Neusoft

东软 NetEye VPN 网关 V3.0
实施指南

东软联系信息

网站：http://neteye.neusoft.com

电子信箱：servicedesk@neusoft.com

服务电话：400 655 6789

目录

前言

本文档介绍如何配置东软 NetEye VPN 网关 （以下简称 “VPN 网关 ”），以使授权用户可以访问受 VPN 网关保护的资源。目标读者为 VPN 网关的管理用户。

文档约定

VPN 网关 	通用服务器 	Web 服务器 	邮件服务器 	文件服务器 
远程用户 	桌面 PC 	笔记本 	平板电脑 	智能手机 
通信链路 	公网 	防火墙 	路由器 	交换机 

相关手册

除了本手册，管理员还可获得产品附带的以下文档：

- *东软 NetEye VPN 网关硬件安装向导 .pdf*
- *东软 NetEye VPN 网关快速部署向导 .pdf*
- *东软 NetEye VPN 网关用户使用指南 .pdf*
- *东软 NetEye Android 版 SSL VPN 客户端用户接入指南 .pdf*
- *东软 NetEye iOS 版 SSL VPN 客户端用户接入指南 .pdf*
- *东软 NetEye macOS 版 SSL VPN 客户端用户接入指南 .pdf*
- *东软 NetEye Windows 版 SSL VPN 客户端用户接入指南 .pdf*
- *东软 NetEye SSL VPN Portal 用户接入指南 .pdf*

1 系统概述

本章介绍 VPN 网关的概要信息，包含以下内容：

1.1 产品概述

VPN 网关是一款专业的 VPN 设备，采用标准 SSL、 TLS 协议，支持两种 VPN 技术：

- IPSec VPN：支持网关到网关和远程访问两种类型的 IPSec VPN 隧道。
  - 网关到网关类型的 IPSec VPN 隧道可用于公司总部与分支机构或合作伙伴、分支机构与分机构之间的安全互连；
  - 远程访问类型的 IPSec VPN 隧道帮助移动用户安全接入公司总部，以实现移动办公。
- SSL VPN：允许出差员工或分支机构员工访问公司资源。

VPN 网关支持两种 SSL VPN 接入方式：

- Web 方式

  通过浏览器访问 SSL VPN 资源。通过此种方式，用户无需安装任何插件即可在各主流系统上使用标准浏览器来访问资源。支持的浏览器包括 IE 7、Firefox 10、Google Chrome 9、 Safari 5、Opera 12 及以上版本 。

  如果用户要访问的资源都是 Web 应用 （如 HTTP 和 HTTPS），推荐使用 Web 模式 SSL VPN。

- 客户端方式

  使用客户端访问 SSL VPN 资源。此种方式需要用户先下载、安装东软 NetEye SSL VPN 客户端，请在 SSL VPN Portal 登录页面下载相应操作系统的客户端软件，解压缩后安装使用。

  如果用户要访问的资源除了 Web 应用，还有其他类型的应用 （如 FTP、 SSH、 Telnet、 RDP 等），推荐使用隧道模式 SSL VPN。

1.2 主要功能

表 1 VPN 网关主要功能特性

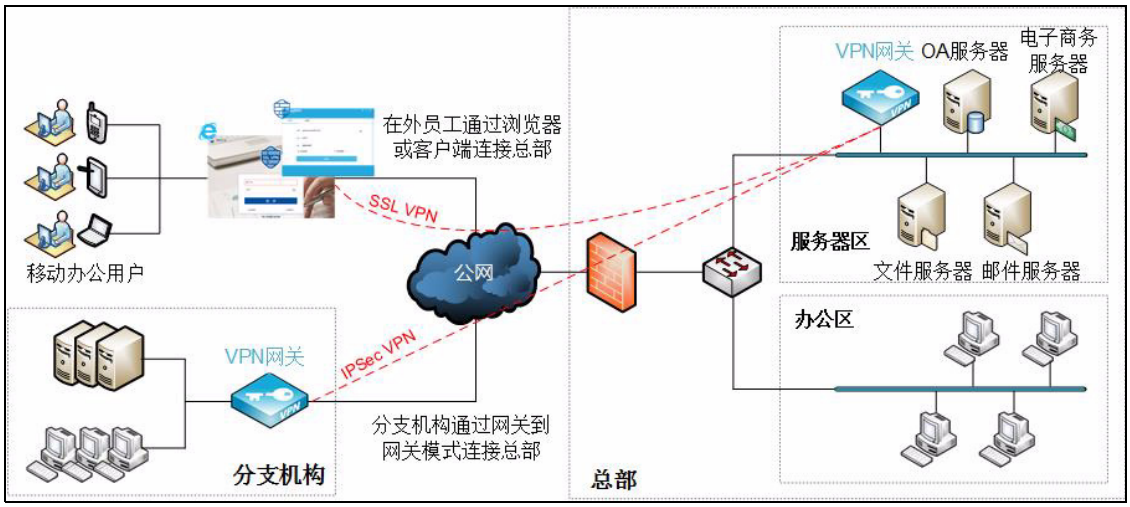
功能模块	功能特性
SSL VPN	• 支持隧道模式 SSL VPN，对客户端到网关的网络传输数据进行加密。 • 支持 Web 模式 SSL VPN，对 HTTP、 HTTPS、 FTP、 RDP、 SSH、 Telnet 等协议基于流式的 html 替换以及缓存压缩提升了替换的准确率和速度。 • 支持 AES、 DES、 3DES、 MD5、 RC4、 RSA 等加密算法，支持加载扩展安全算法模块。 • 支持与现有用户数据库的快速结合，支持 RADIUS、 LDAP、 Active Directory、 eDirectory 等第三方认证方式以及组合认证。 • 支持 LDAP 动态组和安全组，直接复用 LDAP 服务器的安全策略，减轻管理员配置负担。 • 支持 SSO 单点登录，简化用户登录步骤。 • 支持用户访问记录、审计和报表功能，支持站点资源访问统计和历史查询。 • 可限制用户在线时间，支持超时检测和自动离线功能。 • 支持管理员设定邀请码邀请用户自行注册，节省了管理员的工作量，方便了用户的接入。 • 支持 VPN 访问策略，结合时间进行访问控制，可设定局域网用户访问 VPN 资源的权限。 • 支持实时监控，可实时监控用户接入情况或在线中断用户访问，实时监控系统运行状况。
IPSec VPN	• 支持网关到网关和远程访问两种隧道模式，满足用户多种使用场景需求。 • 支持 3DES、AES、TWOFISH、SERPENT、BLOWFISH、CAST 等高强度加密算法以及国密办加密算法，使用 MD5、 SHA1、 SHA2 算法保证数据的完整性。软加密支持国密办 SM3 SM4 算法，同时支持国密办加密卡。 • 支持 IKEv2。 IKEv2 改进了加密打包的方式并优化了部分细节，所以数据的压缩比率更高，失真的可能更小。而且，由于二代的优化策略，其压缩、传输、解压的过程更加快捷方便。
其他	• **客户端**：支持 Windows 7-10、 iOS、 MacOS、 Android 等主流操作系统。 • **CA 中心**：内置 CA 服务器，可本地生成 CA 和用户证书。 • **防火墙**：附带基本的包过滤防火墙功能，支持 NAT，可基于 IP、协议和端口制定访问控制策略。 • **攻击防御**：可检测各种常见的 DDoS 攻击，执行 IP 选项校验。 • **WiFi 接入**：可为内网客户端提供无线服务。 • **流量监控**：可实时监控 VPN 设备各网络接口流量、内网单机实时流量，对流量进行排名，查看移动拨入用户流量，统计站点访问量。 • **管理方式**：支持流行的 Web 管理方式，简单明了的配置界面，使管理员无需花费太多精力就可以得心应手地进行配置。 • **升级**：系统软件更新周期为 3 个月，使用逐步迭代的方式增强系统稳定性和功能。此部分软件更新完全免费。

1.3 部署方式

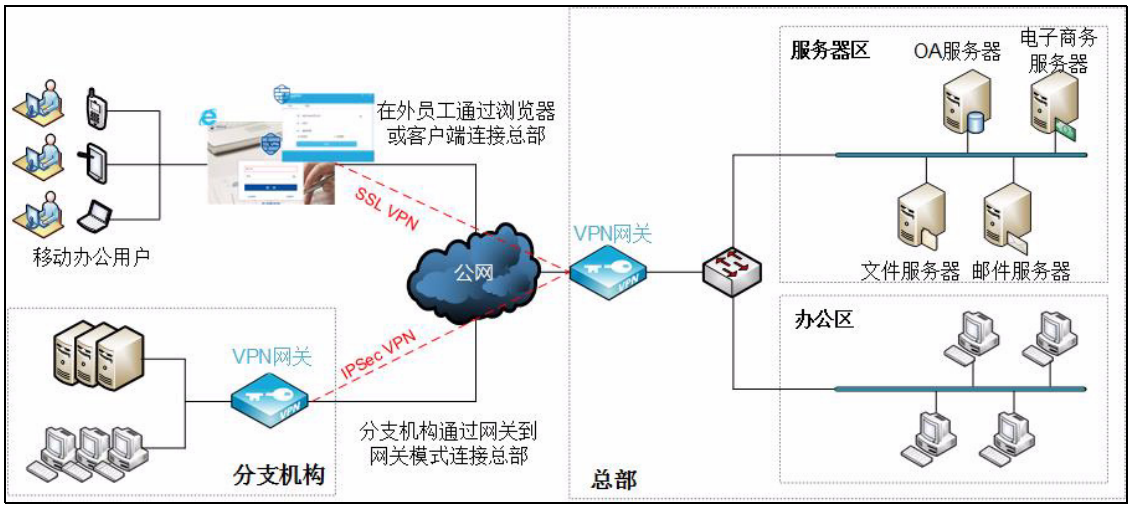
请在使用本产品前，对网络进行必要的规划，确定产品部署方式。如不是全新网络，需考虑部署本产品对原有网络规划及编址的影响。

