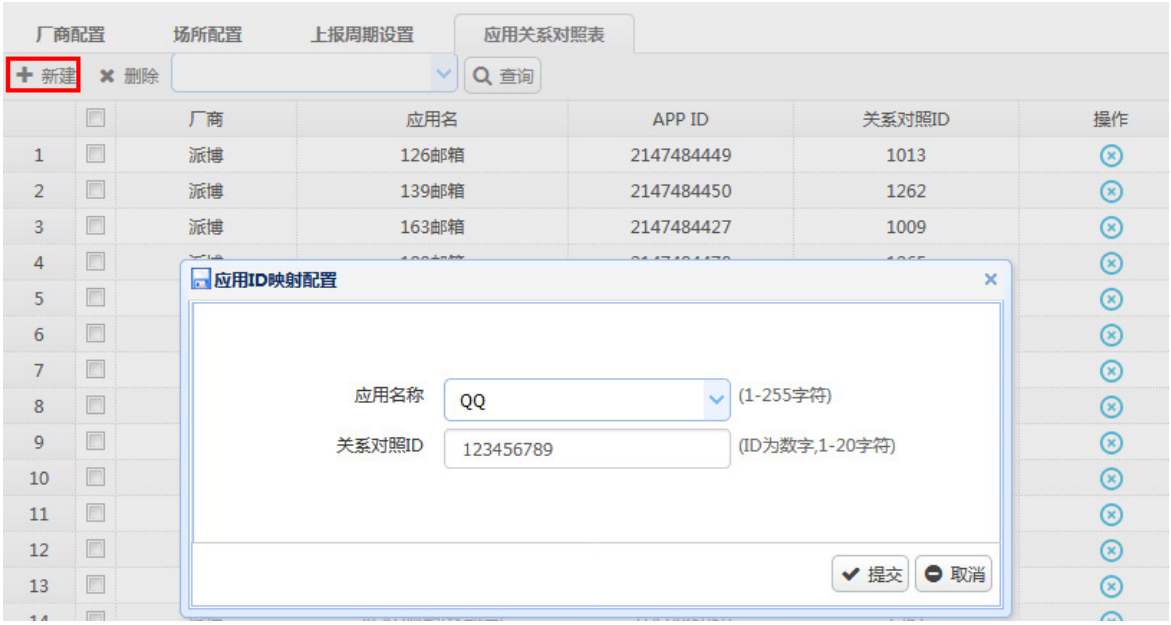
(4) 添加上报周期

如上图所示，进入“系统管理>系统设定>无线非经>厂商配置>上报周期设置”页面，点击<新建>，根据上报平台的要求配置上报周期，提交配置。派博对接平台上报周期为系统内置，不需要进行设定，其它厂商根据实际需要进行配置。

(5) 添加应用关系对照表

如图 15 所示，进入“系统管理>系统设定>无线非经>厂商配置>应用关系对照表”页面，点击<新建>，选择对应厂商及应用名称，并填上对照关系 ID，提交配置。

图15 添加应用关系对照表



3.1.5 配置注意事项

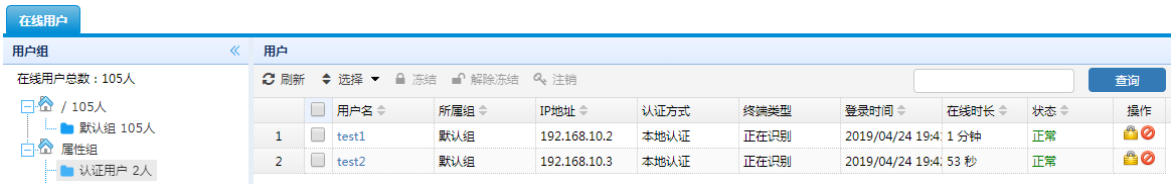
- 特征库在线升级必须要配置 DNS，否则在线升级不成功。
- 非经版本只记录认证用户上网产生的数据，匿名用户数据不记录。
- 对应厂商的应用关系对照表需要进行配置，如果没有，则对应的应用产生的审计数据不进行入库处理。

3.1.6 验证配置

1. 在线用户

如图 16 所示，内网用户访问外网需要先进行 web 认证，在“数据中心>系统监控>在线用户”页面，可以查看到本地认证的在线用户。

图16 本地认证用户



2. 审计日志

如图 17 所示，认证用户访问 IM 软件及社区网站有产生相应的审计日志信息。

图17 审计日志

IM聊天软件日志

查询 重置 **查询结果:** 在 2017-01-07 约 4 条日志记录中，从 1-4 搜索出相关结果 4 条，显示 1-4

	用户	用户mac	应用	账号	行为	处理动作	系统	终端	级别	时间
1	test2	80:be:05:4f:56:40	微信		收消息	放行	iPhone OS 10_2	iPhone	信息	2017-01-07 16:06:17
2	test2	80:be:05:4f:56:40	微信		登录	放行	iPhone OS 10_2	iPhone	信息	2017-01-07 16:06:15
3	test1	c4:07:2f:99:ac:1c	QQ(移动端)		登录	放行	Android 6.0	GEM-703L	信息	2017-01-07 16:04:13
4	test1	c4:07:2f:99:ac:1c	QQ(移动端)		登录	放行	Android 6.0	GEM-703L	信息	2017-01-07 16:02:18

社区日志

查询 重置 **查询结果:** 在 2017-01-07 约 4 条日志记录中，从 1-4 搜索出相关结果 4 条，显示 1-4

	用户	用户mac	应用	账号	行为	处理动作	内容	系统	终端	级别	时间
1	test1	c4:07:2f:99:ac:1c	西泰会馆自贡在线	-	发表	放行	怎么能这样呢？;;	Windows	PC	信息	2017-01
2	test1	c4:07:2f:99:ac:1c	西泰会馆自贡在线	better0903	登录	放行	-	Windows	PC	信息	2017-01
3	test2	80:be:05:4f:56:40	腾讯微博(iOS版)	2451584481	发表	放行	我回来了;;;	iPhone OS 10_2	iPhone	信息	2017-01
4	test2	80:be:05:4f:56:40	腾讯微博(iOS版)	2451584481	登录	放行	-	iPhone OS 10_2	iPhone	信息	2017-01

3. 日志上报

如图 18 所示，在测试平台上查看字段解析正常。

图18 非经日志上报

1	版本号	4.5	
2	事件类型	40	
3	文档版本号	4.3.1	
4	认证类型	1020001	
5	认证账号	test1	
6	登录身份类型	15	
7	登录身份账号	test1	
8	姓名/名称		
9	APP厂商名称		
10	APP应用名称		
11	APP版本号		
12	APP终端认证码		
13	场所编码	11010829123456	
14	场所类型	9	
15	终端上线时间	2017-01-07 16:01:35	
16	终端设备MAC	C4-07-2F-99-AC-1C	
17	内网IP地址	192.168.10.2	
18	源外网IPv4地址	192.168.2.36	
19	源外网IPv6地址		源外网IPv6地址不能为空
20	源外网IPv4起始端口号	38187	
21	源外网IPv4结束端口号	38187	

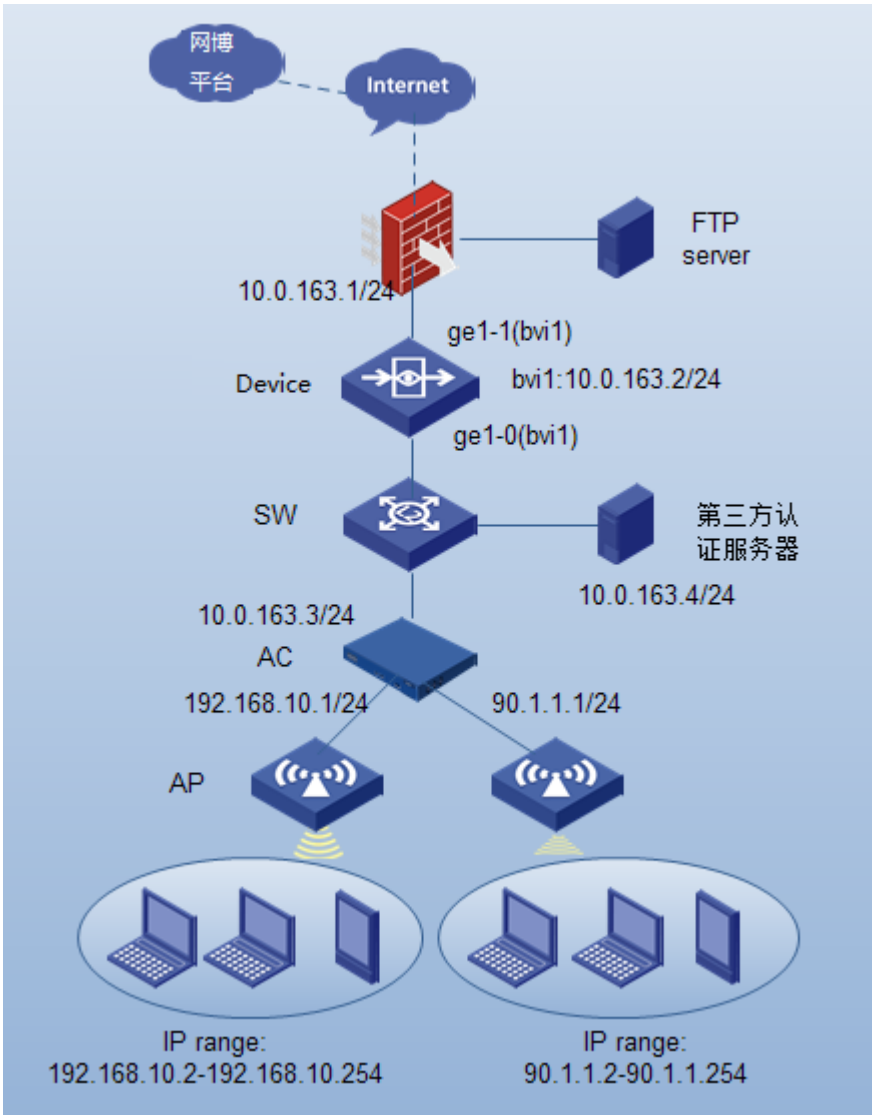
3.2 组网需求2：透明桥模式组网-网博平台对接

3.2.1 组网需求

如图 19 所示，某公司内网办公网段 IP 地址 90.1.1.0/24，其中 90.1.1.1/24 作为内网用户的网关。使用设备的的 ge1-0 和 ge1-1 接口作为透明桥，串接部署在网络中，设备上联出口 FW，下联二层交换机设备；并在 AC 设备上开启 AAA 认证功能，AC 设备只跑路由模式不做 NAT，认证服务器为第三方服务器，第三方服务器将用户上下线日志信息直接发给设备（注：设备不参与认证时，所有的用户信息需要设备与第三方认证服务器通过特定接口对接实现，如泰联和 IMC 服务器是通过 udp9999 端口将用户上下线信息发送至设备）。设备上开启审计和无线非经功能。具体应用需求如下：

- 设备上可以接收到第三方服务器发过来的用户上下线信息。
- 内网用户访问外网的流量通过设备处理上报至网博平台。

图19 透明桥模式组网



3.2.2 配置思路

- 网络基础配置，配置网桥、路由、DNS 等信息。
- 升级特征库。
- 配置 IPv4 审计策略。
- 配置无线非经功能，添加厂商、场所、AP 和上报周期等信息。

3.2.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.2.4 配置步骤

1. 网络基础配置

(1) 配置网桥接口及地址

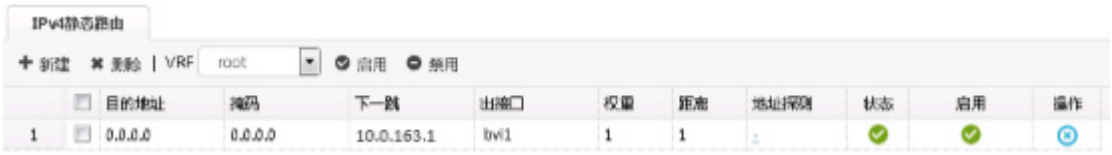
如图 20 所示，进入“网络配置>接口配置>网桥接口”页面，点击<新建>添加网桥，将需要的接口添加至网桥中，并配置网桥接口的 IPv4 地址配置。

图20 配置网桥接口

(2) 添加静态路由

如图 21 所示，进入“网络配置>路由管理>静态路由”页面，点击<新建>添加一条缺省路由。

图21 添加静态路由



(3) 配置 DNS 服务器

如图 22 所示，进入“网络配置>基础网络>DNS 服务>DNS 服务器”页面，勾选“启用 DNS 全局代理”，并配置 DNS 服务器地址，使其设备能够进行域名解析。

图22 配置 DNS 服务器

2. 升级特征库

(1) 升级 license

如图 23 所示，进入“系统管理>系统维护>授权管理”页面，点击<导入许可证>，将 license 文件信息复制到 license 栏点并击提交。

图23 导入许可证

(2) 升级特征库

如图 24 所示，进入“系统管理>系统维护>系统升级”页面，升级应用控制特征库，如果网络较好，可以直接联网点击立即升级，如果网络状况较差，可以将特征库文件下载到本地，进行本地导入升级。

图24 升级特征库

3. 配置 IPv4 审计策略

(1) 添加应用审计策略

如图 25 所示，进入“策略配置>IPv4 审计策略”页面，点击<新建>IPv4 审计策略，审计对象全选，点击提交。

图25 配置 IPv4 审计策略

4. 配置无线非经

(1) 添加厂商配置

如图 26 所示，进入“系统管理>系统设定>无线非经>厂商配置”页面，对接厂商选择<网博>，其它信息根据要求进行配置，提交配置。

图26 添加厂商配置

(2) 添加场所配置

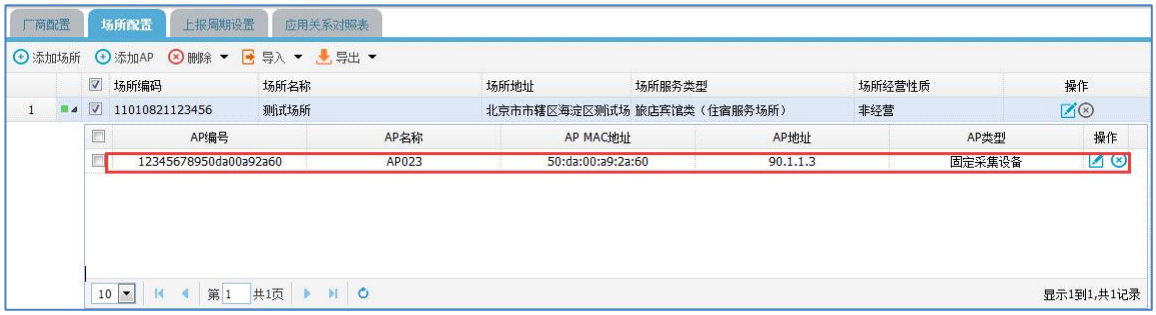
如图 27 所示，进入“系统管理>系统设定>无线非经>厂商配置>场所配置”页面，点击<添加场所>，将场所信息根据要求进行配置，提交配置。

图27 添加场所配置

(3) 添加 AP 配置

如图 28 所示，进入“系统管理>系统设定>无线非经>场所配置”页面，勾选对应场所，并点击<添加 AP>，将 AP 信息根据要求进行配置，提交配置。

图28 添加 AP 配置



(4) 添加上报周期

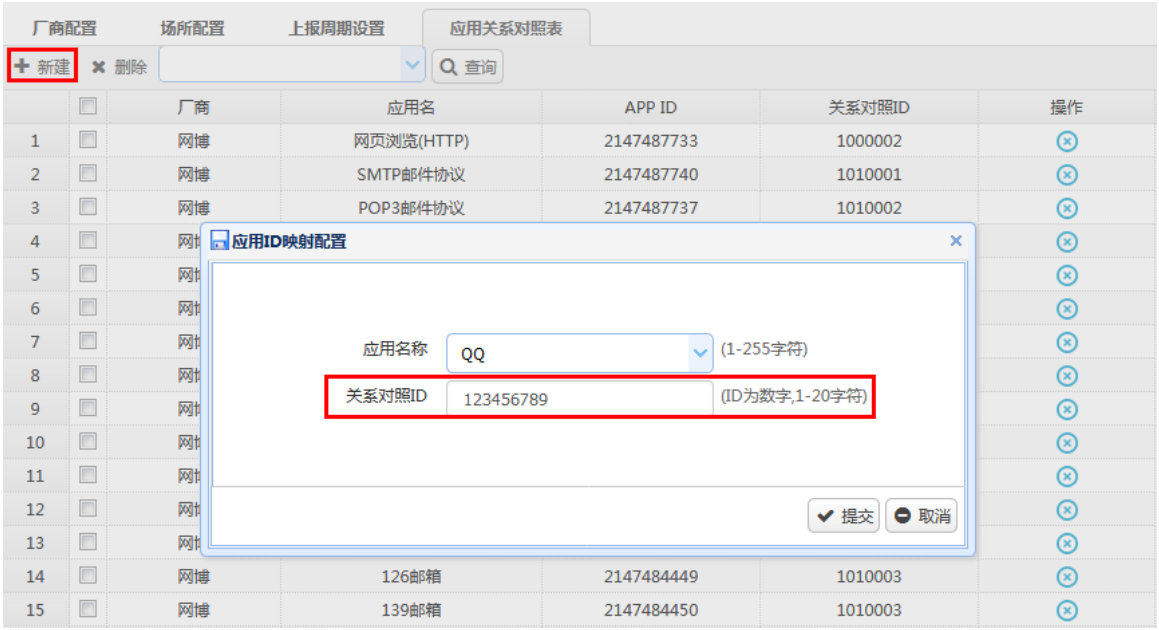
如图 29 所示，进入“系统管理>系统设定>无线非经>厂商配置>上报周期设置”页面，点击<新建>，根据上报平台的要求配置上报周期，提交配置。

图29 添加上报周期

(5) 添加应用关系对照表

如图 30 所示，进入“系统管理>系统设定>无线非经>应用关系对照表”页面，点击<新建>，选择对应厂商及应用名称，并填上对照关系 ID，提交配置。

图30 添加应用关系对照表



3.2.5 配置注意事项

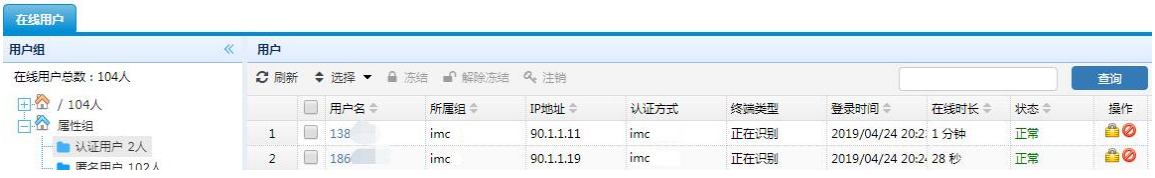
- 第三方服务器与设备必须能够连通，否则设备无法收取到第三方服务器发送的用户认证上下线信息。
- 设备必须配置 DNS 和路由，特征库才能在线升级。
- 非经版本只记录认证用户上网产生的数据，匿名用户数据不记录。
- 对应厂商的应用关系对照表需要进行配置，如果没有，则对应的应用产生的审计数据不进行入库处理。

3.2.6 验证配置

1. 在线用户

如图 31 所示，第三方服务器可以向设备发送用户认证上下线日志信息

图31 在线用户



2. 审计日志

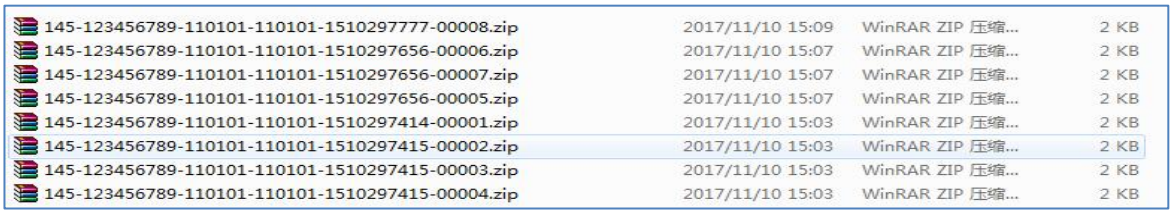
如图 32 所示，认证用户访问外网的流量经过设备，设备可以对流量进行识别并审计。

图32 审计日志

3. 日志上报

如图 33 所示，在 FTP 服务器上可以查看到非经日志上报正常，且字段获取数据正常。

图33 日志上报



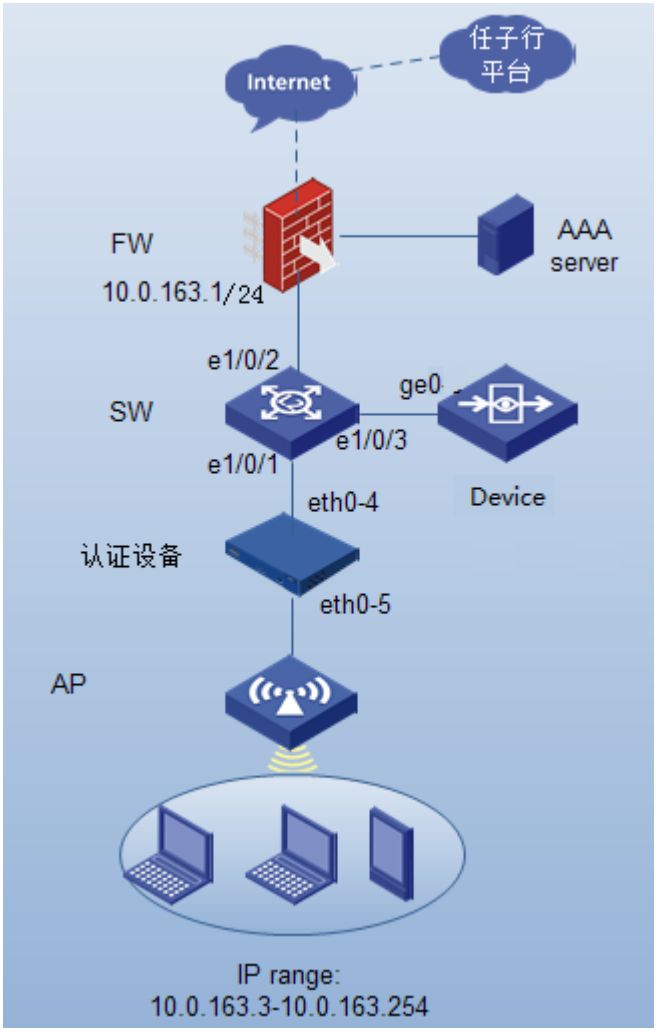
3.3 组网需求3：旁路模式组网-任子行平台对接

3.3.1 组网需求

如图 34 所示，某公司内网无线办公网段 IP 地址 10.0.163.0/24，其中网关为 10.0.163.1。内网用户访问外网开启 AAA 认证功能，并将认证及上网流量通过旁路镜像方式镜像至设备上，设备上开启审计和无线非经功能。具体应用需求如下：

