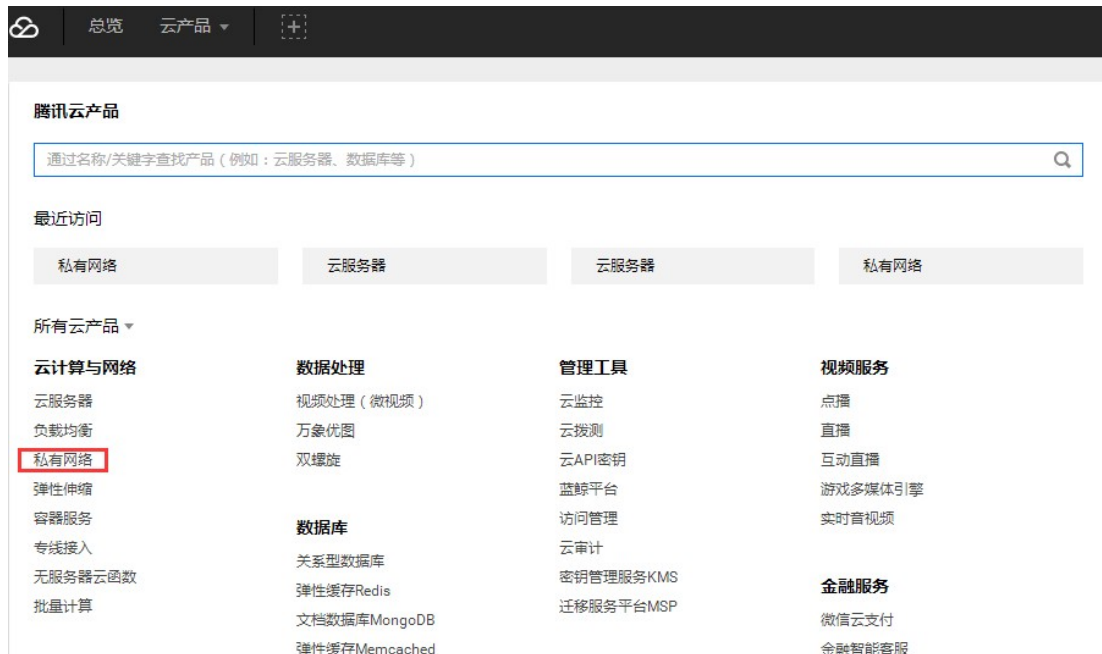


Array SSL VPN 腾讯云部署

1 在 VPC 下部署 Array SSL VPN

1.1 新建 VPC

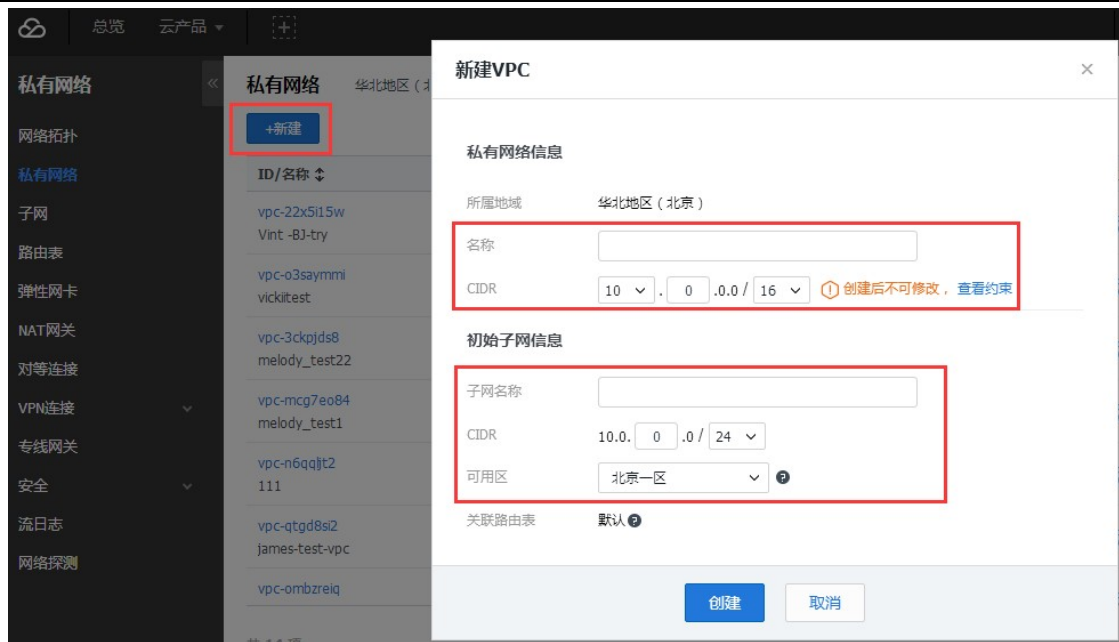
1. 登录腾讯云控制台，<https://console.cloud.tencent.com/>
2. 点击【私有网络】进入私有网络控制台



3. 选择合适的地域，比如【华北地区（北京）】



4. 新建 VPC，并且定义好 VPC 和子网的名称以及 CIDR，以及选择合适的可用区



5. VPC 创建完成。

1.2 新建云主机

1. 登录腾讯云云主机购买页面，<https://buy.cloud.tencent.com/cvm>
2. 选择合适的地域以及可用区（请选择在步骤 1 中创建的 VPC 同个地域、同个可用区）
3. 选择系列、机型、选择服务市场，在服务市场中选择【Array SSL VPN】
(推荐 2 核 CPU、4G 内存及以上机型配置)



服务市场	Array-SSL-VPN	免费使用
基础环境	操作系统：Ubuntu Server 14.04.1 LTS 64位	同意用户协议
全能环境	集成软件：Array-SSL-VPN	
管理与监控	提供商家：华耀(中国)科技有限公司	
建站模板		
安全高可用	天清汉马VPN网关系统（需同时购买对应的运维服务）	免费使用
Docker容器	操作系统：CentOS 7.0 64位	同意用户协议
业务管理	集成软件：无	
	提供商家：北京启明星辰信息安全技术有限公司	
vpn		
	山石网科虚拟化下一代防火墙 旗舰版（需购买授权）	免费使用
	操作系统：Ubuntu 14.04 64位	同意用户协议
	集成软件：stoneos	
	提供商家：北京山石网科信息技术有限公司	
	Veeam Cloud Connect	免费使用
	操作系统：Windows Server 2016 数据中心版 64位中文版	同意用户协议
	集成软件：Veeam Cloud Connect 9.5 Update2	
	提供商家：卫盟软件科技（北京）有限公司	