VPN 网关支持单臂和网关两种部署方式：

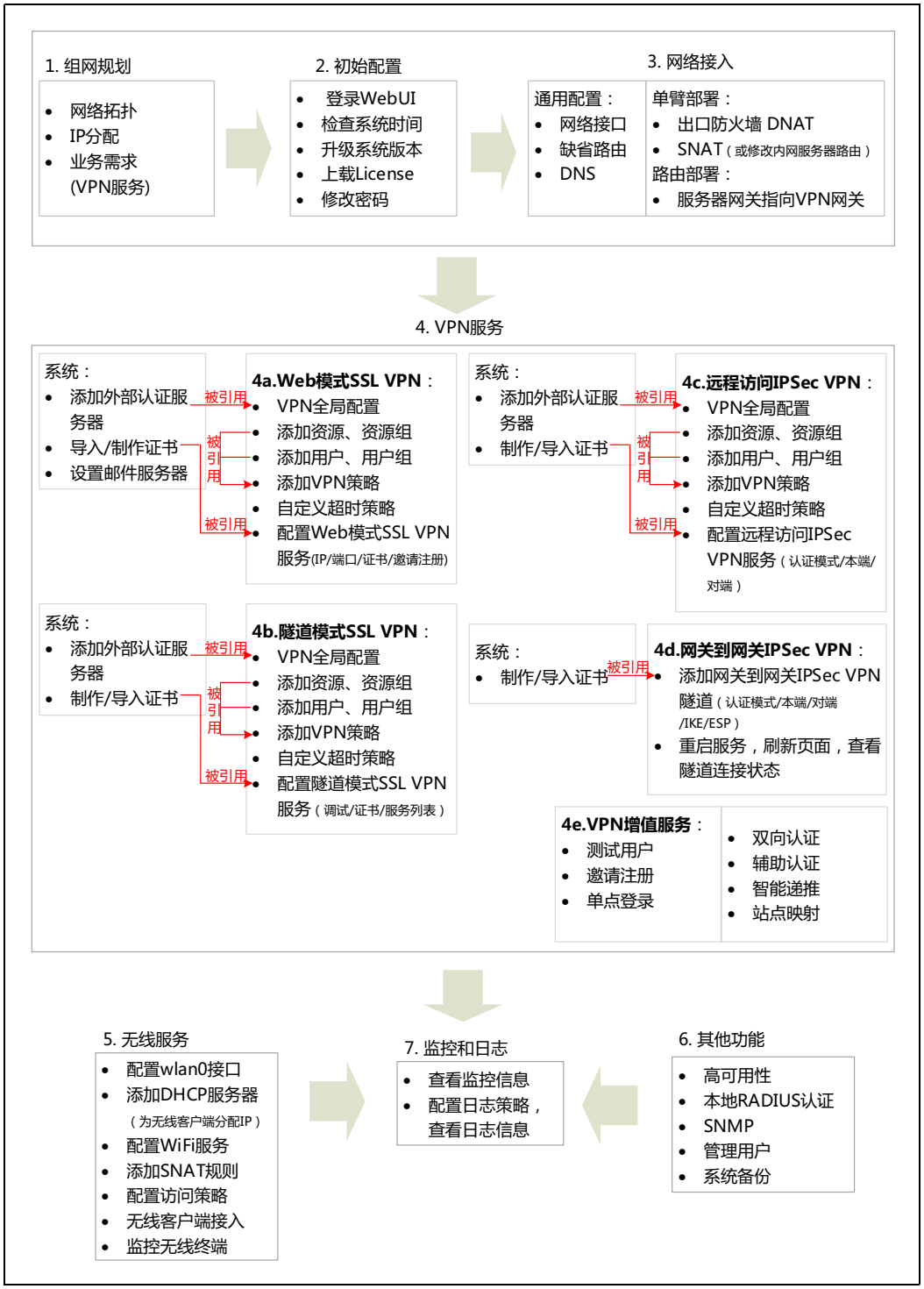
- 单臂模式



- 网关模式



1.4 配置逻辑


1. 组网规划
网络拓扑
IP分配
业务需求
(VPN服务)
2. 初始配置
登录WebUI
检查系统时间
升级系统版本
上载License
修改密码
3. 网络接入
通用配置：
网络接口
缺省路由
DNS
单臂部署：
出口防火墙 DNAT
SNAT（或修改内网服务器路由）
路由部署：
服务器网关指向VPN网关
4. VPN服务
系统：
添加外部认证服务器
导入/制作证书
设置邮件服务器
被引用
4a.Web模式SSL VPN：
VPN全局配置
添加资源、资源组
添加用户、用户组
添加VPN策略
自定义超时策略
配置Web模式SSL VPN服务(IP/端口/证书/邀请注册)
系统：
添加外部认证服务器
制作/导入证书
4c.远程访问IPSec VPN：
VPN全局配置
添加资源、资源组
添加用户、用户组
添加VPN策略
自定义超时策略
配置远程访问IPSec VPN服务（认证模式/本端/对端）
系统：
添加外部认证服务器
制作/导入证书
4b.隧道模式SSL VPN：
VPN全局配置
添加资源、资源组
添加用户、用户组
添加VPN策略
自定义超时策略
配置隧道模式SSL VPN服务（调试/证书/服务列表）
系统：
制作/导入证书
4d.网关到网关IPSec VPN：
添加网关到网关IPSec VPN隧道（认证模式/本端/对端/IKE/ESP）
重启服务，刷新页面，查看隧道连接状态
4e.VPN增值服务：
测试用户
邀请注册
单点登录
双向认证
辅助认证
智能递推
站点映射
5. 无线服务
配置wlan0接口
添加DHCP服务器（为无线客户端分配IP）
配置WiFi服务
添加SNAT规则
配置访问策略
无线客户端接入
监控无线终端
7. 监控和日志
查看监控信息
配置日志策略，查看日志信息
6. 其他功能
高可用性
本地RADIUS认证
SNMP
管理用户
系统备份

1.5 配置步骤

表 2 VPN 网关配置步骤

配置对象	配置步骤	操作路径
初始配置	1. 登录	为管理主机添加 192.168.1.0/24 网段的 IP 地址，在浏览器中输入 VPN 网关缺省管理地址 **https://192.168.1.100:10443**，使用缺省用户名 / 密码 （root/neteye）登录。 **提示**：完成配置后，建议拔掉管理接口的网线。
	2. 检查系统时间	系统管理 > 系统时间 （手动修改系统时间） **提示**：可先配置好自动校时，待网络配置完成后，即可生效。
	3. 更新系统版本	系统管理 > 升级 **提示**：升级包获取地址：neteye.neusoft.com （技术支持 > 下载中心 >VPN 网关）。
	4. 上载 License	系统管理 > License
	5. 修改密码	管理员初始用户名和密码为 “root” 和 “neteye”。为保证系统安全，请及时修改管理员密码： • Web 管理密码：点击界面右上角的登录账号，选择**修改密码**，修改 Web 管理密码。 • SSH 管理密码：可在控制台通过 passwd 命令进行修改。
单臂部署	1. 配置网络接口	网络 / 策略 > 接口 > 配置 （内外网接口为一个接口）
	2. 配置缺省路由	网络 / 策略 > 路由 > 静态路由 （网关指向上游出口防火墙）
	3. 配置 DNS	网络 / 策略 > DNS **提示**：主要用于在自动校时、用户认证和邀请注册过程中解析 NTP 服务器、外部认证服务器和邮件服务器的域名。
	4. 配置出口防火墙 DNAT	在出口防火墙上配置一条 DNAT 规则，将 VPN 服务映射到出口防火墙的外网接口 IP 和端口上。
	5. 针对隧道模式 SSL VPN 的特殊配置	• 由于服务器只有到 VPN 网关的回包路由，没有到 SSL VPN 客户端虚拟子网的回包路由，需要配置一条 SNAT 规则，将 SSL VPN 客户端的子网虚拟 IP 地址池映射到 VPN 网关的内网接口 IP。 • 如果内网服务器端需要监控 SSL VPN 客户端的源 IP，则不能做 SNAT 转换，但可以修改内网服务器的路由表，增加到 SSL VPN 客户端虚拟子网的路由。
路由部署	1. 配置网络接口	网络 / 策略 > 接口 > 配置 （内外网接口为两个接口）
	2. 配置缺省路由	网络 / 策略 > 路由 > 静态路由 （网关指向运营商路由器）
	3. 配置 DNS	网络 / 策略 > DNS **提示**：主要用于在自动校时、用户认证和邀请注册过程中解析 NTP 服务器、外部认证服务器和邮件服务器的域名。
	4. 配置内网服务器网关	服务器的网关指向 VPN 网关内网口。
	5. 配置攻击防御 （可选）	可针对 VPN 网关和后台服务器配置 DDoS 攻击防御，针对后台服务器配置 IP 选项校验。 **提示**：单臂模式下 VPN 网关前面有防火墙，所以不用配。

表 2 VPN 网关配置步骤 (*续*)

配置对象	配置步骤	操作路径
Web 模式 SSL VPN	1. 配置外部认证服务器（可选）	系统管理 > 外部认证服务器 **提示**：如使用外部认证服务器认证 SSL VPN 用户，需添加外部认证服务器，然后在全局配置中选择该外部认证服务器。
	2. 全局配置	基础功能 > 全局配置 （设置认证服务器、 Web 页面缓存 / 压缩策略和超时提醒） **提示**：如使用 LDAP 或 AD 认证服务器，还需配置 LDAP 安全组信息。
	3. 配置资源及资源组	基础功能 > 资源 （除子网和远程 Web 应用外的资源类型） 基础功能 > 资源组
	4. 配置用户及用户组	基础功能 > 用户 （使用本地认证服务器时需添加用户） 基础功能 > 用户组 （使用 LDAP/AD 认证服务器时可添加 LDAP 动态组，适用于用户组成员经常变化的情况）
	5. 配置 VPN 策略	基础功能 > VPN 策略 （指定哪些用户可以访问哪些资源） **提示**：如果使用 LDAP 或 AD 认证服务器，可以通过 LDAP 动态组或安全组添加授权用户。
	6. 配置超时策略 （可选）	基础功能 > 超时策略 （可以使用缺省超时策略）
	7. 导入 / 制作证书	系统管理 > 证书 **提示**： • 推荐使用权威 CA 机构颁发的服务器证书，需要同时导入 CA 和服务器证书； • 也可以在 VPN 网关上制作证书，只不过不受客户端浏览器信任。
	8. 配置 Web 模式 SSL VPN	基础功能 > Web 模式 SSL VPN • 必填：启用服务，指定服务 IP 和端口，选择服务器证书 • 可选：自定义 Portal 模板，邀请注册，系统通知
	9. 配置邮件服务器 （可选）	系统管理 > 邮件服务器 **提示**：开启邀请注册功能时用于发送邀请码和验证码。

表 2 VPN 网关配置步骤 (*续*)

配置对象	配置步骤	操作路径
隧道模式 SSL VPN	1. 配置外部认证服务器（可选）	系统管理 > 外部认证服务器 **提示：**如使用外部认证服务器认证 SSL VPN 用户，需添加外部认证服务器，然后在全局配置中选择该外部认证服务器。
	2. 全局配置	基础功能 > 全局配置 （指定认证服务器） **提示：**如使用 LDAP 或 AD 认证服务器，还需配置 LDAP 安全组信息。
	3. 配置资源及资源组	基础功能 > 资源 （支持全部资源类型） 基础功能 > 资源组
	4. 配置用户及用户组	基础功能 > 用户 （使用本地认证服务器时需添加用户） 基础功能 > 用户组 （使用 LDAP/AD 认证服务器时可添加 LDAP 动态组，适用于用户组成员经常变化的情况）
	5. 配置 VPN 策略	基础功能 > VPN 策略 （指定哪些用户可以访问哪些资源） **提示：**如果使用 LDAP 或 AD 认证服务器，可以通过 LDAP 动态组或安全组添加授权用户。
	6. 配置超时策略	基础功能 > 超时策略 （可以使用缺省超时策略）
	7. 制作 / 导入证书	系统管理 > 证书 **提示：** • CA 证书的公共名一般填写组织机构的域名，如 neusoft.com ； • 服务器证书的公共名必须填写 SSL VPN 服务的公网 IP 或域名。
	8. 配置隧道模式 SSL VPN	基础功能 > 隧道模式 SSL VPN • 必填：启用服务，开启调试，指定 CA 证书和服务器证书，添加服务 • 可选：访问日志，推送 DNS，推送网关，双向认证，数据压缩，摘要 / 加密算法 **提示：** • 当映射到出口防火墙上的服务端口不同于服务原始端口时，需要指定隧道接入地址，即映射到出口防火墙后的服务 IP/域名和端口。 • 对于存在端口限制的网络环境，可以添加 TCP 443 备选服务，保证服务端口被阻断时用户可以通过 443 端口访问服务 （该服务 IP 不能与 Web 模式 SSL VPN 服务的 IP 相同）。

