didSA 零信任安全接入服务端软件

V2.0.0

使用说明

成都比特威锐科技有限公司

2025 年 5 月

文档信息

文档名称	didSA 零信任安全接入服务端软件 V2.0.0 使用说明		
文档编号	/	**文档版本号**	V0.1
适用范围	使用人员	**打印份数**	

接收人		**与文档的主要关系**	**文档权限**

文档编制信息			
版本	**时间**	**说明**	**签署人**
V0.1	2025.5.5	编写	罗正伟

修订记录

修订次序	**章节号**	**修订内容**	**修订原因**	**修订人**	**日期**

目录

第一章　didSA 零信任安全接入服务端软件简介

什么是 didSA 零信任安全接入服务端软件

didSA 零信任安全接入服务端软件（简称 didSA 服务端）主要用于取代传统的 SSL VPN、IPsecVPN、PPTP 或 L2TP 等远程安全接入软件，didSA 服务端是以基于角色的访问控制技术、内核级 UDP 隧道技术、公钥认证技术为核心，以安全、简单、快速为目标开发的第三代安全接入软件。

软件特点

基于角色的权限管理、自动下发客户端配置、无密码认证、内核级 UDP 隧道、自动路由下发、自动地址转换、非对称加密、流加密

管理员通过新建资源与角色来对接入的终端用户与分支用户进行权限管理，支持全网资源、特定网络访问资源、应用资源。支持批量导入用户，支持自动申请并配置 SSL 证书。用户或分支设备通过短信验证码自动从服务端同步配置，客户端连接服务端时通过公钥进行身份认证，然后以内核级（Linux5.6+）UDP 协议建立通信隧道，使用非对称加密算法交换加密密钥，然后使用此密钥进行流加密，实现了安全高效的加密隧道连接。

加密隧道建立时会自动下发总部对应本地子网的路由条目，分支子网对应的路由条目也将自动上传并生效，针对终端或分支访问总部或总部访问分支，或终端接入总部后访问分支等各种复杂的访问场景，didSA 服务端将自动完成 NAT 策略来保障路由可达，减轻实施人员或管理人员的运维负担。

主要技术原理

软件运行主要涉及基于角色的权限管理、非对称加密算法、内核级 UDP 隧道、流加密技术、自动路由下发、自动地址转换：

1. 基于角色的权限管理

一个网络如 192.168.10.0/25、192.168.10.250、192.168.10.110-192.168.10.120 即为一个网络资源，一个 IP 地址与端口组合即为一个应用资源，如 192.168.10.250，TCP,8080 管理员通过新建资源与资源组，然后根据用户的实际业务身份创建角色，即用户需要访问的所有资源集合。用户与资源的一个绑定即为一个角色，软件会为每个角色创建一个访问控制规则，最后通过此访问控制规则对用户的访问行为进行限制（最小化权限白名单策略）。

2. 非对称加密算法

非对称加密算法是当今网络安全与密码学领域的核心技术，使用非对称加密算法前必须先生成一个满足条件的随机数，这个随机数称为私钥，然后根据私钥计算出对应的公钥。用私钥加密的数据可以用公钥解密，用公钥加密的数据可以用私钥解密，私钥由密钥拥有人掌握，公钥可以由任意需要与私钥拥有人通信或建立联系的人掌握。didSA 安全接入客户端软件在通过认证后即使用对方的公钥加密一个随机生成的 Key，服务端收到后使用自己的私钥即可解密 Key。

didSA 安全接入软件可支持以下三种非对称加密算法：

Curve25519： 基于 ECDSA 的非对称加密算法，是目前行业公认最快的椭圆曲线类非对称加密算法，其中 ED25519 常用于数字签名，X25519 常用于密钥交换。

