

# 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	え 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				

# 修订记录

修订次序	章节号	修订内容	修订原因	修订人	日期

第一章	didSA 零信任安全接入服务端软件简介	.2
第二章	使用说明	.7
	终端接入场景 分支接入场暑	.7 14

# 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。

2

#### 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

3

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。

4

# 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	<ul> <li>用户管理:</li> <li>手动填写新建用户、通过表格导入用户、应用配置、搜索用户;</li> <li>显示已有用户的基本信息;</li> <li>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;</li> <li>资源与资源组管理:</li> <li>创建网络资源与应用资源;</li> <li>编辑或删除现有资源;</li> <li>显示现有资源的基本信息;</li> <li>创建资源组;</li> <li>角色管理:</li> <li>通过资源或资源组创建新的角色;</li> <li>编辑或删除角色;</li> </ul>
分支	<ul> <li>用户管理:</li> <li>手动填写新建用户、通过表格导入用户、应用配置、搜索用户;</li> <li>显示已有用户的基本信息;</li> <li>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;</li> <li>资源与资源组管理:</li> <li>创建网络资源与应用资源;</li> <li>编辑或删除现有资源;</li> <li>显示现有资源的基本信息;</li> <li>创建资源组;</li> <li>角色管理:</li> <li>通过资源或资源组创建新的角色;</li> <li>编辑或删除角色;</li> </ul>
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 <b>全局设置:</b> 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; <b>配置下发:</b> 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

👌 didSA安全接入	≡	● 退出
፼3 状态 >	终端接入	
<ul> <li>♥ 分支 &gt;</li> <li>✿ 设置 &gt;</li> </ul>	全局设置 服务地址 O	配置指导 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;
終端接入 分支接入 全局设置 配置下労	localbitv.net <b>梁自动始激</b> 用户虛找IP地址池 ● 192.168.21.024 x 流加更多	<ol> <li>在互联网出口设备上映明监听端口:</li> <li>在互联网上员设备上帧虚拟IP地址的回包路由:</li> <li>新建资源与角色:</li> <li>新建用户或导入用户:</li> <li>(设置配置文件下发功能,申请SSL加密证书;</li> </ol>
1224 1 X 133 日志 139 关于	资源访问选项 ● ● 客戶購虛拟IP访问 ● 服务端代理访问 本地子网 ●	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;
	192.168.32.0724 x 192.168.31.0724 x 192.168.0.253/32 x 192.168.21.0724 x 活力更多	
	监听端口 ❶ 4010 DNS 服务器 ❶	
	1.1.1.1 x Add More	

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

<b>8</b> didSA安全	:接入	=			_		● 退出
<b>企</b> 状态		终端咨望	<b>源管理</b>	添加资源	×		
♣ 终端		~~ >10 5~	<i>ил</i> д - <u>т</u>	名称			
终端用户		十创建					
终端资源		ID	名称	类型		创建时间	操作
终端资源组		5	隧道网段	○ 网络资源 ● 应用资源		2025-04-30 17:15:24	编辑 删除
终端角色		4	物联网网关	IP 地址		2025-04-30 15:59:56	编辑 删除
♥ 分支		3	虚拟化平台	192.168.31.244		2025-04-09 18:42:59	编辑 删除
💠 设置		2	区块链浏览器	传输层协议		2025-04-09 18:42:06	编辑 删除
國 日志				ТСР	<u> </u>		
3 关于		1	全网资源	端口号		2025-04-09 18:32:09	
		正在显示第1至	5条数据,共5条	4000 x		首页 上页 1 下页	末页 <b>每页显示</b> 50 辛 条
				+ 添加更多应用资			
				取消 提3	٤		

