X-LINK 智简系列 IPsecVPN

配置指导手册

2022 年 2 月

Sundray X-LINK

信锐技术

前　言

概述

本文介绍了信锐技术 X-LINK 多业务网关的接入点 IPsecVPN 功能，以下相关功能配置均基于 XMG3.0.3 版本。

修订记录

日期	版本	修订说明	作者
2022-02-24	v1.0	第一次发布	李华森

图示

符号	说明
注意	有潜在风险，请谨慎操作。
窍门	能帮助您解决某个问题或节省您的时间。
说明	是正文的附加信息，是对正文的强调和补充。

SUNDRAY 信锐技术

目录

1 接入点 IPsecVPN 主模式

1.1 网络拓扑

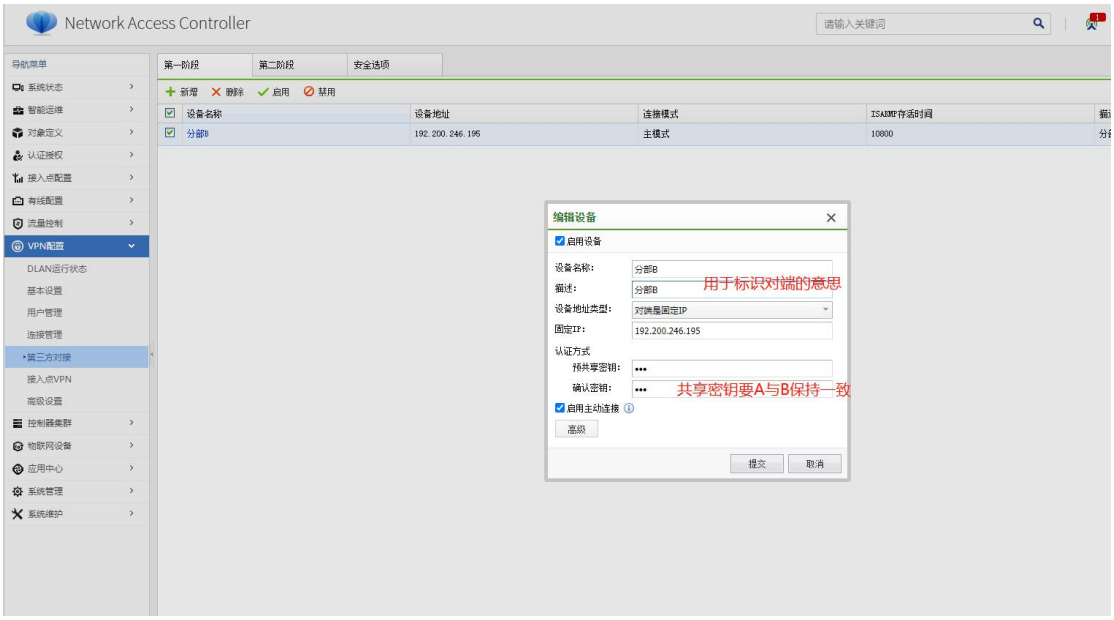
A 内网业务终端通过控制器 IPsecVPN 跨公网访问 B 内网业务资源。

1.2 NAC 上配置

1、【VPN 配置】---【第三方对接】--【第一阶段】选择新增，启用设备填写 IPsecVPN 配置参数，并钩上启用主动连接；

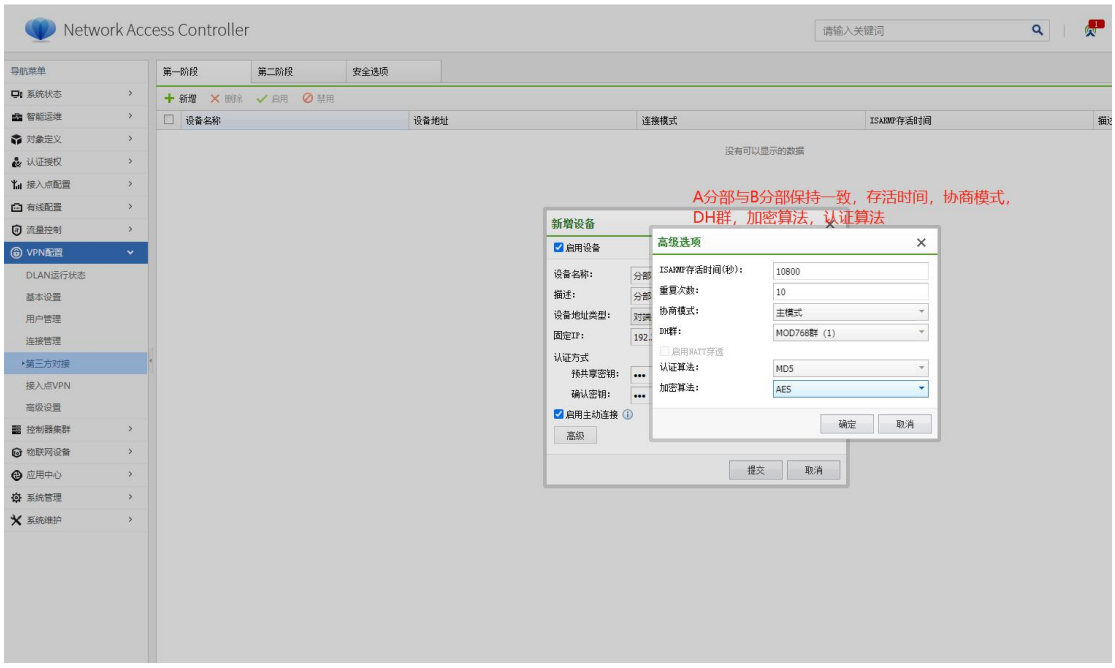
第一阶段作用：对等体之间彼此验证对方，并协商出 IKE SA，保护第二阶段中 IPsec SA 协商过程；