SM2（国密）：基于 ECDSA 的非对称加密算法，被列为中国国家商用密码算法标

准；

Secp256K1：基于 ECDSA 的非对称加密算法，是区块链行业使用最多的非对称加密算法。

3. 内核级 UDP 隧道技术

相比于 SSL VPN 使用的 TCP 协议，内核级 UDP 隧道技术具有协议简单高效快速的特点，此技术已被 Linux5.6+集成到操作系统内核，但 UDP 协议本身并不提供数据传输可靠性保障，需依赖于应用层代码实现。didSA 安全接入软件使用 UDP 协议与数据流验证 HMAC 技术实现了 UDP 隧道的可靠性保障。

4. 流加密技术

流加密与分组加密类似，都是应用广泛的对称加密算法，其中流加密的特点是效率高。didSA 支持 ChaCha20-Poly1305 与 ZUC- HMAC 流加密算法。

5、自动路由下发技术

加密隧道建立时，didSA 服务端会根据系统配置自动向接入的终端或分支设备下发对应的总部本地子网，而分支子网也会自动写入到总部设备。

6、自动地址转换技术

针对终端或分支访问总部或总部访问分支，或终端接入总部后访问分支等各种复杂的访问场景，didSA 服务端将自动完成 NAT 策略来保障路由可达，减轻实施人员或管理人员的运维负担。

主要功能模块介绍

功能	说明
状态	显示当前终端用户与分支用户的连接状态； 可显示用户的内网 IP，外网 IP，角色，接收流量，发送流量，最近握手时间等 显示当前设备的硬件状态：CPU 使用情况、内存使用情况、网卡状态与流量统计
终端	**用户管理：** 手动填写新建用户、通过表格导入用户、应用配置、搜索用户； 显示已有用户的基本信息； 下载用户的配置文件、展示用户配置文件的二维码、禁用或删除用户； **资源与资源组管理：** 创建网络资源与应用资源； 编辑或删除现有资源； 显示现有资源的基本信息； 创建资源组； **角色管理：** 通过资源或资源组创建新的角色； 编辑或删除角色；
分支	**用户管理：** 手动填写新建用户、通过表格导入用户、应用配置、搜索用户； 显示已有用户的基本信息； 下载用户的配置文件、展示用户配置文件的二维码、禁用或删除用户； **资源与资源组管理：** 创建网络资源与应用资源； 编辑或删除现有资源； 显示现有资源的基本信息； 创建资源组； **角色管理：** 通过资源或资源组创建新的角色； 编辑或删除角色；
设置	**终端接入：** 设置服务地址、用户虚拟 IP 地址池、本地子网、监听端口、DNS 服务器等基本信息； 针对每一个配置项目进行说明； 指导用户正常配置服务端； **分支接入：** 设置服务地址、虚拟 IP 地址池、本地子网、监听端口、传输层协议等基

	本信息； 针对每一个配置项目进行说明； 分支接入端： 导入分支设备的配置文件、设置访问策略 **全局设置：** 新建、编辑、删除管理员帐号，设置管理员权限，支持三权分立帐号； 开启或关闭 SSH 服务、通过域名访问控制台、业务访问审计； **配置下发：** 设置企业代码并申请 SSL 证书； 自动配置 SSL 证书；
系统日志	展示所有用户的登录与退出日志； 根据用户名与时间段搜索日志；
关于	展示服务端软件的基本信息：版本、授权用户、授权用户数等； 授权文件导入；

第二章 使用说明

申请授权许可：

didSA 服务端启动后在浏览器中访问：https://IP 地址:51001 访问 Web 控制台（请使用 https 访问），公有云场景请先确认已在防火墙规则中放通 51001 端口；

默认用户名：admin
默认密码：bitvr
打开：设置-全局设置
然后点击导入授权，选择授权文件导入后即可激活，如无授权文件请通过云商店或您的服商购买相应的授权（License）；