- AAA 认证交互报文镜像至设备，设备可以监听到用户认证上下线信息。
- 内网用户访问外网的流量镜像至设备，设备处理完数据上报至任子行平台。

图34 旁路模式组网图



3.3.2 配置思路

- 网络基础配置，配置旁路接口、路由、DNS 等信息。
- 升级特征库。
- 配置 IPV4 审计策略。
- 配置无线非经功能，添加厂商、场所、AP 和上报周期等信息。

3.3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

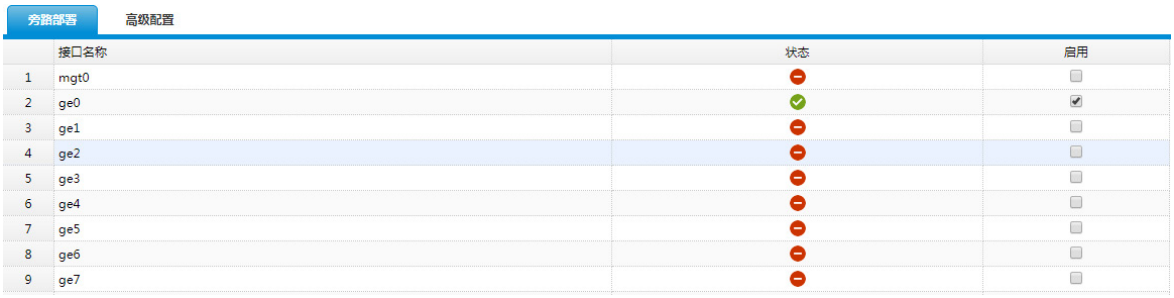
3.3.4 配置步骤

1. 网络基础配置

(1) 配置旁路接口

如图 35 所示，进入“网络配置>基础网络>部署方式>旁路部署”页面，启用对应的物理接口为旁路口。

图35 添加旁路接口



(2) 添加静态路由

如图 36 所示，进入“网络配置>路由管理>静态路由”页面，点击<新建>添加一条缺省路由。

图36 添加静态路由

(3) 配置 DNS 服务器

如图 37 所示，进入“网络配置>基础网络>DNS 服务>DNS 服务器”页面，勾选“启用 DNS 全局代理”，并配置 DNS 服务器地址，使其设备能够进行域名解析。

图37 配置 DNS 服务器

2. 升级特征库

(1) 升级 license

如图 38 所示，进入“系统管理>系统维护>授权管理”页面，点击<导入许可证>，将 license 文件信息复制到 license 栏点并击提交。

图38 导入许可证

(2) 升级特征库

如图 39 所示，进入“系统管理>系统维护>系统升级”页面，升级应用控制特征库，如果网络较好，可以直接联网点击立即升级，如果网络状况较差，可以将特征库文件下载到本地，进行本地导入升级。

图39 升级特征库

3. 配置 IPv4 审计策略

(1) 添加 IPv4 审计策略

如图 40 所示，进入“策略配置>IPv4 审计策略”页面，点击<新建>IPv4 审计策略，审计对象全选，点击提交。

图40 配置 IPV4 审计策略

4. 配置无线非经

(1) 添加厂商配置

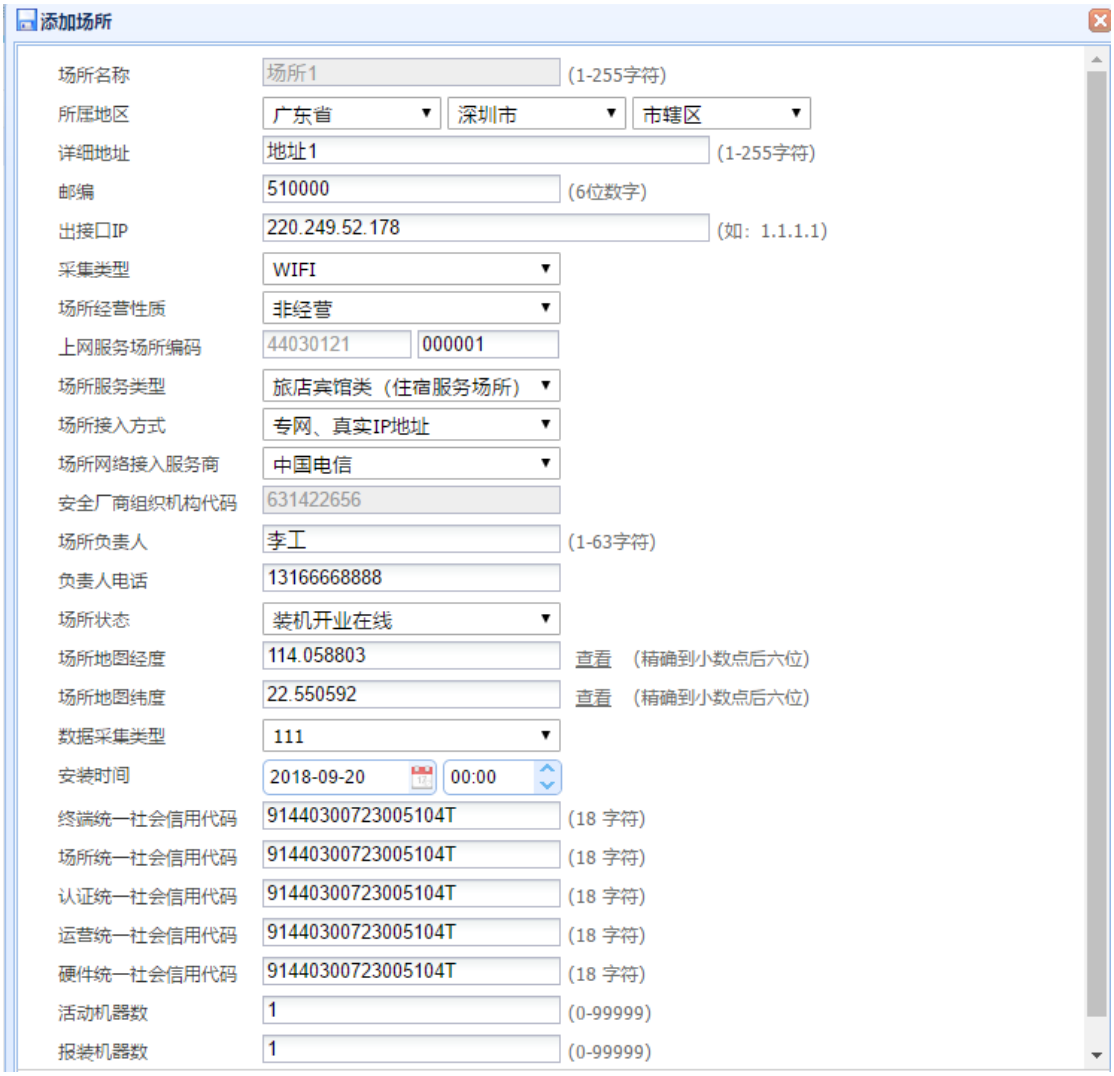
如图 41 所示，进入“系统管理>系统设定>无线非经>厂商配置”页面，对接厂商选择<任子行>，其它信息根据要求进行配置，提交配置。

图41 添加厂商配置

(2) 添加场所配置

如图 42 所示，进入“系统管理>系统设定>无线非经>厂商配置>场所配置”页面，点击<添加场所>，将场所信息根据要求进行配置，提交配置。

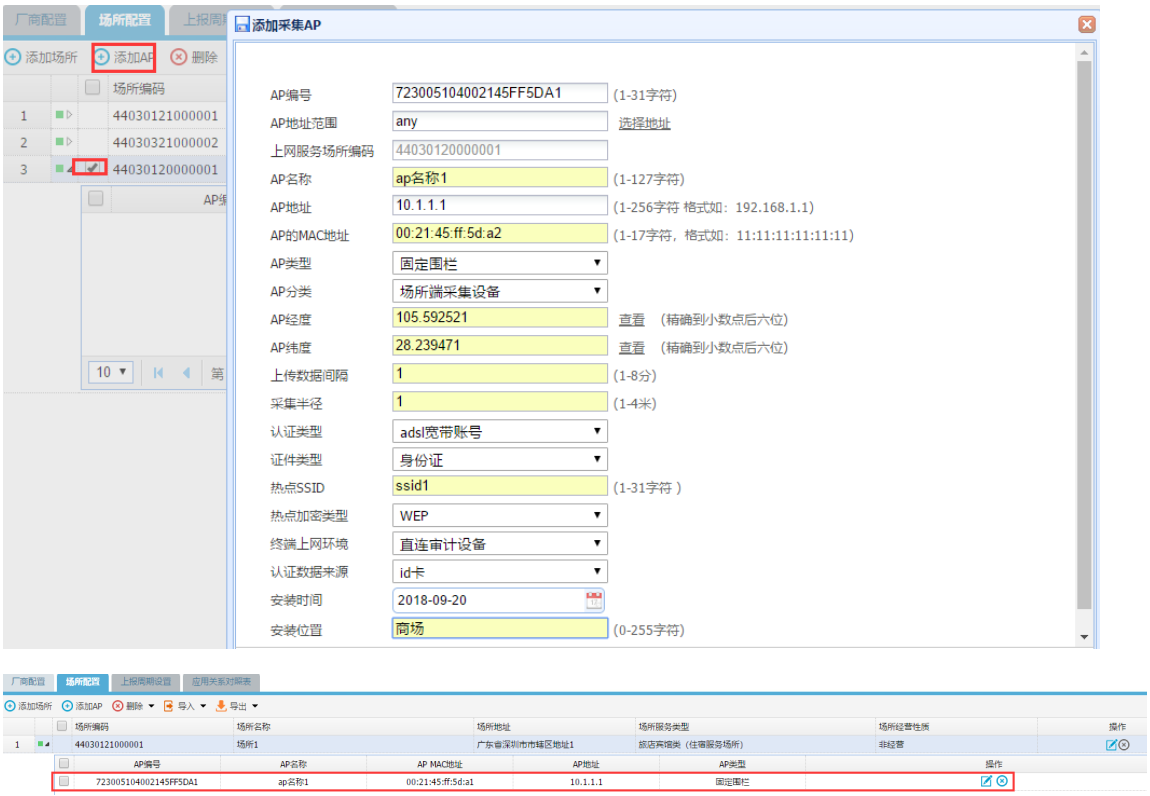
图42 添加场所配置



(3) 添加 AP 配置

如图 43 所示，进入“系统管理>系统设定>无线非经>场所配置”页面，勾选对应场所，并点击<添加 AP>，将 AP 信息根据要求进行配置，提交配置。

图43 添加 AP 配置



(4) 添加上报周期

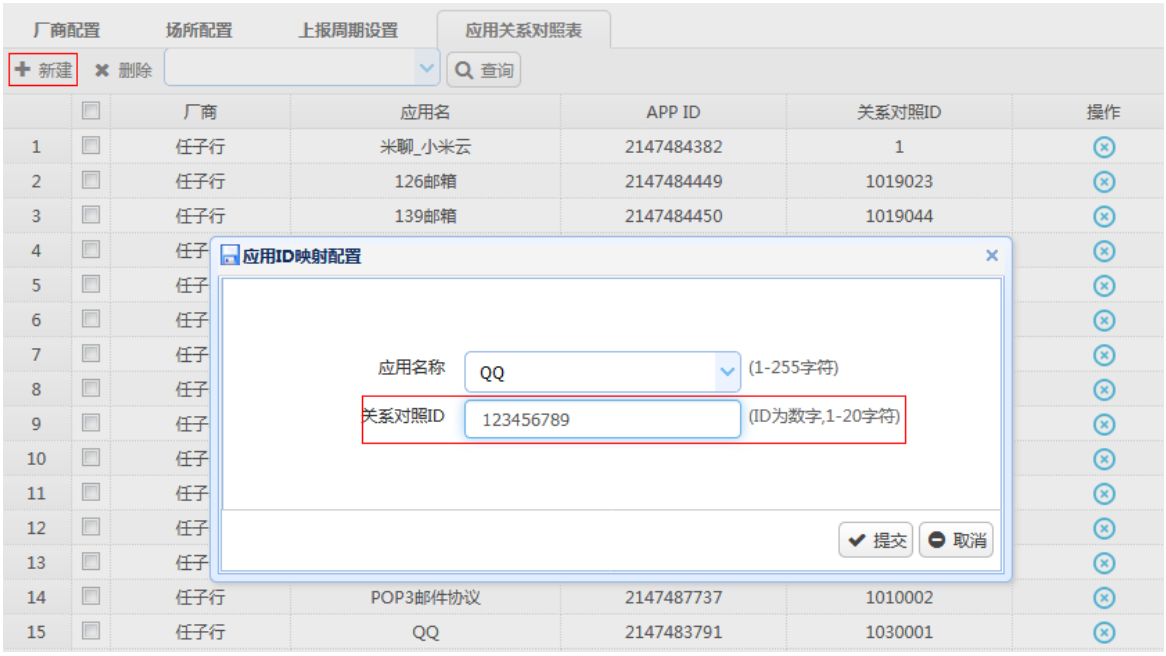
如图 44 所示，进入“系统管理>系统设定>无线非经>厂商配置>上报周期设置”页面，点击<新建>，根据上报平台的要求配置上报周期，提交配置。

图44 添加上报周期

(5) 添加应用关系对照表

如图 45 所示，进入“系统管理>系统设定>无线非经>应用关系对照表”页面，点击<新建>，选择对应厂商及应用名称，并填上对照关系 ID，提交配置。

图45 添加应用关系对照表



3.3.5 配置注意事项

- 用户认证上下线信息报文必须镜像到设备上。
- 设备必须配置 DNS 和路由，特征库才能在线升级。
- 上网流量必须双向镜像至设备上，镜像一个方向的流量至设备，可能会导致部分应用识别不完全，无法审计到需要的信息。
- 对应厂商的应用关系对照表需要进行配置，如果没有，则对应的应用产生的审计数据不进行入库处理。

3.3.6 验证配置

1. 在线用户

如图 46 所示，通过将 Radius 报文镜像至设备上，设备可以获取到认证用户的上下线信息。

图46 在线用户

2. 审计日志

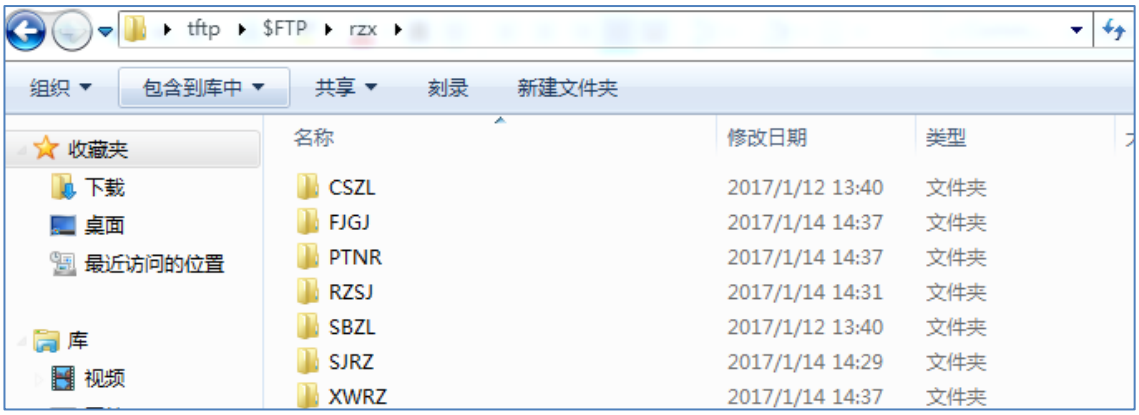
如图 47 所示，认证用户访问外网的流量能够被识别并审计。

图47 审计日志

3. 日志上报

如图 48 所示，在设备串口上可以通过命令 display wireless-count 查看上报统计计数，FTP 服务器上可以查看到非经日志上报正常。

图48 日志上报



3.4 无线非经日志上报原则

3.4.1 日志上报原则

日志上报原则是根据不同厂商的要求，组织对应的字段进行上报，上报方式也按厂商要求进行上报。不同厂商日志上报传输方式及生成日志类型如下所示：

对接平台	日志上报传输方式	日志上报类型
任子行	通过ftp方式传输	7类，分别为CSZL\SBZL\FJGJ\RZSJ\SJRZ\XWRZ\PTNR 其中CSZL\SBZL是通过页面配置场所资料和AP配置进行上报的，其它日志是通过入库的数据表中获取相关字段进行上报
派博	通过tcp、udp方式传输	3类，tcp18590传输用户上下线日志（包括认用户和虚拟用户） udp19590传输上网日志

对接平台	日志上报传输方式	日志上报类型
网博	通过ftp方式传输	8类，分别为上下线日志\虚拟身份日志\上网日志\网站访问日志\厂商日志\场所资料日志\场所状态日志\设备资料日志，其中厂商日志，场所资料日志，场所状态日志，设备资料日志是通过页面配置进行上报的，其它日志是通过入库的数据表中获取相关字段进行上报

目 录

1 DHCP

1.1 DHCP简介

随着网络规模的扩大和网络复杂度的提高，网络配置越来越复杂，经常出现计算机位置变化（如便携机或无线网络）和计算机数量超过可分配的 IP 地址的情况。DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）就是为满足这些需求而发展起来的。

与 BOOTP 相比，DHCP 也采用客户/服务器通信模式，由客户端向服务器提出配置申请（包括分配的 IP 地址、子网掩码、缺省网关等参数），服务器根据策略返回相应配置信息，两种协议的报文都采用 UDP 进行封装，并使用基本相同的报文结构。BOOTP 运行在相对静态（每台主机都有固定的网络连接）的环境中，管理员为每台主机配置专门的 BOOTP 参数文件，该文件会在相当长的时间内保持不变。

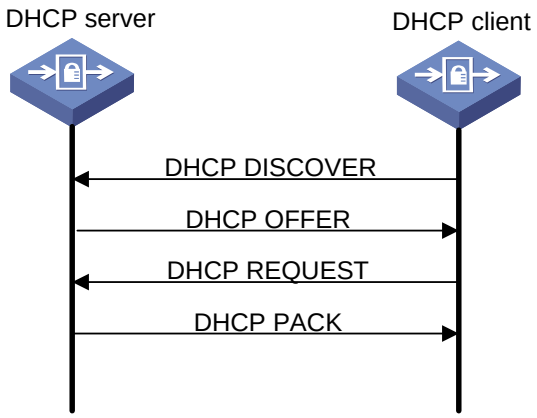
DHCP 从两方面对 BOOTP 进行了扩展：DHCP 可使计算机仅用一个消息就获取它所需要的所有配置信息；DHCP 允许计算机快速、动态地获取 IP 地址，而不是静态为每台主机指定地址。

1.1.1 DHCP Server

设备可以作为 DHCP Server，用于实现对网络中 IP 地址的动态分配和集中管理。动态分配是指当 DHCP 客户端第一次从 DHCP Server 租用到 IP 地址后，并非永久的使用该地址，只要租约到期，客户端就要释放(Release)这个 IP 地址以给其它工作站使用。为了实现 IP 地址的动态分配，必须设置 DHCP Server 拥有一个 IP 地址范围，用来分配给用户，这个用来分配给客户端的地址范围也叫 IP 地址池（IP Pool）。

如图 1 反映了 DHCP 客户端从 DHCP Server 申请 IP 地址的过程。

图1 DHCP 服务器原理图



当客户端第一次登录到网络时，它会向网络广播一个 DHCP DISCOVER 消息，此时由于客户端还不知道自己属于哪一个网路，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。

由于网络上可能不止一个 DHCP Server，凡是具有有效 IP 地址信息的 DHCP Server 均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。

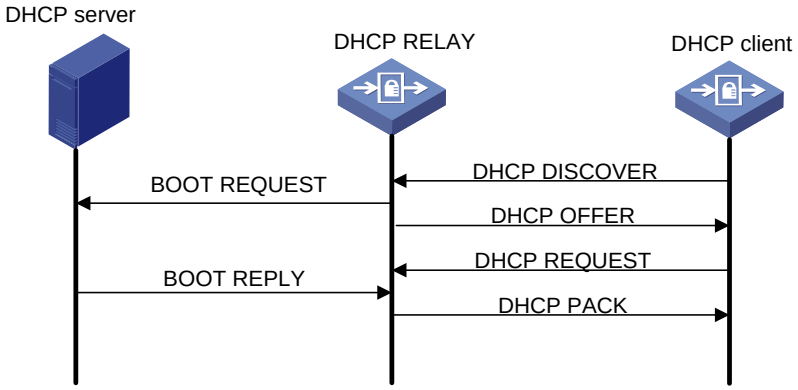
客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP Server 响应该消息，确认已接受请求并开始租用。

客户端收到确认后开始使用此地址。

1.1.2 DHCP 中继代理(Relay)

DHCP 中继代理是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP 中继代理存在的原因是因为 DHCP 客户端还没有 IP 环境设定，这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。当然也可以在每一个网段之中安装 DHCP Server 但这样的话设备成本会增加而且管理上面也比较分散。DHCP 中继代理的工作原理如图 2 所示。