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

🙆 didSA安全接入	≡						● 退出
<b>£</b> 39 状态	终端角色管	理	修改角色	c			
▲ 终端			名称				
终端用户	十创建		访问区块链浏览器				
终端资源	ID	名称	待选择资源组	已选择资源组	创建	时间	操作
终端资源组	4	物联网网关	筛选	筛选	2025-04-3	30 16:00:40	編輯 删除
终端角色	3 私	有云平台管理	>>	<<	2025-04-	09 18:44:14	編輯 删除
● 分支	2 访问	可区块链浏览器			2025-04-0	09 18:43:58	編輯  删除
💠 设置	1	访问全网			2025-04-	09 18:43:37	編辑 删除
5 日志	正在显示第1至4条数据	, 共4条	待选择资源	已选择资源		首页 上页 1 下页	末页 每页显示 50 ♀ 条
<ol> <li>关于</li> </ol>			筛选	筛选			
			>>	<<			
			全网资源 虚拟化平台 物联网网关 隧道网段	区块链浏览器			
			取消	撮交			

(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

8 didSA安全接入	= /					●退出
aaa (11-1-1-)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)(二)	终端用户管理	编辑张小虎 ×				
▲ 终端 >		用户名称				
终端用户	+ 新建用户 14 导入用户 14 导出用	张小虎				
终端资源	搜索: 所有	手机号				
终端资源组		186 47	d P			
终端角色	用户名称 角色	角色	कर	创建时间	更新时间	操作
♥ 分支 >	张小虎 访问区块链浏 1	访问区块链浏览器 × 数联网网关 ×	2	2025/04/09	2025/05/02	下载 二维码 更多 *
💠 设置 🔹 🔸	览器, 物联网网 关	IP地址		18:44:55	10:43:32	
。 日志	~	192.168.21.1/32 x 添加更多				
④ 关于		下发路由				
		192.168.32.0/24 x 192.168.31.0/24 x 192.168.0.253/32 x				
	正在显示第1至1条数据,共1条	192.168.21.0/24 x 添加更多			首页 上页 1 下页	末页 每页显示 50 \$ 条
		重定向网关 🚯				
		使用指定DNS 🕕				
		✓ 启用该用户				
		▶ 密钥 ①				
		<b>取消</b> 保存				

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

🧕 didSA安全接入	=	<b>6</b> 漫出
🕰 状态	配置自动下发服务	
🎝 终端		
● 分支	SSL加密证书申请	配置指导
💠 设置	域名前缀	1、此项功能是为了让用户能通过短信验证码自动获取并下载自己的配置文件,配置 文化中令有用户的私钥、清掃醒用户买等保等。
终端接入	请输入不超过20位的字母或数字或下划线组成的域名前缀(企业代码)	2、域名前缀请填写客户单位或企业的简称,如提示域名前缀重复请更换;
分支接入	开始申请	3、申请SSL加密证书的目的是确保用户配置下发过程不被中间人劫持,保障配置下发 过程中共产业的绝对中全。
全局设置		4、SSL加密证书申请过程约10分钟,请耐心等待;
配置下发		
😼 日志		
● 关于		

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;

👌 didSA安全接入	=	(1) 通出
22a 状态 >	配置自动下发服务	
<b>≜</b> ⊕终端 >	지므로나미성	<b>訂型化</b> 尺
● 分支 >	配直下发版劳	配直指导
🗢 设置 🖌 🖌	配置自动下发服务成功 用户注闭https://	1、此项功能是为了让用户能通过短信验证码自动获取并下载自己的配置文件,配置 文件中含有用户的私钥,请提醒用户妥善保管;
终端接入	通过加密信道自动获取并下载配置文件,配置文件导入到客户端后即可建立安全接入	2、域名前缀请填写客户单位或企业的简称,如提示域名前缀重复请更换;
分支接入	隧道。	3、申请SSL加密证书的目的是确保用户配置下发过程不被中间人劫持,保障配置下发 过程中技术上的绝对安全;
全局设置		4、SSL加密证书申请过程约10分钟,请耐心等待;
配置下发		
66 日志		
● 关于		

# (6) 下载客户端与配置文件后一键连接

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

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;