一、终端接入场景

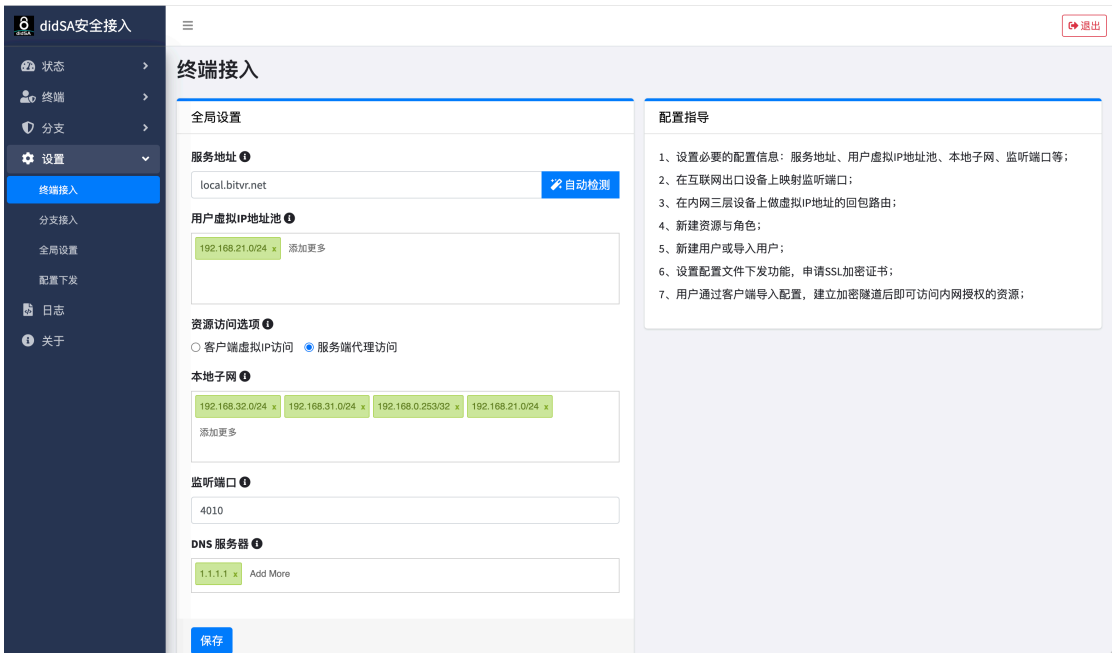
主要步骤：

1、设置必要的配置信息：服务地址、用户虚拟 IP 地址池、本地子网、监听端口等；
2、在互联网出口设备上映射监听端口；
3、在内网三层设备上做虚拟 IP 地址的回包路由；
4、新建资源与角色；
5、新建用户或导入用户；
6、设置配置文件下发功能，申请 SSL 加密证书；
7、用户通过客户端导入配置，建立加密隧道后即可访问内网授权的资源；

（1）设置必要的配置信息

didSA 服务端启动后在浏览器中访问：https://IP 地址:51001 访问 Web 控制台（请使用 https 访问），公有云场景请先确认已在防火墙规则中放通 51001 端口；