固定 IP 地址是建立 IPsecVPN 隧道的公网 IP 地址，该网段不能和控制器内网业务地址冲突；



2、下一步选择高级【编辑高级选项】

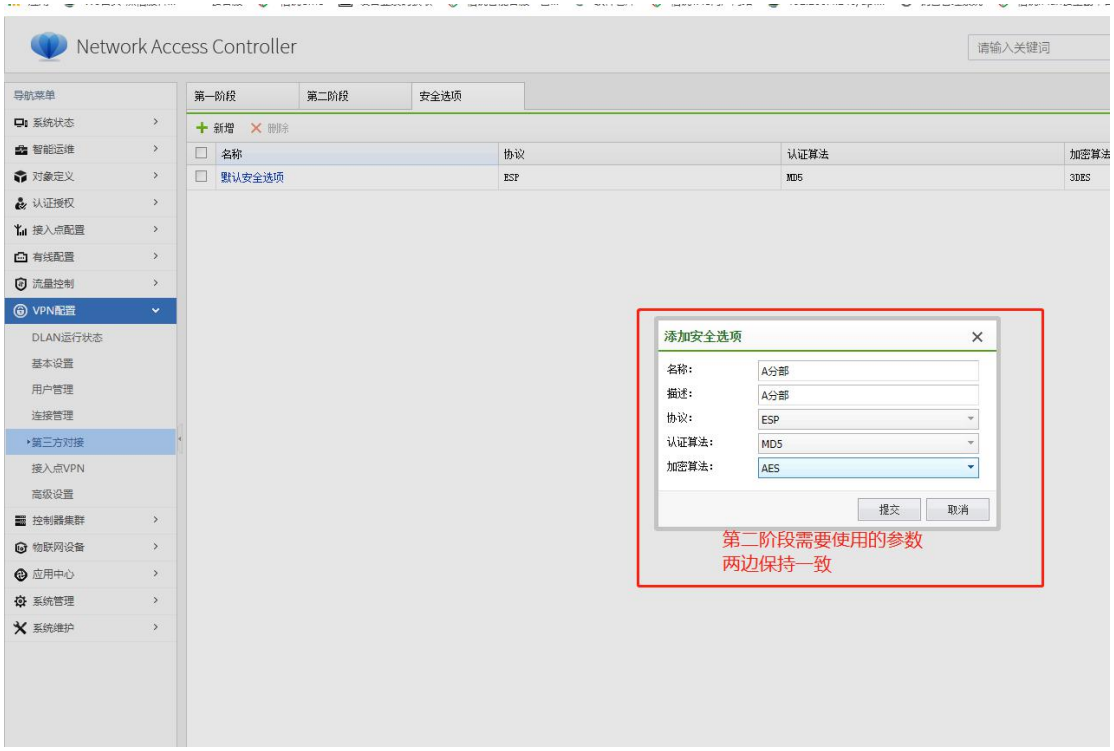
选择协商模式为【主模式】；



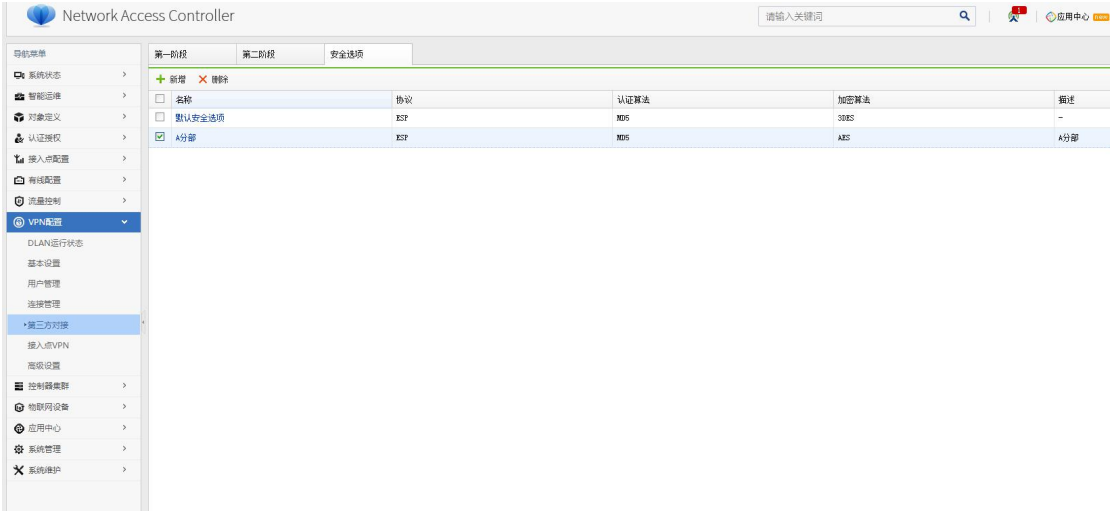
3、选择【安全选项】--【新增】添加安全选项

安全选项是用于第二阶段协商使用的参数；

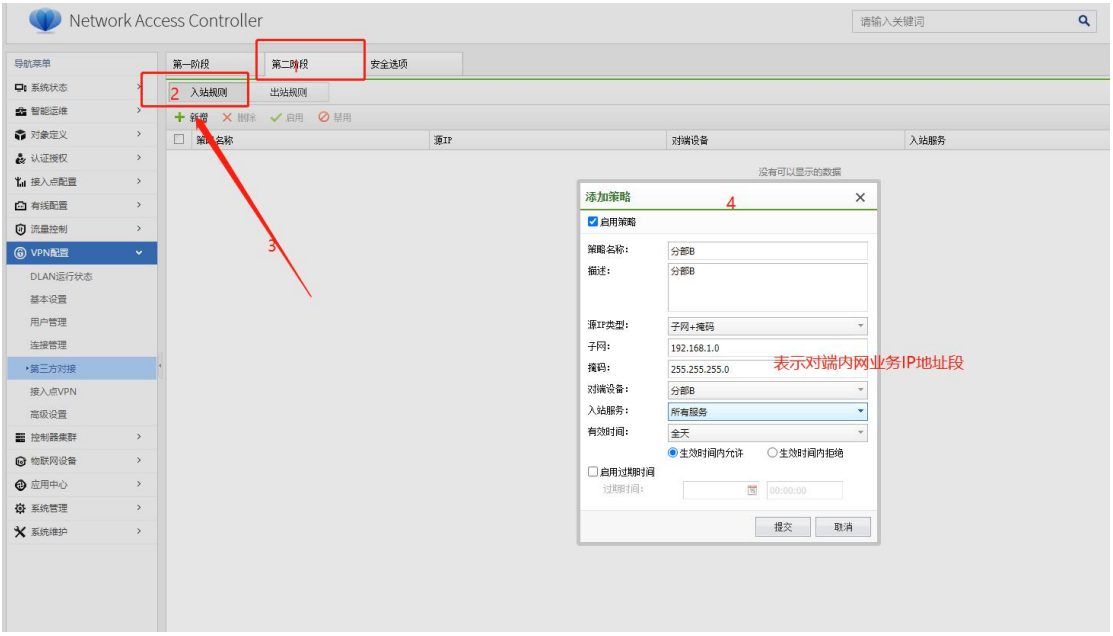
第二阶段作用：协商 IPsec VPN 单向 SA，为保护 IPS 数据流而创建，要保持两边数据一致；