图2 DHCP 代理原理图



1.2 DHCP服务

通过菜单“网络配置 > 基础网络 > DHCP 服务”，进入如图 3 所示页面。在该页面上，可以“编辑”，设置各个接口下的 DHCP 服务类型。

图3 DHCP 服务页面

点击<编辑>按钮，进入如图 4 所示的页面，进行接口下 DHCP 服务类型的配置。各个配置项的含义如表 1 所示。

图4 接口 DHCP 服务类型配置页面

表1 DHCP 服务配置项含义描述表

标题项	说明
接口名称	配置DHCP服务的接口名称
空	接口不启用任何DHCP服务
DHCP中继代理	接口启用DHCP中继代理服务
DHCP服务器	接口启用DHCP服务器服务
服务器IP	接口启用DHCP RELAY服务后，DHCP服务器的IP地址

1.3 DHCP服务器

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 服务器”，进入如图 5 所示页面。在该页面上可以新建、编辑、删除、浏览 DHCP 服务器的配置。

图5 服务器页面

点击页面上的<新建>按钮，可以新建 DHCP 服务器配置。新建页面如图 6 所示。各个配置项的含义如表 2 所示。

图6 DHCP 服务器配置

表2 DHCP 服务器配置项含义描述表

标题项	说明
名称	DHCP服务器配置名称
子网/掩码	DHCP服务器的子网和掩码
网关	DHCP服务器的网关
IP地址开始	DHCP服务器地址池的开始地址
IP地址结束	DHCP服务器地址池的结束地址
租约	DHCP服务器分配的地址的租约时间 • 无限：DHCP 服务器分配的 IP 地址永久有效 • 有限期：配置有效时间，该时间内 DHCP 服务器分配的 IP 地址有效

标题项	说明
DNS1	DHCP服务器的主DNS
DNS2	DHCP服务器的备DNS
Wins1	DHCP服务器的主Wins
Wins2	DHCP服务器的备Wins
域	DHCP服务器的域名
AC	DHCP option43字段中的AC的ip地址，可配置2两个

点击<提交>按钮，提交配置。提交配置后可在如图 7 所示的页面上查看配置的 DHCP 服务器信息。

图7 DHCP 服务器概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.4 排除范围

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 排除范围”，进入如图 8 所示页面。在该页面上可以新建、编辑、删除、浏览排除范围的配置。

图8 排除范围页面

点击页面上的<新建>按钮，可以新建排除范围配置。新建页面如图 9 所示。各个配置项的含义如表 3 所示。

图9 新建排除范围页面

表3 排除范围各个配置项的含义描述表

标题项	说明
起始IP	排除范围的起始IP地址
结束IP	排除范围的结束IP地址

点击<提交>，提交配置。提交配置后可在如图 10 所示的页面上查看配置的排除范围信息。

图10 排除范围页面概览

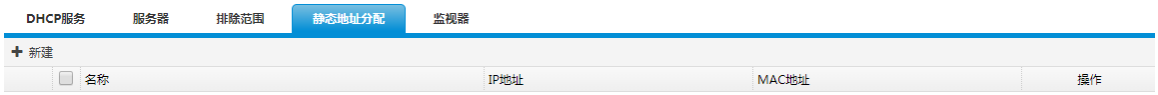
点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.5 静态地址分配

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 静态地址分配”，进入如图 11 所示页面。在该页面上可以新建、编辑、删除、浏览 IP-MAC 绑定的配置。

图11 静态地址分配



点击页面上的<新建>按钮，可以新建静态地址分配的配置。新建页面如图 12 所示。各个配置项的含义如表 4 所示。

图12 新建 IP-MAC 绑定页面

表4 IP-MAC 绑定各个配置项的含义描述表

标题项	说明
名称	IP-MAC绑定配置的名称，可输入1到31个字符
IP地址	IP-MAC绑定的IP地址
MAC地址	IP-MAC绑定的MAC地址

点击<提交>按钮，提交配置。提交配置后可在如图 13 所示的页面上查看配置的 IP-MAC 绑定信息。

图13 静态地址分配页面概览

点击<编辑>按钮，可对选中条目进行编辑。

点击<删除>按钮，可对选中条目进行删除。

1.6 监视器

通过菜单“网络配置 > 基础网络 > DHCP 服务 > 监视器”，进入如图 14 所示页面。在该页面上可以查看 IP 地址的分配使用情况。表中各项的含义如表 5 所示。

图14 监视器页面

表5 监视器各项含义描述表

标题项	说明
IP地址	已分配正在使用的IP地址
MAC地址	已分配正在使用的IP地址对应的MAC地址
开始时间	已分配正在使用的IP地址的开始使用时间
结束时间	已分配正在使用的IP地址的回收时间

点击<清除>按钮，可以清除已分配的 IP 地址。

1.7 DHCP典型配置举例

1.7.1 DHCP Server 典型配置举例

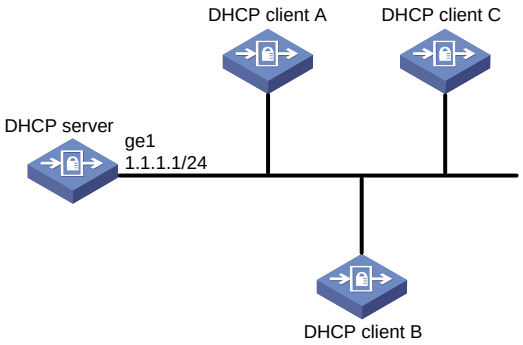
1. 组网需求

客户端通过 DHCP Server 获取动态 IP 地址。

- DHCP 客户端和设备在同一局域网内。
- DHCP 客户端启用自动获取 IP 地址。

2. 组网图

图15 DHCP Server 组网图



1.8 使用版本

本举例是在 E6442 版本上进行配置和验证的。

1. 配置步骤

(1) 按照组网图组网。

(2) 设备接口配置为 DHCP Server。如图 16 所示。

图16 接口 ge1 配置为 DHCP SERVER

	接口	服务	中继服务器地址	操作
1	ge0	无		
2	ge1	DHCP服务器		
3	ge3	无		
4	ge4	无		
5	ge5	无		
6	ge6	无		
7	ge7	无		
8	ge8	无		
9	agg0	无		
10	ge1.1	无		
11	bvi0	无		

(3) 配置 DHCP Server。如图 17 所示。

图17 配置 DHCP 地址池

点击<提交>按钮，提交配置。

2. 验证配置

配置完成后，在 PC 上查看 IP 地址获取情况，看到 PC 获取到 IP 地址为 1.1.1.2，DNS 为 8.8.8.8 和 8.8.4.4。

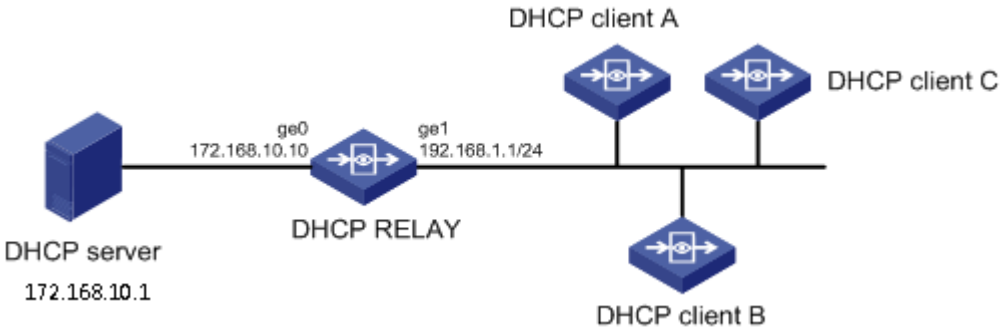
1.8.2 DHCP RELAY 典型配置举例

1. 组网需求

客户端通过 DHCP RELAY 获取动态 IP 地址。

- PC 和设备在同一局域网内。
- PC 启用自动获取 IP 地址。
- 设备所在的另一网段内存在有 DHCP Server。

图18 DHCP RELAY 组网图



1.9 使用版本

本举例是在 E6442 版本上进行配置和验证的。

1. 配置步骤

(1) 按照组网图组网。

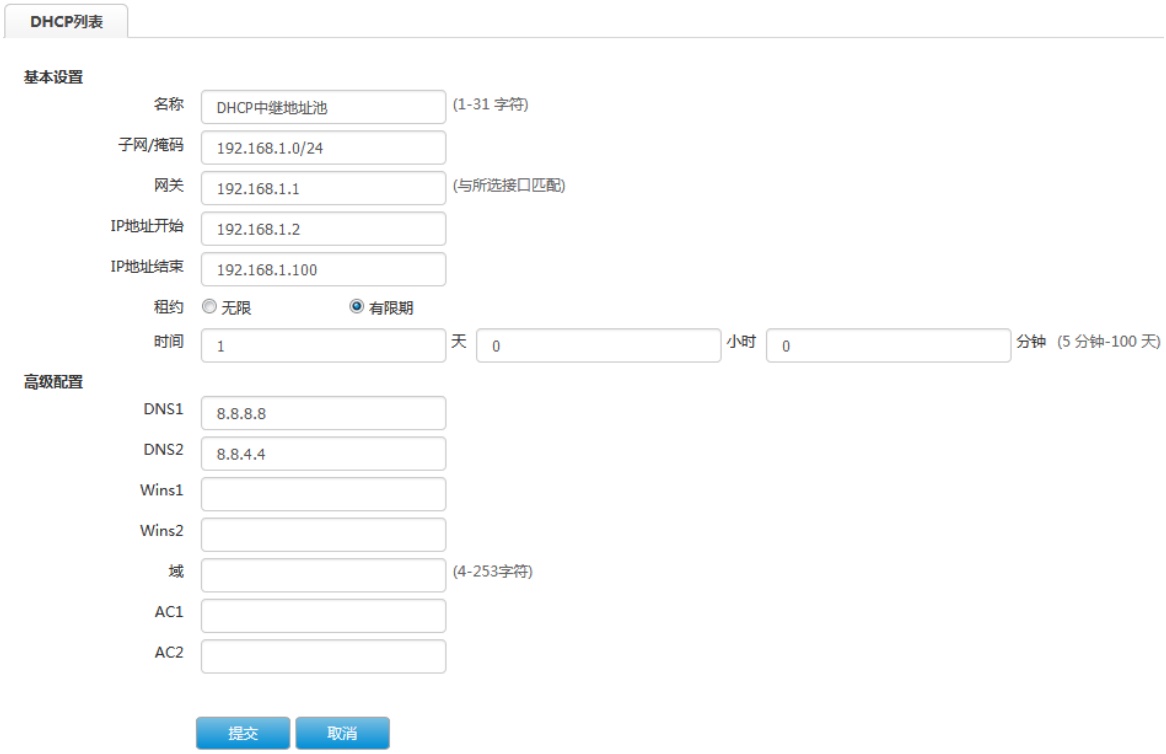
(2) 配置 DHCP server 端。

DHCP SERVER 配置页面。如图 19。

图19 DHCP SERVER 配置

DHCP RELAY 配置页面。如图 20 所示。（中继环境下 DHCPserver 的地址池网关需要写 DHCP 中继的入接口地址。）

图20 DHCP RELAY 配置界面



DHCP SERVER 设备静态路由配置页面。如图 21 所示。（DHCPserver 回指一条到中继 DHCPserver 的地址池的静态路由。）

图21 DHCP server 设备静态路由配置页面

(3) 设备配置为 DHCP RELAY。如图 22 所示。

图22 DHCP RELAY 配置页面

点击<提交>，提交配置。

2. 验证配置

配置完成后，在 PC 上查看 IP 地址获取情况，看到 PC 获取到由 DHCP Server 分配的 IP 地址，及 DNS。

目 录

1 简介

通用路由封装（GRE）定义了在任意一种网络层协议上封装任意一个其它网络层协议的协议，通过创建一条点到点的 tunnel 来完成二次封装数据的转发，且 GRE 隧道只支持点到点的业务接入。

GRE 是三层的隧道协议，它利用一种协议的传输能力为另一种协议建立了点到点的隧道，被封装的报文将在隧道的两端进行封装和解封装。使用 GRE 协议可以与对端网关设备建立虚拟的、点对点通信，GRE 仅对报文进行封装而不加密。

简单说，GRE 的是将 3 层报文封装到 IP 报文里，送到 tunnel 对端后再解开的技术。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 GRE 特性。

3 使用限制

无。

4 GRE over IPSec 配置举例

4.1 组网需求

设备 A 和设备 B 之间建立 GRE 隧道 Tunnel0，Tunnel0 的网段为 172.16.1.0/24。另外，我们还需要在 GRE 隧道上运行动态路由协议 OSPF，使设备 A 和设备 B 彼此通过动态路由协议学习到对方站点身后网络路由（1.1.1.0/24 和 2.2.2.0/24）。最后配置 IPSec VPN，以对两个站点间的 GRE 流量进行加密。

4.2 配置思路

(1) 配置网络接口；

(2) 配置 GRE 隧道；

(3) 配置动态路由协议 OSPF；

(4) 配置 IPSec VPN 保护站点间 GRE 流量；

(5) 在 GRE 隧道中指定下一跳；

(6) 配置 GRE 路由。

4.3 使用版本

本举例是在 E6442 及以上版本进行配置和验证的。

4.4 配置步骤

(1) 基本网络配置

设备 A：

```
host(config)# interface ge2
host(config-ge2)#ip address 202.100.1.1/24
host(config-ge2)# allow access all
host(config)# interface lo0
host(config-lo0)#ip address 1.1.1.1/24
host(config-lo0)## allow access all
host(config)#ip route 0.0.0.0/0 202.100.1.10
```

Internet：

```
host(config)# interface ge3
host(config-ge3)#ip address 202.100.1.10/24
host(config-ge3)# allow access all
host(config)# interface ge4
host(config-ge4)#ip address 61.128.1.10/24
host(config-ge4)# allow access all
```

设备 B：

```
host(config)# interface ge2
host(config-ge2)#ip address 61.128.1.1/24
host(config-ge2)# allow access all
host(config)# interface lo0
host(config-lo0)#ip address 2.2.2.1/24
host(config-lo0)## allow access all
host(config)#ip route 0.0.0.0/0 61.128.1.10
```

(2) 配置 GRE 隧道

配置设备 A 的 GRE 隧道：

```
host(config)# interface tunnel 0 mode gre
host(config-tunnel0)#ip address 172.16.1.1/24
host(config-tunnel0)#tunnel source 202.100.1.1
host(config-tunnel0)#tunnel destination 61.128.1.1
host(config-tunnel0)#allow access all
```

配置设备 B 的 GRE 隧道：

```
host(config)# interface tunnel 0 mode gre
host(config-tunnel0)#ip address 172.16.1.2/24
host(config-tunnel0)#tunnel source 61.128.1.1
host(config-tunnel0)#tunnel destination 202.100.1.1
host(config-tunnel0)#allow access all
```

(3) 配置动态路由协议 OSPF

配置设备 A 的动态路由协议 OSPF：

```
host(config)# router ospf
host(config-ospf)# network 172.16.1.0/24 area 0
host(config-ospf)# network 1.1.1.0/24 area 0
```

配置设备 B 的动态路由协议 OSPF：

```
host(config)# router ospf
host(config-ospf)# network 172.16.1.0/24 area 0
host(config-ospf)# network 2.2.2.0/24 area 0
```

(4) 配置 IPSec VPN 保护站点间 GRE 流量

设备 A 一阶段：

```
host# configure terminal
host(config)# vpn ipsec phase1
host(config-phase1)# edit gateway ph1
host(config-phase1-ph1)# set mode main
host(config-phase1-ph1)# set remotegw 61.128.1.1
host(config-phase1-ph1)# authentication pre-share
host(config-phase1-ph1)# set preshared-key 123456
host(config-phase1-ph1)# lifetime 86400
host(config-phase1-ph1)# set dpd retry 5
host(config-phase1-ph1)# set nat 10
host(config-phase1-ph1)# group 1
host(config-phase1-ph1)# set policy 1
host(config-phase1-ph1-policy1)# encrypt 3des
host(config-phase1-ph1-policy1)# hash md5
host(config-phase1-ph1-policy1)# exit
host(config-phase1-ph1)# exit
host(config-phase1)# exit
```

设备 A 二阶段：

```
host(config)# vpn ipsec phase2
host(config-phase2)# edit tunnel ph2

host(config-phase2-ph2)# set peer ph1
host(config-phase2-ph2)# mode tunnel
host(config-phase2-ph2)# set proposal
host(config-phase2-ph2)# set peer ph1
host(config-phase2-ph2)# mode tunnel
```

```
host(config-phase2-ph2)# set proposal1 esp-3des-md5 ah-null
host(config-phase2-ph2)# exit
```

设备 A 加密隧道：

```
host(config)# interface tunnel 1 mode ipsec
host(config-tunnel1)#tunnel-ipsec ph2
host(config-tunnel1)#tunnel-ipsec interested-subnet pair 202.100.1.1/24 61.128.1.1/24
```

设备 B 一阶段：

```
host# configure terminal
host(config)# vpn ipsec phase1
host(config-phase1)# edit gateway ph1
host(config-phase1-ph1)# set mode main
host(config-phase1-ph1)# set remotegw 202.100.1.1
host(config-phase1-ph1)# authentication pre-share
host(config-phase1-ph1)# set preshared-key 123456
host(config-phase1-ph1)# lifetime 86400
host(config-phase1-ph1)# set dpd retry 5
host(config-phase1-ph1)# set nat 10
host(config-phase1-ph1)# group 1
host(config-phase1-ph1)# set policy 1
host(config-phase1-phypt 1-policy1)# encr 3des
host(config-phase1-ph1-policy1)# hash md5
host(config-phase1-ph1-policy1)# exit
host(config-phase1-ph1)# exit
host(config-phase1)# exit
```

设备 B 二阶段：

```
host(config)# vpn ipsec phase2
host(config-phase2)# edit tunnel ph2
host(config-phase2-ph2)# set peer ph1
host(config-phase2-ph2)# mode tunnel
host(config-phase2-ph2)# set proposal1 esp-3des-md5 ah-null
host(config-phase2-ph2)# exit
```

设备 B 加密隧道：

```
host(config)# interface tunnel 1 mode ipsec
host(config-tunnel1)#tunnel-ipsec ph2
host(config-tunnel1)#tunnel-ipsec interested-subnet pair 61.128.1.1/24 202.100.1.1/24
```

(5)　在 GRE 隧道中指定下一跳

设备 A：

```
host(config)# interface tunnel 0 mode gre
host(config-tunnel0)#next-tunnel tunnel 1
```

设备 B:

```
host(config)# interface tunnel 0 mode gre
host(config-tunnel0)#next-tunnel tunnel 1
```

(6)　配置 GRE 路由

配置设备 A 的 GRE 路由：

```
host(config)# ip route 2.2.2.0/24 tunnel0
```

配置设备 B 的 GRE 路由：

```
host(config)# ip route 1.1.1.0/24 tunnel0
```

4.5 验证配置

4.5.1 查看设备 A 的 GRE 接口状态

host(config)# display interface tunnel0

---

interface tunnel1

description:

Admin UP　Link UP

kernel ID: 35

MTU: 1476

IP address: 172.16.1.1/24

tunnel mode: gre

tunnel source addr: 202.100.1.1 (ge2)

tunnel destination addr: 161.128.1.1

4.5.2 查看设备 B 的 GRE 接口状态

host(config)# display interface tunnel0

---

interface tunnel1

description:

Admin UP　Link UP

kernel ID: 35

MTU: 1476

IP address: 172.16.1.2/24

tunnel mode: gre

tunnel source addr: 161.128.1.1 (ge2)

tunnel destination addr: 202.100.1.1

4.5.3 查看设备 B 的 GRE 隧道口流量转发

host# display statistics interface

```
2051-HA-zhu:WD-D(config)#  end
2051-HA-zhu:WD-D# display statistics interface
-------------------------------------------------------------------------------------------------------
Interface                RXPKTS          RXOCTS     RXbps          TXPKTS          TXOCTS     TXbps
-------------------------------------------------------------------------------------------------------
dc0                    87964700       6470524536   51.86K          151203        15127067         0
ge0                 17009452729    1163703283693    3.47M     12240825713    6625780856988    28.12M
ge1                 12242681478    6629865168160   27.51M     17012420781    1167818634157     3.47M
ge2                           0                0        0               0                0         0
ge3                           0                0        0               0                0         0
ge4                           0                0        0               0                0         0
ge5                           0                0        0               0                0         0
ge6                           0                0        0               0                0         0
ge7                           0                0        0               0                0         0
ge8                           0                0        0               0                0         0
ge9                           0                0        0               0                0         0
ge10                          0                0        0               0                0         0
ge11                          0                0        0               0                0         0
ge12                          0                0        0               0                0         0
ge13                3163945848     678988453503    1.50M      2636891643     554057402139     1.09M
ge14                          0                0        0               0                0         0
ge15                          0                0        0               0                0         0
ge16                          0                0        0               0                0         0
ge17                          0                0        0               0                0         0
ge18                          0                0        0               0                0         0
ge19                          0                0        0               0                0         0
ge20                          0                0        0               0                0         0
ge21                          0                0        0               0                0         0
ge22                          0                0        0               0                0         0
ge23                          0                0        0               0                0         0
xge0                          0                0        0               0                0         0
xge1                          0                0        0               0                0         0
bvi100                        0                0        0               0                0         0
bvi200                        0                0        0               0                0         0
tunnel0                       0                0        0          723152        554347524     5.02M
tunnel1                       1               88        0          201168        152769236     2.49M
local-traffic           1583112        277560581    2.57K         6738178       5284454616     1.22K
```

目 录

1 简介

本文档介绍设备的管理员双因子认证功能配置举例，在配置前，先了解如下定义：

- 管理员双因子认证： 结合管理员合法账号和 Ukey 双重身份的认证方式。
- Ukey： 具有识别和导入用户证书功能的 USB 设备。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