4. 其他步骤，按照要求选择，其中请务必选择【私有网络】、【选择购买】以及分配合适的带宽。如下配置可供参考：

1.选择地域与机型 2.选择镜像 **3.选择存储与网络** 4.设置信息

网络类型 基础网络 私有网络

基础网络与私有网络不能互通，购买后不能更换网络类型，请谨慎选择

网络 共253个子网IP，剩251个可用

如现有的网络不合适，您可以去控制台 [新建私有网络](#) 或 [新建子网](#)

用作公网网关

公网IP

带宽计费模式 [详细对比](#)

带宽 Mbps

已选配置

- 计费模式: 按量计费
- 地域: 华北地区 (北京)
- 可用区: 北京一区
- 机型: 系列2、标准型S2、4核CPU、8G内存
- 镜像: Array-SSL-VPN Rel_9_4_0_66
- 存储: 系统盘 (云硬盘 100G)、无数据盘
- 所属网络: Vint -BJ-try-Vint 北京 子网2
- 带宽计费模式: 按使用流量(带宽上限5Mbps)
- 购买量: 1台

费用:

配置费用	网络费用
1.32 元/小时 (阶梯计费 ? 计费详情)	0.80 元/GB

[上一步](#) [开通](#)

5. 最后点击【开通】，稍等片刻，Array SSL VPN 云主机即可创建完成。
(依据所选择的云硬盘种类加载时间会稍有不同，一般全部加载完成在 5~10 分钟之间)

ID/主机名	监控/状态	可用区	主机类型	配置	主IP地址	主机计费模式	所属项目	操作
搜索找到1条结果, 返回列表								
<input type="checkbox"/> ins-c6vt0bit melody_vpn		北京一区	标准型S2	4核 8GB 5Mbps 系统盘: 普通云硬盘 网络: Vint -BJ-try	139.199.35.174 (公) 192.168.2.11 (内)	按量计费 2018-03-31 20:24 创建	默认项目	登录 更多

2 Array SSL VPN 登录配置

2.1 登录 Array SSL VPN

1. 使用浏览器登录 <https://array> 设备 VPN 外网 IP : 8888 ; 默认的 Array SSL VPN

设备帐号 array 密码是 admin

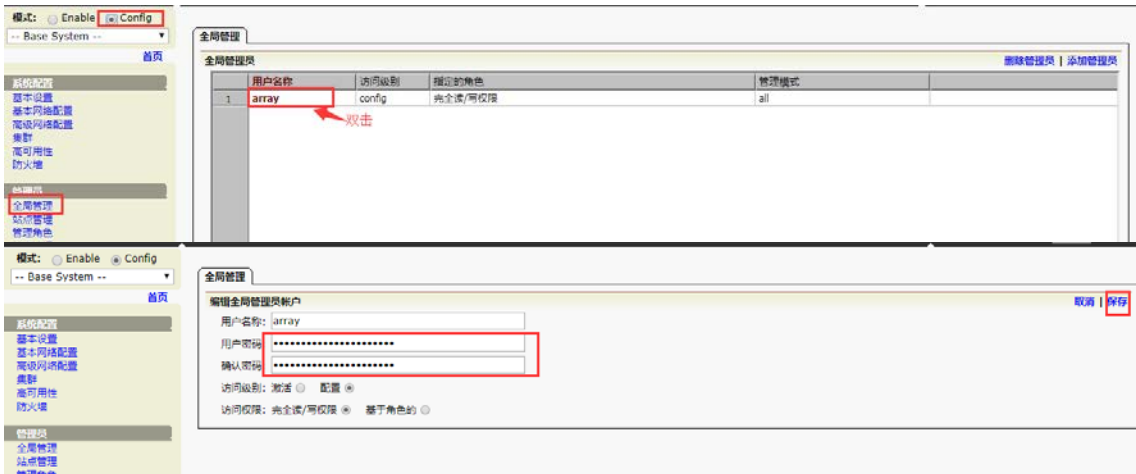


提示：如果无法访问，请检查安全组的配置，务必放通端口 8888。

重要：请登录尽快进行 array 管理账号的密码修改！！！！

修改方法如下：

进入 config 配置模式，转到全局管理，双击 array 账号，输入新密码保存即可。



2.2 License 配置

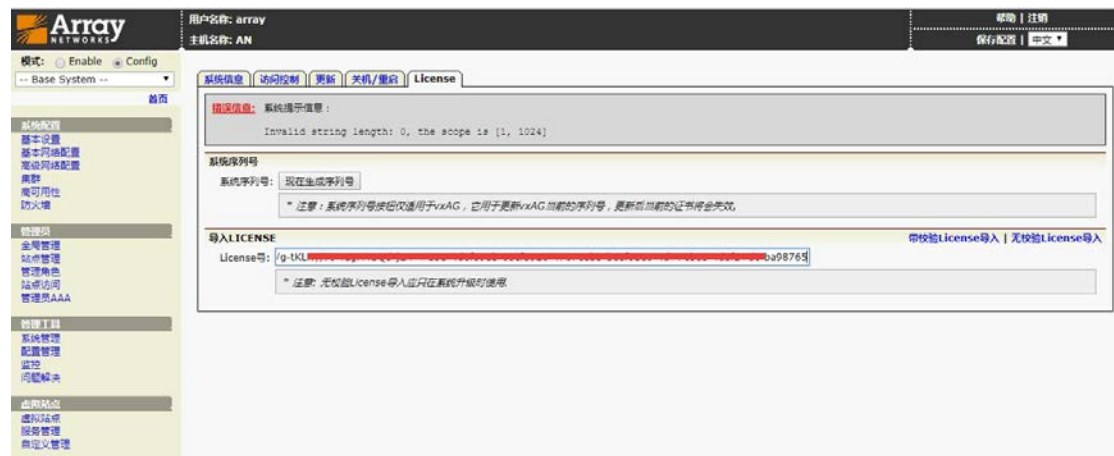
1. 登录界面查看是否有有序列号，如果有则发邮件到 qcloud@arraynetworks.com.cn 或通过 QQ : 2777386539 联系厂商申请 License。



2. 如果没有看到序列号，则需要手动生成序列号。具体位置为系统管理→license



3. 获取到 License 之后，按照下图填写，然后点击【带校验 License 导入】→【保存配置】即可。



2.3 站点配置

1. 配置模式下，点击虚拟站点标签：



2. 添加虚拟站点



3. 填写相关信息，并保存

用户名称: array
主机名称: AN

帮助 | 注销
保存配置 | 中文

虚拟站点 | QuickLink | IPsec | 证书信息 | 访问报告

添加新的虚拟站点 取消 | 保存 & 添加下一个 | 保存

基本安装 [虚拟站点类型: exclusive ▼]