表 2 VPN 网关配置步骤 (*续*)

配置对象	配置步骤	操作路径
远程访问 IPSec VPN	1. 配置外部认证服务器（可选）	系统管理 > 外部认证服务器 **提示**：如使用外部认证服务器认证 IPSec VPN 用户，需添加外部认证服务器，然后在全局配置中选择该外部认证服务器。
	2. 全局配置	基础功能 > 全局配置 （指定认证服务器） **提示**：如使用 LDAP 或 AD 认证服务器，还需配置 LDAP 安全组信息。
	3. 配置资源及资源组	基础功能 > 资源 （支持全部资源类型） 基础功能 > 资源组
	4. 配置用户及用户组	基础功能 > 用户 （使用本地认证服务器时需添加用户） 基础功能 > 用户组 （使用 LDAP/AD 认证服务器时可添加 LDAP 动态组，适用于用户组成员经常变化的情况）
	5. 配置 VPN 策略	基础功能 > VPN 策略 （指定哪些用户可以访问哪些资源） **提示**：如果使用 LDAP 或 AD 认证服务器，可以通过 LDAP 动态组或安全组添加授权用户。
	6. 配置超时策略	基础功能 > 超时策略 （可以使用缺省超时策略）
	7. 制作 / 导入证书 （可选）	系统管理 > 证书 （如果使用证书认证模式） **提示**： • CA 证书的公共名一般填写组织机构的域名，如 neusoft.com ； • 服务器证书的公共名必须填写 SSL VPN 服务的公网 IP 或域名。 • 如果用户使用 Android 版 IPSec VPN 客户端，还需要为用户制作个人证书，公共名填写用户名称。
	8. 配置远程访问 IPSec VPN	基础功能 > IPSec VPN 启用服务，开启日志，选择认证模式 （证书 / 预共享密钥），设置本端地址和 ID 信息，设置对端客户端虚拟地址池。 **提示**： • 系统默认提供一条 Remote Access 隧道，仅能查看和编辑。 • 使用证书认证时，本端 ID 类型为证书主题， ID 信息必须与所指定证书的主题信息保持一致。 • 如果隧道协商失败，点击日志 > 调试 >IPSec VPN 协商日志，查看协商失败原因。
网关到网关 IPSec VPN	1. 制作 / 导入证书 （可选）	系统管理 > 证书 （如果使用证书认证模式） **提示**： • CA 证书的公共名一般填写域名，如 neusoft.com ； • 服务器证书的公共名一般填写本端 / 对端的 IP/ 域名。
	2. 创建网关到网关 IPSec VPN 隧道 （本端和对端）	基础功能 > IPSec VPN • 必填：启用服务，开启日志，选择认证模式 （证书 / 预共享密钥），设置本端 IP 地址、 ID 类型和本端子网，配置对端 IP 地址 / 域名、 ID 类型和对端子网 • 可选：选择 IKE 和 ESP 提议集

表 2 VPN 网关配置步骤 (*续*)

配置对象	配置步骤	操作路径
	3. 查看结果	重启服务，刷新页面，查看隧道连接状态。 • 如果隧道状态为**已连接**，表示隧道协商成功，系统会自动生成允许本端和对端子网互访的访问策略，可到网络 / 策略 > 访问策略 > 配置 IPSec VPN 访问策略界面查看； （管理员可根据需要添加细化的访问策略，限制用户对特定资源的访问权限。） • 如果隧道状态为**未连接**，表示隧道协商失败，可到日志 > 调试界面查看 IPSec VPN 协商日志，查找协商失败原因。
VPN 增值功能	测试用户	• 通过界面右上角的快捷菜单，可测试用户名密码是否匹配。 • 基础功能 >VPN 策略 > 测试用户匹配，可测试用户是否具有资源访问权限。
	邀请注册 （Web 模式 SSL VPN）	1. 基础功能 > 用户组，创建被邀请求用户组 （包含用户为空）。 2. 基础功能 > 资源 / 资源组，配置允许被邀请用户访问的资源和资源组。 3. 基础功能 >VPN 策略，设置被邀请用户的资源访问权限。 4. 系统管理 > 邮件服务器，配置邮件服务器，用于发送包含邀请码或验证码的邮件。（需正确配置 DNS 服务器，确保 VPN 网关与邮件服务器可以通信。） 5. 基础功能 >Web 模式 SSL VPN> 配置邀请码，启用邀请注册功能，配置可邀请用户数、注册用户组、邀请码、邀请邮件模板。 6. 管理员在配置邀请码界面设置收件人地址，发送邀请码；SSL VPN 用户登录 Portal，邀请注册。 7. 被邀请人登录 Portal，注册成为 SSL VPN 用户。
	单点登录 （Web 模式 SSL VPN）	基础功能 > 资源 1. 添加或编辑 HTTP/HTTPS 资源，开启自动登录。 2. 启用 SSO。（如果使用资源系统账号，登录 Portal 之后还需要设置访问目标资源的独立账号。） 3. 配置认证地址 （必填）和认证参数 （根据网站实际情况抓取填写，用户名和密码参数必填，支持引用 js 脚本）。 4. 根据网站实现不同，可能还需要设置 Header 和 Cookie 参数。 5. 如果认证参数依赖认证之前的交互页面，需要使用正则表达式配置动态参数。 6. 如果使用资源系统账号，还需要设置登录页面地址。 7. 如有需要，还可以设置重定向地址，即用户登录后默认访问的页面。
	双向认证 （隧道模式 SSL VPN）	1. 管理员制作用户个人证书和 E-Key。 2.SSL VPN 用户使用 E-Key 和 SSL VPN 客户端拨号。

表 2 VPN 网关配置步骤 (*续*)

配置对象	配置步骤	操作路径
	辅助认证	**短信认证：** 1. 确定要使用的短信平台，到短信平台注册并获取所需参数信息。 2. 到 VPN 网关指定使用的短信平台并配置相关参数信息。 3. 开启短信认证，并添加认证用户及绑定手机号码。 4.SSL VPN 用户登录时获取短信验证码完成登录。 **OTP 认证：** 1. 确定系统时间正确，保证不会因为系统时间导致 OTP 认证失败。 2. 开启 OTP 认证，添加认证用户并绑定 OTP 设备。 3.SSL VPN 用户登录时输入 OTP 设备上显示的一次性动态口令完成登录。 **硬件特征码认证：** 1. 开启硬件特征码认证，并设置特征码收集和审批策略。 2.SSL VPN 用户尝试登录，完成特征码收集。 3. 管理员对收集到的用户和特征码信息进行审批。
	智能递推	1. 添加需要智能递推的资源。 2. 开启智能递推，指定递推范围。 3. 添加待优化递推链接，并设置访问速度优化策略。
	站点映射	1. 添加待映射站点资源。 2. 开启站点映射，指定映射端口。 3.SSL VPN 用户通过访问 VPN 网关地址及映射端口访问映射资源。
监控和日志	1. 监控流量和系统状态	监控 > 系统监控 > 接口流量统计 监控 > 在线用户 > 实时并发用户 监控 > 在线用户 > Web 模式在线用户 监控 > 在线用户 > 隧道模式在线用户 监控 > 在线用户 > IPSec VPN 在线用户 监控 > 历史监控 > 并发用户趋势图 监控 > 历史监控 > 接口流量趋势图 监控 > 历史监控 > CPU 使用趋势图 监控 > 历史监控 > 磁盘使用率趋势图 监控 > 历史监控 > 内存使用趋势图 监控 > 历史监控 > 应用排行 监控 > 历史监控 > 用户排行
	2. 查看日志信息	日志 > 日志配置 （Syslog 服务器和本地日志存储策略） 日志 > 管理日志 日志 > 访问日志 > Web 模式访问日志 日志 > 访问日志 > 隧道模式访问日志 日志 > 访问日志 > IPSec VPN 访问日志 日志 > 调试 > 隧道模式调试日志 日志 > 调试 > IPSec VPN 协商日志

表 2 VPN 网关配置步骤 (*续*)

配置对象	配置步骤	操作路径
其他功能	1. 配置 WiFi 服务	**提示**：仅 NVPN3000 机型支持 WiFi，具备 wlan0 接口。 1. 网络 / 策略 > 接口 > 配置，配置 wlan0 接口： • 为其配置 IP 地址，作为三层口使用。 • 作为二层口，将其与其他内网接口一起划入 Bridge 接口，为 Bridge 接口配置 IP 地址。 2. 网络 / 策略 > DHCP 服务器，配置 DHCP 服务器，用于为内网无线客户端分配 IP，推送网关和 DNS。 • 接口选三层 wlan0，网关为 wlan0 的 IP ； • 接口选包含 wlan0 的 Bridge 接口，网关为 Bridge 接口 IP 3. 网络 / 策略 > WiFi > 配置，配置 WiFi 服务，为内网无线客户端提供无线接入服务。 4. 网络 / 策略 > 地址转换 > 源地址转换，配置 SNAT 规则，将内网无线客户端地址转换为外网口地址。 5. 网络 / 策略 > 访问策略，配置访问策略，允许内网无线客户端访问外网。（入口接口选三层 wlan0 或包含 wlan0 的 Bridge 接口。） 6. 使用无线终端接入无线网络。 7. 网络 / 策略 > WiFi > 监控，监控在线无线终端。
	2. 配置高可用性	系统管理 > 高可用性 > 配置同步 / 集群 1. 在一端网关上配置集群，并完成所有其他配置。 2. 在两端网关上设置配置同步，在完成所有配置的网关上点击立即同步，将所有配置信息同步到对端。 **提示**： • VPN 网关高可用性仅支持主备模式。 • 单臂模式下只需在两端设备配置一个虚拟路由器，网关模式下则需要配置两个虚拟路由器，出口和入口各一个。
	3. 配置本地 RADIUS 认证	系统管理 > 本地 RADIUS 认证服务 （对外提供 RADIUS 认证服务）
	4. 配置 SNMP	系统管理 > SNMP 配置
	5. 添加管理用户	系统管理 > 管理员 （可添加管理员、审计员或 HA 用户）
	6. 备份系统配置	系统管理 > 备份 / 恢复