下一步点击提交

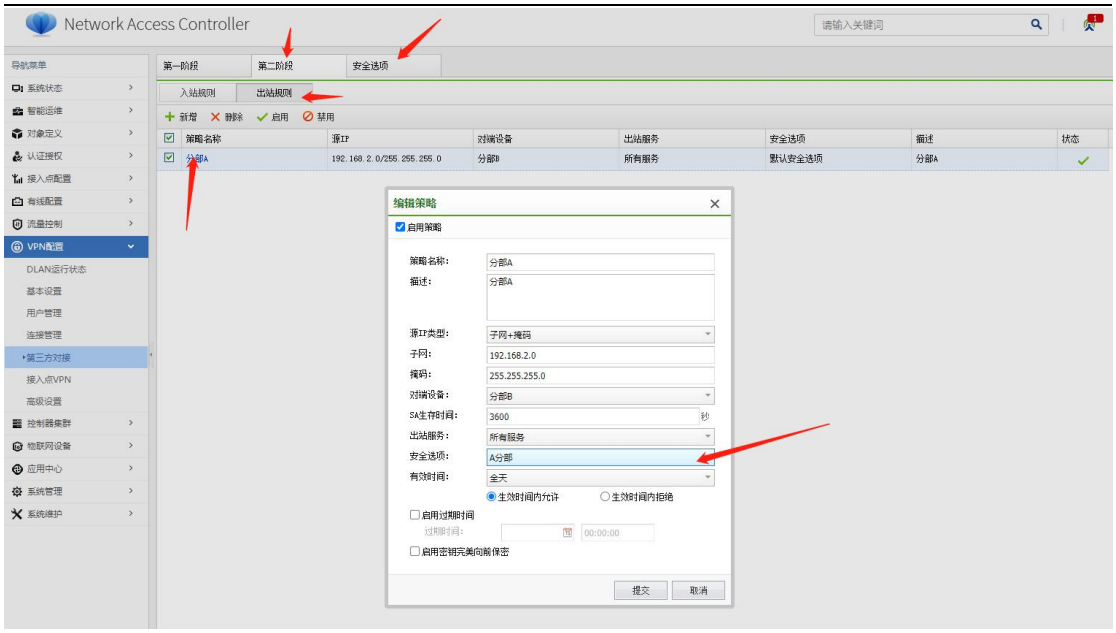


4、选择【第二阶段】---【入站规则】



5、选择【第二阶段】---【出站规则】

新增出站规则，填写本端的内网业务地址段，并选择已经配置好的安全选项；

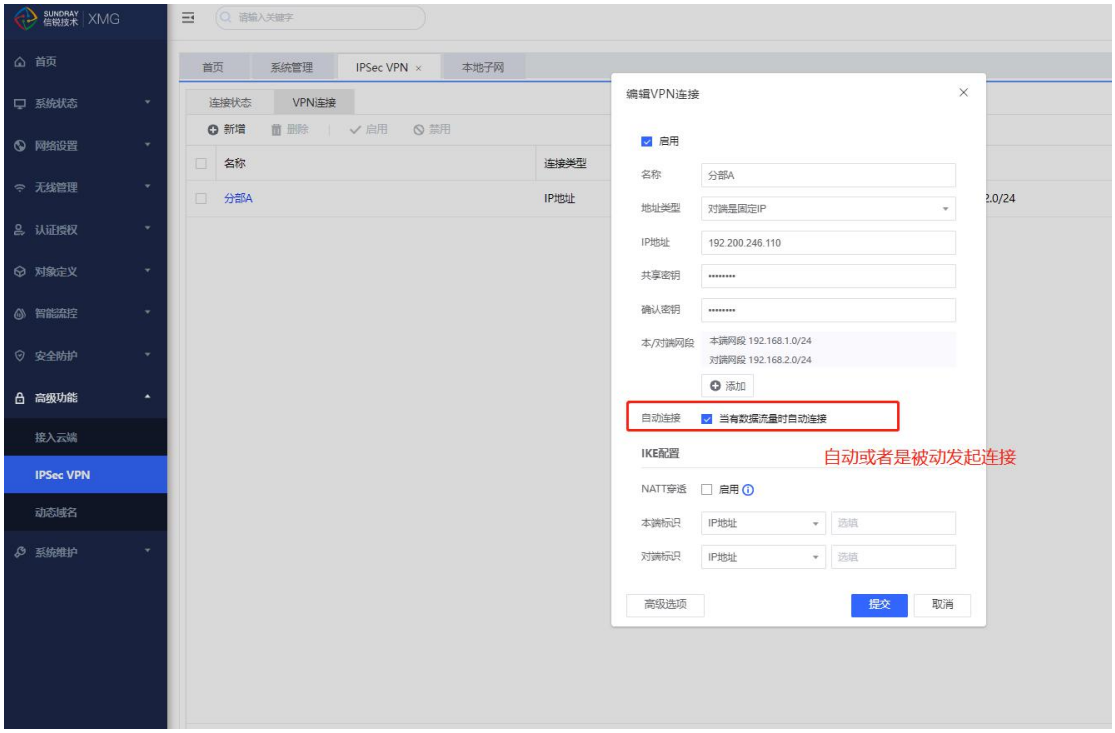


1.3 XMG 上配置

1、【高级功能】---【IPsec VPN】--【VPN 连接】选择新增，启用设备填写 IPsecVPN 配置参数，并钩上自动连接；

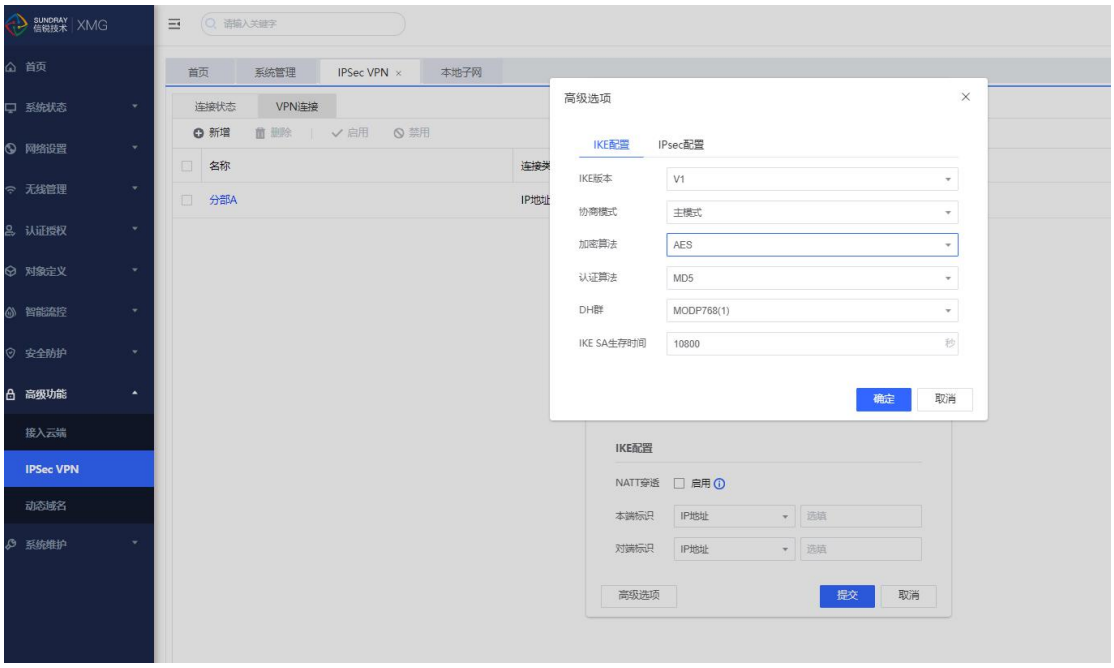