然后打开：设置-终端接入页面



服务地址请填写 didSA 服务端所有网络的公网 IP 地址；

用户虚拟 IP 地址池可保持默认；

资源访问选项如选择客户端虚拟 IP 访问则需要在内网三层设备上做回包路由，如不理解此选项建议选择服务端代理访问；

本地子网为 didSA 服务端所在网络可访问的内部网段，即需要发布给终端用户访问的网段；

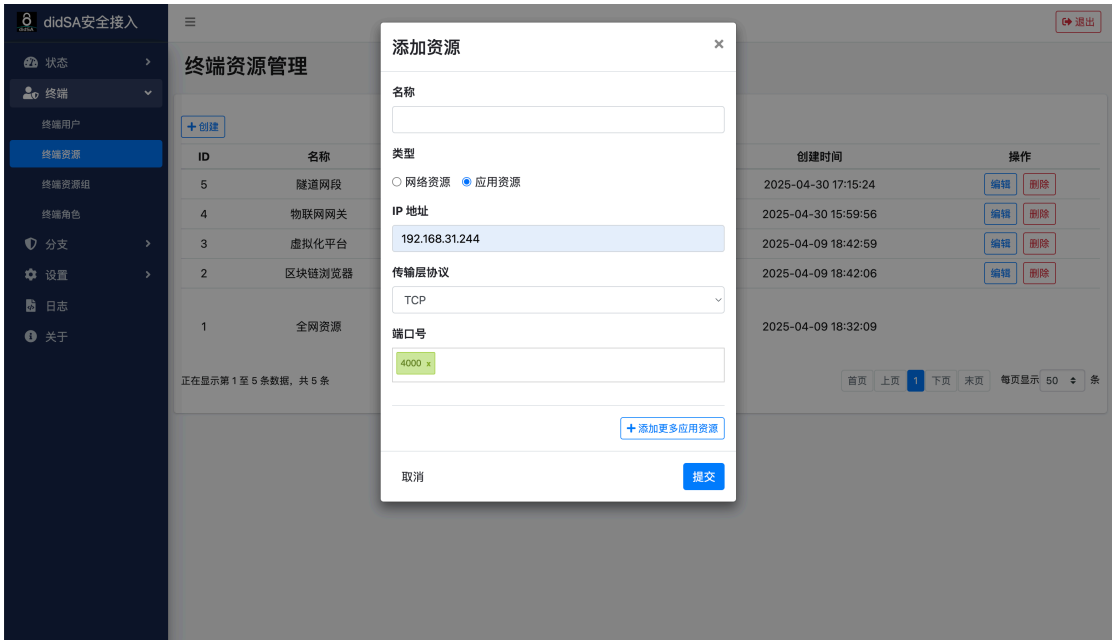
监听端口为加密隧道所使用的 UDP 端口，可以保持默认，如果 didSA 服务为单臂部署在内网，则这里填写的端口需要在出口网关上进行映射；