← → C (2 B ■ ■ ■ bitvr.net:51001/download_config		☆ 💊 🗶 👻 🚓 🛛 🔻 🗖 😣 🎦 🛛	重新启动即可更新	12:42	#?∎
				设置 零信任接入	+
				lisi	
				Luo-test.conf	
				下载配置 luotes 清输入配置文件的HTTP链接	
				取消 确定 tmp01	
	didSA配置下载			us1	
	请输入您的手机号以获取配置文件			US2	
	手机号 获取验证码	]		te u d	Q ♥
	验证码			$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	i o p
	下载配置文件			a s d f g ĥ j	k İ
					m 🛛
				中文 123 符 • _ / .co	m 换行
				•	



# 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

root@iZuf6ip62b	o133h36ib9t7Z:~#										
root@iZuf6ip62bo133h36ib9t7Z:~# ./didsa_linux_installer											
▶ 正在安装 didSA											
🖌 didSA 安装完成!											
清输入服务器地址 (如 http://192.168.32.248:5100): https:// =   ■ ▲a.bitvr.net:51001											
请输入手机号: 18	<b>请输入手机号: 18608097147</b>										
🔪 发送验证码请:	发送验证码请求										
☑ 验证码已发送	: 验证码已发送										
请输入收到的验证	码: 118695										
🔪 获取 didSA 酝	置										
💀 配置文件获取)	成功:验证成功,	记置文件已生成。									
IP:172.16.254.1											
监测地址: 172.10	6.254.0										
🖋 启动 didSA VI	PN										
Ø创建 didSA sys	stemd 服务										
@创建 didSA 监测	则服务										
會创建 didSA 监测	则 systemd 服务										
會创建 didSA 定	时器										
協用 systemd )	服务										
Created symlink	/etc/systemd/sys	stem/multi-user.t	arget.w	ants/c	didSA.se	ervice → /etc/systemd/system/didSA.service.					
Created symlink	/etc/systemd/sys		arget.w		didsa-m	onitor.service → /etc/systemd/system/didsa-monito					
Created symlink	/etc/systemd/sys	stem/timers.targe		/didsa	a-monito	or.timer → /etc/systemd/system/didsa-monitor.time					
會启动 didSA 服											
🗹 didSA 开机自动	动启动 & 监测已配	置完成!									
root@iZuf6ip62b	o133h36ib9t7Z:~#										
root@iZuf6ip62b	o133h36ib9t7Z:~#	netstat -rn									
	ng table										
			Flags	MSS W							
172.17.0.0											
						0 br-d387c6b62696					
root@iZuf6ip62b	o133h36ib9t7Z:~#										

## 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

â, didSA安全接入	=	(	健治
<ul> <li>관 状态 &gt;</li> <li>▲● 终端 &gt;</li> </ul>	分支接入		
<ul> <li>♥ 分支 &gt;</li> <li>◆ 设置 ~</li> <li>终端接入</li> </ul>	总部服务端设置	配置指导	
<b>分支接入</b> 全局设置	服务地址 ① local.bitv.net 学自动检测 公式设备账证证证 ①	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; 2、在印刷二层记念上映射出时始地的同常用。	
配置下发 150 日志 13 关于	10.51.0.084 ★ 添加更多	<ol> <li>、</li></ol>	
	本地子网 ❶ 192.168.32.0/24 x 192.168.31.0/24 x 192.168.21.0/24 x 添加更多	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;	
	监听端口 ❶ 6008 传输层协议		
	● UDP ◎ TCP 保存		

(2) 新建分支资源或资源组

ê ersa	didSA安全接)	<b>\</b>	=					●退出
æ	状态		分支资源	原管理				
20	终端							
Ø	分支		十创建					
	分支用户		ID	名称	类型	资源值	创建时间	操作
	分支资源		4	32.248	网络资源	192.168.32.248/28 192.168.32.11	2025-04-30 11:56:32	编辑  删除
	分支资源组		3	区块链浏览器	应用资源	192.168.31.244:TCP:4000	2025-04-29 15:37:05	编辑  删除
	分支角色		2	32	网络资源	192.168.32.0/24	2025-04-29 15:35:46	编辑  删除
\$	设置		1	全网资源	全网资源	192.168.32.0/24	2025-04-29 14:56:41	
\$	日志			11111111	111110	192.168.31.0/24		
6	关于		正在显示第1至4	1条数据,共4条			首页 上页 1 下页	末页 每页显示 50 \$ 条