2、本/对端网段表示两端内网业务地址；

3、NATT 穿透，IPsec 对等体是内网 IP 地址才需要开启该穿透模式；



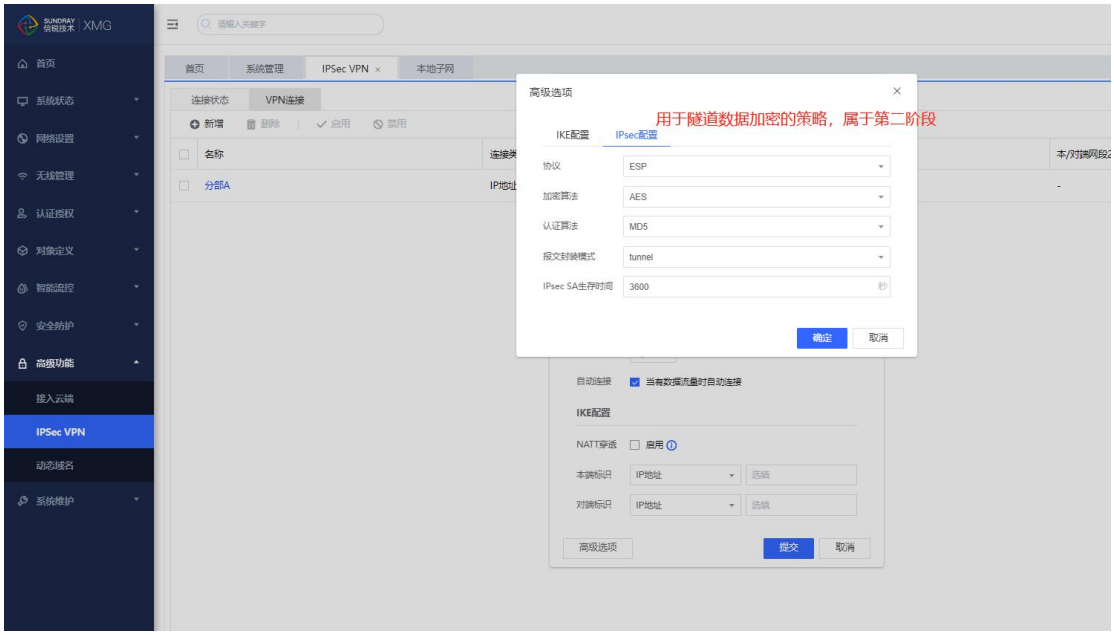
4、下一步选择【高级选项】选择 IKE 配置，选择主模式并填完以下参数，与 NAC 的第一阶段参数保持一致；

【注释：IKE 配置属于 IPsecVPN 的第一阶段】



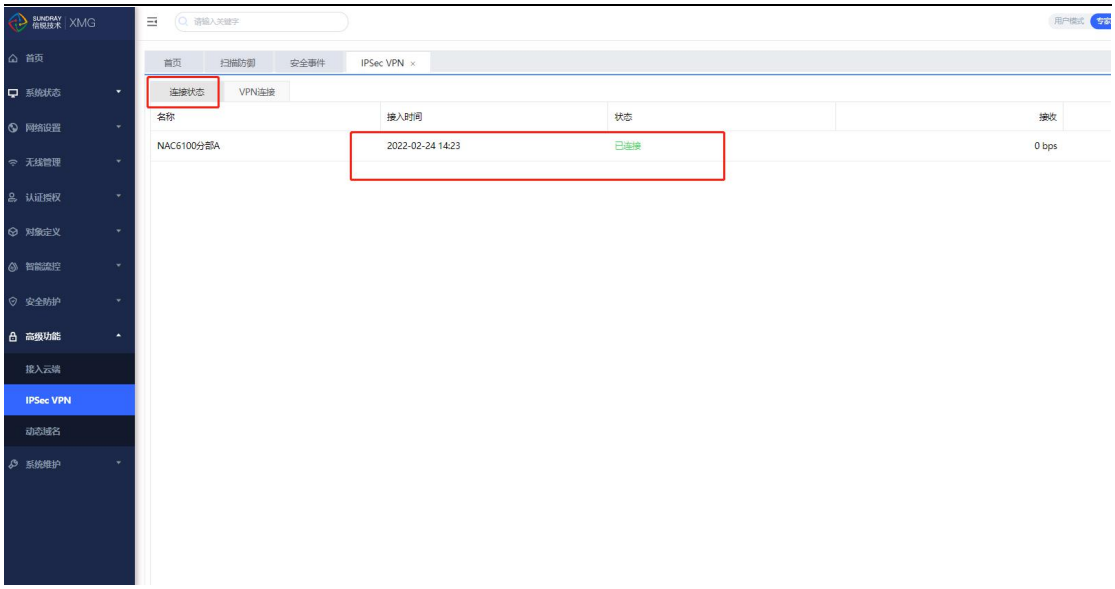
5、下一步选择【IPsec 配置】，填写完成以下参数，与 NAC 的第二阶段参数保持一致；