- Ukey 管理软件： 对 Ukey 设备进行初始化授权。
- Ukey 客户端软件： 对 Ukey 设备导入用户证书。

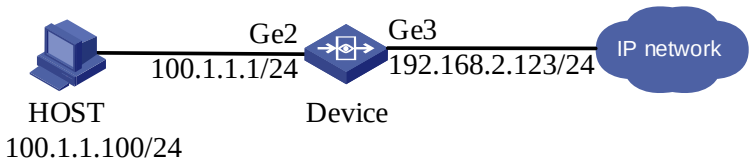
本文档假设您已了解管理员双因子认证特性。

3 管理员双因子认证功能配置举例

3.1 组网需求

如图 1 所示，某公司网络管理员对设备访问权限进行了严格控制，在设备上开启管理员双因子认证，要求同时拥有合法管理员账号和 Ukey 设备的用户才能登录设备进行操作 。

图1 管理员双因子认证组网



3.2 配置思路

- 在设备上配置各接口地址，如拓扑图所示。
- 生成 CA 根证书。
- 生成用户证书并签发。
- 导出用户证书（P12 格式）。
- 将 Ukey 初始化。
- 将用户证书导入 Ukey。
- 开启管理员双因子认证。
- 验证配置。

3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.4 配置步骤

1. 配置路由接口

如图 2、图 3 所示，在设备上配置各接口地址。点击“网络配置>接口配置>物理接口”，配置接口 IP 地址。

图2 配置 ge2 接口

图3 配置 ge3 接口

2. 生成 CA 根证书

如图 4 所示，点击“策略配置>对象管理>CA 服务器>根 CA 配置管理”，在根证书管理中点击生成 CA 根证书，配置 CA 信息。

图4 配置 CA 根证书

如图 5 所示，查看已生成的 CA 根证书。

图5 查看已生成的 CA 根证书

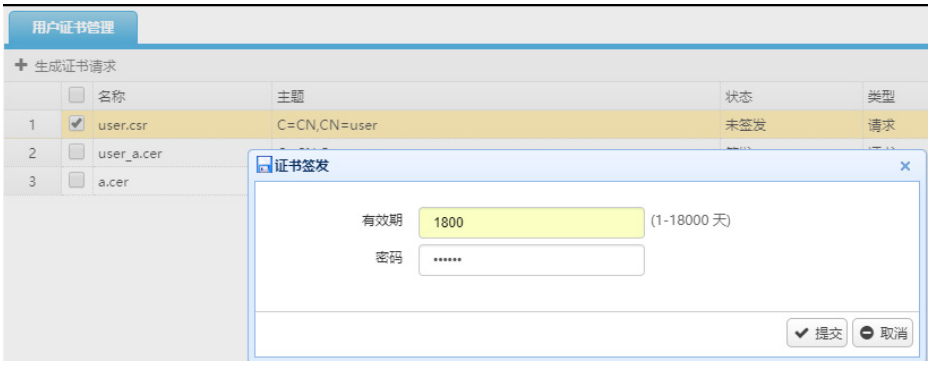
3. 生成用户证书并签发

如图 6 所示，点击“策略配置>对象管理>CA 服务器>用户证书管理>生成证书请求”，配置用户证书信息。

图6 配置用户证书

如图 7 所示，点击签发证书，输入证书有效期和密码，提交。

图7 签发用户证书



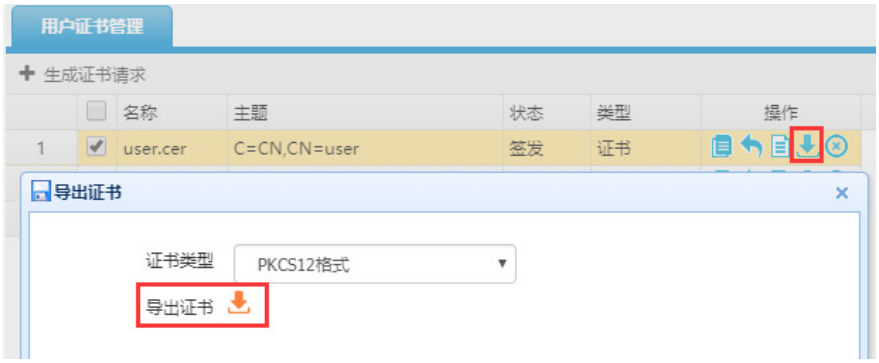
如图 8 所示，查看已生成并签发的用户证书。

图8 签发用户证书

4. 导出用户证书

如图 9 所示，点击“策略配置>对象管理>CA 服务器>用户证书管理”，点击导出用户证书。

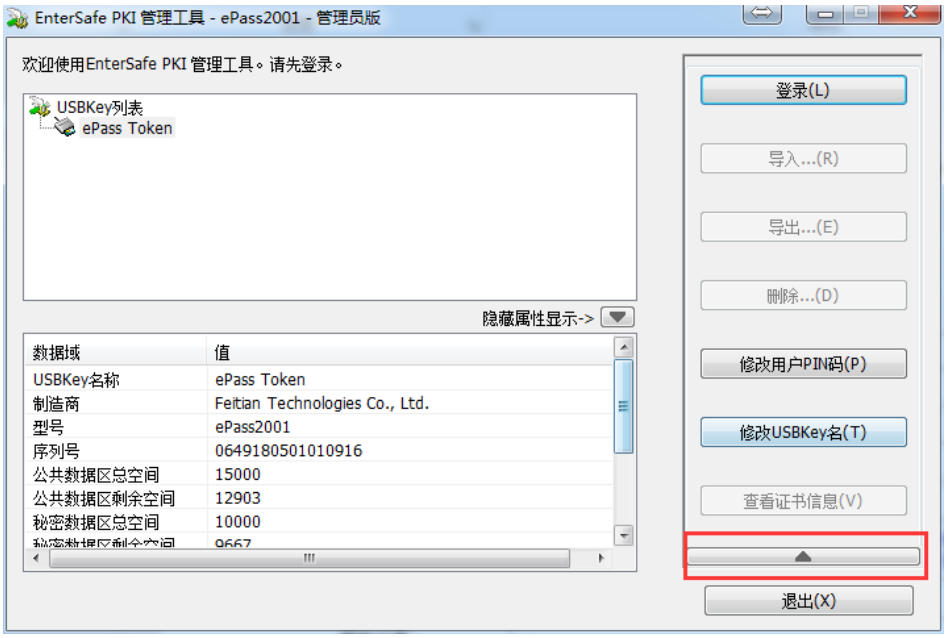
图9 导出用户证书



5. 将 Ukey 初始化（首次使用 Ukey）

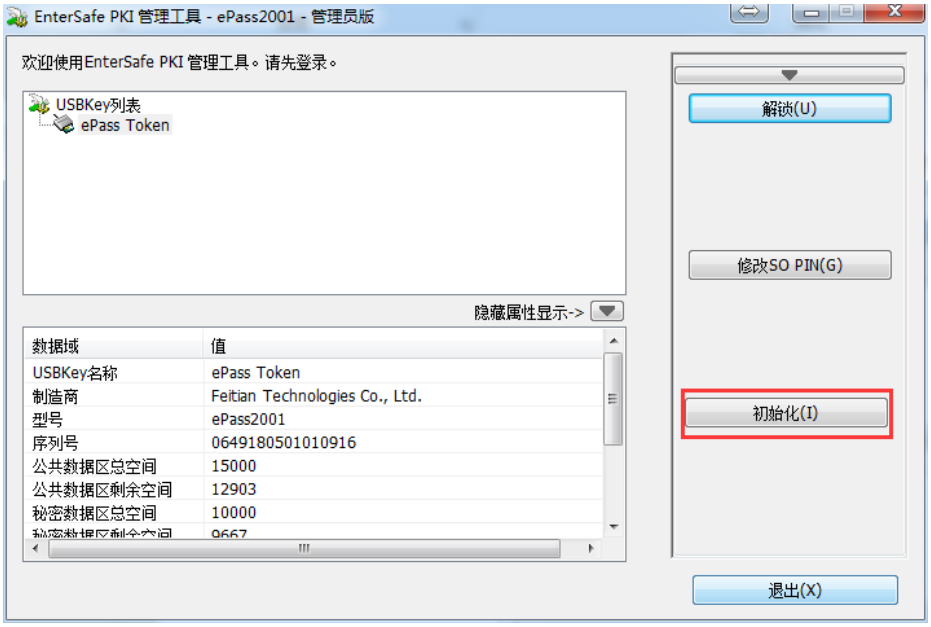
(1) 如图 10 所示，在“系统管理>系统设定>管理设定”中下载 Ukey 客户端软件安装，管理员电脑插上 Ukey，然后下载 Ukey 管理软件，并双击打开。

图10 Ukey 管理软件界面



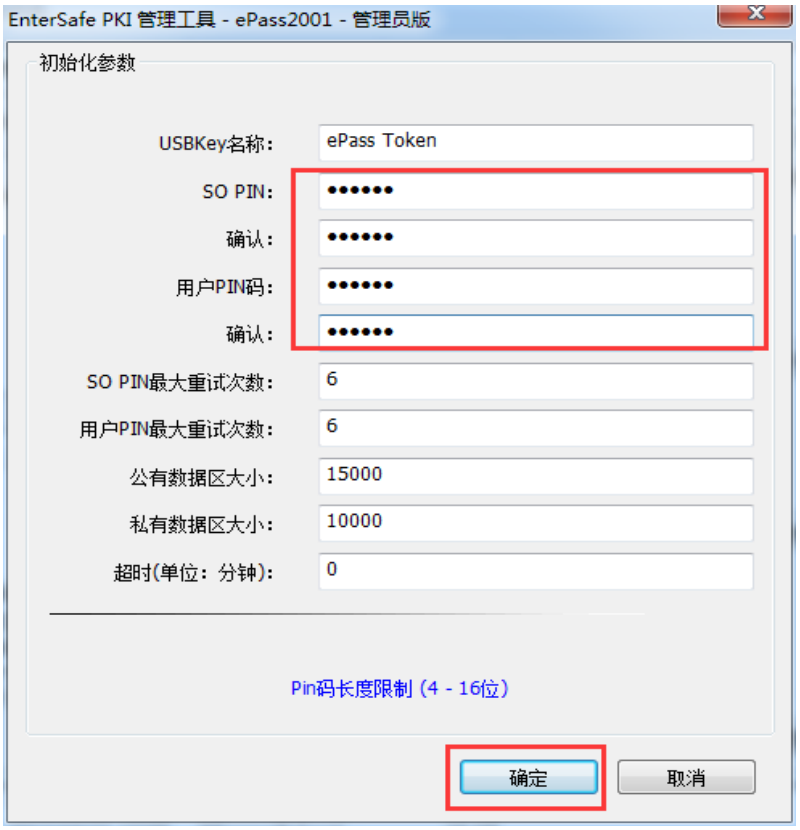
(2) 如图 11 所示，点击图中向上的箭头。

图11 Ukey 管理软件初始化按钮



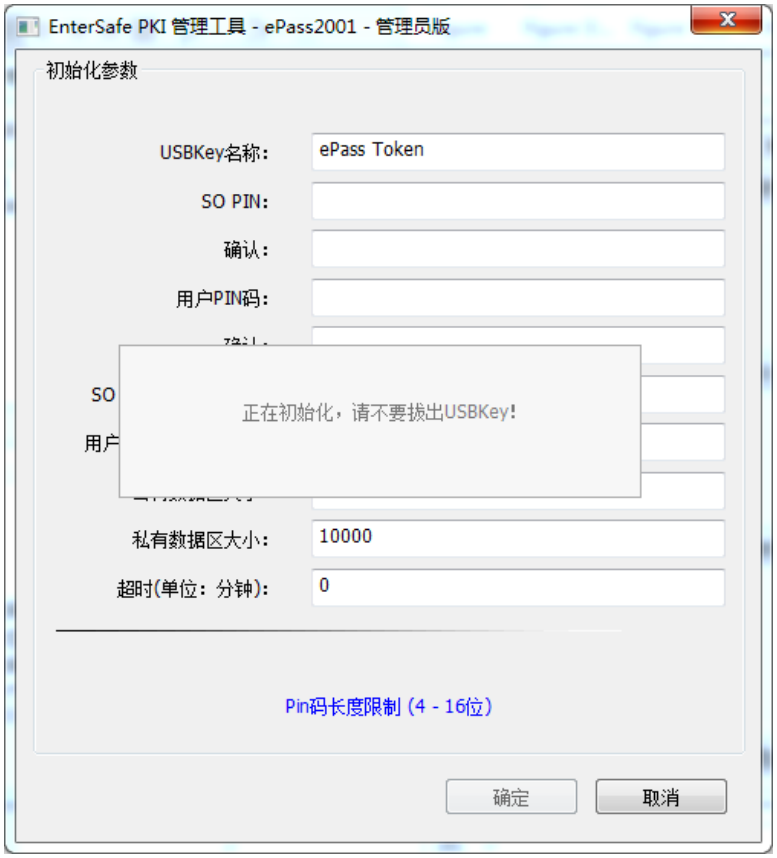
(3) 如图 12 所示，点击上图初始化按钮，配置并确定，完成 Ukey 初始化。

图12 Ukey 管理软件初始化界面



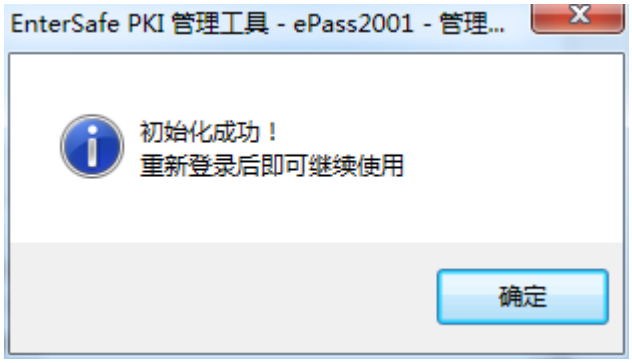
如图 13 所示，Ukey 管理软件初始化过程。

图13 Ukey 管理软件初始化过程界面



如图 14 所示，Ukey 管理软件初始化成功弹框提示。

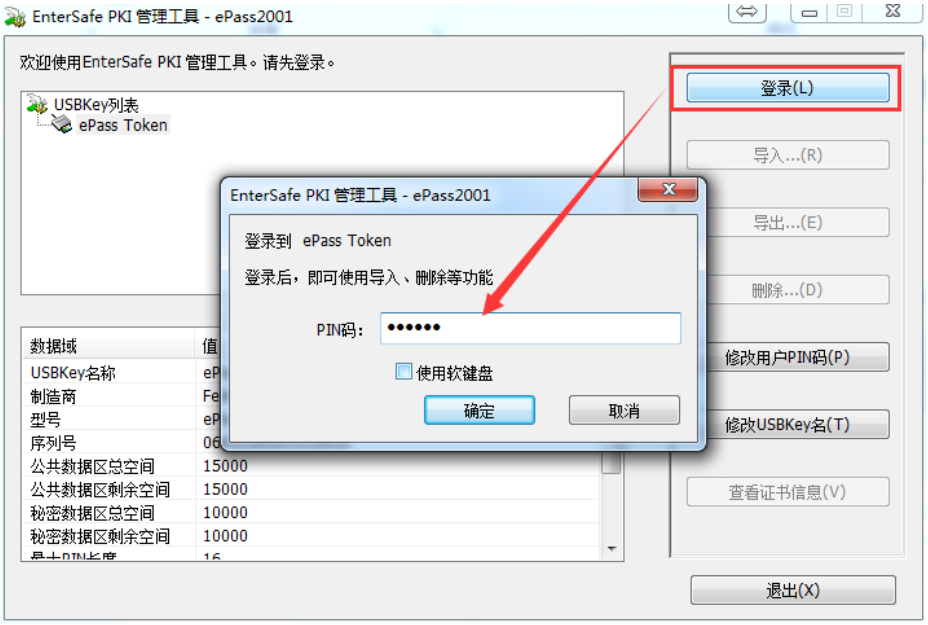
图14 Ukey 管理软件初始化成功界面



6. 将用户证书导入 Ukey

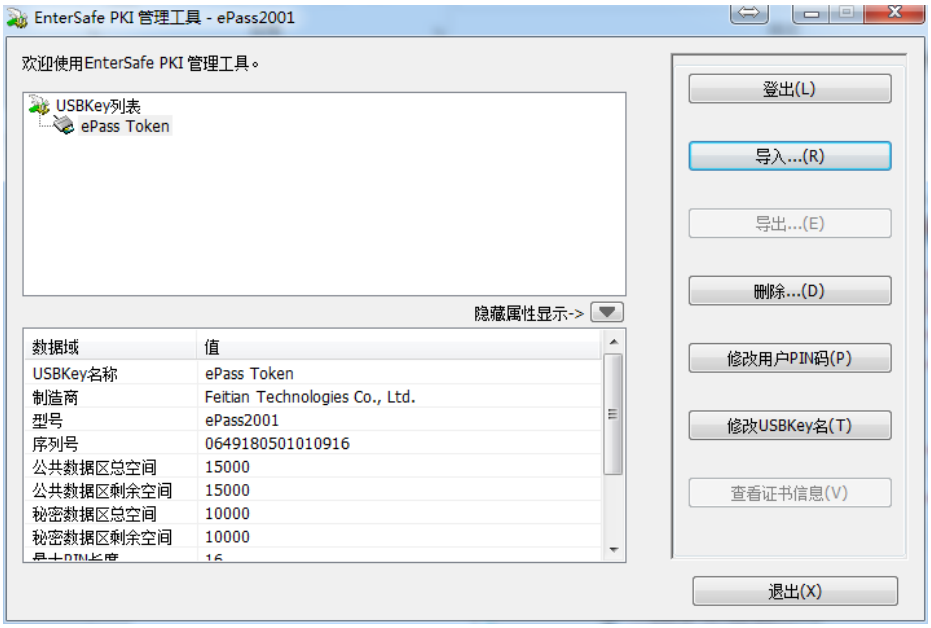
(1) 如图 15 所示，将 Ukey 管理软件关闭退出，双击打开已安装的 Ukey 客户端软件，输入之前设置的 PIN 码后，登录成功。

图15 Ukey 客户端软件登录界面



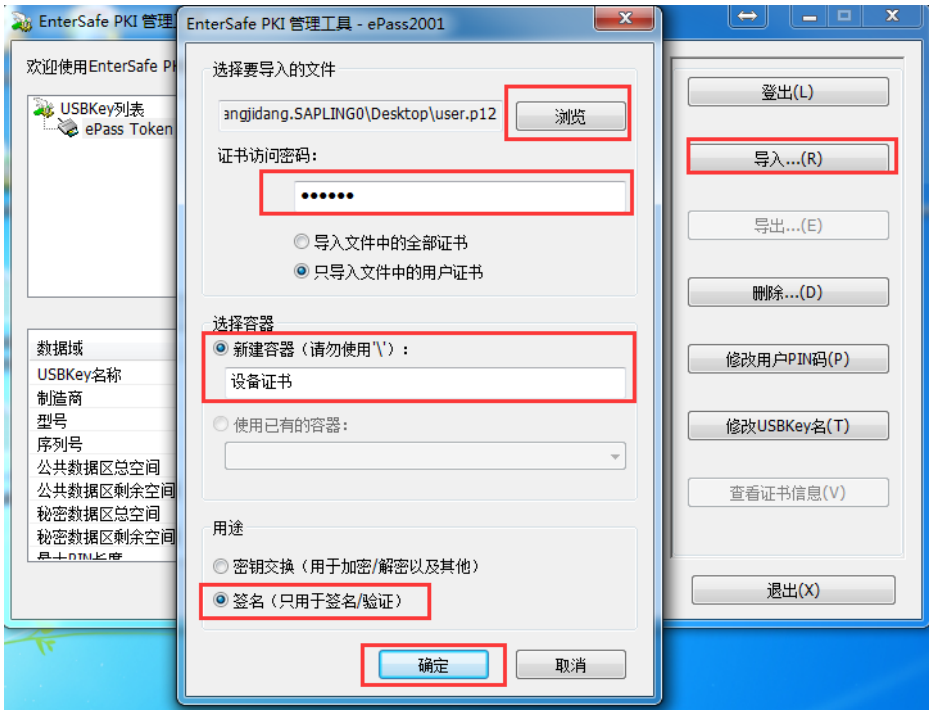
(2) 如图 16 所示，Ukey 管理软件登录成功界面。

图16 Ukey 客户端软件登录成功界面



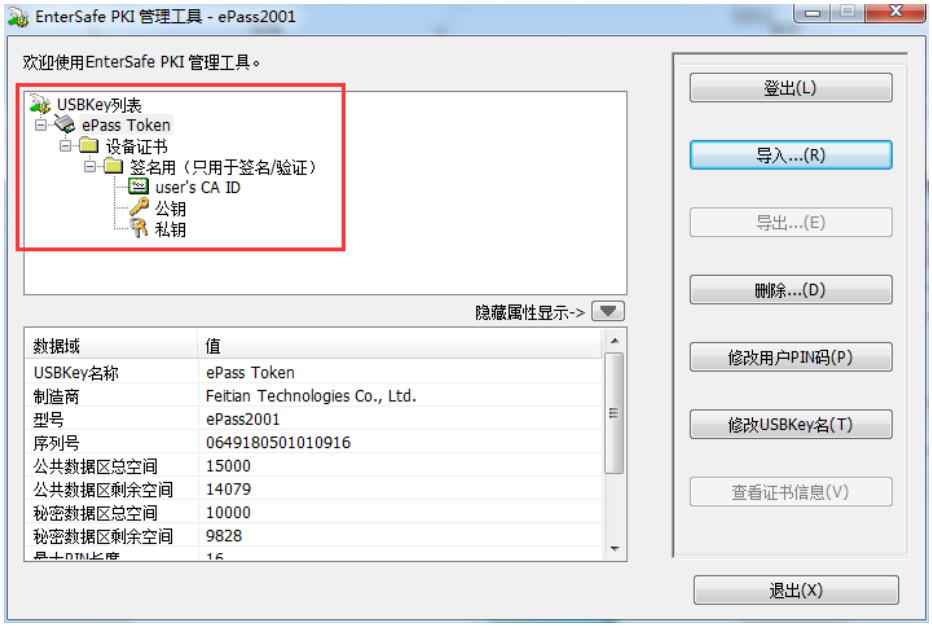
(3) 如图 17 所示，点击导入，通过<浏览>找到之前下载的用户证书 user.p12，输入证书访问密码，新建容器命名名称，用途选择<签名>，确定提交。