DNS 服务器为需要下发给终端用户的 DNS，这里填写后还需要在用户设置处进行勾选，大部分场景可以不填写；

（2）配置资源与角色

打开：终端-终端资源-创建页面

创建一个应用资源，填写 IP 地址、协议、端口号



打开：终端-终端角色-创建

创建一个访问区块链浏览器的角色，这个角色绑定刚才创建的区块链浏览器的资源

（3）创建终端用户

打开：终端-终端用户-新建用户

新建一个用户并关联访问区块链浏览器的角色

这里的 IP 地址会自动从第一步设置的虚拟 IP 地址池中选取，下发路由也会自动从本地子网上读取，保持默认就可以了；

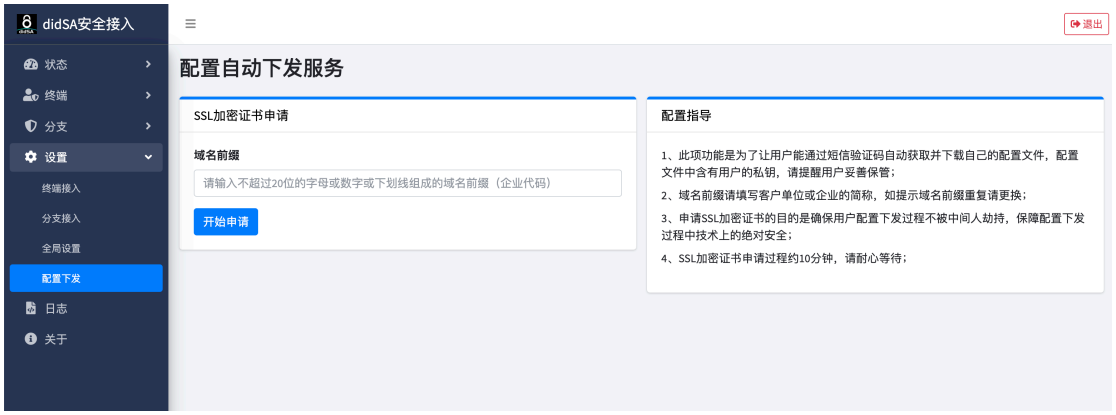
重定向网关功能勾选后终端用户将使用总部的网络连接互联网，默认为不勾选；

使用指定 DNS 勾选后将使用第一步设备的 DNS 作为终端用户的 DNS，默许不勾选；

（4）在互联网出口网关或防火墙上放通或映射隧道端口

（5）配置自动下发服务

打开：设置-配置下发页面

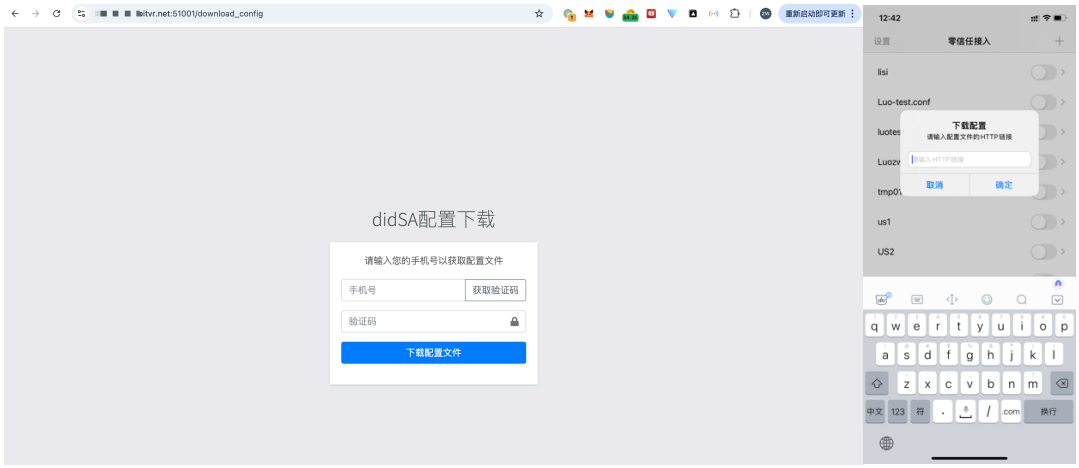


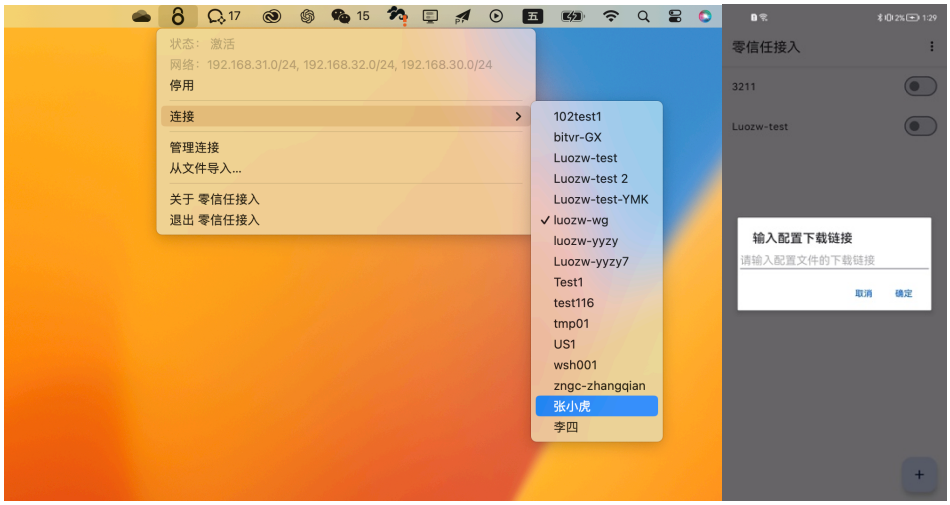
按要求填写域名前缀后约 10 分钟即可自动申请并配置 SSL 证书成功；

（6）下载客户端与配置文件后一键连接

Windows amd64: *https://local.bitvr.net:40172/f/3b24ff6ae2bd46629ab2/*
Windows arm64: *https://local.bitvr.net:40172/f/a077f910a48a4db994b6/*
macOS：*https://testflight.apple.com/join/tQ3DVw5P*
Linux(Ubuntu18+或 Centos7+)：*https://local.bitvr.net:40172/f/61795a94981944138de6/*
手机或平台统一下载连接：*https://m.malink.cn/s/3qABJv*