【注释：IKE 配置属于 IPsecVPN 的第二阶段】



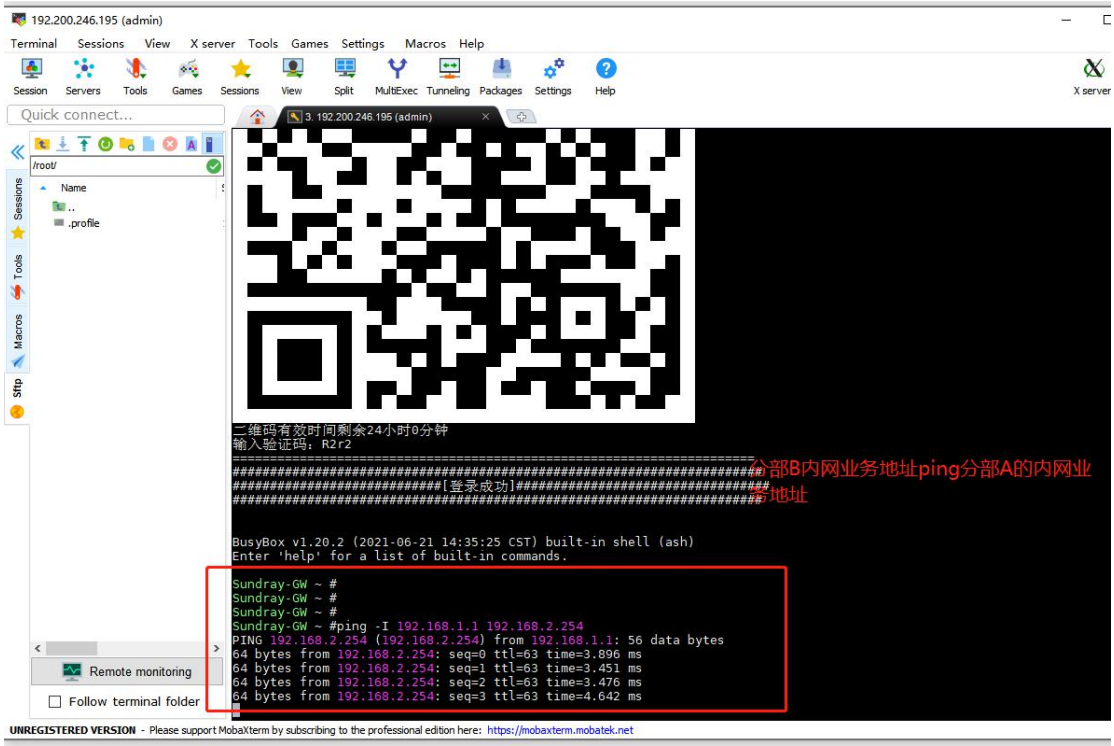
6、IPsecVPN 连接状态

完成 IPsecVPN 配置后，点击【IPsec VPN】---【连接状态】即可查看 IPsecVPN 的运行状态情况；



7、业务测试

以下截图为 A 分部与 B 分部的业务模拟测试，客户可根据实际业务网段进行 ping 测试；



2 接入点 IPsecVPN 野蛮模式

2.1 网络拓扑

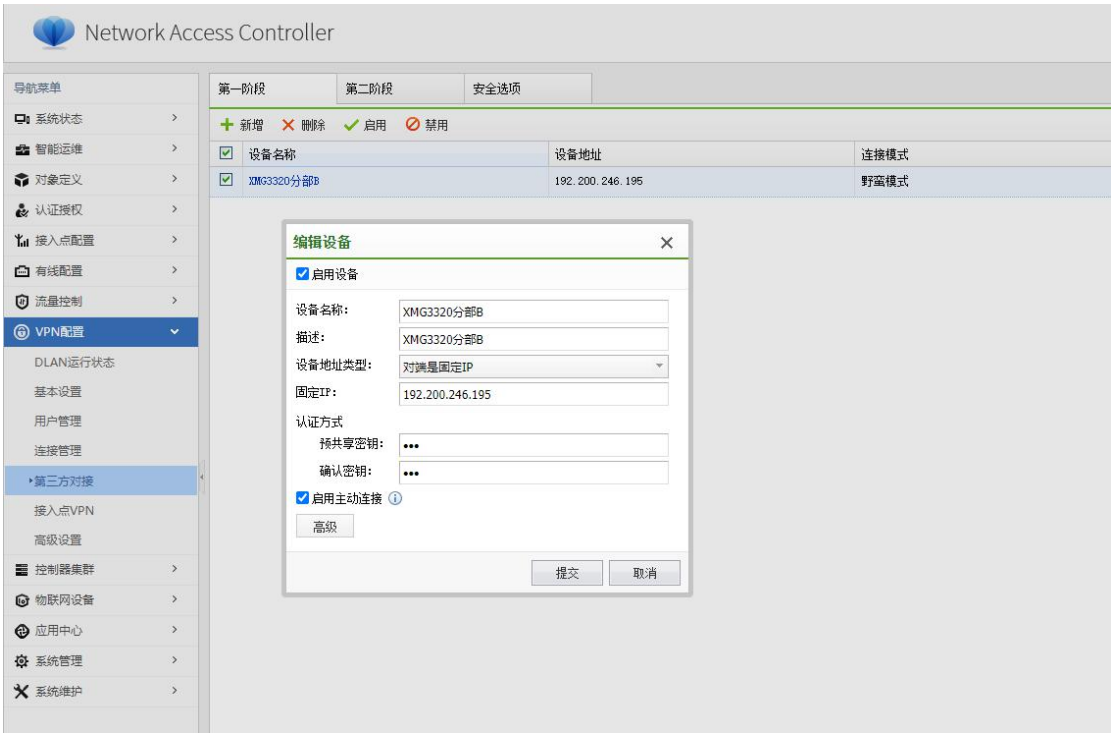
A 内网业务终端通过控制器 IPsecVPN 跨公网访问 B 内网业务资源。

2.2 NAC 上配置

1、【VPN 配置】---【第三方对接】--【第一阶段】选择新增，启用设备填写 IPsecVPN 配置参数，并钩上启用主动连接；

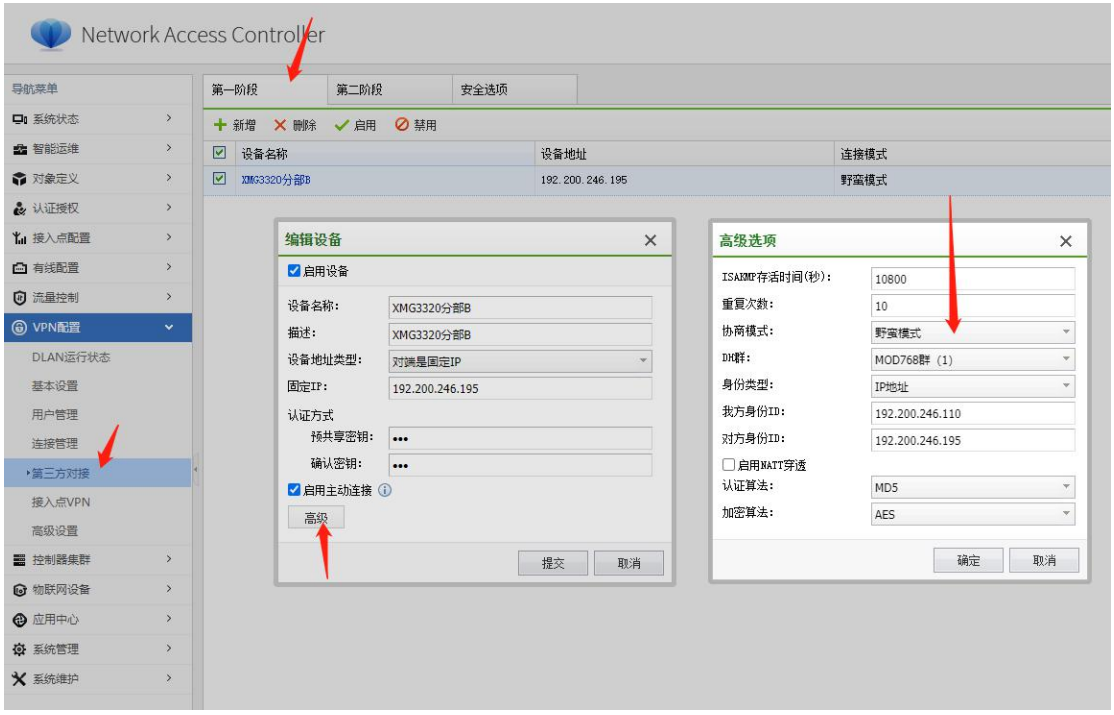
第一阶段作用：对等体之间彼此验证对方，并协商出 IKE SA，保护第二阶段中 IPsec SA 协商过程；

固定 IP 地址是建立 IPsecVPN 隧道的公网 IP 地址，该网段不能和控制器内网业务地址冲突；



2、下一步选择高级【编辑高级选项】

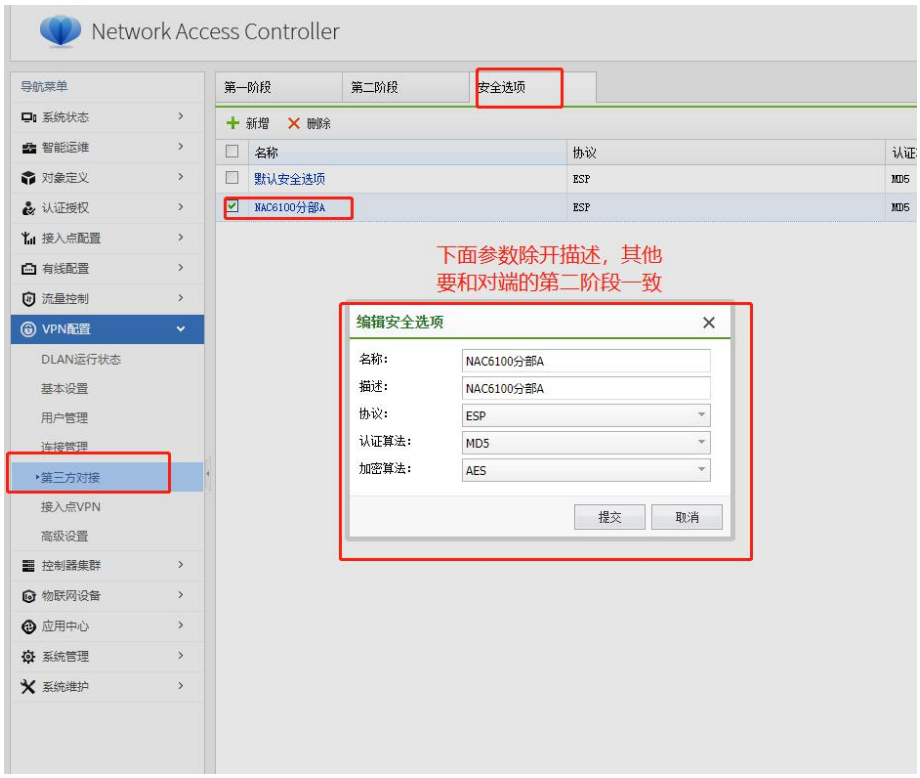
选择协商模式为【野蛮模式】，同时需要选择身份类型，要对应 XMG 的(本端/对端)标识;