图17 Ukey 客户端软件导入用户证书界面



(4) 如图 18 所示，用户证书导入成功。

图18 用户证书导入成功界面



7. 开启管理员双因子认证

如图 19 所示，点击“系统管理>系统设定>管理设定”，开启管理员双因子认证功能。

图19 开启管理员双因子认证

3.5 配置注意事项

- 开启管理员双因子认证前需要先生成 CA 根证书。
- 在管理员双因子认证功能已正常开启的情况下，如果设备 CA 证书发生变更，需要先关闭管理员双因子认证功能然后再次开启，以便重新关联新的 CA 根证书。

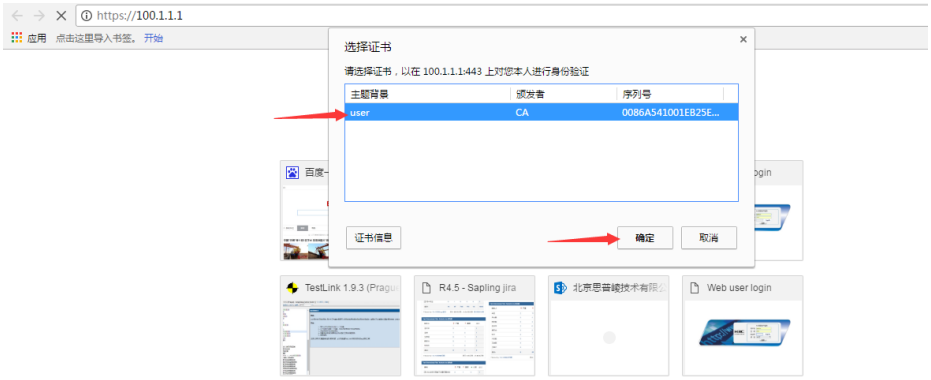
3.6 验证配置

如图 20 所示，管理员 Host 不插入 Ukey，直接使用 https 方式访问设备，不会显示登录界面，提示没有登录证书。

图20 管理员访问设备 WEB 界面失败

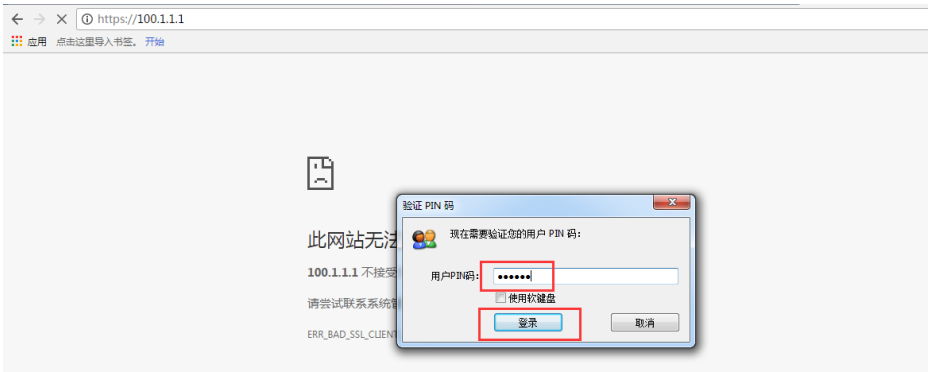
如图 21 所示，插上 Ukey 后，再次使用 https 方式访问设备，会弹出证书选择界面，选择证书，点击确定。

图21 选择证书



如图 22 所示，弹出框验证 PIN 码，输入正确的 PIN 码：。

图22 输入验证 PIN 码



返回设备 WEB 登录界面，输入正确的管理员用户名密码，即可登录设备。

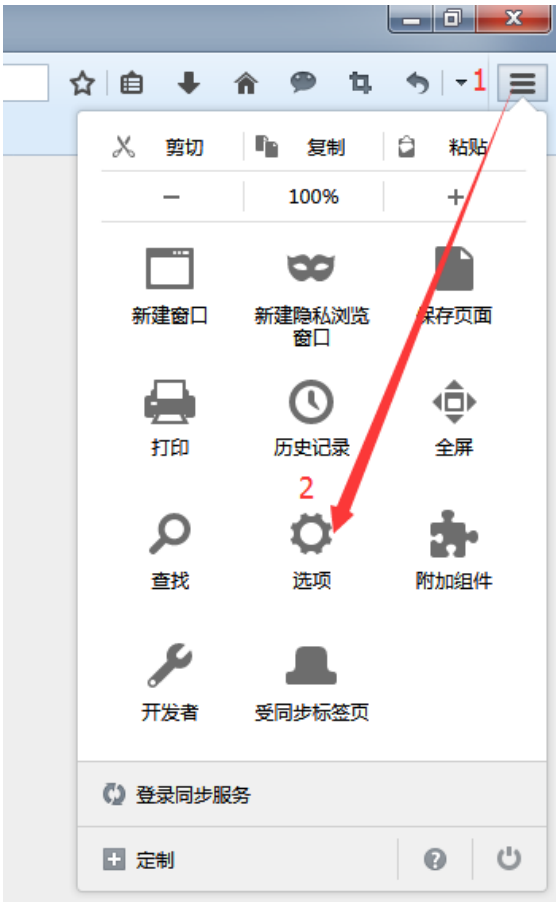
4 管理员双因子认证功能使用限制及注意事项

- 开启管理员双因子认证前需要先生成 CA 根证书
- 在管理员双因子认证功能已正常开启的情况下，如果设备 CA 证书发生变更，需要先关闭管理员双因子认证功能然后再次开启，以便重新关联新的 CA 根证书
- IE 浏览器因对证书安全检验级别较高，不受信任的证书网站浏览器会禁止用户继续访问，导致无法通过 https 访问设备
- 火狐浏览器需要做兼容性设置，否则无法调用 Ukey 中的证书，设置方法参见后面第 5 节：火狐浏览器兼容性设置方法
- USBKey 目前仅支持 epass 一个厂商

5 火狐浏览器兼容性设置

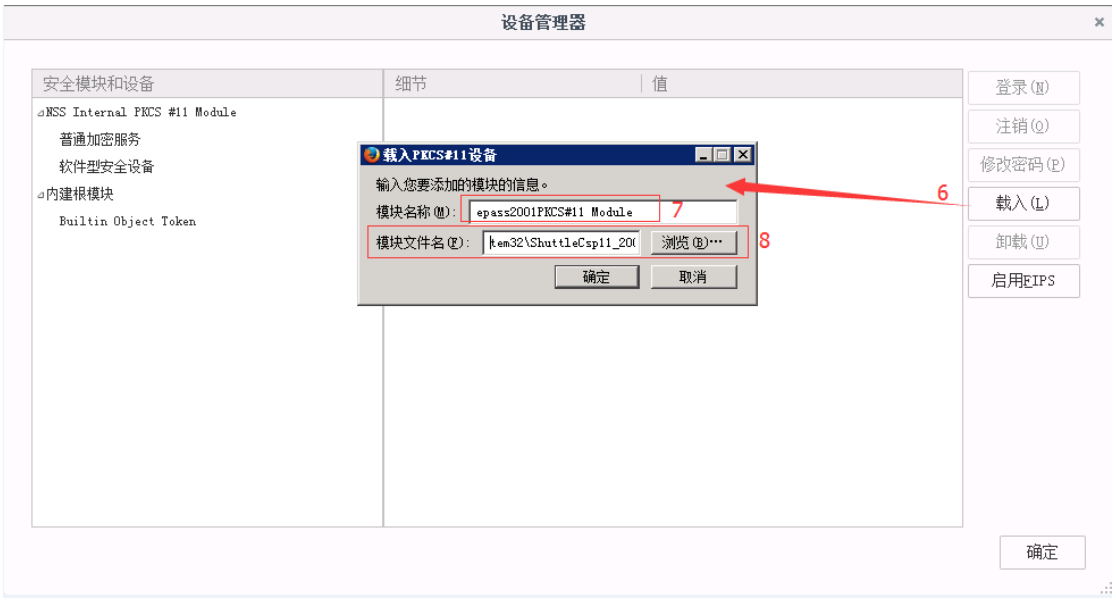
说明：示例浏览器版本号 55.0.3（32 位），因浏览器版本不同，设置方法可能会略有差异

(1) 按如下截图操作，选择<菜单>- <选项>

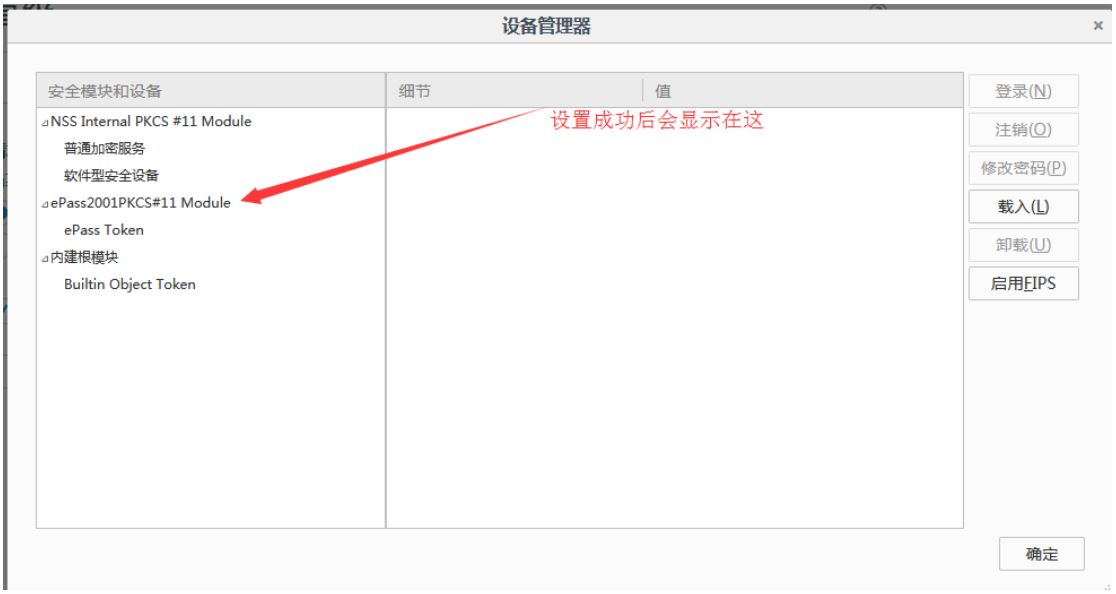


(2)　按如下截图操作，选择<高级>-<证书>-<安全设备>

(3) 按如下截图操作并配置，选择<载入>，模块名称填写：epass2001PKCS#11 Module， 模块文件名选择浏览并填写路径 C :\Windows\System32\ ShuttleCsp11_2001.dll（此为默认安装路径）



(4) 查看是否设置成功：



目录

1 简介

本文档介绍设备的三权分立功能配置举例，包括各管理员权限划分及权限分配的管理。

设备三权分立共有四种管理员，分别为原内嵌管理员 admin，三权分立后 account 用户、authority 用户、audit 用户，可以分别有以下权限：

- admin 账户：内嵌管理员用户，三权模式下由 authority 用户对其进行功能授权，以实现对功能点权限为只读或可读写，进而对功能进行操作控制。
- account 用户：account 负责账号创建，可新建自定义系统管理员；可进行操作日志查看。
- authority 用户：可以系统管理员功能模块授权，模块细分读写或只读模式。
- audit 用户：审核管理员可对用户权限监控及操作日志查看。

设备的三权分立主要为一些资质审核公司要求管理员互相制约互相监控的功能。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解三权管理功能特性。

3 使用限制

- 设备的切换为三权分立后无法切回普通模式。
- 设备的切换三权分立后由于 admin 账号无功能授权登录后无任何功能执行权限，需由 authority 账号进行权限分配。

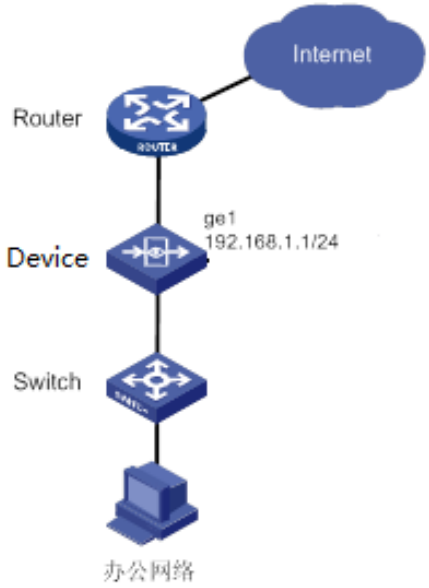
4 配置举例

4.1 组网需求

如图 1 所示，设备的以透明模式串接在某公司网络的核心交换机和出口路由器之间，具体应用需求如下：

- 设备的开启三权模式，设备的使用的 IP 地址为 192.168.1.1/24。
- 需要 authority 用户给 admin 用户分配权限，分别为分配：网络配置、网络优化、对象管理、上网行为管理的执行权限。
- 设备的 account 用户新建自定义用户为 test，只分配监控统计、日志查询、上网行为管理的只读权限。

图1 三权分立功能配置组网图



4.2 配置思路

- 设备的管理模式为“三权模式”。
- 使用 account 用户新建管理员 test。
- 使用 authority 用户对 admin 用户进行读写授权，分别为分配：网络配置、网络优化、对象管理、上网行为管理的执行权限。
- 使用 authority 用户对 test 用户进行分配监控统计、日志查询、上网行为管理的只读权限。

4.3 使用版本

本举例是在设备的的 E6442 版本验证的。

4.4 配置注意事项

- 账户新建只能由 account 用户新建。
- 切换三权模式需慎重，不可回切。
- 所有用户初始密码均为 admin。

4.5 配置步骤

4.5.1 配置设备

1. 配置模式切换

(1) 模式切换为三权模式

如图 2 所示，进入“系统管理>系统设定>管理设定> 模式切换”，选择<三权模式>并确定。

图2 切换三权模式

(2) 使用 account 用户新建自定义用户

如图 3 所示，使用 account 用户登录，点击<新建>，配置用户名为“test”，密码为自定义符合复杂度密码，其它配置保持默认，并点击<提交>。

图3 新建自定义管理员 test 用户

如图 4 所示，创建成功的用户配置如下。

图4 自定义管理员用户配置成功

权限管理

	用户名	角色	认证类型	描述	管理地址	权限状态	操作
1	anonym	系统管理员	本地		0.0.0.0/0	待分配	
2	admin	系统管理员	本地	admin	0.0.0.0/0	待分配	
3	test	系统管理员	本地	test		待分配	
4	account	账号管理员	本地		0.0.0.0/0	内置	
5	authority	权限管理员	本地		0.0.0.0/0	内置	
6	audit	审核员	本地		0.0.0.0/0	内置	

(3) 使用 authority 用户对 admin 用户进行权限分配

如图 5 所示，使用 authority 用户登录，点击 admin 账号后 图标，分配：网络配置、策略配置的执行权限，将全选只读勾掉，在此页面上点击<提交>。

图5 分配执行权限

如图 6 所示，使用 authority 用户登录，点击 test 账号后 图标，分配：主页、数据中心，在此页面上点击<提交>。

图6 分配：监控统计、数据中心权限

4.6 验证配置

(1) 验证 admin 用户权限

如图 7 所示，使用 admin 用户对网络配置等授权功能模块可读可写可执行。

图7 UNIS 设备 设备 admin 用户权限验证

(2) 如图 8 所示，使用自定义 test 用户对监控等授权只读模块只有只读权限。

图8 UNIS 设备 设备自定义 test 用户权限验证

(3) 如图 9 所示，audit 用户登录只有审核员权限。

图9 UNIS 设备的 audit 审核员登录

		用户名	角色	认证类型	描述	管理地址	权限状态	操作
1		anonym	系统管理员	本地		0.0.0.0/0	待分配	
2		admin	系统管理员	本地	admin	0.0.0.0/0	已分配	
3		test	系统管理员	本地	test	0.0.0.0/0	已分配	
4		account	账号管理员	本地		0.0.0.0/0	内置	
5		authority	权限管理员	本地		0.0.0.0/0	内置	
6		audit	审核员	本地		0.0.0.0/0	内置	

4.7 配置文件

```
admin-switch three-power-mode!
```

目录

1 简介

配置文件是设备启动时要加载的配置项，用户可以对配置文件进行保存、更改和清除、选择设备启动时加载的配置文件等操作，此功能支持设备备份多个配置文件，在配置失误，网络出现故障时可以回退到以前的正常配置，保证网络正常运行。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解多配置管理特性。

3 使用限制

- 只支持保存配置文件后缀格式为.cfg 格式。
- 最多可配置 6 个配置文件，所有配置文件大小所占空间最大为 200M。

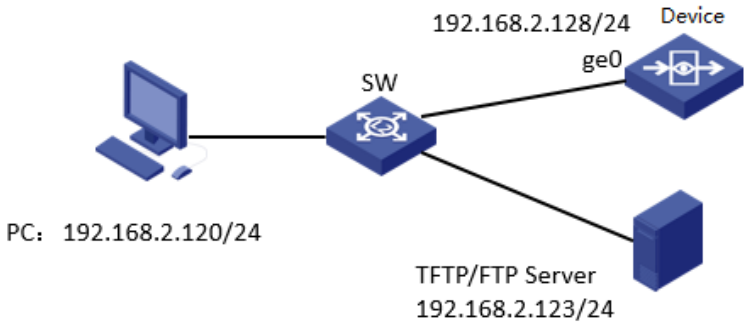
4 配置举例

4.1 组网需求

如下图所示，PC 可通过 cli 正常管理设备，设备与 TFTP/FTP 服务器可正常通信：

- 将当前配置进行配置文件备份，并查看保存的配置文件。
- 将主启动配置文件进行配置文件备份。
- 导出配置文件到 TFTP/FTP 服务器。
- 导入配置文件到设备。
- 将配置文件切换为主启动配置、备份启动配置，设备重启查看启动配置文件信息。
- 对比当前配置和主启动配置文件、备份配置文件信息是否一致。

图1 多配置管理组网图



4.2 配置思路

按照组网图组网。

(1) CLI 方式登录设备（设备配置有接口、路由、NAT、安全策略等模块的相关配置）。

(2) 将当前配置进行配置文件备份，并查看保存的配置文件列表。

(3) 将主启动配置文件进行配置文件备份。

(4) 导出配置文件到 TFTP/FTP 服务器。

(5) 导入配置文件到设备。

(6) 将配置文件切换为主启动配置，设备重启查看启动配置文件信息。

(7) 对比当前配置和配置文件、主启动配置文件信息是否一致。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

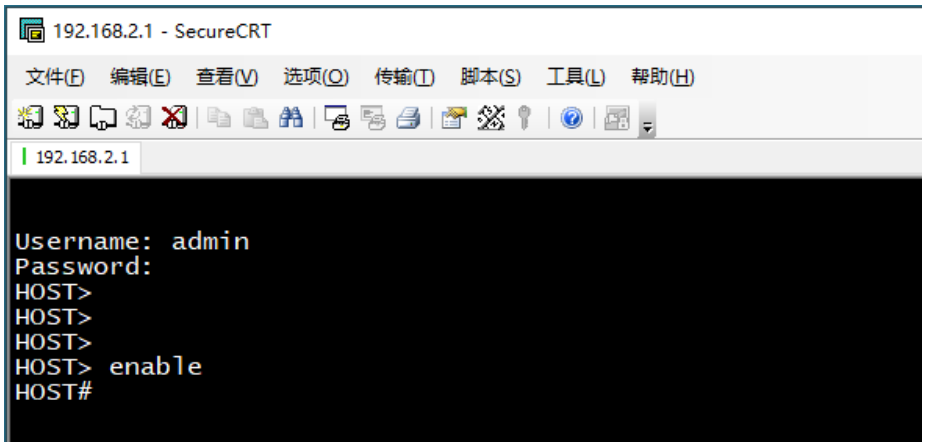
4.4 配置步骤

4.4.1 配置设备

1. CLI 方式登录设备

如图 2 所示，使用 console 或 ssh、telnet 方式登录设备的，ssh、telnet 默认的用户名和密码是 admin/admin。

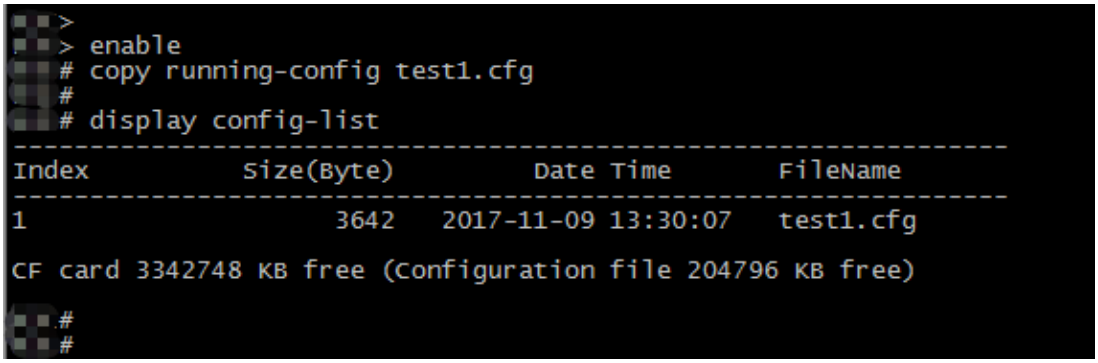
图2 CLI 方式登录设备



2. 将当前配置进行配置文件备份，并查看保存的配置文件列表

如下图所示，enable 进入全局配置视图，使用命令行“copy running-config test1.cfg”保存当前运行配置到配置文件 test1.cfg，使用“display config-list”查看配置文件列表。