客户端安装完成后还需要打开上一步配置下发的链接，用户输入手机号进行验证码验证通过后即会自动下载包含密钥的用户的个人配置文件，用户在客户端导入此配置文件后即可自动连接；




状态：激活
网络：192.168.31.0/24, 192.168.32.0/24, 192.168.30.0/24
停用
连接
管理连接
从文件导入...
关于 零信任接入
退出 零信任接入
102test1
bitvr-GX
Luozw-test
Luozw-test 2
Luozw-test-YMK
luozw-wg
luozw-yyzy
Luozw-yyzy7
Test1
test116
tmp01
US1
wsh001
zngc-zhangqian
张小虎
李四
零信任接入
3211
Luozw-test
输入配置下载链接
请输入配置文件的下载链接
取消
确定

Linux 终端用户接入说明：

第一次接入请解压后到直接运行：

tar -xzvf ./didsaClient_linux_install.tar.gz
mv didsaClient_linux_install didsaClient
cd didsaClient
./didsa_linux_installer

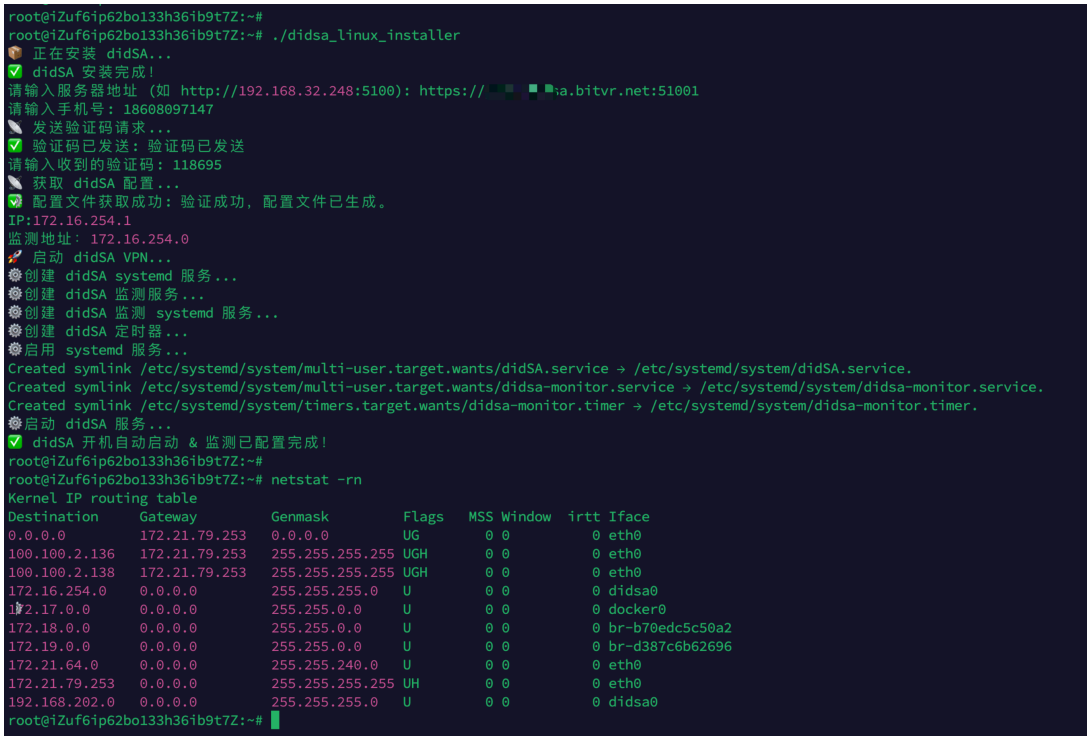
然后按提示输入手机号与验证码后即可正常接入，客户端默认会自动创建开机自动运行与网络监测服务；