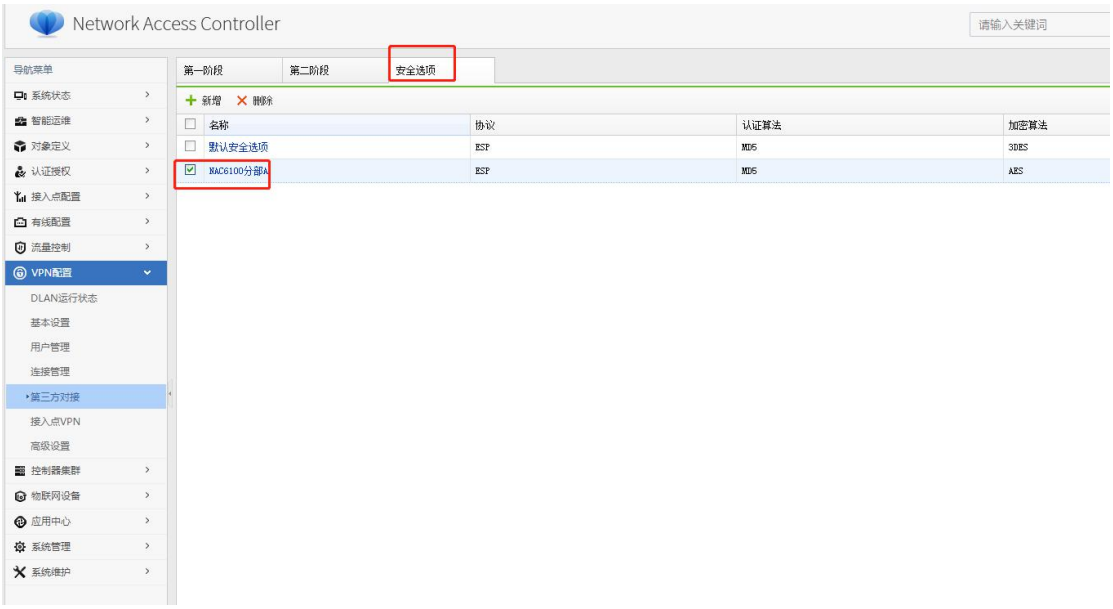
3、选择【安全选项】--【新增】添加安全选项

安全选项是用于第二阶段协商使用的参数；

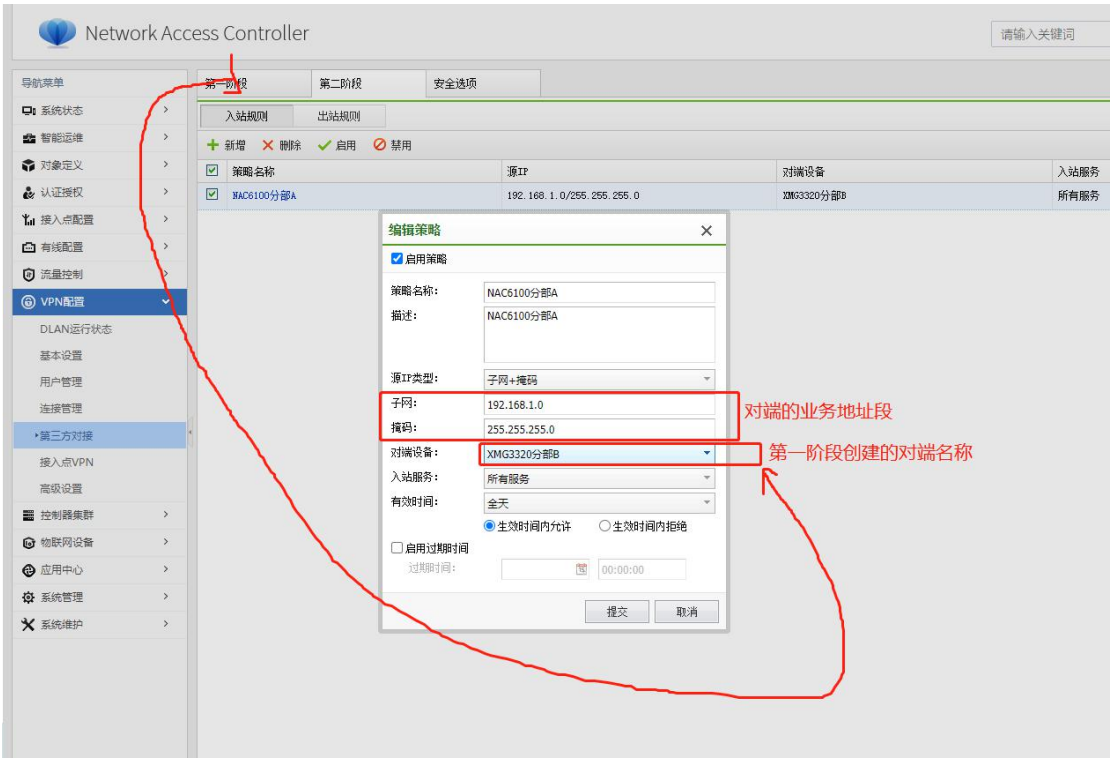
第二阶段作用：协商 IPsec VPN 单向 SA，为保护 IPS 数据流而创建，要保持两边数据一致；