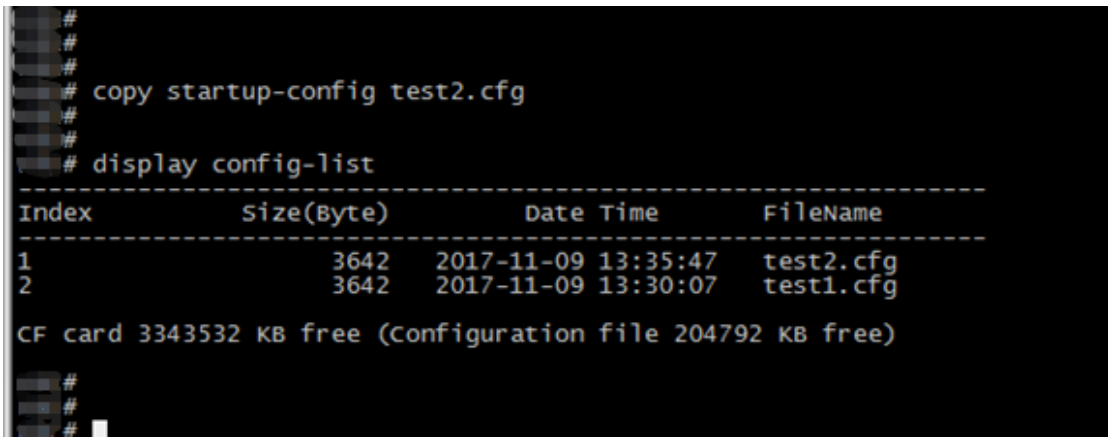
图3 保存当前运行配置到配置文件，查看配置文件列表



3. 将主启动配置文件进行配置文件备份配置

如下图所示，在全局配置视图下，使用命令行“copy startup-config test2.cfg”将主启动配置文件进行配置文件备份配置。

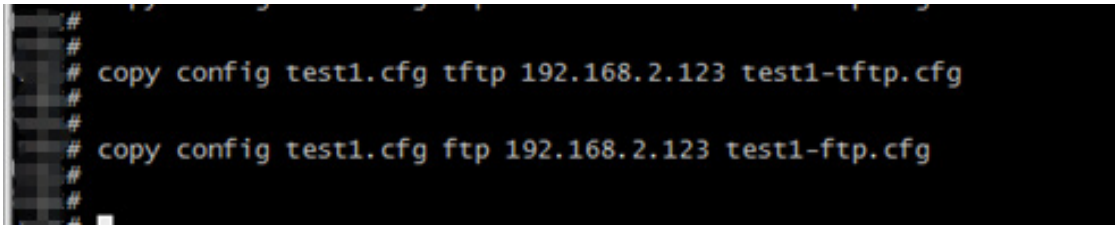
图4 将主启动配置文件进行配置文件备份配置



4. 导出配置文件到 TFTP/FTP 服务器

如下图所示，在全局视图下分别使用命令行“copy config test1.cfg tftp 192.168.2.123 test1-tftp.cfg”、“copy config test1.cfg ftp 192.168.2.123 test1-ftp.cfg”以 tftp 和 ftp 的方式导出配置文件到服务器。

图5 导出配置文件到 TFTP/FTP 服务器



5. 导入配置文件到设备

如下图所示，在全局视图下分别使用命令行“copy tftp 192.168.2.123 test1-tftp.cfg config test1-tftp.cfg”、“copy ftp 192.168.2.123 test1-ftp.cfg config test1-ftp.cfg”以 tftp 和 ftp 的方式导入配置文件到设备。

图6 导入配置文件到设备

```
<[illegible]>#
<[illegible]>#
<[illegible]># copy tftp 192.168.2.123 test1-tftp.cfg config test1-tftp.cfg
Download file test1-tftp.cfg ....

The configuration file successfully upgraded, reboot to take effect.
<[illegible]>#
<[illegible]># copy ftp 192.168.2.123 test1-ftp.cfg config  test1-ftp.cfg
Download file test1-ftp.cfg ....

The configuration file successfully upgraded, reboot to take effect.
<[illegible]>#
<[illegible]>#
<[illegible]># display config-list
-----------------------------------------------------------------
Index          Size(Byte)         Date Time       FileName
-----------------------------------------------------------------
1                    3642   2017-11-09 13:48:18   test1-ftp.cfg
2                    3642   2017-11-09 13:47:31   test1-tftp.cfg
3                    3642   2017-11-09 13:35:47   test2.cfg
4                    3642   2017-11-09 13:30:07   test1.cfg

CF card 3343528 KB free (Configuration file 204785 KB free)

<[illegible]>#
```

6. 将配置文件切换为主启动配置，设备重启后查看设备启动使用的配置文件

如下图所示，在全局视图下分别使用命令行“display startup”、“copy test1.cfg startup-config”查看设备当前启动使用的配置文件信息及将主配置启动文件切换为配置文件 test1.cfg 的配置。

图7 将配置文件切换为主启动配置，设备重启后查看设备启动使用的配置文件

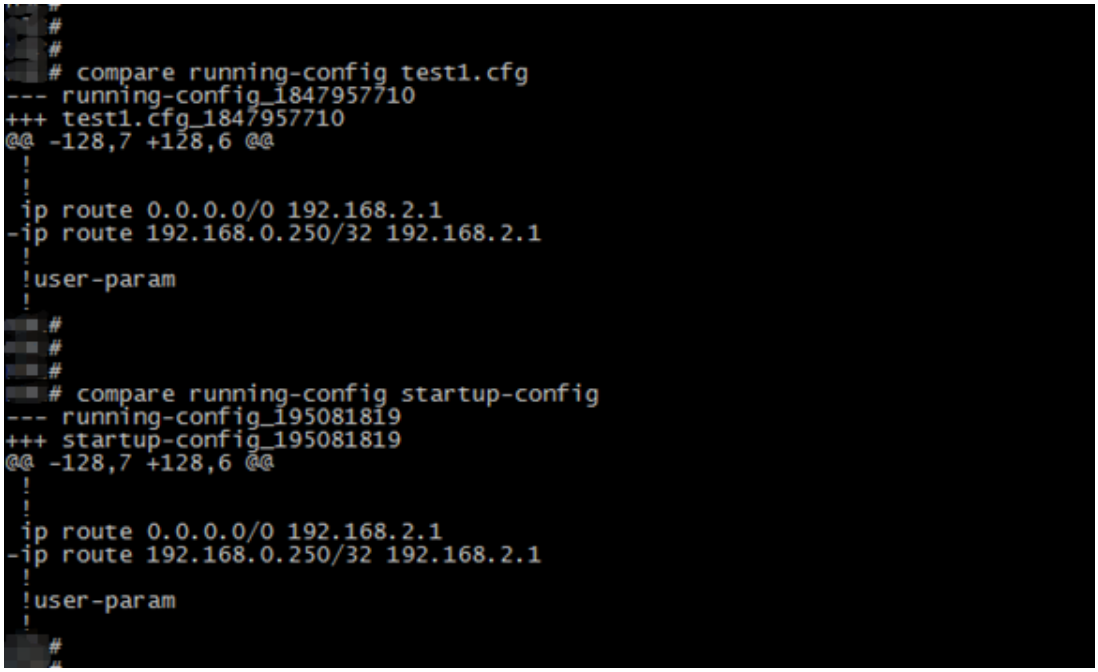
```
<[illegible]>#
<[illegible]>#
<[illegible]># display startup
Current startup configuration file:     NULL
Next startup configuration file:        NULL

<[illegible]># copy test1.cfg startup-config
The configuration file successfully upgraded, reboot to take effect.
<[illegible]>#
<[illegible]># reboot
Save current configuration? Please enter "y/n"  to confirm:  n
The system will be rebooted! Please enter "y/n"  to confirm:  y
```

```
<[illegible]>#
<[illegible]>#
<[illegible]># display startup
Current startup configuration file:     test1.cfg
Next startup configuration file:        test1.cfg

<[illegible]>#
<[illegible]>#
```

7. 对比当前配置和配置文件、主启动配置文件信息是否一致

如下图所示，在全局视图下分别使用命令行“compare running-config test1.cfg”、“compare running-config startup-config”对比当前配置和配置文件、主启动配置文件信息是否一致，不一致时会打印出相应的配置信息。

图8 对比当前配置和配置文件、主启动配置文件信息是否一致



目 录

1 简介

本文档介绍设备的管理员外部认证功能配置举例，设备上管理员认证方式配置管理员外部认证之后，登录设备优先使用外部服务器账号密码进行验证，如果外部服务器异常才能走本地认证方式，以保证管理员账号的安全性以及可维护性。

管理员外部认证支持到 LDAP 和 Radius 两种服务器认证。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解管理员外部认证特性。

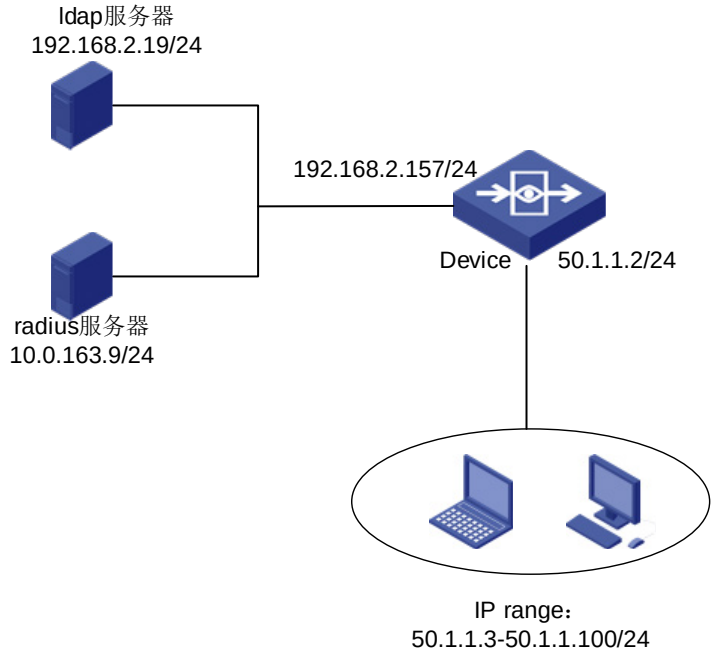
3 管理员外部认证配置举例

3.1.1 组网需求

如图 1 所示，某企业设备管理是通过管理员本地认证方式进行校验登录，现企业部署了 LDAP 服务器，需要通过 LDAP 服务器上的账号登录设备进行认证登录，即启用管理员 LDAP 外部认证方式登录设备。

- 设备到外部服务器可达。
- 如果设备到外部服务器不可达，开启服务器异常进行本地认证，使用本地账号可以登录。

图1 管理员外部认证组网



3.1.2 配置思路

- 配置设备接口地址、路由及 NAT。
- 配置 LDAP 服务器。
- 配置管理员外部认证选择 LDAP 服务器。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge0、ge2<编辑>按钮，分别配置 ge0 和 ge2 为 192.168.2.157/24、50.1.1.2/24。

图2 配置接口地址

(2) 配置静态路由

如图 3 所示，进入“网络配置>路由管理>静态路由”，配置访问外网的默认路由。

图3 配置静态路由

(3) 配置源 NAT

如图 4 所示，进入“策略配置>NAT 转换策略>源 NAT”，配置源 NAT。

图4 配置源 NAT

(4) 配置 LDAP 服务器

如图 5 所示，进入“用户管理>认证管理>认证服务器”，点击<新建>LDAP 服务器，配置 LDAP 服务器参数，点击<提交>。

图5 配置 LDAP 服务器

(5) 配置管理员外部认证选择 LDAP 服务器

如图 6 所示，进入“系统管理>系统设定>管理设定”，管理员认证方式选择“外部认证”，认证服务器选择“Ldap”，LDAP 服务器选择步骤 4 已配置的服务器对象，服务器异常开启本地认证选择“开”，点击<提交>。

图6 配置管理员外部认证

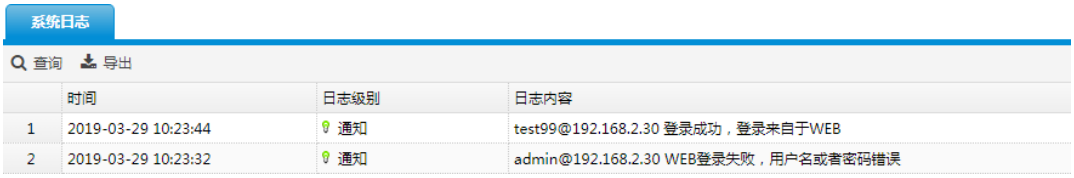
3.1.5 配置注意事项

- 服务器异常开启本地认证开关建议开启，如果设备与服务器通信出现异常，可以通过设备本地账号进行登录并管理；如果不开启，则如果设备与服务器通信出现异常，设备将无法管理，出现脱管状态，此开关关闭需谨慎操作。

3.1.6 验证配置

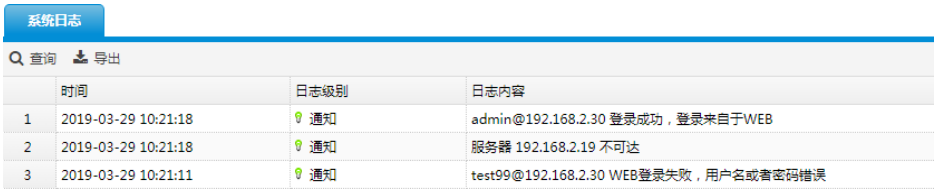
如图 7 所示，设备与服务器通信正常情况下，管理员通过设备本地账号 admin 登录设备无法登录成功，通过 LDAP 服务器上的账号 test99 登录设备成功，系统日志上可以查看到登录结果。

图7 设备与服务器通信正常管理员登录设备系统日志



如图 8 所示，设备与服务器通信异常情况下，管理员使用 LDAP 服务器上的账号 test99 登录设备失败，服务器异常开启本地认证开关已开启，使用设备本地账号 admin 进行登录，可以登录成功，通过系统日志可以查看到结果。

图8 设备与服务器通信异常管理员登录设备系统日志



4 配置文件

```
!config
authorized-table admin
    description Default authority table with all authority enable
    authorized read all
    authorized write all
!
authorized-table audit
    description Default authority table used for audit administrator
    authorized read all
!
ldap 192.168.2.19
 ldap 192.168.2.19 389
 cnid cn
 dn ou=webauth,dc=adtest,dc=com
 bindtype simple user cn=administrator,cn=Users,dc=adtest,dc=com secret
u0PTeDe6mLnwpt6j0KGB27MRAfi5ktR+I84wyRWUGlHNkAH8PLacJOscIFGXWKL
!
admin auth-mode remote auth-type ldap server 192.168.2.19 local enable
!
```

```
interface ge0
 ip address 192.168.2.157/24
 allow access https
 allow access http
 allow access ping
 allow access ssh
 allow access telnet
 allow access center-monitor
!
interface ge1
!
interface ge2
 ip address 50.1.1.2/24
 allow access https
 allow access http
 allow access ping
 allow access ssh
 allow access telnet
 allow access center-monitor
!
ip route 0.0.0.0/0 192.168.2.1
!
ip nat source ge0 any any any interface log 1
!
```

目 录

1 简介

本文档介绍设备的旁路认证和阻断功能配置举例，设备上配置旁路认证和阻断功能之后，针对用户识别范围内的用户会进行旁路认证或者旁路阻断，对于没有认证的用户发送 http 302 报文重定向，防火墙控制策略为拒绝时，对匹配上安全策略的 TCP 报文发送 reset 报文，阻止用户访问网络。

开启旁路认证后需要配置用户认证策略，开启旁路阻断后需要配置 IPV4 控制策略。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

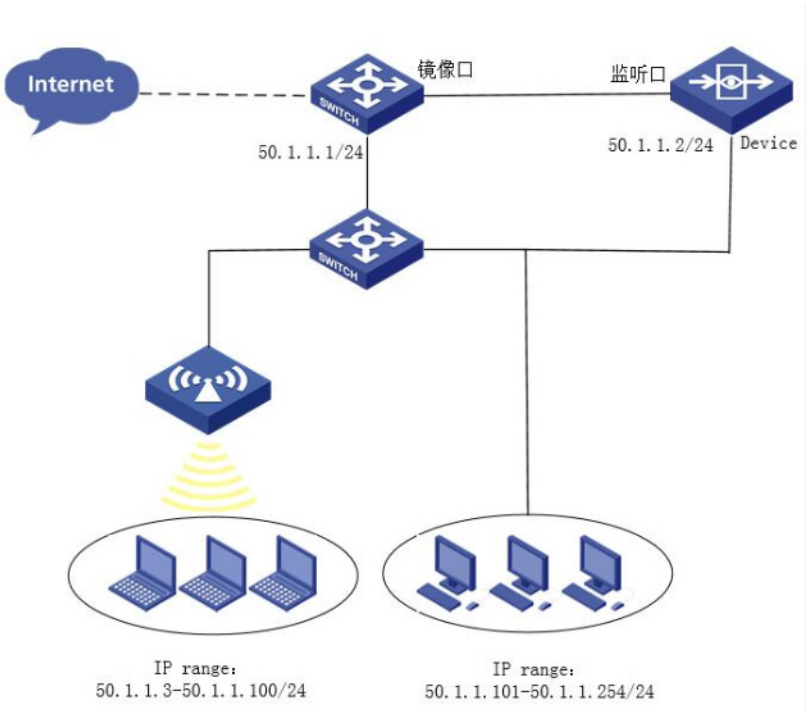
本文档假设您已了解旁路认证和阻断的特性。

3 旁路认证和阻断配置举例

3.1.1 组网需求

如图 1 所示，某企业对内网用户 50.1.1.3-100/24 工作时间都将进行用户认证和内网用户 50.1.1.101-254/24 工作时间都进行行为控制，不提供任何 NAT，DHCP 或者 DNS 服务。部署在交换机旁边，通过镜像的方式，仅仅提供认证和阻断的功能。旁路模式不修改网络结构，不关心网络细节，关机也不掉线，不会影响企业内部网络。

图1 旁路认证和阻断组网



3.1.2 配置思路

- 配置设备接口地址。
- 配置设备旁路部署。
- 配置设备旁路认证。
- 配置设备旁路阻断。
- 配置用户识别范围。
- 配置用户认证策略。
- 配置 IPv4 控制策略。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge6<编辑>按钮，配置 ge6 的 IP 地址为 50.1.1.2/24。

图2 配置接口地址

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0				00:21:45:c8:15:c0	route	full	1000	down		
2	ge1				00:21:45:c8:15:c1	route	full	1000	down		
3	ge2				00:21:45:c8:15:c2	route	full	1000	down		
4	ge3				00:21:45:c8:15:c3	route	full	1000	down		
5	ge4				00:21:45:c8:15:c4	route	full	1000	down		
6	ge5				00:21:45:c8:15:c5	route	full	1000	down		
7	ge6		50.1.1.2/24		00:21:45:c8:15:c6	route	full	1000	up		
8	ge7				00:21:45:c8:15:c7	route	full	1000	down		
9	ge8				00:21:45:c8:15:c8	listen	full	1000	up		
10	ge9				00:21:45:c8:15:c9	route	full	1000	down		

(2) 配置部署方式

如图 3 所示，进入“网络配置>基础网络>部署方式”，配置勾选 ge8 口启用。

图3 配置部署方式

(3) 配置旁路认证和阻断

如图 4 所示，进入“网络配置>基础网络>部署方式>高级配置”，配置旁路认证和旁路阻断。

图4 配置旁路认证和旁路阻断

(4) 配置内网用户地址对象

如图 5 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建内用户地址对象 50.1.1.0/24、50.1.1.3 和 50.1.1.101，点击<提交>。

图5 配置内网用户地址对象

(5) 配置用户识别范围

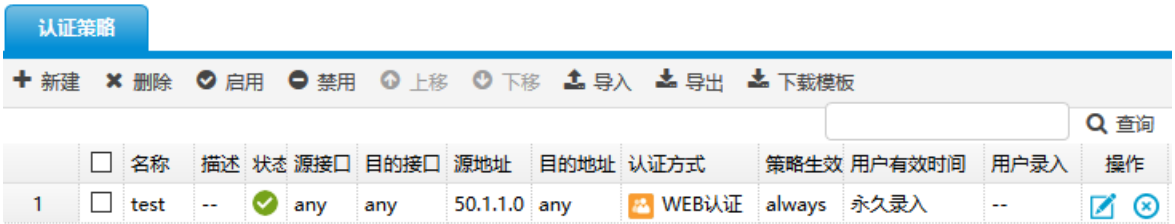
如图 6 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“50.1.1.0”，其它配置默认，提交配置。

图6 用户识别范围

(6) 配置用户认证策略

如图 7 所示，进入“用户管理>认证管理>认证策略”，新建一条认证方式为本地认证的认证策略，源地址选择 50.1.1.3，其它配置默认，<提交>策略。

图7 配置用户认证策略



(7) 配置 IPv4 控制策略

如图 8 所示，进入“策略配置>IPv4 控制策略”，源地址选择 50.1.1.101，行为选择拒绝，其它配置默认，<提交>策略。

图8 配置 IPv4 控制策略

3.1.5 配置注意事项

- 用户认证策略和 IPV4 策略的源接口以及目的接口必须配置接收镜像流量的旁路部署接口或者是 any。
- 旁路认证和阻断务必保证旁路设备到上网 PC 可达，否则功能无法使用。

- 旁路阻断只针对于 TCP 报文生效，对于 UDP、ICMP 等报文无法进行阻断。

3.1.6 验证配置

如图 9 所示，内网用户（50.1.1.3）访问外网需要进行本地认证，本地认证成功后，访问外网成功。

图9 内网用户需要进行本地认证

如图 10 所示，内网用户（50.1.1.101）访问外网资源会被阻断。

图10 内网用户访问外网阻断

4 配置文件

!