如需断开连接请执行：

./stop_didsa_linux

重新启动请执行：

./start_didsa_linux



二、分支机构接入场景

主要步骤：

1、设置必要的配置信息：服务地址、分支设备隧道 IP 地址池、本地子网、监听端口、传输层协议等；

2、在互联网出口设备上映射监听端口；

3、在总部与分支机构的三层设备上写入到对方的路由条目；

4、新建分支资源与角色；

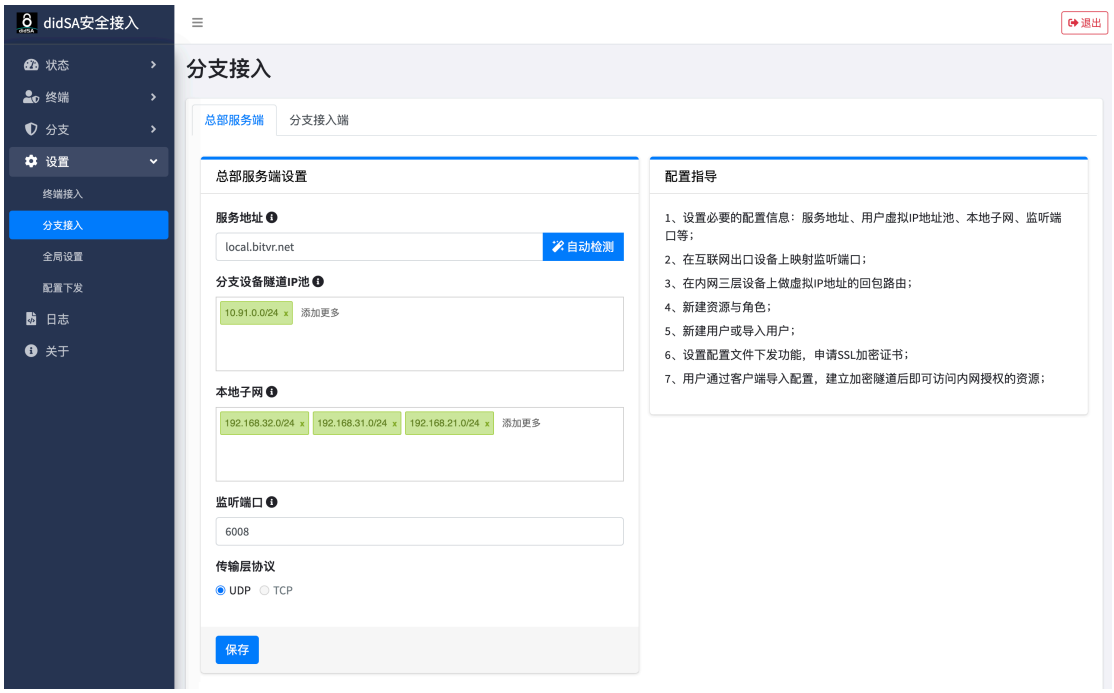
5、新建分支用户或导入用户；

6、下载分支用户配置文件，导入到分支设备后即可自动建立隧道连接；

（1）设置必要的配置信息

在总部设备上操作

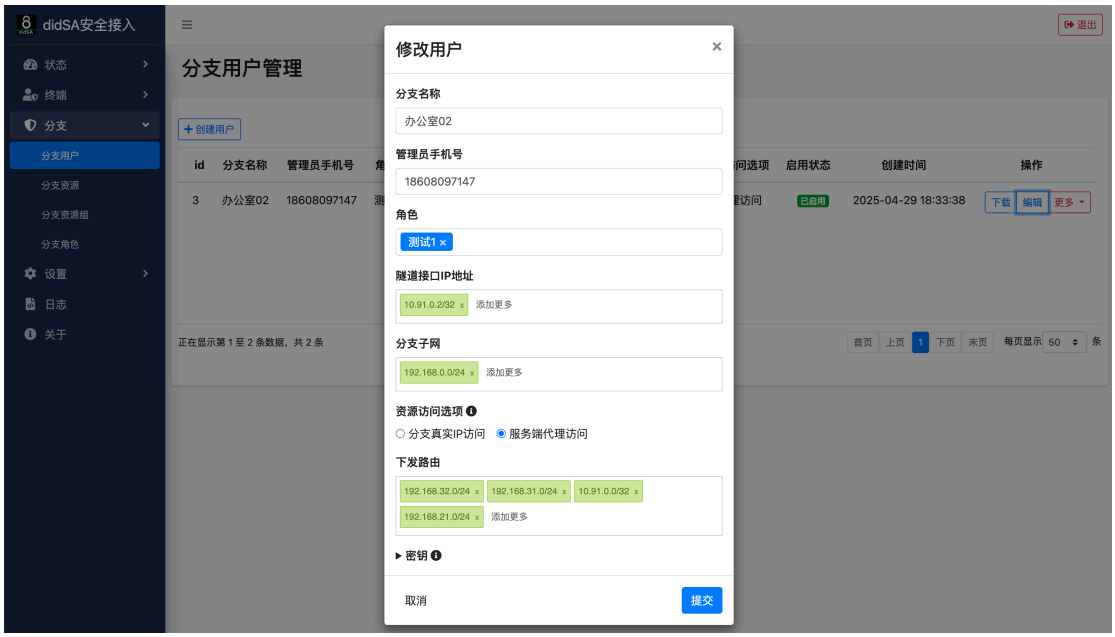
打开：设置-分支接入-总部服务端