下一步点击提交

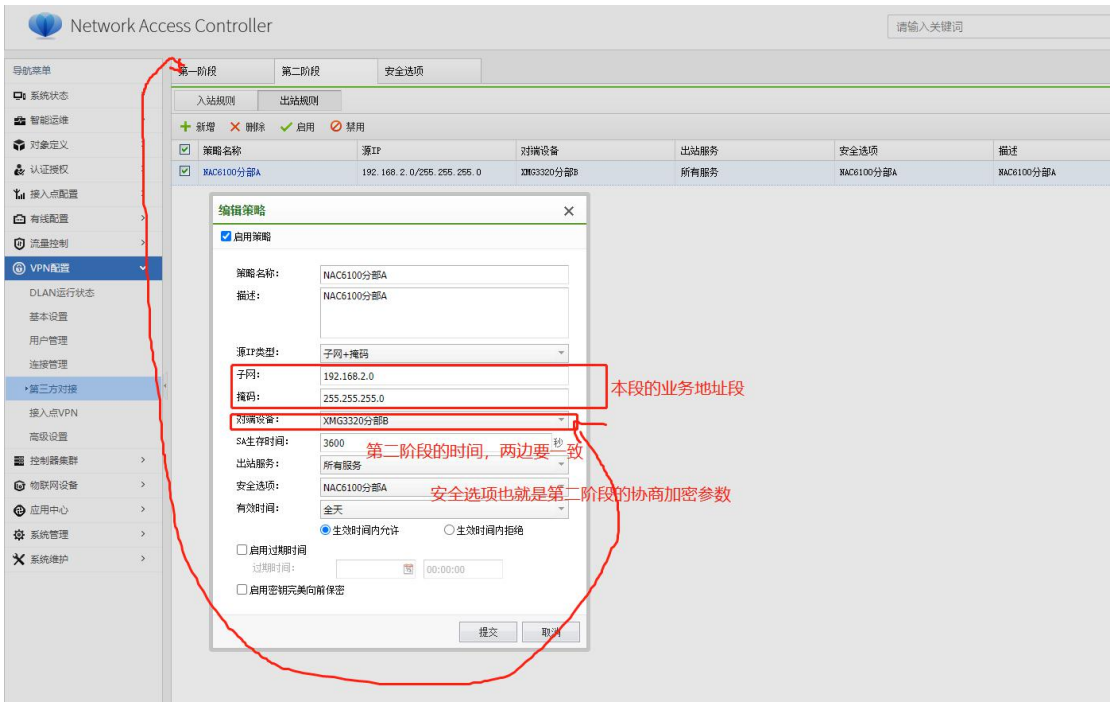


4、选择【第二阶段】---【入站规则】



5、选择【第二阶段】---【出站规则】

新增出站规则，填写本端的内网业务地址段，并选择已经配置好的安全选项；

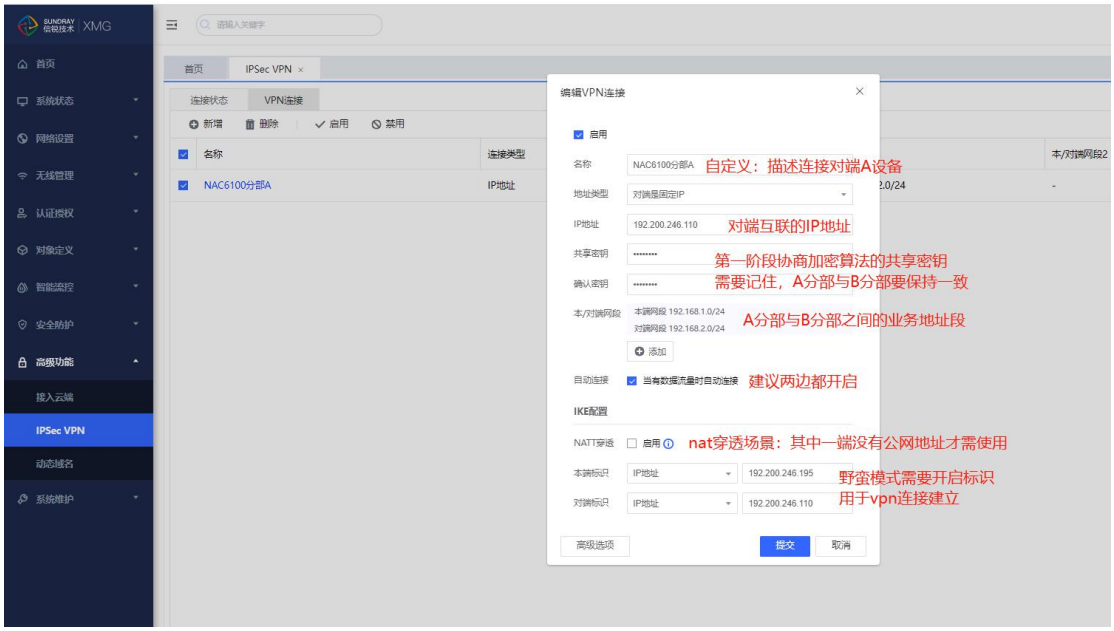


1.3 XMG 上配置

1、【高级功能】---【IPsec VPN】--【VPN 连接】选择新增，启用设备填写 IPsecVPN 配置参数，并钩上自动连接；

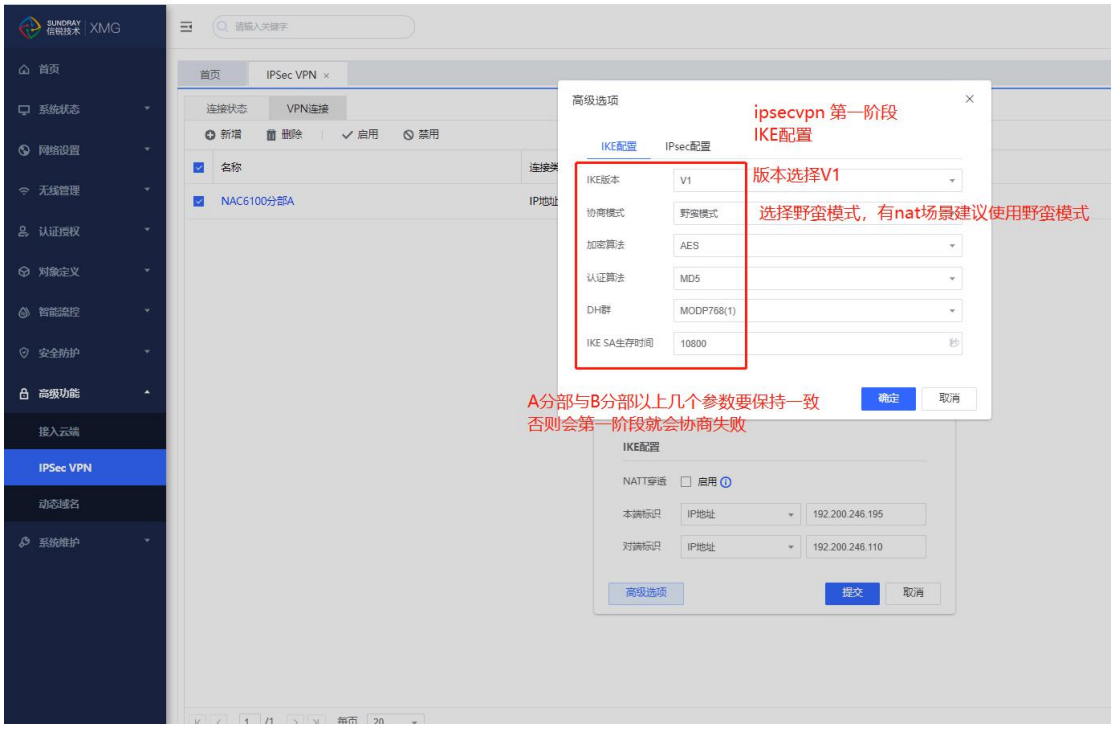
2、本/对端网段表示两端内网业务地址；

3、NATT 穿透，IPsec 对等体是内网 IP 地址才需要开启该穿透模式；



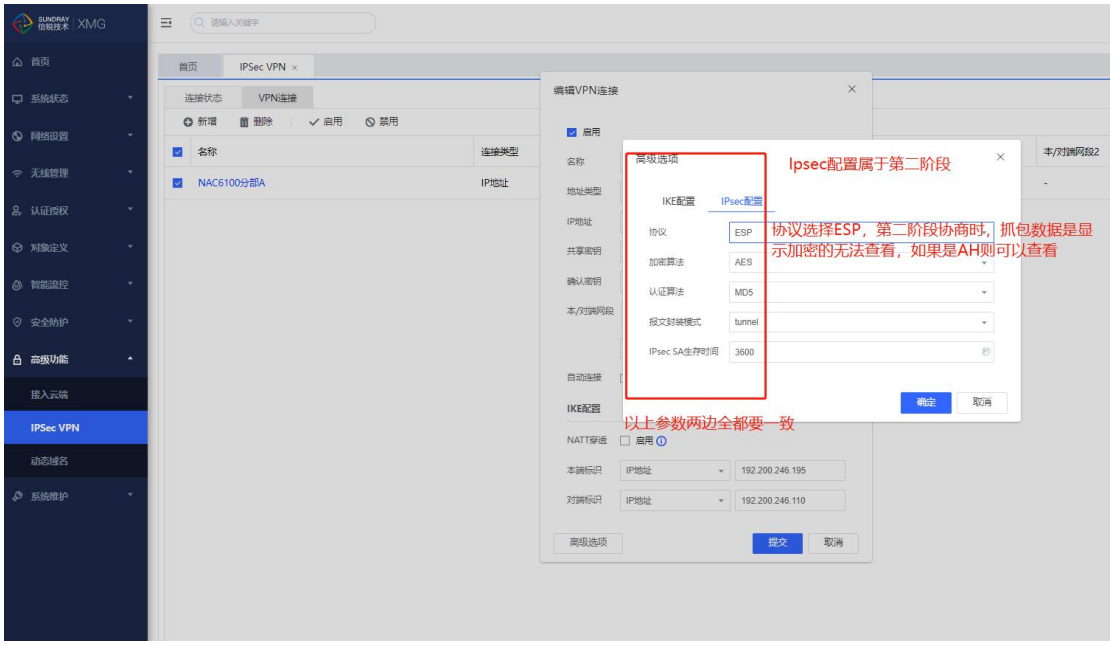
4、下一步选择【高级选项】选择 IKE 配置，选择野蛮模式并填完以下参数，与 NAC 的第一阶段参数保持一致；

【注释：IKE 配置属于 IPsecVPN 的第一阶段】