2 典型配置场景

本章给出以下常见功能的配置范例：

2.1 VPN 部署模式

VPN 网关的部署模式可以为单臂模式或网关模式，请根据实际需求选择相应的模式。

- 2.1.1 单臂模式
- 2.1.2 网关模式

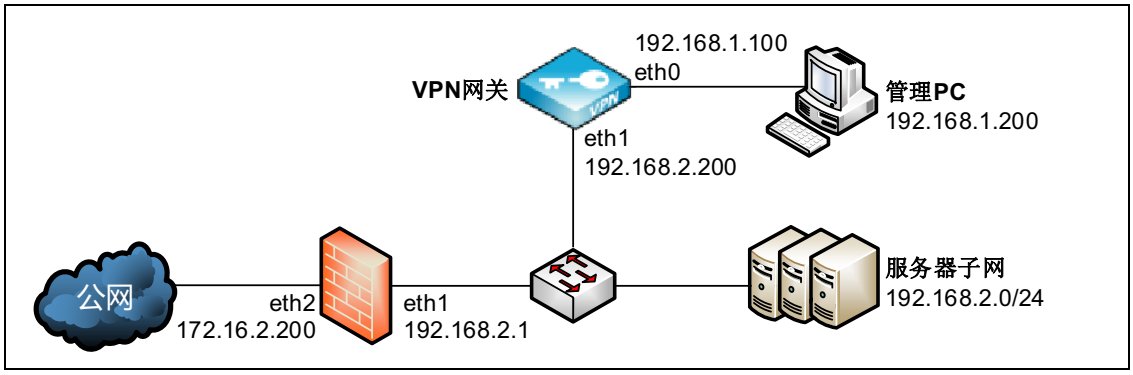
提示：推荐保留 VPN 网关的以太网接口 eth0 （缺省 IP 地址为 192.168.1.100）作为管理接口。管理员可以在管理 PC 上通过 eth0 接口对 VPN 网关进行管理和配置。

本节介绍两种模式的基本配置信息，关于 SSL VPN 和 IPSec VPN 的详细配置信息，请参见以下范例：

- 2.3 Web 模式 SSL VPN
- 2.4 隧道模式 SSL VPN
- 2.5 远程访问 IPSec VPN
- 2.6 网关到网关 IPSec VPN

2.1.1 单臂模式

组网拓扑



配置要点

- 配置接口
- 配置网关

配置步骤

配置接口

1. 选择**网络 / 策略 > 接口 > 配置**，点击 eth1 接口对应的 ，根据实际环境进行设置。

2. 点击**确定**。

配置网关

1. 选择**网络 / 策略 > 路由 > 静态路由**。

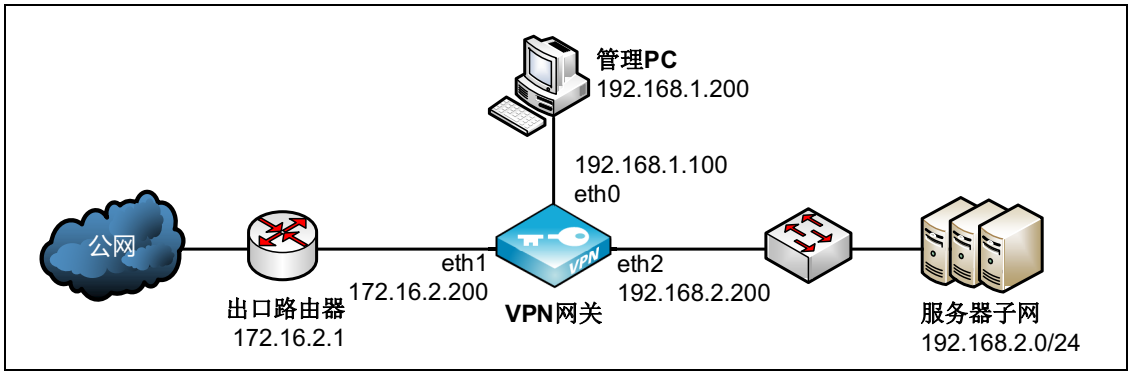
2. 点击**添加**，添加一条缺省路由，将出口接口设置为 eth1、网关设置为 192.168.2.1。

3. 点击**确定**。

提示：为了使外网客户端能够访问到内网服务器，还需要在出口防火墙上配置一条目的地址转换规则，将目的地址为服务器公网 IP 地址的访问转换为到 VPN 网关 eth1 接口的访问。

2.1.2 网关模式

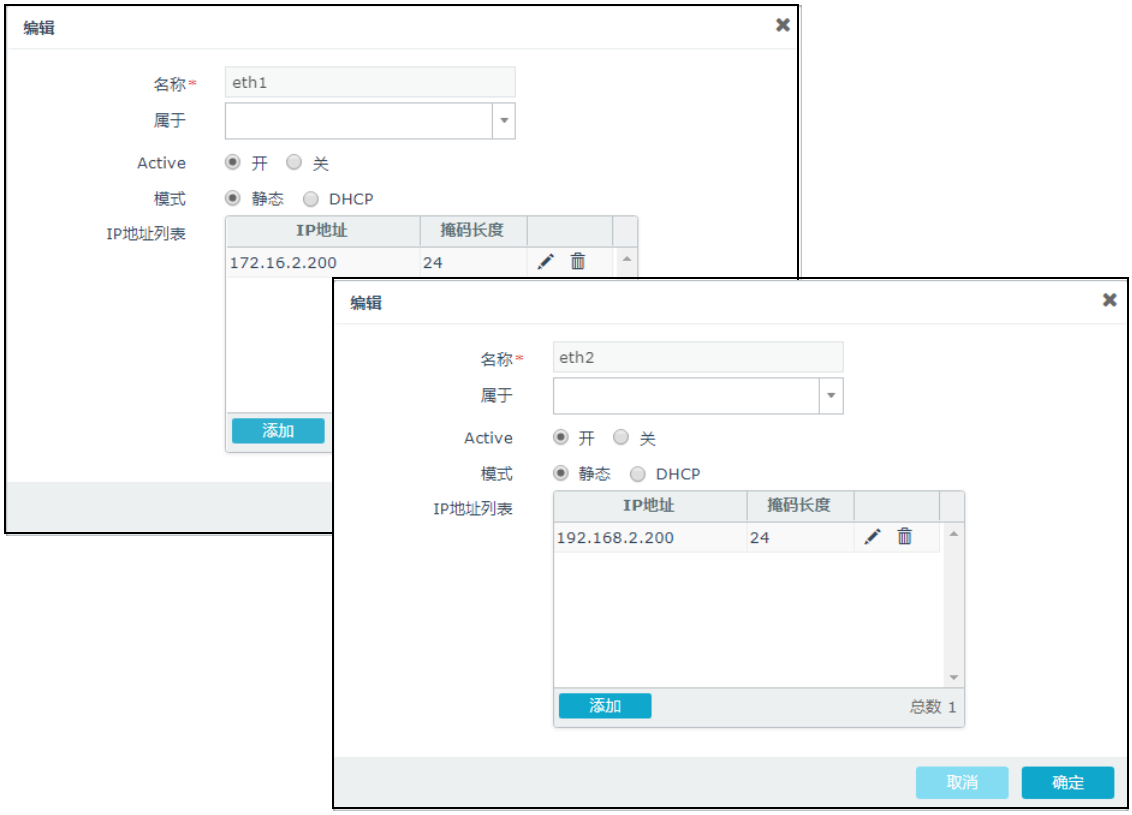
组网拓扑



推荐 eth1 为外网口，连接公网； eth2 接口为内网口，连接内网服务器。

配置接口

1. 选择**网络 / 策略 > 接口 > 配置**，点击 eth1 和 eth2 对应的 ，根据实际环境进行设置。



2. 点击**确定**。

配置缺省路由

1. 选择**网络 / 策略 > 路由 > 静态路由**。
2. 添加缺省路由，出口接口设为 eth1，网关设为 172.16.2.1。

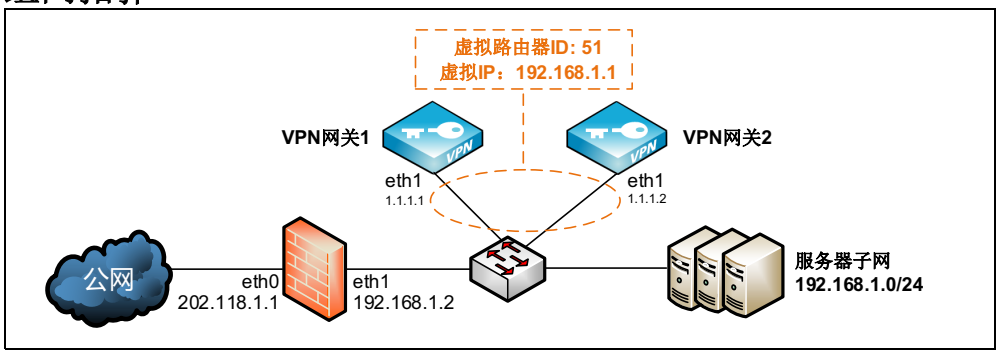
3. 根据需要添加其他静态路由。

2.2 高可用性部署

VPN 网关支持单臂和路由两种部署模式，所以本范例分别给出两种部署模式下的高可用性配置方式：

2.2.1 单臂模式高可用性

组网拓扑



配置要点

- 配置集群
- 设置配置同步

配置步骤

配置集群

1. 假设所有配置都是在**VPN网关1**上进行的，在**VPN网关1**上选择**系统管理>高可用性>集群**。
2. 可以看到系统默认提供一个虚拟路由器 ID 为 51 的虚拟路由器配置条目。

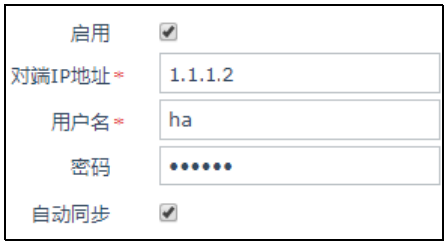
3. 点击 对其进行修改。

4. 点击**确定**。点击**提交**。

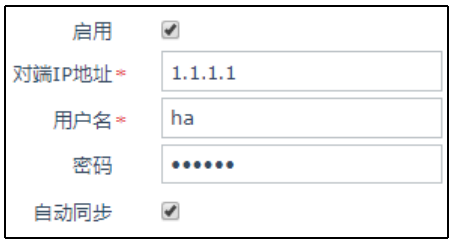
设置配置同步

1. 在 **VPN 网关 1** 和 **VPN 网关 2** 上选择**系统管理 > 高可用性 > 配置同步**。
2. 点击**添加**，添加要同步配置的对端设备。

VPN 网关 1



VPN 网关 2

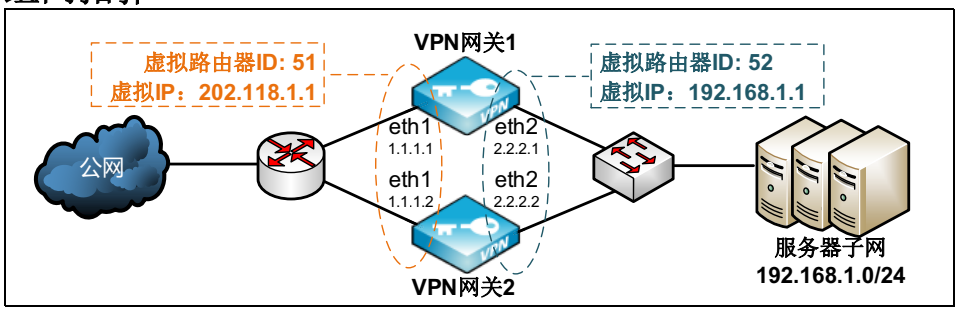


用户名和密码为对端设备的 HA 用户的用户名和密码，这里使用缺省值 ha/neteye。

3. 点击**确定**。点击**提交**。
4. 提交配置后，在**提交**按钮后面将出现一个**立即同步**按钮。待对端也完成了配置同步的设置，在 **VPN 网关 1** 上点击该按钮，可立即同步本端配置信息到对端。