!

interface ge6

```
 ip address 50.1.1.2/24
 allow access https
 allow access http
 allow access ping
 allow access ssh
 allow access telnet
 allow access center-monitor
!
interface ge7
!
interface ge8
!
interface ge9
 deploy-mode listen enable
policy any any 50.1.1.101 any any any any always any deny 1
policy default-action permit
policy white-list enable
!
!policy-decrypt
!
policy listen block enable
!
user-policy listen authentication enable
user-policy https-portal enable
user-policy any any 50.1.1.3 any always local-webauth enable test no-record forever
```

目录

1 简介

本文档介绍设备的移动终端管理配置举例，包括移动终端检测、冻结和告警功能。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解移动终端管理特性。

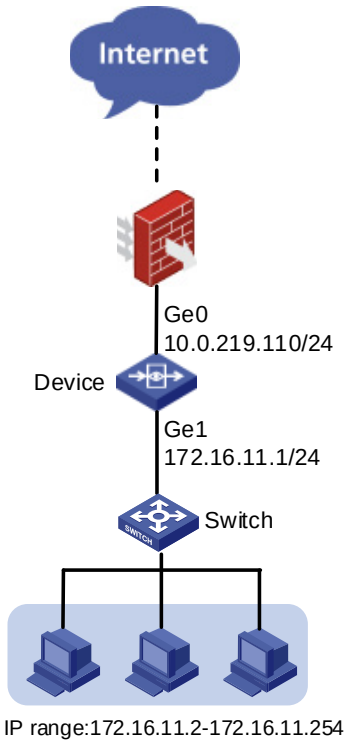
3 配置举例

3.1 组网需求

如图 1 所示，某公司为了提高工作效率，实行移动终端管理上网控制。要求除固定地址可以接入移动终端，其余地址不允许接入移动终端设备。使用设备的的 ge0 和 ge1 接口透明模式部署在网络中，在设备上配置移动终端管理功能。具体要求如下：

- 公司内网地址段：172.16.11.1/24。
- 可以接入移动终端地址：172.16.11.17。

图1 移动终端管理配置组网图



3.2 配置思路

- 配置地址对象。
- 配置用户识别范围。
- 配置移动终端管理策略。

3.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.4 配置步骤

3.4.1 配置设备

1. 配置地址对象

(1) 配置地址对象

如图 2 所示，进入“策略配置>对象管理> 地址对象”，点击<新建>，配置“内网地址”为 172.16.11.1/24，点击<提交>。

图2 配置地址对象

2. 配置用户识别范围

(1) 配置用户识别范围

如图 3 所示，进入“用户管理>认证管理>高级选项”，进入全局配置页面，点击识别范围选择框，选择<内网地址>地址对象，点击<提交>。

图3 配置用户识别范围

3. 配置移动终端管理策略

(1) 配置移动终端管理策略

如图 4 所示，进入“策略配置>移动终端管理”，点击<终端接入配置>页签，进入终端接入配置页面，勾选<启用移动终端管理>按钮，点击<提交>。

图4 终端接入配置页面

(2) 配置移动终端冻结

如图 5 所示，进入“策略配置>移动终端管理”，点击<终端接入配置>页签，进入终端接入配置页面，勾选<冻结上网>按钮，可以修改冻结时长，在信任 IP 中添加 172.16.11.17 地址，点击<提交>。

图5 配置移动终端冻结

(3) 配置终端告警

如图 6 所示，进入“策略配置>移动终端管理”，点击<终端接入配置>页签，进入终端接入配置页面，点击<配置告警邮件>链接，在弹出页面，开启移动终端告警功能，点击<提交>。

图6 配置终端告警

(4) 配置邮件告警

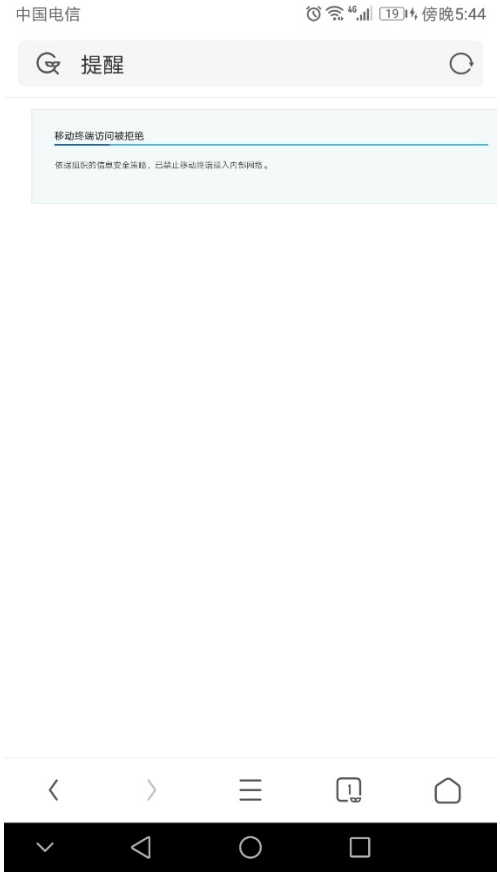
如图 7所示，在终端接入配置页面，点击<配置告警邮件>链接，在弹出页面，单击选择“邮件配置”标签页，配置邮件功能，点击<提交>。

图7 配置邮件告警

3.5 验证配置

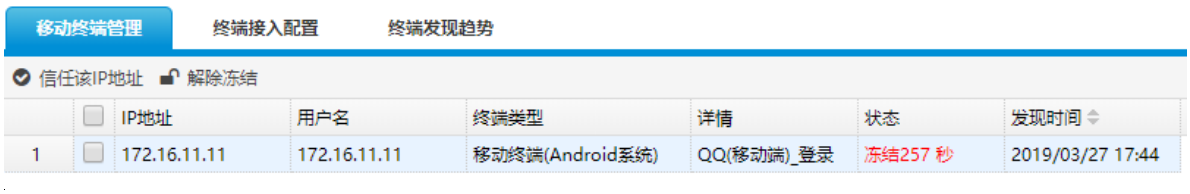
如图 8所示，内网用户使用移动终端访问网站时，会被阻断且有阻断提示 。

图8 终端用户冻结验证



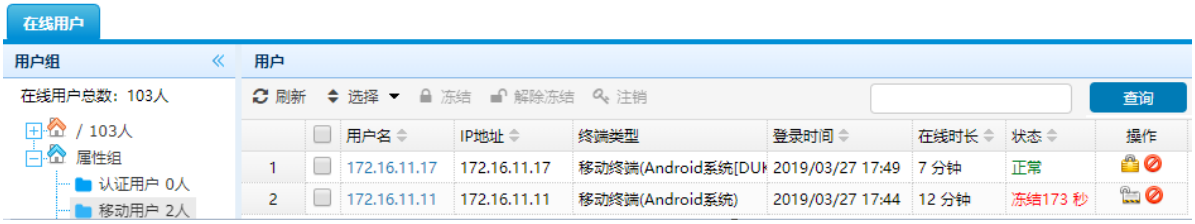
如图 9 所示，进入“策略配置>移动终端管理”，进入移动终端管理页面，可以查看到移动终端阻断信息。

图9 终端用户冻结验证



如图 10 所示，进入“数据中心>系统监控>在线用户”，进入在线用户页面，可以查看到 172.16.11.17（信任 IP）地址的移动终端可以正常上网。

图10 信任 IP 功能验证



如图 11 所示，开启了邮件告警功能，可以在邮件中收到设备发送的告警邮件。

图11 邮件告警功能验证

目 录

1 简介

本文档介绍设备的全局白名单功能配置举例，设备上配置全局白名单功能之后，针对配置白名单的用户网络基础转发会匹配，应用识别会匹配，其它策略模块流程将都不会匹配，直接放通处理。

全局白名单配置支持 IP 地址和 MAC 地址两种格式。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

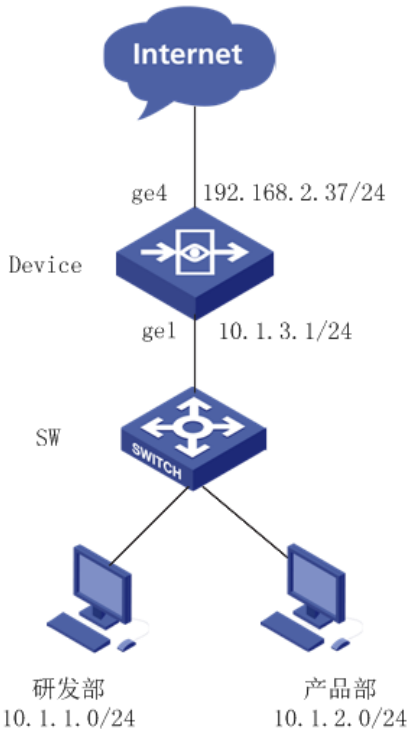
本文档假设您已了解全局白名单特性。

3 全局白名单配置举例

3.1.1 组网需求

如图 1 所示，某企业对内网用户 10.1.1.0/24 和 10.1.2.0/24 工作时间都将进行审计并控制登录即时通讯软件，但是对该内网用户中 10.1.2.2 地址不需要进行审计和控制，通过全局白名单实现该需求。

图1 全局白名单组网



3.1.2 配置思路

- 配置设备接口地址、路由及 NAT。
- 配置内网用户地址对象及地址对象组。
- 配置时间对象。
- 配置用户识别范围。
- 配置 IPv4 审计策略。
- 配置 IPv4 控制策略。
- 配置全局白名单。

3.1.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

3.1.4 配置步骤

(1) 配置接口地址

如图 2 所示，进入“网络配置>接口配置>物理接口”，点击 ge1、ge4<编辑>按钮，分别配置 ge1 和 ge4 为 10.1.3.1/24、192.168.2.37/24。

图2 配置接口地址

	接口名称	描述	IP地址	IPv6地址	MAC地址	工作模式	双工模式	速率(Mbps)	连接状态	启用状态	操作
1	ge0		90.90.1.37/24		00:21:45:3f:de:9a	route	full	100	up		
2	ge1		10.1.3.1/24		00:21:45:3f:de:9b	route	full	100	up		
3	ge2				00:21:45:3f:de:9c	route	full	1000	down		
4	ge3				00:21:45:3f:de:9d	route	full	1000	up		
5	ge4		192.168.2.37/24		00:21:45:3f:de:9e	route	full	100	up		
6	ge5				00:21:45:3f:de:9f	route	full	1000	up		

(2) 配置静态路由

如图 3 所示，进入“网络配置>路由管理>静态路由”，配置访问外网的默认路由及去往内网用户网段 10.1.1.0/24,10.1.2.0/24 路由。

图3 配置静态路由

	目的地址	掩码	下一跳	出接口	权重	距离	地址探测	状态	操作
1	0.0.0.0	0.0.0.0	192.168.2.1	ge4	1	1	-		
2	10.1.1.0	255.255.255.0	10.1.3.2	ge1	1	1	-		
3	10.1.2.0	255.255.255.0	10.1.3.2	ge1	1	1	-		

(3) 配置源 NAT

如(3)图 4 所示，进入“策略配置>NAT 转换策略>源 NAT”，配置源 NAT。

图4 配置源 NAT

(4) 配置内网用户地址对象

如(4)图 5 所示，进入“策略配置>对象管理>地址对象>IPv4 地址对象”，点击<新建>按钮创建内网用户地址对象 10.1.1.0/24 和 10.1.2.0/24，点击<提交>。

图5 配置内网用户地址对象

(5) 配置地址组对象

如图 6 所示，进入“策略配置>对象管理>地址对象>地址组对象”，点击<新建>按钮创建地址组对象，将研发部和产品部两个地址对象添加至地址组中。

图6 配置地址组对象

(6) 配置用户识别范围

如(6)图 7 所示，进入“用户管理>认证管理>高级选项>全局配置”页面，识别范围选择“内网用户”，其它配置默认，提交配置。

图7 用户识别范围

(7) 配置 IPv4 审计策略

如图 8 所示，进入“策略配置>IPv4 审计策略”，源地址选择内网用户，审计对象配置所有，时间选择工作时间，其它配置默认，<提交>策略。

图8 配置 IPv4 审计策略

(8) 配置 IPv4 控制策略

如图 9 所示，进入“策略配置>IPv4 控制策略”，源地址选择内网用户，应用控制策略配置一条应用选择即时通讯类动作配置拒绝，日志级别配置通知，时间选择工作时间，其它配置默认，<提交>策略。

图9 配置 IPv4 控制策略

(9) 配置全局白名单

如图 10 所示，进入“策略配置>全局白名单”，点击<新建>配置一条地址 10.1.2.2 的全局白名单策略。

图10 配置全局白名单

3.1.5 配置注意事项

- 配置的全局白名单地址必须在用户识别范围中，且全局白名单地址只匹配会话中源 IP 和源 MAC。

3.1.6 验证配置

如图 11 所示，分别使用白名单用户（10.1.2.2）和非白名单用户（10.1.1.11）工作时间访问外网，白名单用户访问外网没有相关上网行为审计日志，非白名单用户访问外网有相关上网行为审计日志。

图11 非白名单用户访问外网审计日志

访问网站日志

查询 重置 导出 查询结果：在 2019-03-26 约 103 条日志记录中，从 1 - 103 搜索出相关结果 103 条

	用户	用户mac	URL分类	网页标题	URL	级别	时间	操作
1	10.1.1.11	64:9a:be:8b:85:44	网上交易	淘宝网-淘！我喜欢		信息	2019-03-26 16:42:52	详细
2	10.1.1.11	64:9a:be:8b:85:44	网上交易	淘宝网-淘！我喜欢		信息	2019-03-26 16:42:45	详细
3	10.1.1.11	64:9a:be:8b:85:44	网上交易	淘宝网-淘！我喜欢		信息	2019-03-26 16:42:26	详细
4	10.1.1.11	64:9a:be:8b:85:44	网上交易	淘宝网-淘！我喜欢		信息	2019-03-26 16:42:17	详细
5	10.1.1.11	64:9a:be:8b:85:44	新闻媒体	搜狐网		信息	2019-03-26 16:41:44	详细
6	10.1.1.11	64:9a:be:8b:85:44	新闻媒体	搜狐网		信息	2019-03-26 16:41:37	详细
7	10.1.1.11	64:9a:be:8b:85:44	门户网站与搜索引擎	百度一下，你就知道		信息	2019-03-26 16:40:30	详细

如图 12 所示， 白名单用户（10.1.2.2）非白名单用户（10.1.1.11）工作时间分别登录 QQ 和微信即时通讯聊天软件，只有白名单用户能登录，无相关日志；非白名单用户无法登录，有相应的应用控制阻断日志。

图12 非白名单用户登录即时聊天软件被阻断日志

应用控制日志

查询 重置 导出 查询结果：在 2019-03-26 约 69 条日志记录中，从 1 - 69 搜索出相关结果 69 条

	用户	用户mac	应用分类	应用	策略类型	处理动作	终端类型	级别	时间
1	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
2	10.1.1.11	64:9a:be:8b:85:44	即时通讯	QQ(移动端)_登录	应用控制	阻断	移动终端	通知	2019-03-26
3	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
4	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
5	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
6	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
7	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
8	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
9	10.1.1.11	64:9a:be:8b:85:44	即时通讯	微信_登录	应用控制	阻断	移动终端	通知	2019-03-26
10	10.1.1.11	64:9a:be:8b:85:44	即时通讯	QQ(移动端)_登录	应用控制	阻断	移动终端	通知	2019-03-26
11	10.1.1.11	64:9a:be:8b:85:44	即时通讯	QQ(移动端)_登录	应用控制	阻断	移动终端	通知	2019-03-26

4 配置文件

```
!
interface ge1
 ip address 10.1.3.1/24
 allow access https
 allow access http
 allow access ping
 allow access ssh
 allow access telnet
!
interface ge4
 traffic-mode extern
 ip address 192.168.2.37/24
 allow access https
 allow access http
```

```
 allow access ping
 allow access ssh
 allow access telnet
!
address 研发部
 ip subnet 10.1.1.0/24
!
address 产品部
 ip subnet 10.1.2.0/24
!
address-group 内网用户
 member 研发部
 member 产品部
!
schedule-day 工作时间
 periodic start 09:00 end 18:00
!
whitelist 10.1.2.2
 enable
 address 10.1.2.2
!
policy any any 内网用户 any any any any 工作时间 any permit 1
  app-policy control 1 action deny log-level notice
  app-policy control 1 application IM_Software
  app-policy control 1 enable
policy default-action permit
policy white-list enable
!
audit_policy any any 内网用户 any any 工作时间 all any 1
    log level info
audit associate enable
!
ip route 0.0.0.0/0 192.168.2.1
ip route 10.1.1.0/24 10.1.3.2
ip route 10.1.2.0/24 10.1.3.2
!
user-param recognition scope 内网用户 strict
!
```

```
ip nat source ge4 any any any interface 1
!
```

目录

1 简介

本文档介绍设备的入侵防御功能配置举例。随着互联网的飞速发展，网络环境也变得越来越复杂，恶意攻击、木马、蠕虫病毒等混合威胁不断增大，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全，而入侵防御系统则是提供深层防护体系的保障。

入侵防御涉及以下概念：

- 事件：一个事件对应着一个攻击，事件除了包含有检测攻击的特征之外，还有日志、级别、行为等内容。
- 事件集：事件集是一个或多个事件的集合，根据当前实际的网络情况，系统默认提供了 4 个事件集，最大事件集、常规事件集、应用事件集、攻击事件集，用户也可以根据需要添加自定义的事件集。
- 防护级别：防护级别是事件集的一个属性，同一条事件，对于不同的防护级别，有着不同的动作，防护级别越高，动作越严格。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解入侵防御特性。

3 使用限制

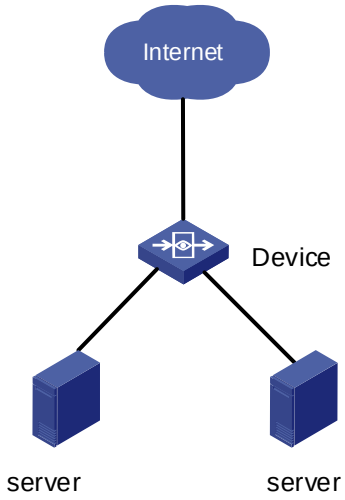
无。

4 配置举例

4.1 组网需求

如图 1 所示，服务器通过 Internet 提供 web 和 FTP 服务，在设备上启用入侵防御功能来保护 Web 和 FTP 服务器。同时通过自定义规则来禁止使用除 210 以外的端口访问 ftp 服务器，且不允许上传文件和新建目录。

图1 入侵防御功能配置组网图



4.2 配置思路

- 配置事件集，决定需要对哪些事件做检测，并决定检测到攻击之后的日志和动作，可以使用系统预定义的事件集，也可以自定义新的事件集。
- 配置安全策略，在安全策略中配置入侵防御策略，引用已经配置的事件集，对命中安全策略的流量做入侵防御相关的检测。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- 入侵防御策略匹配是由上至下进行匹配，策略匹配到之后将不会往下继续匹配。
- 若选择自定义的 IPS 规则，应在 IPv4 控制策略中勾选启用自定义规则。

4.5 配置步骤

4.5.1 配置入侵防御事件集

进入“安全设置>入侵防御>入侵防御配置”，进入入侵防御配置页面，新建事件集，选择防护等级并添加事件，如图 24.1 图 1 所示。

图2 配置入侵防御事件集

4.5.2 配置 IPv4 策略

进入“策略配置>IPv4 控制策略”，进入 IPv4 控制策略页面，如图 3 所示，新建策略，在入侵防御子菜单中启用功能并选择事件集“test”，完成后点击提交。

图3 配置 IPv4 策略

4.5.3 配置自定义入侵防御规则

进入“安全设置>入侵防御>ISP 自定义规则”，进入 ISP 自定义规则配置页面，如图 4 所示，禁止使用除 210 以外的端口访问 ftp 服务器，且不允许上传文件和新建目录。

图4 配置自定义入侵防御规则

4.6 验证配置

4.6.1 默认入侵防御功能验证

使用测试 PC 进行攻击操作。在“日志中心>安全日志>入侵检测日志”中可看到相应攻击日志信息，如图 5 所示。

图5 入侵检测日志


入侵检测日志

查询 导出

	时间	日志级别	用户名称	源地址	归属地	目的地址	事件名称	事件类型	行为	操作
1	2020-01-02 09:4	信息	192.168.1.50	192.168.1.50:52021	局域网	124.243.229.42:80	Ruby on Rails 多个安全漏洞	安全漏洞	允许	详细
2	2020-01-02 09:4	信息	1.1.170.180	1.1.170.180:2843	泰国	1.2.225.90:80	HTTP 漏洞信息扫描	可疑行为	允许	详细
3	2020-01-02 09:4	通知	1.2.209.206	1.2.209.206:80	泰国	1.1.203.156:57310	Lotus Notes 多个第三方文件查看器栈缓	缓冲溢出	允许	详细
4	2020-01-02 09:4	通知	1.1.122.207	1.1.122.207:3459	日本	1.2.61.104:69	TFTP GET passwd 访问	可疑行为	允许	详细
5	2020-01-02 09:4	通知	1.1.32.222	1.1.32.222:42305	中国 广东	1.2.164.111:9080	HTTP IBM Rational Focal Point Webse	安全漏洞	允许	详细
6	2020-01-02 09:4	信息	1.1.221.211	1.1.221.211:65391	泰国	1.2.110.234:8080	VMware 2 网络服务穷举探测	穷举探测	允许	详细
7	2020-01-02 09:4	信息	1.1.166.40	1.1.166.40:27299	泰国	1.2.231.20:80	HTTP 漏洞信息扫描	可疑行为	允许	详细
8	2020-01-02 09:4	信息	1.1.135.186	1.1.135.186:5863	泰国	1.2.247.221:21	ftp-forbidden	IPS自定义规则	拒绝	详细
9	2020-01-02 09:4	信息	1.1.111.150	1.1.111.150:45844	日本	1.2.131.203:80	HTTP 漏洞信息扫描	可疑行为	允许	详细
10	2020-01-02 09:4	警告	1.1.177.118	1.1.177.118:59375	泰国	1.2.236.187:80	HTTP Windows ISAPI Media服务 nsiisl	缓冲溢出	拒绝	详细
11	2020-01-02 09:4	信息	1.1.118.94	1.1.118.94:6397	日本	1.2.143.47:80	HTTP 漏洞信息扫描	可疑行为	允许	详细

4.6.2 自定义入侵防御功能验证

配置完成自定义 IPS 规则后，用户只能使用 210 端口访问 ftp 服务器，可以下载文件，但是无法上传和创建目录。否则无法登录服务器，并记录相应日志信息。使用测试 PC 进行 FTP 服务器登录操作，在“日志中心>安全日志>入侵检测日志”中可看到相应日志信息，如图 6 所示。