站点名称: default-site

描述: (可选)
192.168.2.12

站点FQDN:
192.168.2.12

* 注意：每一行都是一个完整的完全资格域名。
完全资格域名 (FQDN)，又被称为绝对域名，用于表示计算机在域名系统 (DNS) 树状图下的一个确实位置。FQDN 包括两部分：主机名和域名。举个例子，一台设备的主机名为myhost，它所属域的域名为example.com，那么它的完全资格域名为myhost.example.com。

IP地址:
192.168.2.12

* 注意：请在地址和端口之间添加一个空格。添加新的地址/端口时，请在新的一行输入。
比如：单行地址/端口:192.168.2.1 443
多行地址/端口:192.168.2.1 443
192.168.2.2 443

SSL服务器证书 [生成 | 导入 | 通过TFTP导入]

* 注意：以下字段用于生成一个证书签发请求 (CSR) 以及一个测试用的SSL证书。如果没有配置这些字段，且系统中不存在已有的CSR，则该虚拟站点的SSL服务将不可用，且不能通过门户站点访问。

CSR密钥长度: 1024比特 | 2048比特 | 4096比特

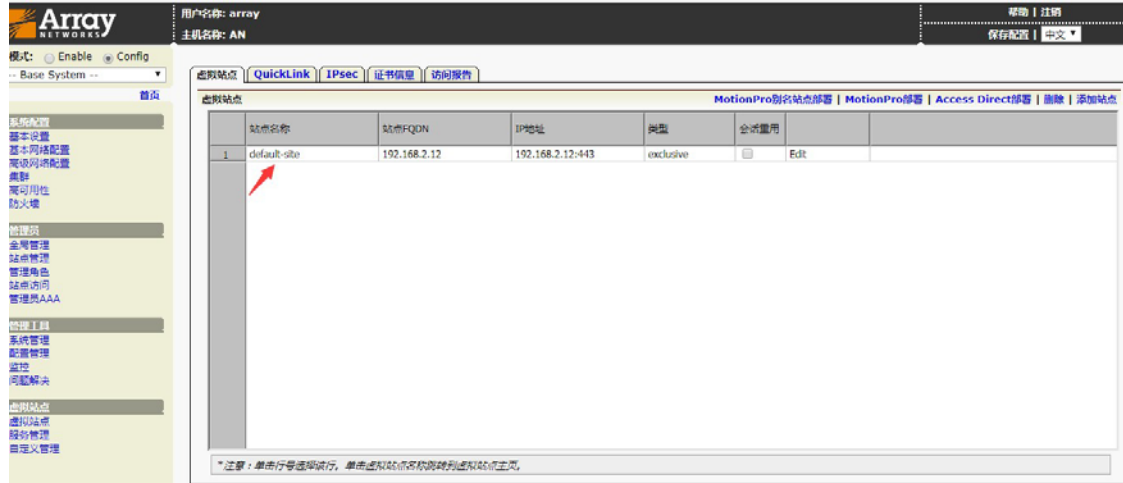
CSR签名算法: SHA1 | SHA256 | SHA384 | SHA512