2.2.2 网关模式高可用性

组网拓扑



配置要点

- 配置集群
- 设置配置同步

配置步骤

配置集群

1. 假设所有配置都是在**VPN网关1**上进行的，在**VPN网关1**上选择**系统管理>高可用性>集群**。
2. 可以看到系统默认提供一个虚拟路由器 ID 为 51 的虚拟路由器配置条目。

3. 点击 对其进行修改。

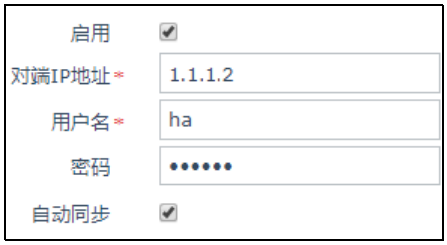
4. 点击**确定**。
5. 点击**添加**，添加虚拟路由器 ID 为 52 的条目。

6. 点击**确定**。
7. 点击**提交**。

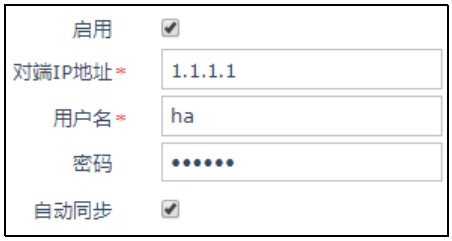
设置配置同步

1. 在 **VPN 网关 1** 和 **VPN 网关 2** 上选择**系统管理 > 高可用性 > 配置同步**。
2. 点击**添加**，添加要同步配置的对端设备。

VPN 网关 1



VPN 网关 2



用户名和密码为对端设备的 HA 用户的用户名和密码，这里使用缺省值 ha/neteye。

3. 点击**确定**。点击**提交**。
4. 提交配置后，在**提交**按钮后面将出现一个**立即同步**按钮。待对端也完成了配置同步的设置，在 **VPN 网关 1** 上点击该按钮，可立即同步本端配置信息到对端。

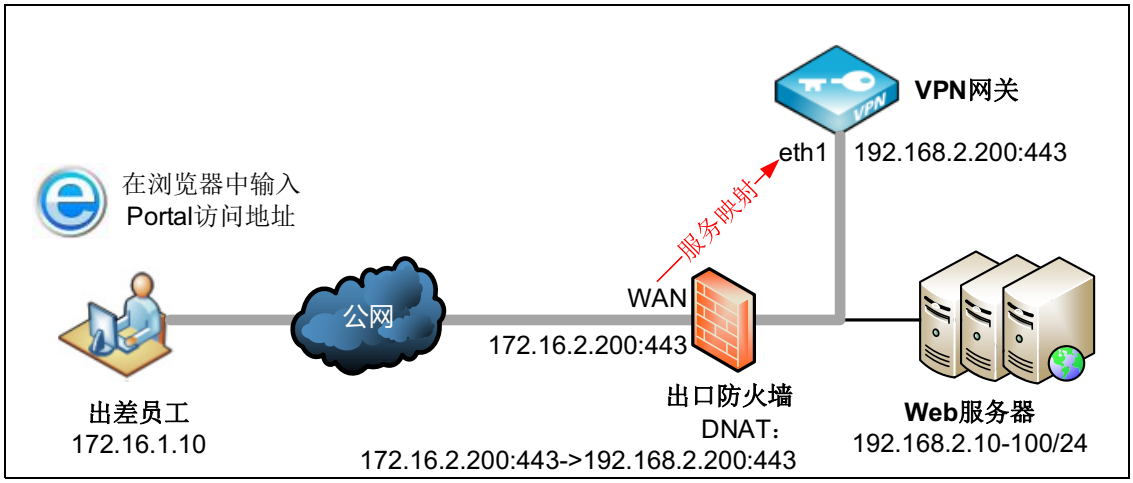
2.3 Web 模式 SSL VPN

基本需求

在外出差员工需要访问公司办公系统，实现远程办公。为防止企业机密数据泄露，公司计划部署 VPN 网关，让在外员工能够安全地访问公司内部资源，并且能够为用户设置访问资源的权限。

由于办公系统多为 Web 服务器，管理员需在 VPN 网关上配置 Web 模式的 SSL VPN，使出差员工无需安装客户端软件即可通过浏览器登录公司办公系统办公。

组网拓扑



配置要点

- 配置全局设置
- 配置资源和资源组
- 配置用户和用户组
- 配置 VPN 策略
- 导入 SSL VPN 服务器证书
- 配置 Web 模式 SSL VPN
- 配置出口防火墙 DNAT
- 验证结果

配置步骤

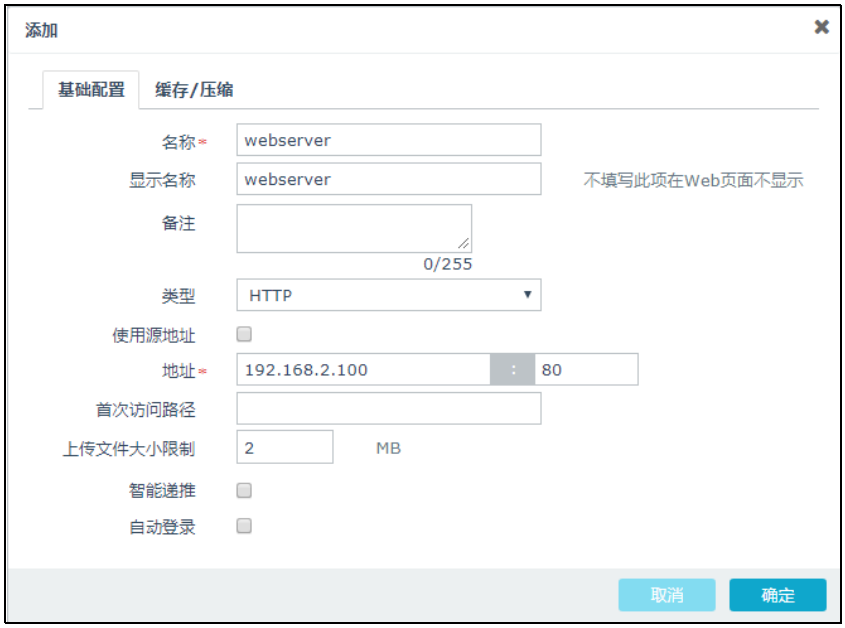
配置全局设置

1. 选择**基础功能 > 全局设置**。
2. 选择本地认证服务器，设置缓存 / 压缩策略和会话超时时间。

3. 点击**提交**。

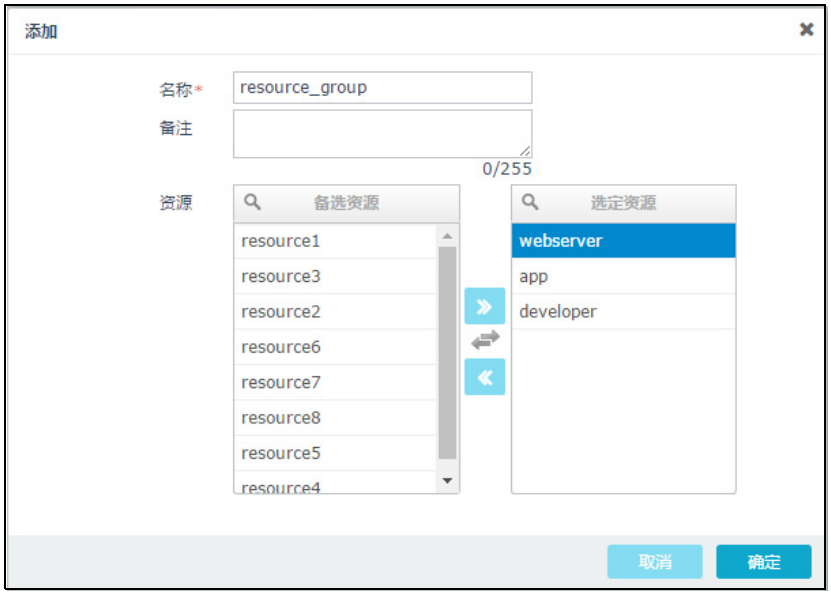
配置资源和资源组

1. 选择**基础功能 > 资源**。
2. 点击**添加**，填写资源相关信息，使用全局的缓存 / 压缩设置。



提示：请务必填写**显示名称**，否则在客户端资源列表中将不显示该资源。

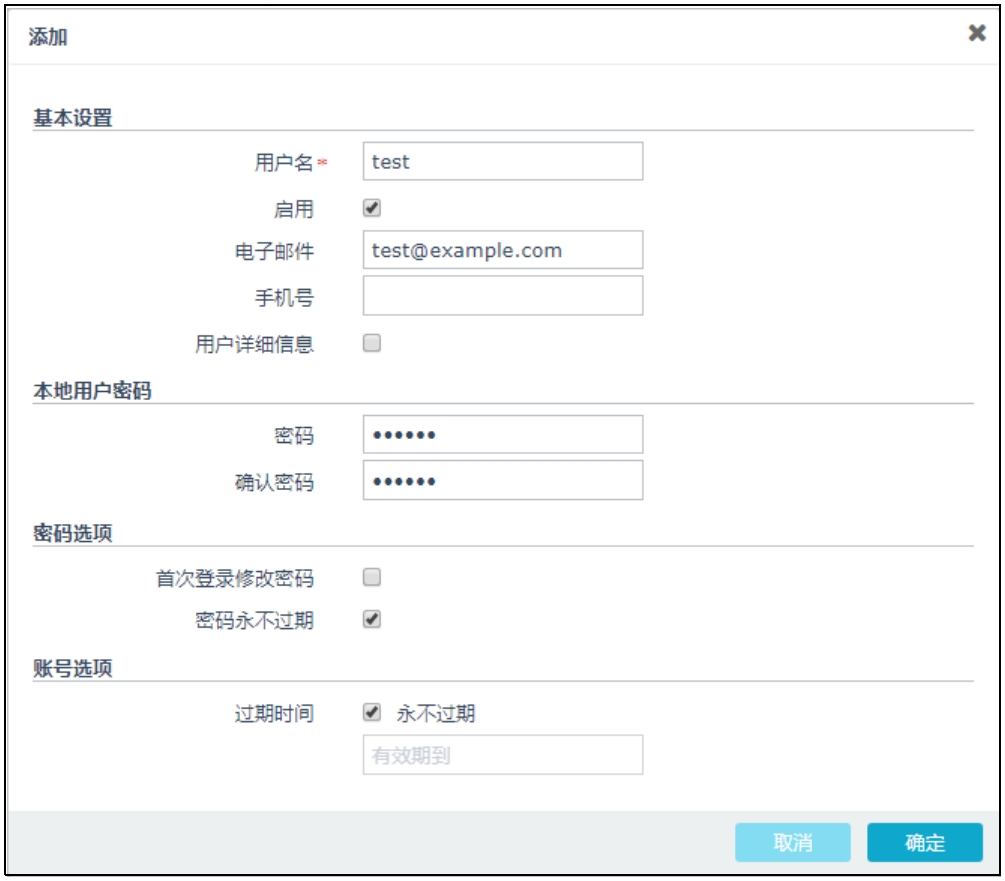
3. 点击**确定**。
4. 以同样方式添加其他资源。
5. 选择**基础功能 > 资源组**。
6. 点击**添加**，设置资源组名称并选择要加入资源组的资源。