# (3) 新建分支角色

6 shtta	didSA安全接入	ς	=					☞ 退出
£	)状态	>	分支角色管理	浬				
2	> 终端	<b>`</b>						
¢	り 分支	•	+创建					
	分支用户		ID	名称	资源组	资源	创建时间	操作
	分支资源		2	测试1		区块链浏览器 32.248	2025-04-29 15:38:23	编辑删除
	分支资源组		1	运维		全网资源	2025-04-29 11:30:11	编辑  删除
	分支角色		正在显示第1至2条数据,	共2条			首页 上页 1 下页	末页 每页显示 50 \$ 条
\$	;设置	<b>`</b>						
\$	日志							
6	9 关于							

# (4) 新建分支用户

å didSA安全接入	=					☞ 退出
<b>企 </b> 状态 >	分支用户管理	修改用户 × ×				
<b>≟</b> ₀终端 >		分支名称				
● 分支 ・	+ 创建用户	办公室02				
分支用户	id 分支名称 管理员手机号 角	管理员手机号	问选项	启用状态	创建时间	操作
分支资源	2 +/\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	18608097147	82±723		2025 04 20 40:22:20	
分支资源组	3 小公室02 1860809/14/ 测	角色	£1/01∩J	已启用	2025-04-29 18-33-38	下载编辑更多▼
分支角色						
✿ 设置 >		隧道接口IP地址				
。 日志		10.91.0.2/32 x 添加更多				
3 关于	正在显示第1至2条数据,共2条	分支子网			首页 上页 1 下页 オ	雨 毎页显示 50 \$ 条
		192.168.0.0/24 x 添加更多				
		资源访问选项 🕕				
		○ 分支真实IP访问 ● 服务端代理访问				
		下发路由				
		192.168.32.0/24 x 192.168.31.0/24 x 10.91.0.0/32 x				
		192.168.21.0/24 x 添加更多				
		▶密钥 ❶				
		取消提交				

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

â didSA安全接入	=											● 退出
	分支接	λ		添加	分支			×				
<b>皇</b> 。终端 >		•		配置文	件							
♥ 分支 >	总部服务:	谱 分支接入端		选择	<b>文件</b> 未选择任何:	文件						
<b>\$</b> 设置 •	+添加:	<i>}</i> ₹		允许总	部主动访问分支							
终端接入	ID	分支名称	隧道接口IP	分支 🗆 允许					发送流量	状态	最近握手	操作
分支援入				对总部	进入分支流量做源;	地址转换						
全局设置	12	办公室02	10.91.0.2/32	192.16	ŧ			1B	8.46 MB		2025-05-05 03:49:22	连接编辑删除
配置下发	正在显示	第1至1条数据,共14	5	取消				报交			संच । ज न	□ 末□ 毎页显示 59 \$ 条
國 日志							_					
⑥ 关于												
<u>8</u> didSA安全接入	=											● 退出
● # 状态 >	分支接	λ										
🎝 终端 >												
♥ 分支 >	总部服务	需 分支接入端										
💠 设置 🗸 🗸	+添加:	支										
终端接入	ID	分支名称	隧道接□IP	分支子网	下发路由	允许总部访问	传输层协议	接受流量	发送流量	状态	最近握手	操作
分支接入					192.168.32.0/24							
全局设置	12	办公室02	10.91.0.2/32	192.168.0.0/24	10.91.0.0/32	是	UDP	92 B	180 B	~	2025-05-05 14:01:47	断开编辑剧除
配置下发	正在显示	第1至1条数据,共1条	ę		192.168.21.0/24						首页 上页 1 下	页 末页 每页显示 ∞ ♠
<b>尚</b> 日志												
① 关于												

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;