国家代码: cn

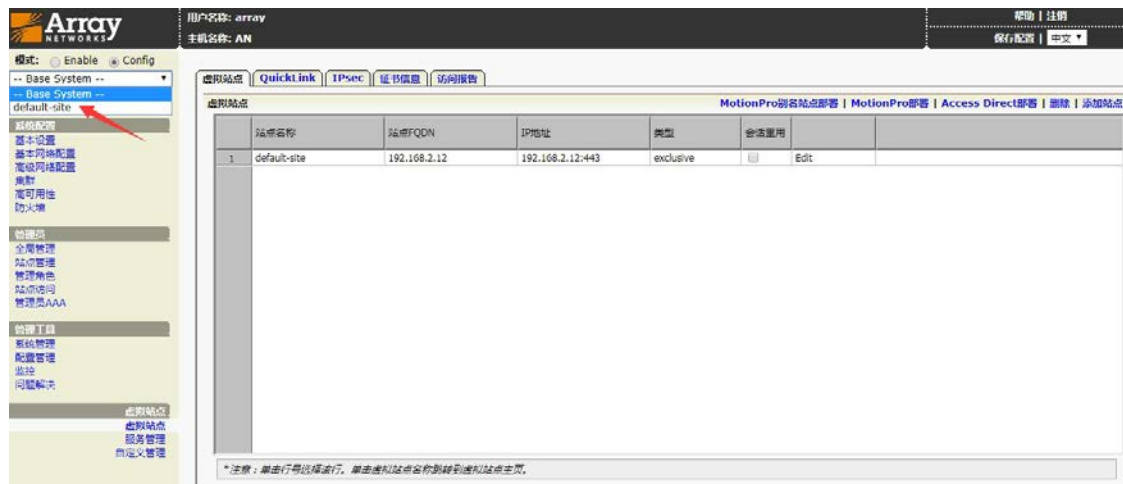
州/省: gd

其中站点 FQDN 请填写接入的公网域名或者 IP，也可填写内网 ip，下面 IP 地址部分请填写虚拟机分配的内网 ip 地址。

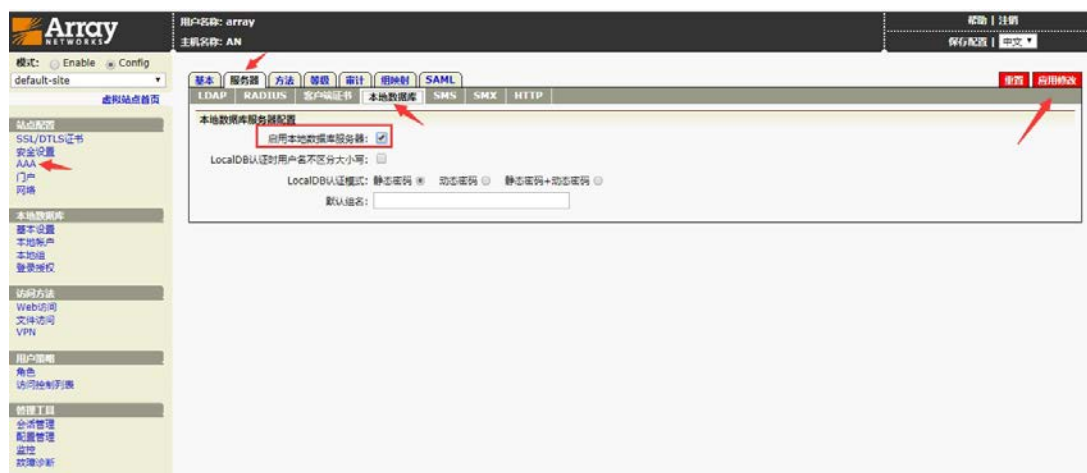
4. 点击保存，即可看到刚刚创建好的站点



5. 进入站点



6. 配置 AAA



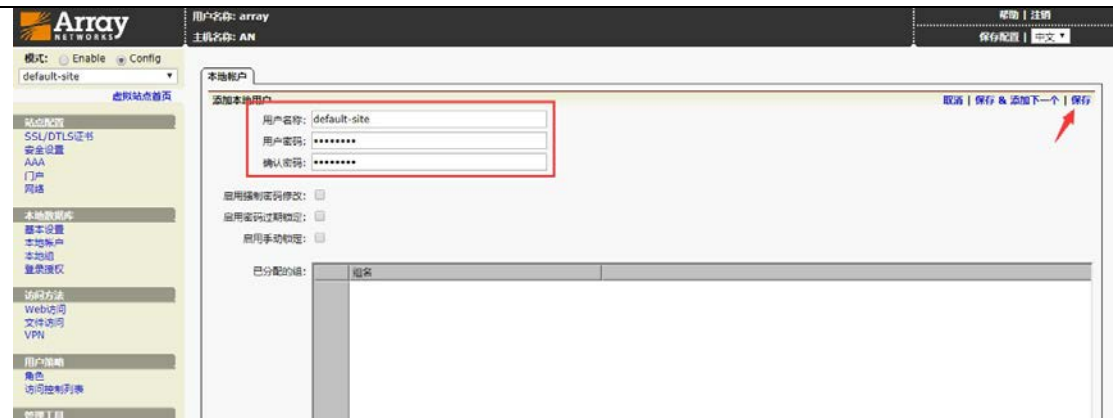
添加 AAA 方法



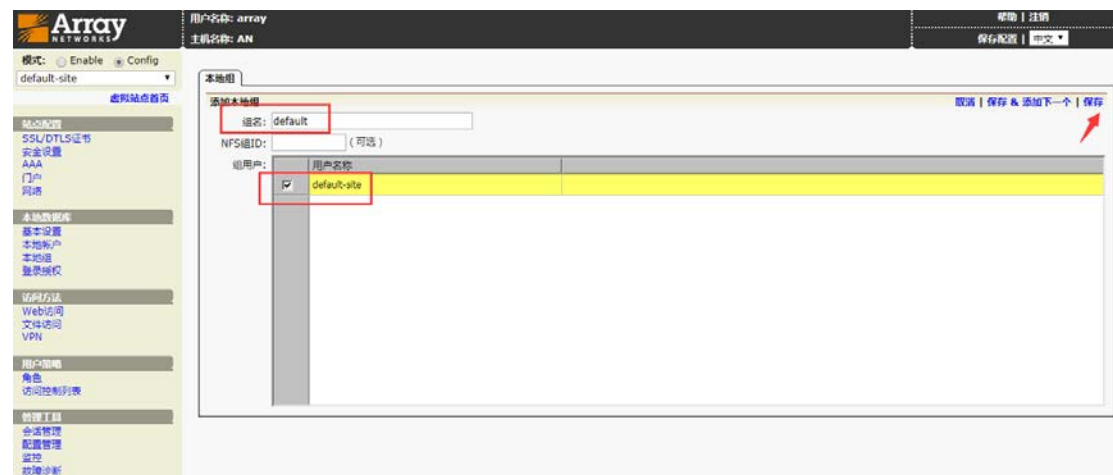
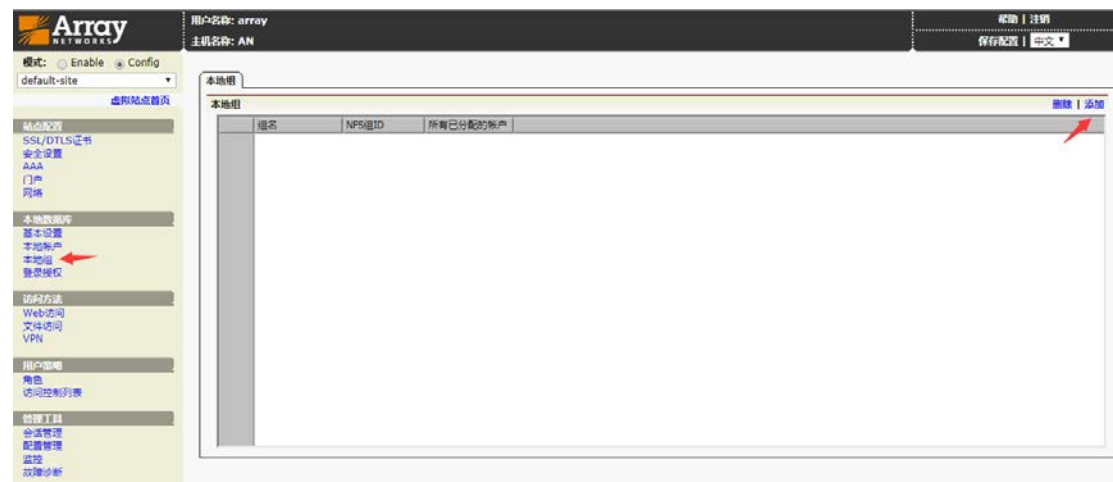
7. 添加用于登录 VPN 的账号，路径为：array 用户登陆->切换到 default-site->Config