7. 点击**确定**。

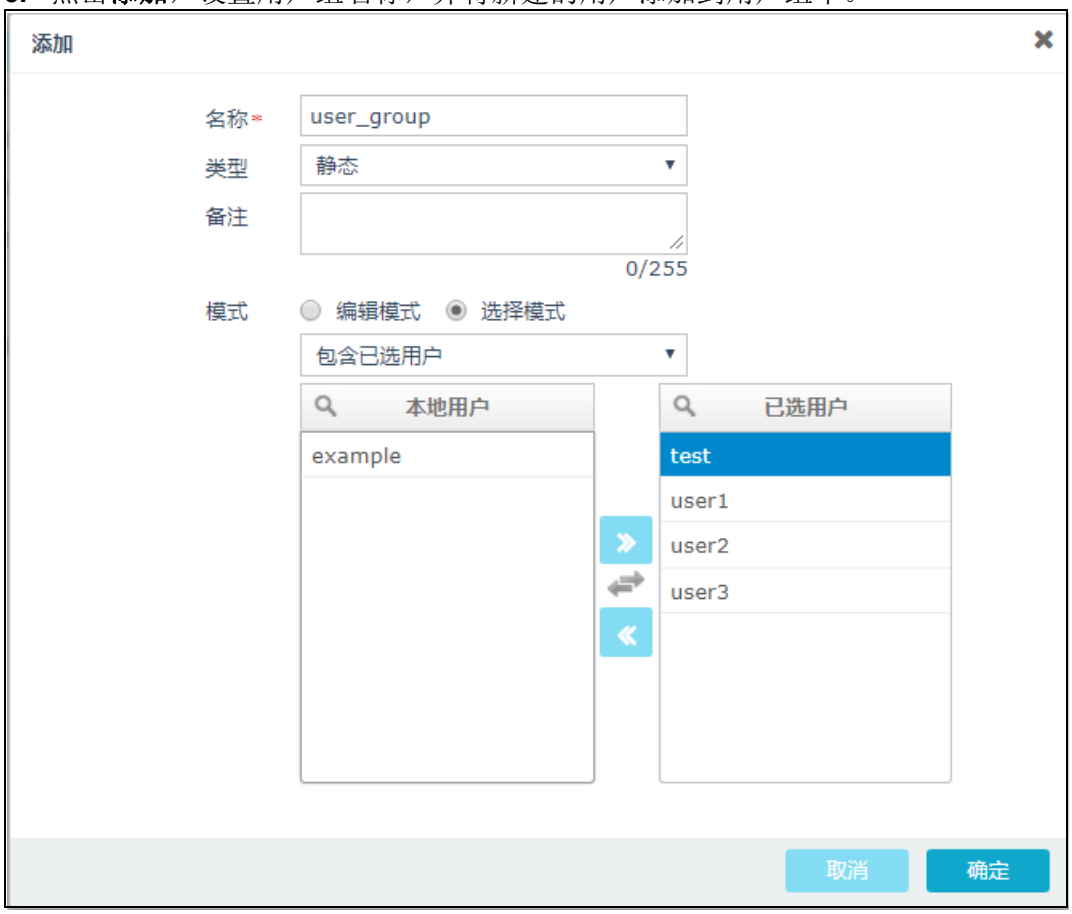
配置用户和用户组

1. 选择**基础功能 > 用户**。
2. 点击**添加**，新建本地认证用户。



3. 点击**确定**。
4. 以同样方式添加其他用户。

5. 选择**基础功能 > 用户组**。
6. 点击**添加**，设置用户组名称，并将新建的用户添加到用户组中。



7. 点击**确定**。

配置 VPN 策略

1. 选择**基础功能 > VPN 策略**。
2. 点击**添加**，在弹出的对话框中设置相关信息。
   a. 在**基础配置**页签，设置策略名称，勾选**启用**和 **Web 模式 SSL VPN**，**动作**设为**允许**。

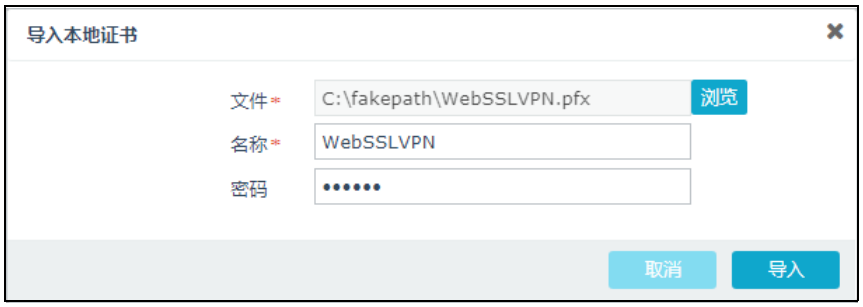
   b. 在**用户组**页签选择策略应用于的用户组。

   c. 在**资源组**页签选择策略应用于的资源组。

3. 点击**确定**。

导入 SSL VPN 服务器证书

1. 选择**系统管理 > 证书**。
2. 点击**导入**，选择**本地证书**，导入 SSL VPN 服务器证书：



提示：推荐使用权威 CA 机构颁发的服务器证书。

3. 点击**导入**。

配置 Web 模式 SSL VPN

1. 选择**基础功能 > Web 模式 SSL VPN > Portal**。
2. 启用 Web 模式 SSL VPN 和访问日志功能，配置服务器地址和本地证书，勾选重定向和登录验证码复选框。

3. 点击**提交**。

配置出口防火墙 DNAT

在出口防火墙上配置目的地址转换：

规则	描述
172.16.2.200:443->192.168.2.200:443	将防火墙公网 IP 和端口映射到 VPN 服务 IP 和端口。

验证结果

1. 配置结束后，用户 test 可以在浏览器中输入 https://172.16.2.200 登录，通过点击资源列表中的资源名称访问后端服务器资源。

2. 当SSL VPN用户连接成功后，可在**监控 > 在线用户 > Web模式在线用户**页面查看到用户在线信息。

提示：为保证用户访问响应速度，系统默认关闭 Web 模式 SSL VPN 在线用户流量监控功能。如需监控在线用户流量信息，请通过页面右上角的流量开关开启该功能。

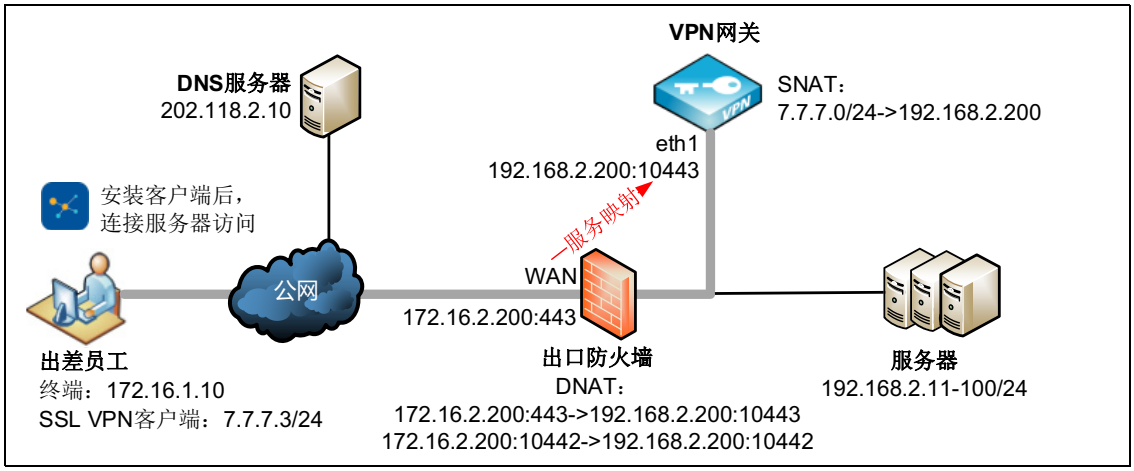
3. 如有需要，可以通过**离线**按钮强制用户下线。

2.4 隧道模式 SSL VPN

基本需求

在外出差员工需要访问公司内部服务器资源（如 Web 应用、 FTP 资源、邮件等），为保护敏感信息不泄露，公司计划部署东软 NetEye VPN 网关，通过建立隧道模式 SSL VPN，让出差员工能够安全地访问公司内部资源，同时能够对用户的访问权限进行严格限制和实时监控。

组网拓扑



系统为 SSL VPN 客户端分配的虚拟子网地址池是 7.7.7.0/24。

- 为了确保使用 SSL VPN 客户端的用户能够访问内网服务器，需要将 7.7.7.0/24 转换成 eth1 的 IP 地址。
- 为了让 SSL VPN 用户能够通过域名访问内网服务器，需要为 SSL VPN 客户端推送 DNS 服务器地址。

配置要点

- 配置全局设置
- 配置资源和资源组
- 配置用户和用户组
- 配置 VPN 策略
- 添加 CA 证书和本地证书
- 配置隧道模式 SSL VPN
- 配置源地址转换
- 配置出口防火墙 DNAT
- 验证结果