图6 入侵检测日志


入侵检测日志

查询 导出

	时间	日志级别	用户名称	源地址	归属地	目的地址	事件名称	事件类型	行为	操作
1	2019-12-30 20:27:11	信息	192.168.1.100	192.168.2.116:210	局域网	192.168.1.100:57191	ftp	IPS自定义规则	拒绝	详细
2	2019-12-30 20:27:04	信息	192.168.1.100	192.168.2.116:210	局域网	192.168.1.100:57187	ftp	IPS自定义规则	拒绝	详细
3	2019-12-30 20:26:29	信息	192.168.1.100	192.168.2.116:210	局域网	192.168.1.100:57169	ftp	IPS自定义规则	拒绝	详细
4	2019-12-30 20:26:22	信息	192.168.1.100	192.168.2.116:210	局域网	192.168.1.100:57165	ftp	IPS自定义规则	拒绝	详细
5	2019-12-30 20:19:26	信息	192.168.1.100	192.168.1.100:57096	局域网	192.168.2.116:80	ftp	IPS自定义规则	拒绝	详细

目 录

1 简介

本文档介绍设备的病毒防护配置举例，设备可以针对内外网入口处，进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防护，我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解病毒防护特性。

3 使用限制

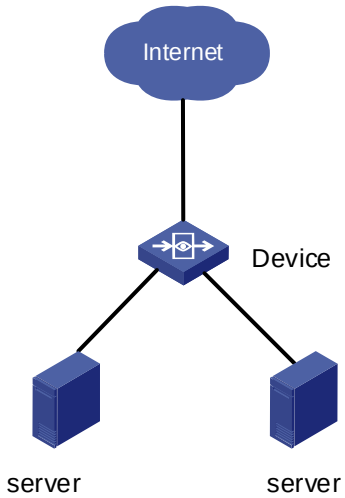
- 压缩包最大解压层数为 20 层。
- 病毒文件大小小于 2M。
- 不支持 rar 文件格式解压。

4 配置举例

4.1 组网需求

如图 1 所示，某公司内网存在两台服务器，测试设备可以针对内外网入口处进行实时病毒扫描，实现服务器主动病毒防护功能，模拟测试服务器通过 FTP 进行下载带有病毒文件操作或局域网内上传带有病毒文件操作。

图1 病毒防护测试组网图



4.2 配置思路

- 配置防病毒设定，设置病毒文件扫描类型
- 配置安全策略，启用病毒防护功能

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

1. 配置防病毒设定，设置病毒文件扫描类型

如图 2 所示，进入“策略配置 > 安全设备 > 病毒防护 > 防病毒设定”，勾选<启用解压>，选择最大解压层数，选择扫描文件类型或勾选<扫描所有文件>。

图2 配置防病毒设定

2. 配置安全策略，启用病毒防护功能

如图 3 所示，进入“策略配置>IPv4 控制策略”，进入 IPv4 控制策略页面，新建策略，病毒防护子菜单中启用功能并选择防护项，完成后点击提交。

图3 配置安全策略

4.5 验证配置

(1) 验证病毒防护功能

在导航栏中选择“数据中心>日志中心>安全日志>病毒防护日志”，进入病毒防护日志页面，可以查看到病毒防护日志信息。

图4 病毒防护日志查看

目录

1 简介

暴力破解是指攻击者通过穷举的方法登录相应服务从而获得可以登录的用户名密码对。用户可配置防暴力破解功能，通过检测出流量中的暴力破解行为并进行阻断。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解防暴力破解特性。

3 使用限制

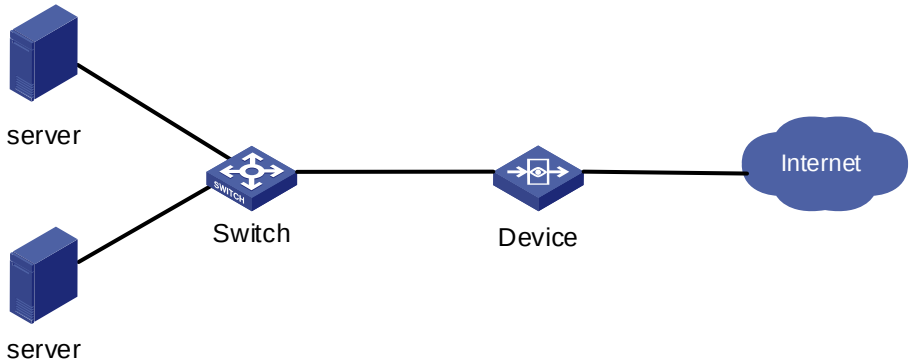
- 管理员可以设定最大登录重试次数默认为 5 次。
- 如果某账户连续输入错误的口令次数超过最大登录重试次数，系统将锁定该账户。为了防止攻击者通过不断尝试，故意造成的 DOS 攻击，设备在一定时间后会自动解锁，在不影响正常使用的同时，尽可能的降低攻击风险。

4 配置举例

4.1 组网需求

如图 1 所示，服务器通过 Internet 提供 FTP 服务，在设备上启用防暴力破解功能来监测攻击行为，当攻击次数达到阈值触发防暴力破解记录攻击事件。同时实施相应措施保护 FTP 服务器。

图1 防暴力破解功能配置组网图



4.2 配置思路

- 配置服务类型，在防暴力破解配置页面选择监测的服务。

- 配置检测时长，选择防暴力破解的检测周期。
- 配置阈值，达到阈值触发防暴力破解记录攻击事件。阈值范围为 3-1000。
- 配置响应行为，是否将攻击者加入黑名单，阻断攻击行为。

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

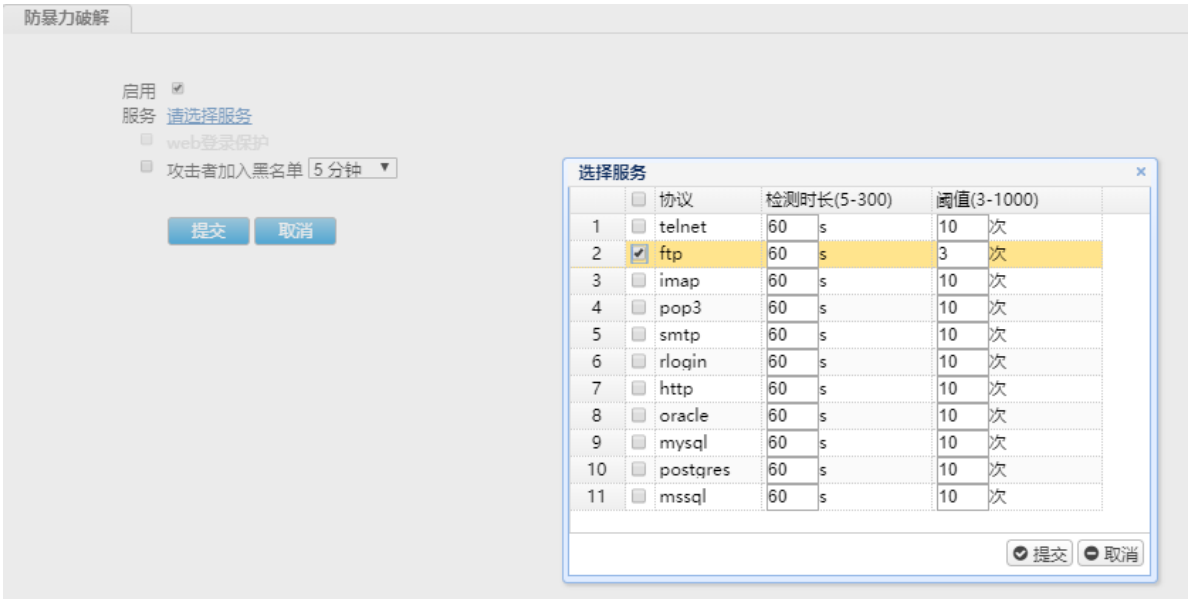
- 防暴力破解功能支持的服务类型包括 ftp、telnet、smtp、http、imap、mssql、mysql、oracle、pop3、postgres。
- 各个服务单独配置暴力破解检测时长和阈值。
- 系统支持配置是否把攻击者加入黑名单。本例分别在两种情况下进行。

4.5 配置步骤

4.5.1 启用防暴力破解功能

进入“安全设置>安全防护>防暴力破解”，进入防暴力破解配置页面，如图 2 所示。设置启用防暴力破解功能，选择服务类型为 FTP，检查次数 3。提交配置。

图2 配置防暴力破解



4.5.2 配置攻击者加入黑名单

进入“安全设置>安全防护>防暴力破解”，进入防暴力破解配置页面，如图 3 所示，设置攻击者加入黑名单时长，提交配置。

图3 配置 IPv4 策略

4.6 验证配置

使用测试 PC 进行 FTP 爆破测试。

(1) 未配置攻击者加入黑名单情况下进行 FTP 爆破测试

在导航栏中选择“数据中心>日志中心>安全日志>防暴力破解日志”，进入防暴力破解日志页面，可以查看到防暴力破解日志信息。如图 4 所示。

图4 防暴力破解日志

防暴力破解日志

查询 导出

	时间	源地址	归属地	目的地址	服务	防御动作
1	2020-01-02 16:22:23	192.168.20.50	局域网	192.168.1.116	ftp	加入黑名单
2	2020-01-02 16:19:07	192.168.20.50	局域网	192.168.1.116	ftp	忽略
3	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
4	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
5	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
6	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
7	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
8	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
9	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
10	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
11	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略
12	2020-01-02 16:18:57	192.168.20.50	局域网	192.168.1.116	ftp	忽略

(2) 配置攻击者加入黑名单下情况进行 FTP 爆破测试

在导航栏中选择“数据中心>系统监控>黑名单记录”，进入黑名单页面，可以查看到防暴力破解加入黑名单信息。如图 5 所示。

图5 黑名单记录

黑名单 黑名单记录

查询

	源IP	生命周期	生效时间	添加方式
1	192.168.20.50	5分0秒	2020-01-02 16:22:23	防暴力破解

目 录

1 简介

对于密码明文传输的服务，从登录报文中提取出密码并判断出密码强度，若为弱密码则产生日志但不阻断登录。支持的服务包括 ftp、imap、pop3、smtp、telnet。用户可以配置开启或者关闭弱密码检测功能，目标服务，弱密码密码强度。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解弱密码防护特性。

3 使用限制

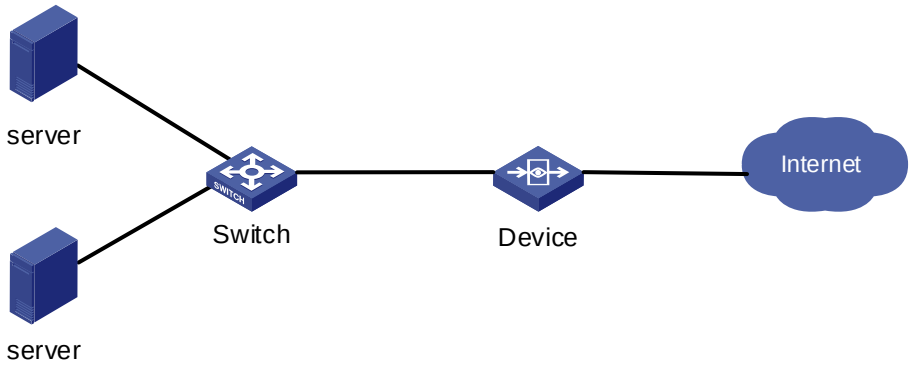
无。

4 配置举例

4.1 组网需求

如图 1 所示，某公司内网存在两台服务器，测试设备可以针对内外网进行弱密码防护日志记录，实现弱密码防护功能，测试服务器通过 FTP 对另一台服务器进行弱密码登录。

图1 弱密码防护测试组网图



4.2 配置思路

- 配置弱密码防护功能
- 配置默认规则库与自定义弱密码

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置步骤

1. 弱密码防护配置

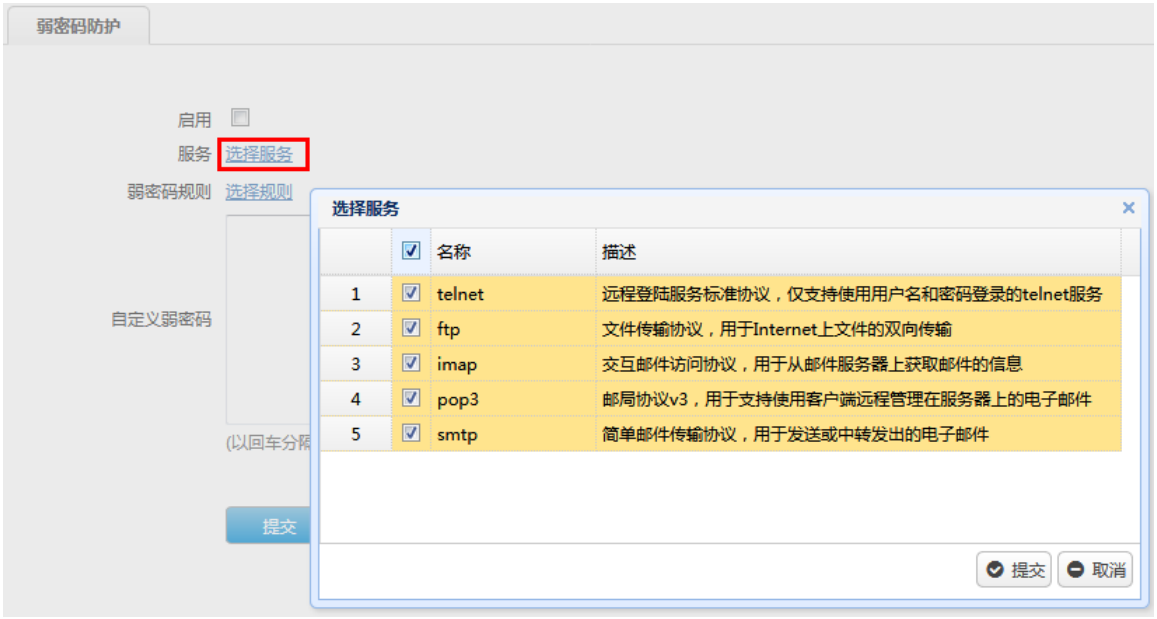
如图 2 所示，在导航栏中选择“策略配置>安全设置>安全防护>弱密码防护”，进入弱密码防护的配置界面，勾选启用。

图2 开启弱密码防护设定

2. 防护服务类型选择

如图 3 所示，点击“选择服务”弹框出现服务配置页面，选择弱密码防护服务。

图3 配置弱密码防护服务



4.5 验证配置

(1) 验证弱密码防护功能

如图 4 所示，在导航栏中选择“数据中心>日志中心>安全日志>弱密码防护日志”，进入弱密码防护日志页面，可以查看到弱密码防护日志信息。

图4 弱密码防护验证

目录

1 简介

随着网络信息化的发展，越来越多的企业利用 WEB 应用系统提供客户服务，进行产品推广、市场宣传、培训服务、远程服务协作甚至网上交易。WEB2.0 的发展更是加强了用户和 WEB 服务之间的交互性，但是各种安全问题也随之而来。WEB 应用数据被窃取、网页被篡改，甚至 WEB 站点成为传播木马的傀儡，给更多访问者造成危害，带来损失；也对政府、公司形象造成严重的破坏。目前 WAF 防火墙产品是用户用来保护 WEB 应用的首要选择。为了能够给客户提供一套更完全的安全解决方案，Web 应用防护作为一个功能模块，整体上基于当前的平台设计实现，增加 WEB 应用防护策略，匹配条件是源地址、目的地址（WEB 服务器地址）和端口，同时在策略下配置各个防护功能（精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏），当报文匹配策略时，就会逐一进行防护功能的处理，并执行相应的动作。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 WEB 防护特性。

3 使用限制

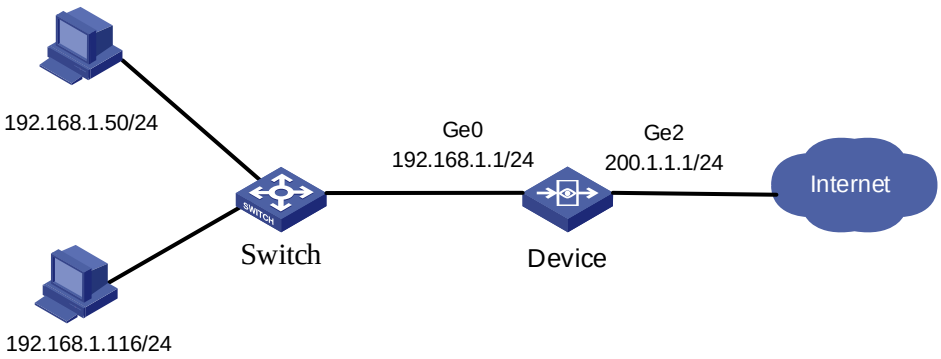
WEB 防护的优先级是精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏，在未阻断情况下依次防护。

4 配置举例

4.1 组网需求

如图 1 所示，公司内网中存在主机 192.168.1.50/24 和 192.168.1.116/24 两台主机，在设备上启用 WEB 防护功能，增加 WEB 应用防护策略，以此来实现主机访问网络的安全防护。

图1 WEB 防护功能配置组网图



4.2 配置思路

- 新建防护策略
- 配置规则防护
- 配置防盗链
- 配置 CSRF
- 配置 CC 攻击防护
- 配置网页防篡改
- 配置应用隐藏

4.3 使用版本

本举例是在 E6442 版本上进行配置和验证的。

4.4 配置注意事项

- WEB 防护功能包含精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏 7 个模块，每个模块都需配置相应策略。
- 根据严重程度的不同，日志分为以下几个级别：紧急、告警、严重、错误、警告、通知、信息。
- 规则防护日志对应下面 web 防护策略中的规则防护；精确访问控制、规则防护、防盗链、CSRF 攻击防护、CC 攻击防护、网页防篡改、应用隐藏等功能模块产生的日志记录在高级防护日志中。

4.5 配置步骤

4.5.1 配置 WEB 防护策略

进入“策略配置>安全设置>WEB 防护>防护策略”，点击“新建”进入 WEB 防护策略配置页面，完成后点击提交，如图 2 所示。

图2 配置 WEB 防护策略

4.5.2 配置规则防护

在 WEB 防护策略配置页面选择规则防护子菜单，启用规则防护，选择防护等级，完成后点击提交。如图 3 所示。

图3 配置规则防护

4.5.3 配置防盗链

在 WEB 防护策略配置页面选择防盗链子菜单，勾选启用，选择防护范围，完成后点击提交。如图 4 所示。

图4 配置防盗链

4.5.4 配置 CSRF

在 WEB 防护策略配置页面选择 CSRF 攻击防护子菜单，勾选启用，新建防护的 url，完成后点击提交。如图 5、图 6 所示。

图5 配置 CSRF

图6 配置 CSRF 防护规则

4.5.5 配置 CC 防护

在 WEB 防护策略配置页面选择 CC 攻击防护子菜单，勾选启用，选择防护范围，访问次数，处理动作。如图 7 所示，

图7 配置 CC 防护

4.5.6 配置网页防篡改

在 WEB 防护策略配置页面选择网页防篡改子菜单，勾选启用，填写防护 url，处理动作。如图 8 所示。

图8 配置网页防篡改

4.5.7 配置应用隐藏

在 WEB 防护策略配置页面选择应用隐藏子菜单，勾选启用，选择防护类型。如图 9 所示，

图9 配置应用隐藏

4.6 验证配置

使用测试 PC 进行攻击测试。

在导航栏中选择“数据中心>日志中心>安全日志>WEB 防护日志”，进入 WEB 防护日志页面，可以查看到 WEB 防护日志规则防护信息。如图 10 所示。

图10 WEB 规则防护日志

在导航栏中选择“数据中心>日志中心>安全日志>WEB 防护日志”，点击进入高级防护日志页面，可以查看到 WEB 防护高级防护信息。如图 11 所示

图11 WEB 高级防护日志

规则防护日志 高级防护日志

查询 导出

	时间	日志级别	源地址	归属地	请求方法	请求URL	事件类型	事件描述	处理动作	操作
1	2020-01-03 15:19:34	信息	192.168.20.116	局域网		http://42.236.98.110/hquery	应用隐藏	server字段被隐藏	允许	详细
2	2020-01-03 15:14:55	信息	192.168.20.116	局域网		http://tile-service.weather.m	应用隐藏	server字段被隐藏	允许	详细
3	2020-01-03 15:04:15	信息	192.168.20.116	局域网		http://ctldl.windowsupdate.c	应用隐藏	server字段被隐藏	允许	详细
4	2020-01-03 15:03:15	信息	192.168.20.116	局域网		http://mscrl.microsoft.com/p	应用隐藏	server字段被隐藏	允许	详细
5	2020-01-03 15:02:27	信息	192.168.20.116	局域网		http://ctldl.windowsupdate.c	应用隐藏	server字段被隐藏	允许	详细
6	2020-01-03 14:59:17	信息	1.1.187.114	泰国		http://AmOJuCGO/ZmhQOG	应用隐藏	server字段被隐藏	允许	详细
7	2020-01-03 14:59:14	信息	1.1.187.114	泰国		http://AmOJuCGO/ZmhQOG	应用隐藏	server字段被隐藏	允许	详细
8	2020-01-03 14:59:10	信息	1.1.231.174	泰国		http://NxAYWab/video.flv	应用隐藏	server字段被隐藏	允许	详细
9	2020-01-03 14:59:07	信息	1.1.100.164	日本		http://TpyJVDBFRPxXhORyR	应用隐藏	server字段被隐藏	允许	详细
10	2020-01-03 14:59:04	信息	1.1.166.40	泰国		http://172.16.1.2/~jxia/poc.p	应用隐藏	server字段被隐藏	允许	详细
11	2020-01-03 14:59:00	信息	1.1.166.40	泰国		http://172.16.1.2/~jxia/poc.h	应用隐藏	server字段被隐藏	允许	详细
12	2020-01-03 14:58:57	信息	1.1.255.230	泰国		http://172.16.1.11/~swarelis,	应用隐藏	server字段被隐藏	允许	详细