模式->本地数据库->本地账户->添加

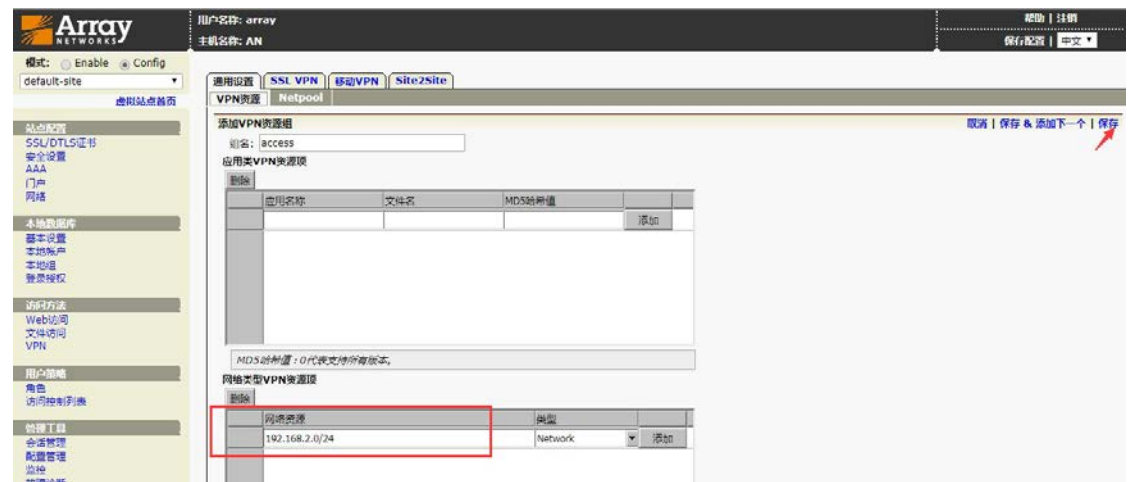
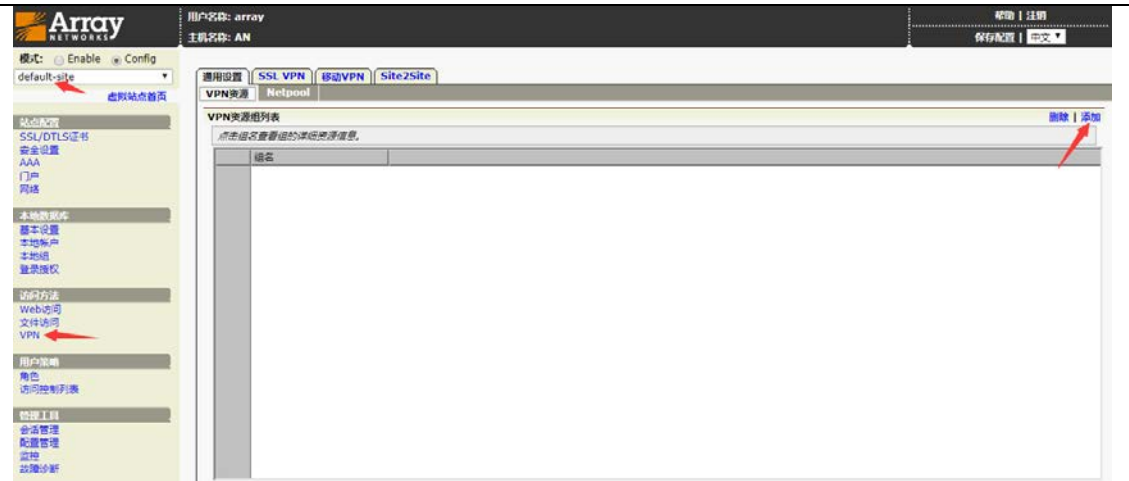




8. 添加组



9. 配置 vpn 资源访问池，定义到哪些网段地址需要走 vpn 隧道

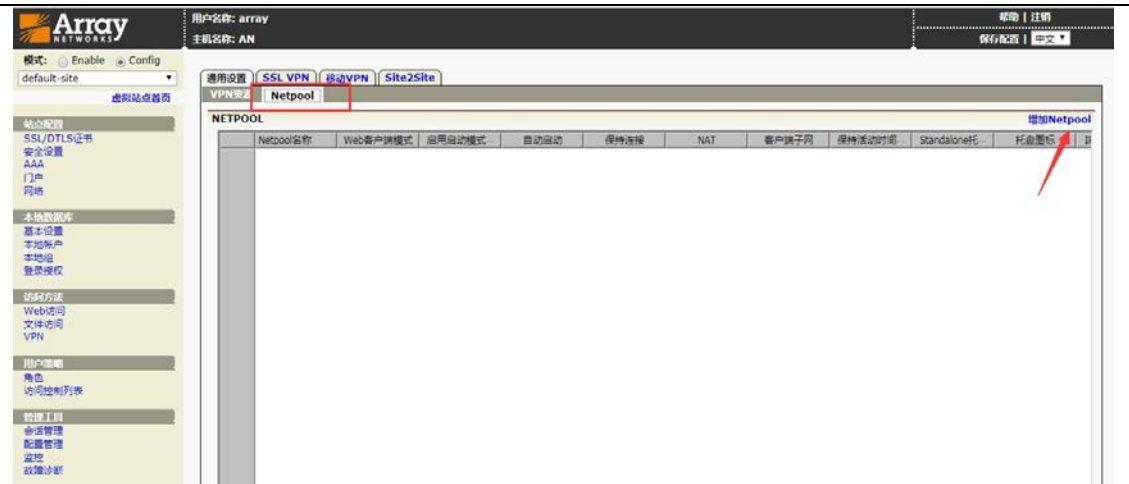


网络类型 VPN 资源项，指的是需要通过 vpn 访问的内网资源 ip

10. 开启站点的 SSLVPN 功能



11. 添加 ip 地址池



添加 ip 地址池网段



这里动态 IP 地址范围是指分配给客户端的三层 vpn 虚拟 ip 地址，如果使用 nat 模式就可以随便填（nat 模式是指客户端的虚拟地址转换为 VPN 虚机的内网接口地址访问应用）

选择VPN Netpool: pool [返回上级菜单]

常规 执行命令 高级 DNS

基本 Windows管理员 内部代理

Netpool保持活动间隔: 30 (1-60秒,默认值为30)

路由网关IP列表:

路由网关IP	HA单元名称

用于所有流量 仅作为默认网关

启用NAT: (不适用于移动VPN)
 (使用全局的NAT配置)

启用客户端子网: (不适用于移动VPN)

启用IPSec over SSL:

启用NetBIOS over TCP/IP:

自动运行客户端: 关闭 启用 出错时停止

启用流量日志:

12. 添加角色

Array NETWORKS 用户名称: array 主机名称: AN 编辑 | 注销 保存配置 | 中文

模式: Enable Config default-site 虚拟站点首页

站点配置 SSL/DTLS证书 安全设置 AAA 门户 网络

本地数据库 基本设置 本地用户 本地组 登录授权

访问方法 Web访问 文件访问 VPN

用户功能 角色 访问控制列表 管理工具 公钥管理 配置管理 监控 故障诊断

角色 角色资格 角色资源

角色列表

角色名称	描述	优先级	会话策略	添加
test				添加

13. 添加角色资格

Array NETWORKS 用户名称: array 主机名称: AN 编辑 | 注销 保存配置 | 中文

模式: Enable Config default-site 虚拟站点首页

站点配置 SSL/DTLS证书 安全设置 AAA 门户 网络

本地数据库 基本设置 本地用户 本地组 登录授权

访问方法 Web访问 文件访问 VPN

用户功能 角色 访问控制列表 管理工具 公钥管理 配置管理 监控 故障诊断

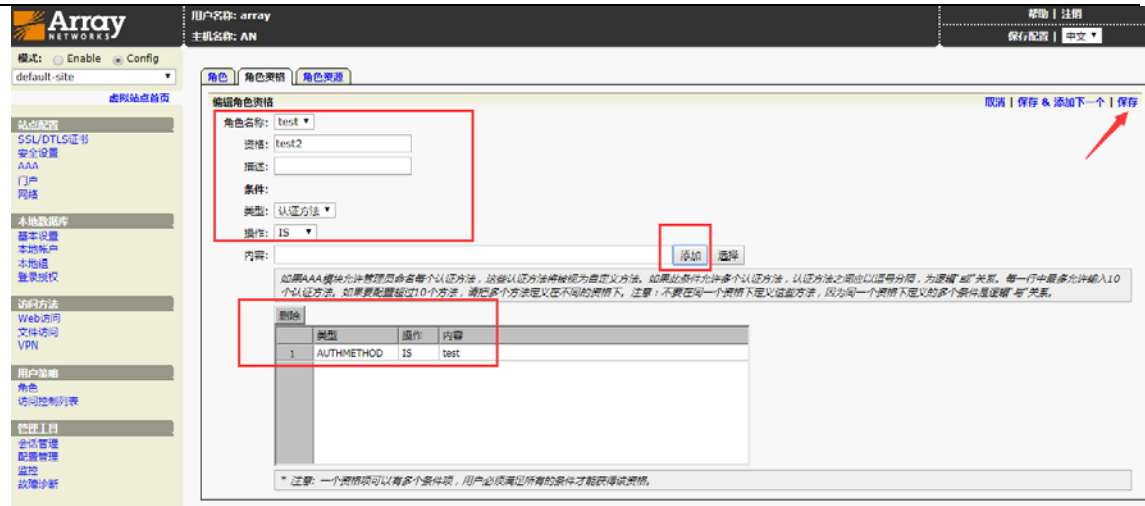
角色 角色资格 角色资源

角色资格列表

* 注意: 一个角色可以有多个资格, 用户获得其中任何一个资格即可获得该角色。一个资格可以有多个条件, 用户必须满足所有的条件才能获得该资格。

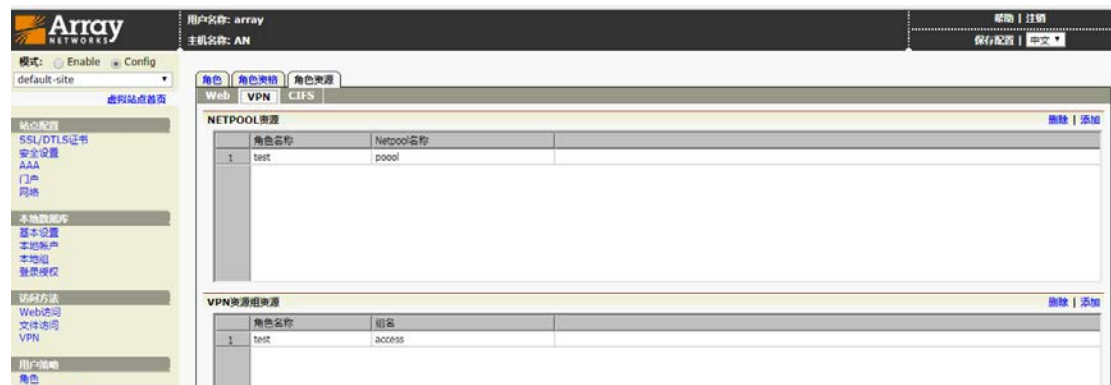
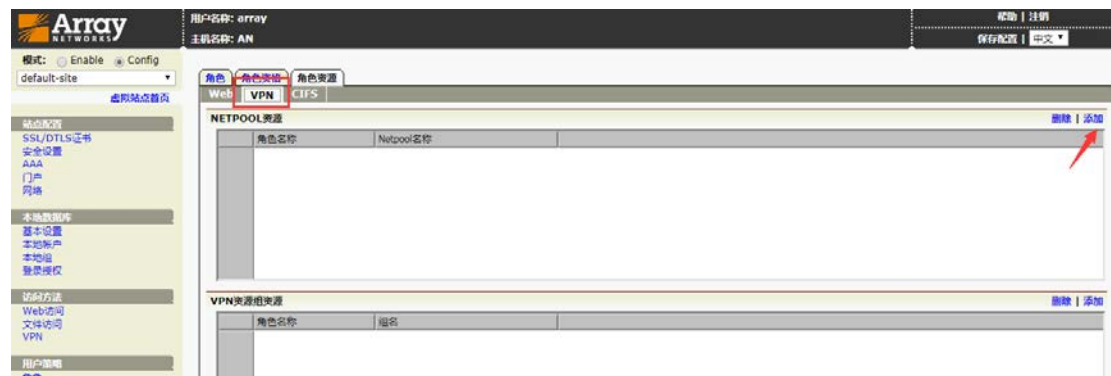
角色名称	资格	描述	条件

删除 | 添加



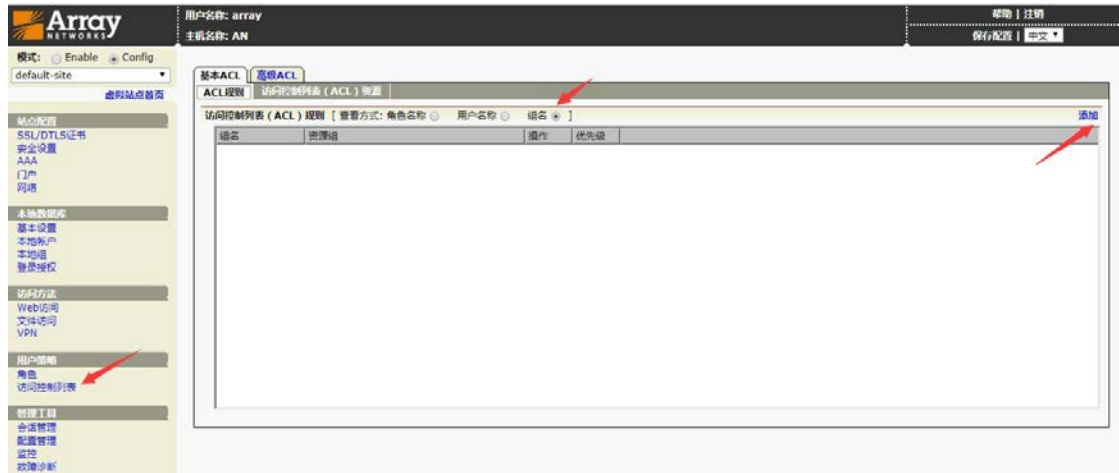
角色资格定义的是用户需要满足什么要求才属于这个角色，有多种条件可供选择，一般常用的资格是组名，或者是认证方法；请通过“添加”旁边的“选择”按钮进行选择。