配置步骤

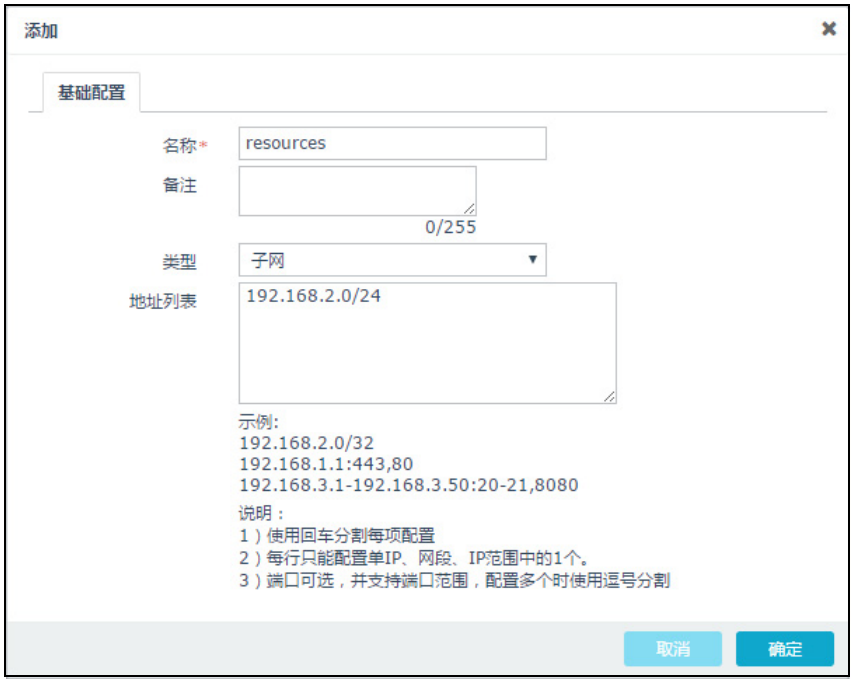
配置全局设置

1. 选择**基础功能 > 全局设置**。
2. 选择本地认证服务器，设置缓存 / 压缩策略和会话超时时间。

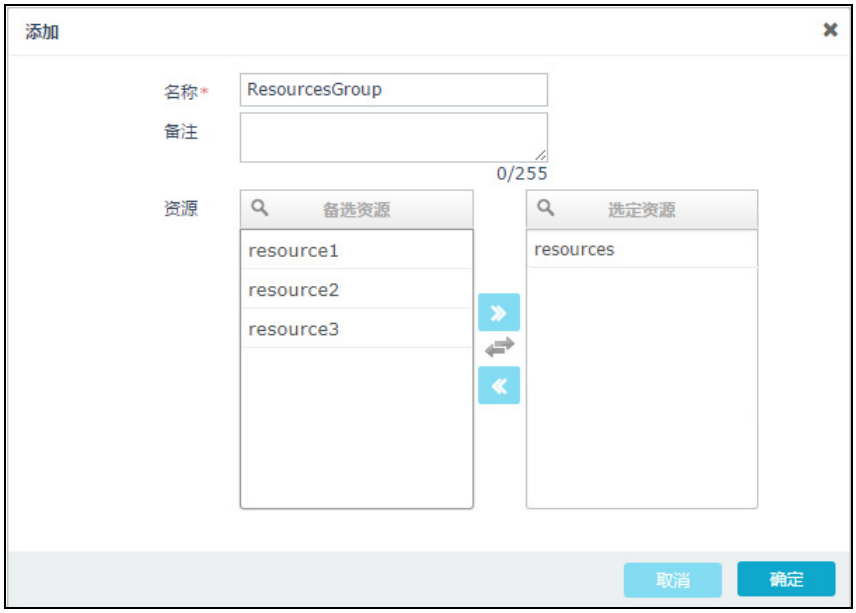
3. 点击**提交**。

配置资源和资源组

1. 选择**基础功能 > 资源**。
2. 点击**添加**，添加允许 SSL VPN 用户访问的子网资源。



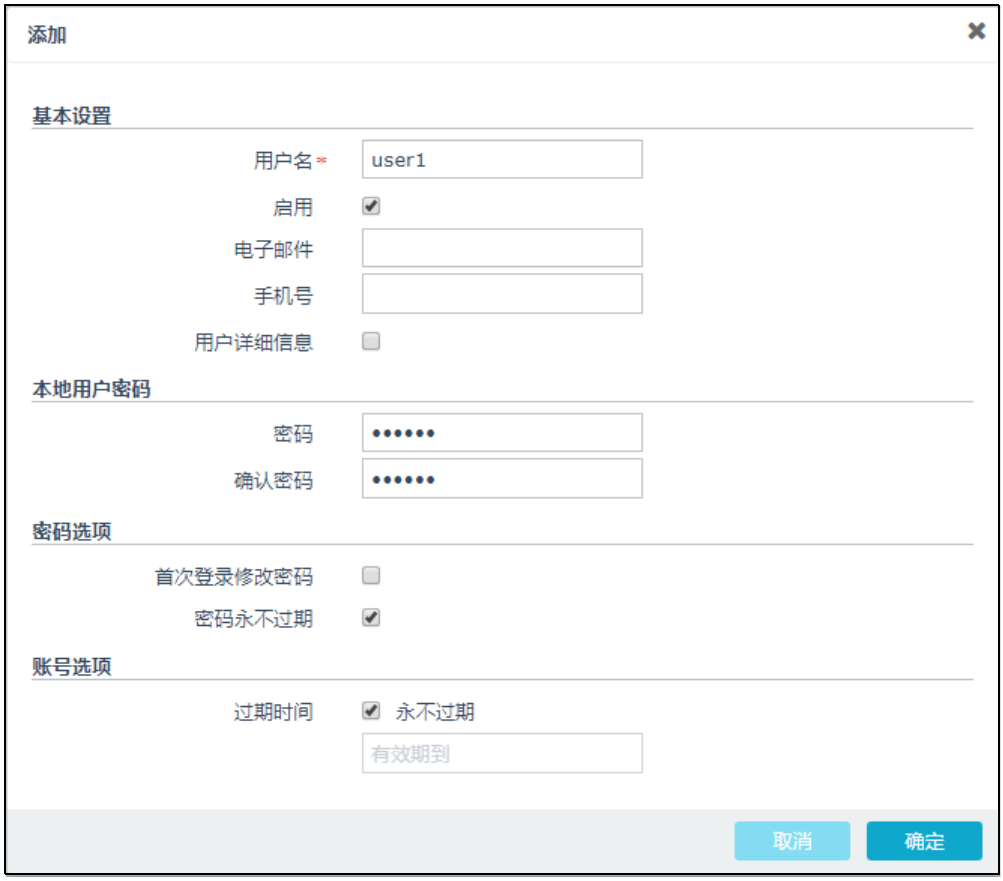
3. 点击**确定**。
4. 选择**基础功能 > 资源组**。
5. 点击**添加**，添加资源组，对资源组命名并选择要加入资源组的资源。



6. 点击**确定**。

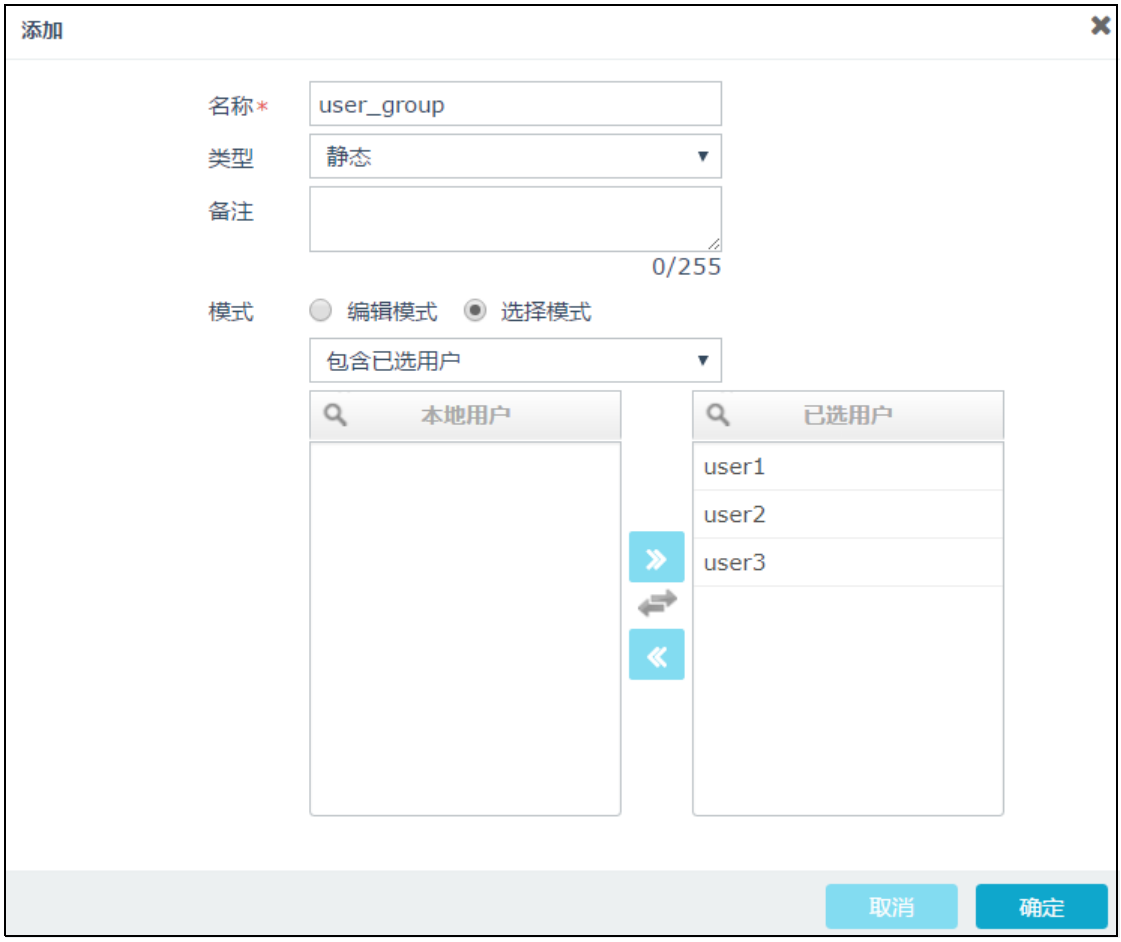
配置用户和用户组

1. 选择**基础功能 > 用户**。
2. 点击**添加**，新建本地用户 user1。



3. 点击**确定**。
4. 以同样方式添加其他 SSL VPN 用户。

5. 选择**基础功能 > 用户组**。
6. 点击**添加**，添加用户组。设置用户组名称，将允许访问资源的用户添加到用户组中。



7. 点击**确定**。

配置 VPN 策略

1. 选择**基础功能 > VPN 策略**。
2. 点击**添加**，在弹出的对话框中进行相关配置。
   a. 在**基础配置**页签，配置策略名称，勾选**启用**和**隧道模式 SSL VPN**，动作选择**允许**。

   b. 在**用户组**页签选择策略应用于的用户组。

   c. 在**资源组**页签选择策略应用于的资源组。

3. 点击**确定**。

添加 CA 证书和本地证书

1. 选择**系统管理 > 证书**。
2. 点击**添加**，选择**根 CA 证书**，添加根 CA 证书。

3. 点击**确定**。

4. 点击**添加**，选择**本地证书**，添加服务器证书。

5. 点击**确定**。

配置隧道模式 SSL VPN

1. 选择**基础功能 > 隧道模式 SSL VPN**。
2. 启用策略，开启调试和日志开关，选择之前添加的 CA 证书和本地服务器证书，设置推送的 DNS 服务器地址，添加服务。

为了兼容服务端口被占用或阻断的情况，建议添加一条保底的 TCP 443 服务，即服务端口被占用或阻断时，保证用户可以通过 443 端口访问该服务。

提示：添加的虚拟子网不能与真实子网的网段相同，如上面的虚拟子网不能设为 172.16.1.0/24。

---

3. 点击**提交**。

配置源地址转换

1. 选择**网络 / 策略 > 地址转换 > 源地址转换**。
2. 点击**添加**，添加一条源地址转换规则，将 SSL VPN 客户端使用的虚拟子网地址 7.7.7.0/24 转换为内网接口 eth1 的 IP 地址。