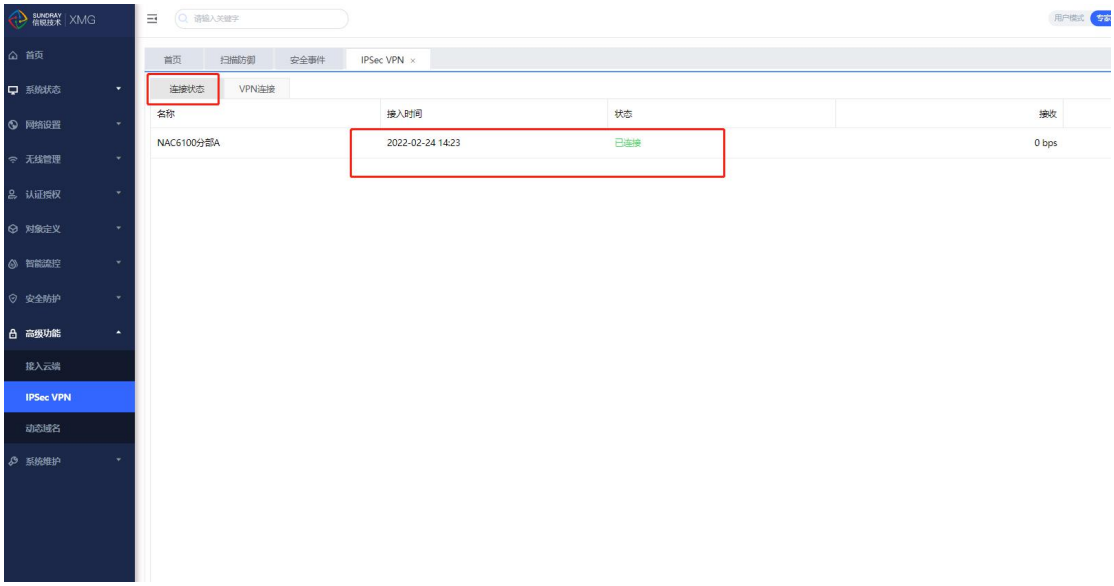
5、下一步选择【IPsec 配置】，填写完成以下参数，与 NAC 的第二阶段参数保持一致；

【注释：IKE 配置属于 IPsecVPN 的第二阶段】



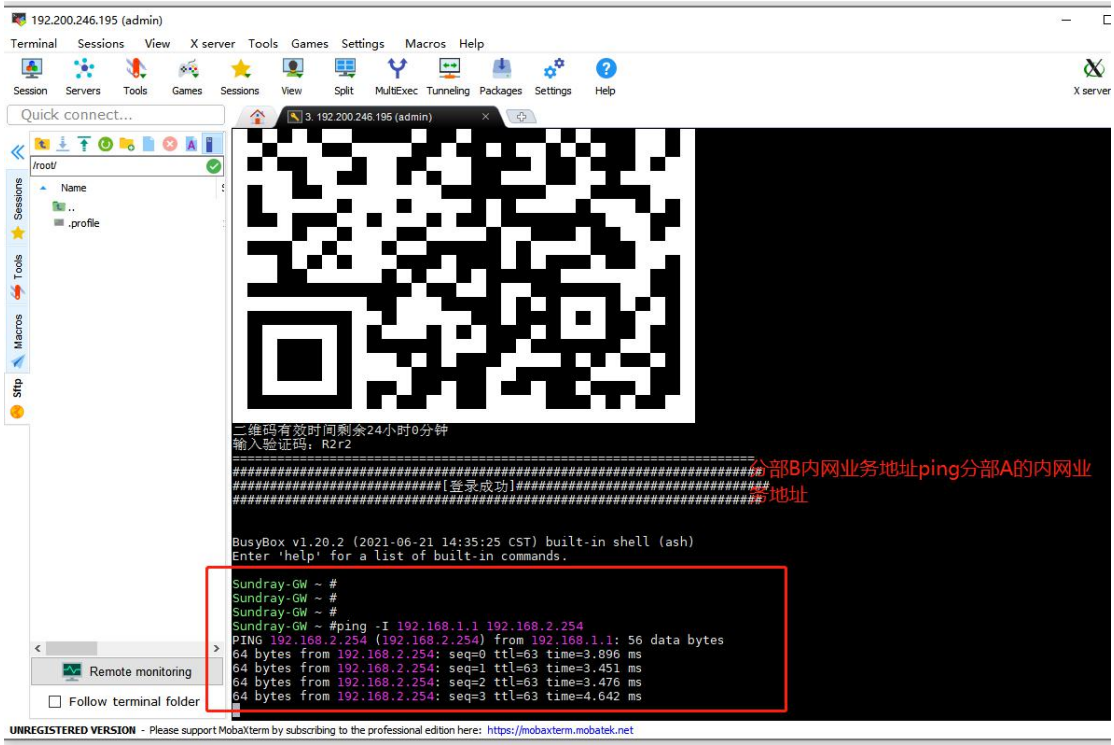
6、IPsecVPN 连接状态

完成 IPsecVPN 配置后，点击【IPsec VPN】---【连接状态】即可查看 IPsecVPN 的运行状态情况；



7、业务测试

以下截图为 A 分部与 B 分部的业务模拟测试，客户可根据实际业务网段进行 ping 测试；



3 注意事项

1、接入点 IPsecVPN 主模式/野蛮模式中 IP 地址都不能与内网业务 IP 地址冲突。

2、接入点 IPsecVPN 野蛮模式中，XMG 多业务网关必须填写（本端/对端）标识。

3、在配置 IPsecVPN 中，A、B 两个分部之间，其中一个分部必须是公网 IP 地址，才能建立 IPsecVPN 连接配置；