14. 配置角色的资源



15. 访问控制设置

访问控制可根据情况进行配置，它可以实现更加细粒度的访问控制，如访问单个 ip 及对应的服务端口



对指定的角色进行授权，优先级越小越优先，策略允许代表除了资源列表中的网络条目，其他的都拒绝



2.4 VPN 客户端下载

Array SSL VPN 默认支持网页登录 (IE 浏览器)，也可以下载客户端进行登录，下载地址

为：<http://client.arraynetworks.com.cn:8080/zh/troubleshooting>

【AG系列产品客户端软件下载】

【注意】

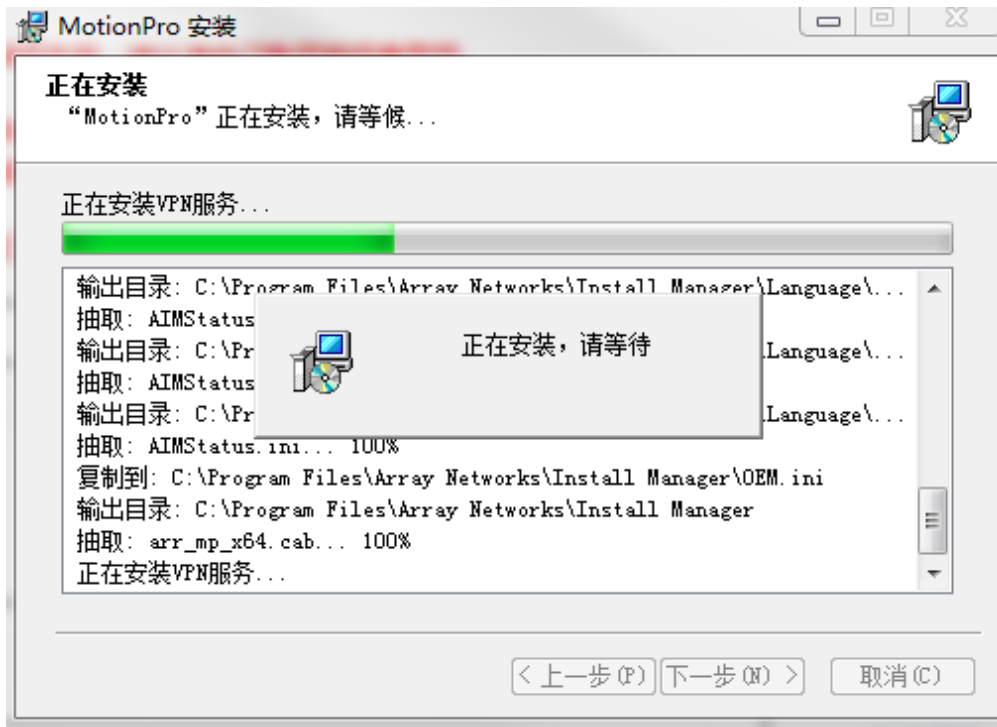
下列软件主要适用于AG产品，请认清自己购买的设备型号。

在64位Win vista/Win7/Win8/win10系统下，使用64位浏览器登录VPN，需手工安装64-bit客户端软件后才能启动L3vpn功能。

Win10系统下的修复工具，[请点击这里下载](#)

MotionPro客户端 (9.3/9.4版本通用)	
适用于Windows操作系统下使用 (更新至v1.1.8)	适用于32位操作系统 适用于64位操作系统 msi安装 使用手册
适用于MacOS操作系统 (更新至v1.1.6)	软件下载 使用手册
适用于CentOS操作系统 (更新至v1.1.1)	软件下载 使用手册
适用于Redhat操作系统 (更新至v1.1.1)	软件下载(For 32bit) 软件下载(For 64bit)