（2）新建分支资源或资源组

（3）新建分支角色

（4）新建分支用户



分支子网请填写分支机构所有需要连接总部的网段；

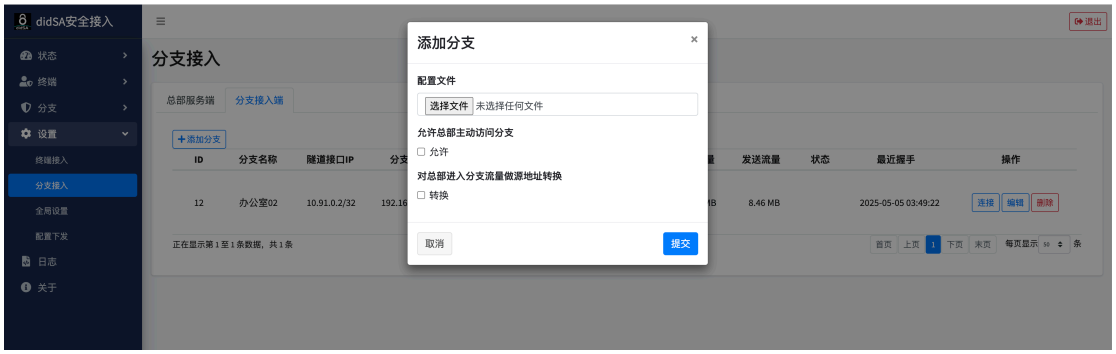
资源访问选项选择分支真实 IP 访问时需要在总部的三层设备上做回包路由，选择代理访问时无需做回包路由，分支的 IP 会被转换为总部设备的 IP；

（5）在总部的互联网出口或防火墙映射并放通监听端口

（6）下载分支用户的配置文件，在分支设备上导入

在分支设备上操作

打开：设置-分支接入-分支接入端-添加分支



如不勾选允许总部主动访问分支则总部无法主动对分支发起访问；

勾选对总部进入分支流量做源地址转换后，分支设备会将总部的源 IP 转换为分支设备的 IP 地址，分支的三层设备上无需再手动写入总部的路由条目；