选择适用于自己的客户端版本，然后下载，安装。



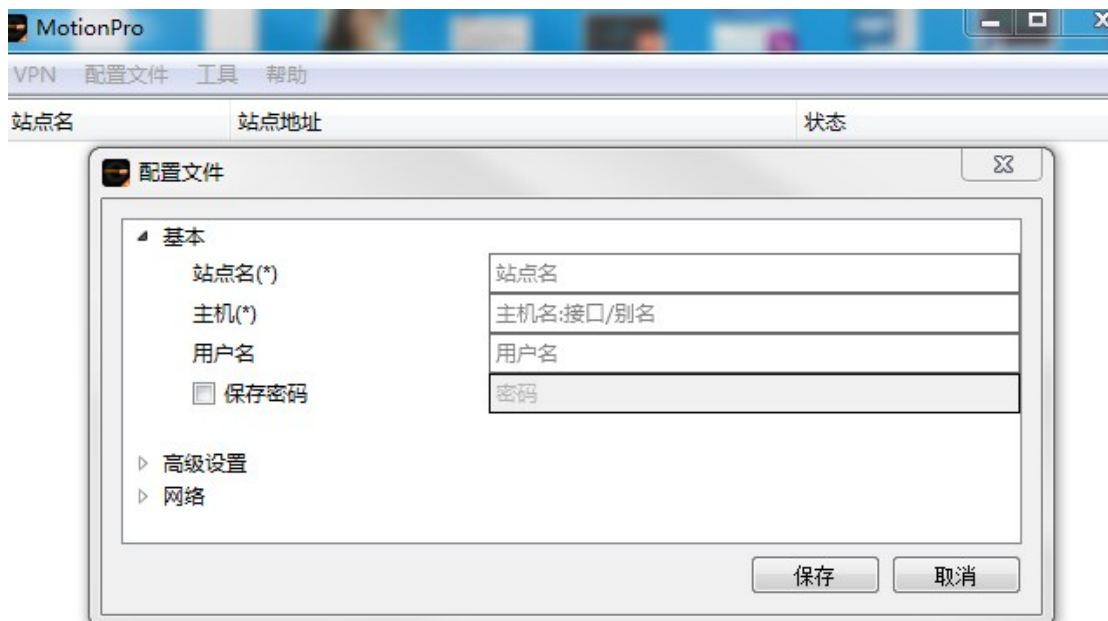


3 VPN 客户端使用

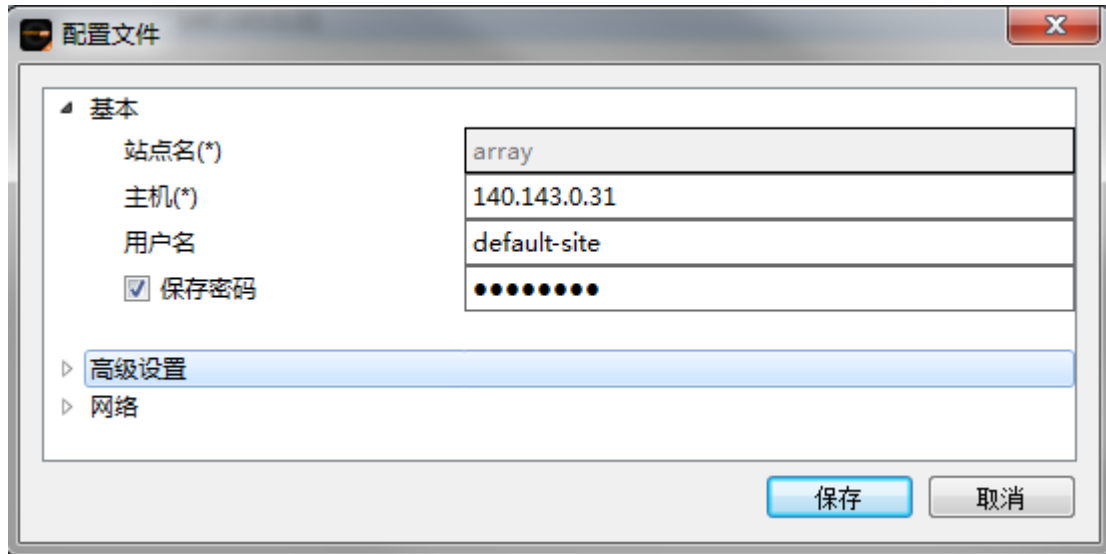
- 1、 启动 motionpro , 并打开



- 2、 在打开的界面中选择配置文---添加，然后添加如下内容

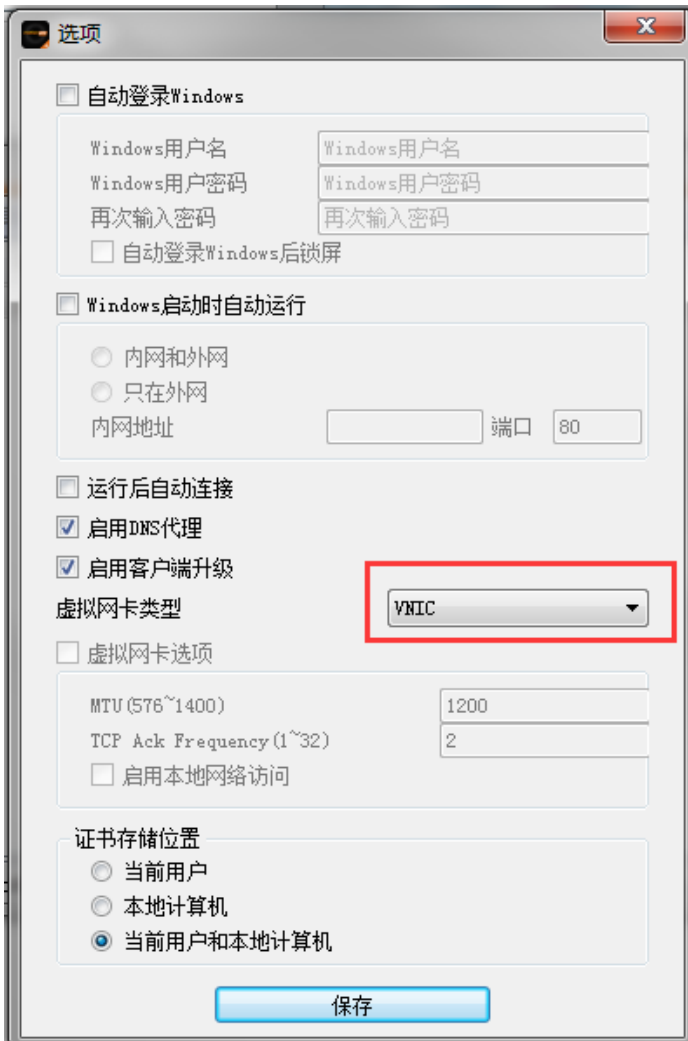


3、 将站点相关信息填入，并点击保存

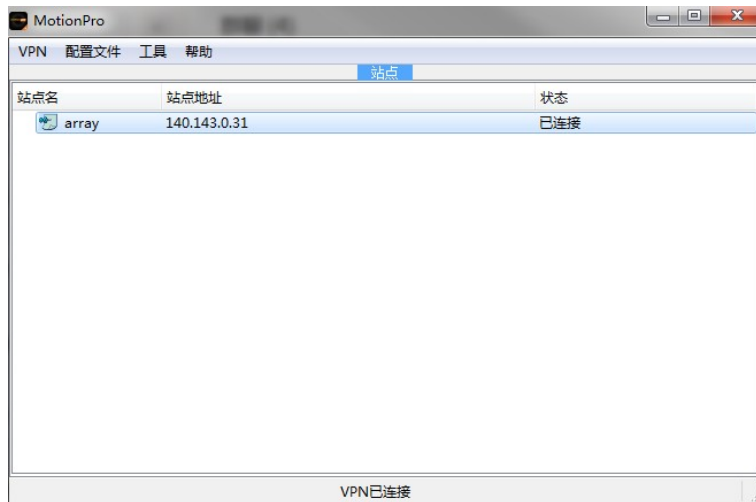


4、 配置 VPN-选项

有两种网卡类型可供选择，默认为 sstp，如果使用默认的网卡类型无法连接，请尝试使用另外一种 vnic 网卡类型进行连接



5、 连接成功

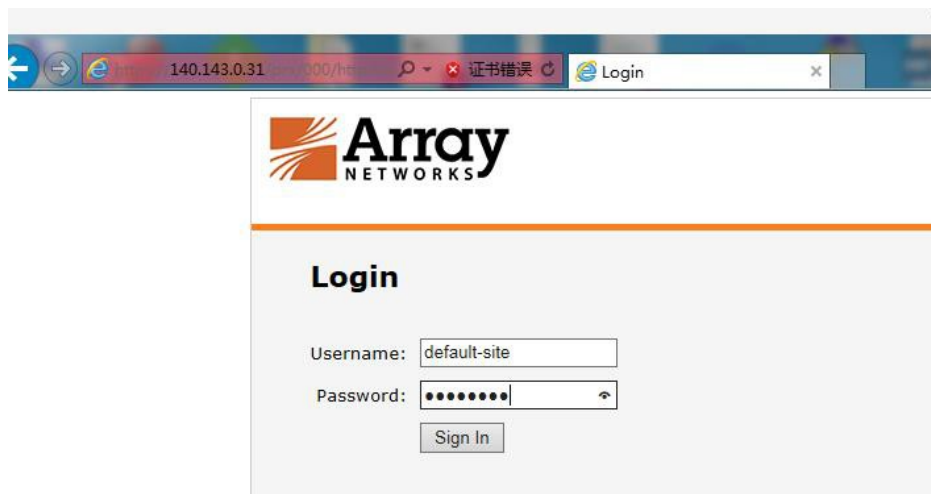


6、 这时用户可以关闭 motionpro 主窗口，在任务栏里能看到红 **A**，代表连接成功。



7、 可直接点击红 **A**，对 VPN 连接状态进行操作。

8、 也可以通过 IE 来访问，访问 https://公网 IP 地址



连接成功