3. 点击**确定**。

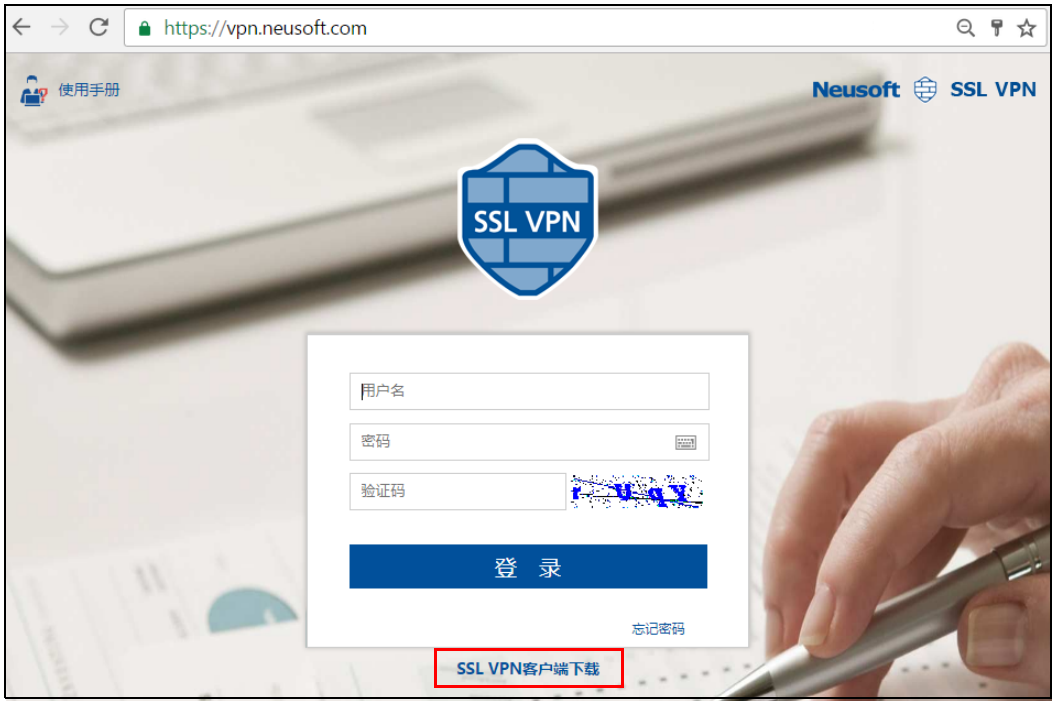
配置出口防火墙 DNAT

在出口防火墙上配置目的地址转换：

规则	描述
172.16.2.200:10442->192.168.2.200:10442	10442 为客户端从 SSL VPN 服务器获取配置信息的端口，可以在客户端上修改。
172.16.2.200:443->192.168.2.200:10443	将防火墙公网 IP 和端口映射到 VPN 服务 IP 和端口。 10443 为 SSL VPN 服务端口，可以在 VPN 网关上修改。

验证结果

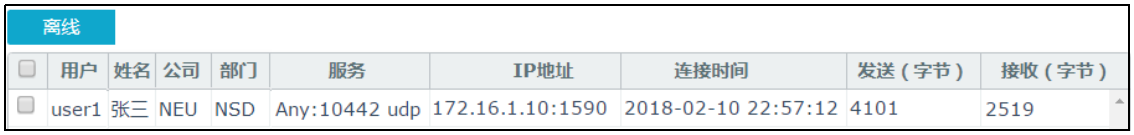
1. 网络用户通过东软 SSL VPN 客户端连接之后，能够访问公司内部服务器。
   a. 访问对应的 SSL VPN Portal 站点，下载并安装 SSL VPN 客户端软件。



   b. 使用客户端软件建立 SSL VPN 连接 （以 Windows 版客户端为例）。

c. 点击**资源列表**中的资源链接访问内网服务器。

2. 管理员登录 VPN 网关，选择**监控 > 在线用户 > 隧道模式在线用户**，能够查看到 VPN 用户的在线信息。



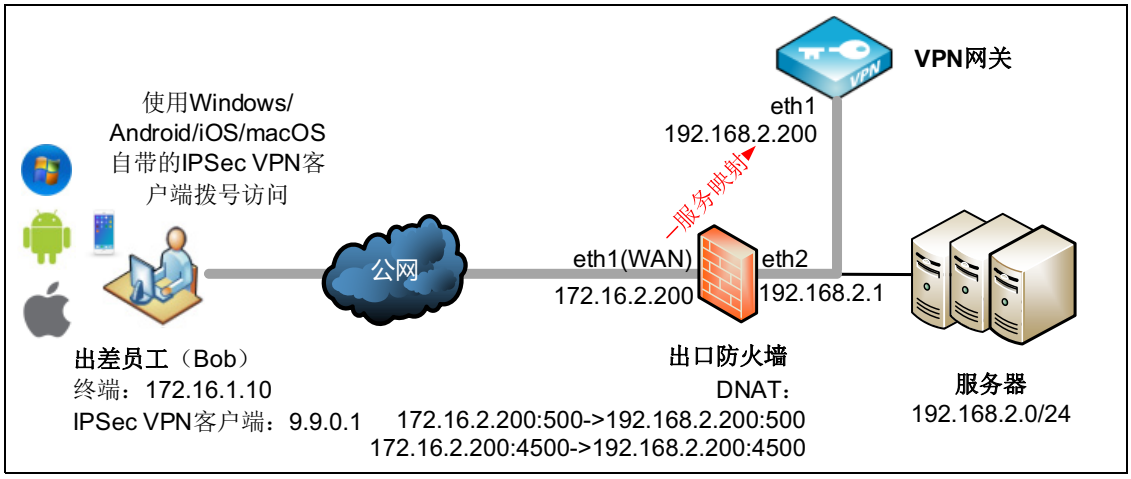
提示：如有需要，可以通过**离线**按钮强制用户下线。

2.5 远程访问 IPSec VPN

基本需求

出差员工需要访问公司内部服务器资源（如 Web 应用、FTP 资源、邮件等），为保护敏感信息不泄露，公司计划部署东软 NetEye VPN 网关，通过建立 IPSec VPN 隧道，让出差员工能够安全地访问公司内部资源，同时能够对用户的访问权限进行严格限制和实时监控。

组网拓扑



配置要点

- 单臂模式部署设备
- 配置全局设置
- 配置资源和资源组
- 配置用户和用户组
- 配置 VPN 策略
- 添加 CA 证书和本地证书
- 配置远程访问 IPSec VPN
- 配置出口防火墙 DNAT
- 配置 Windows 内置 IPSec VPN 客户端
- 配置 Android 内置 IPSec VPN 客户端
- 配置 iOS 内置 IPSec VPN 客户端
- 配置 macOS 内置 IPSec VPN 客户端
- 验证结果

配置步骤

单臂模式部署设备

1. 配置接口：配置 eth1 的 IP 地址为 192.168.2.200，掩码长度 24。
2. 配置网关：添加缺省路由，出口设置为 eth1，目的地址为 0.0.0.0/0，网关为 192.168.2.1。

配置全局设置

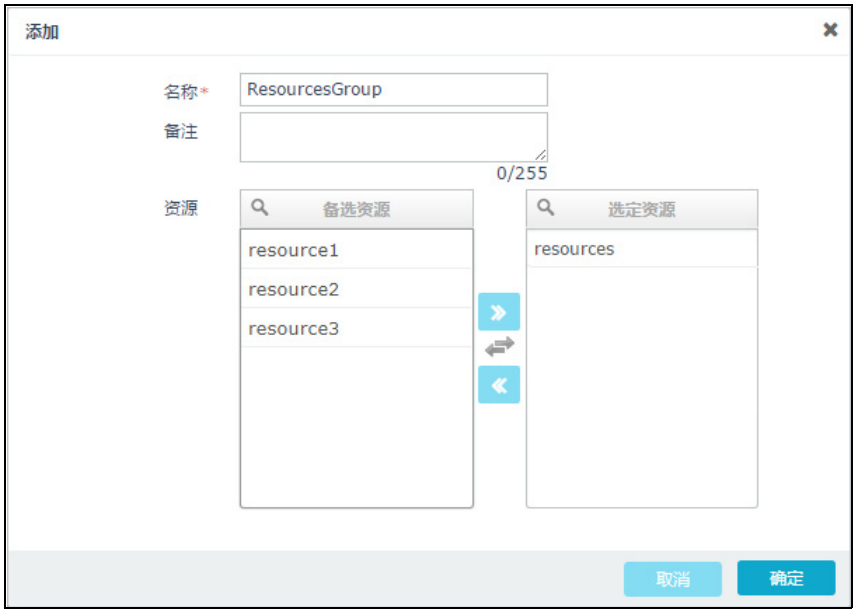
1. 选择**基础功能 > 全局设置**。
2. 配置认证服务器，使用本地认证服务器 Local 认证 SSL VPN 用户。

3. 点击**提交**。

配置资源和资源组

1. 选择**基础功能 > 资源**。
2. 点击**添加**，添加允许 IPSec VPN 用户访问的子网资源。

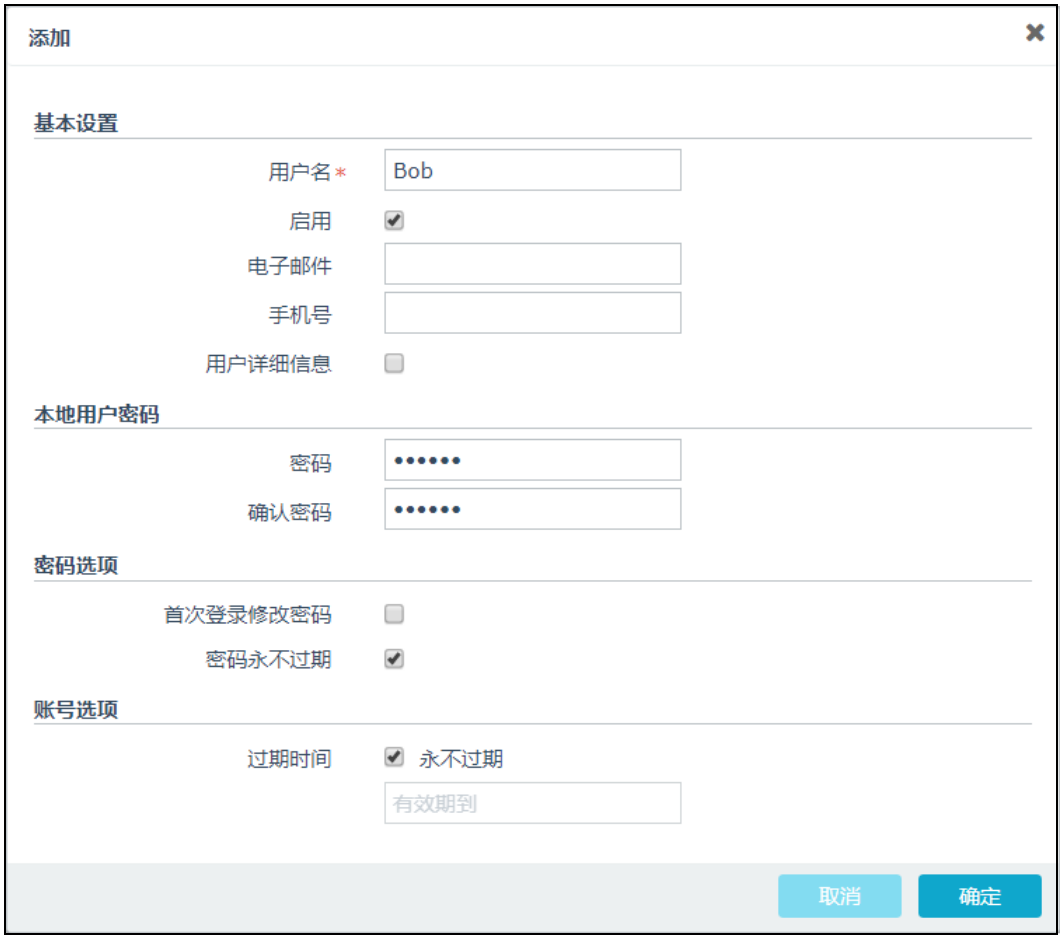
3. 点击**确定**。
4. 选择**基础功能 > 资源组**。
5. 点击**添加**，添加资源组，对资源组命名并选择要加入资源组的资源。



6. 点击**确定**。

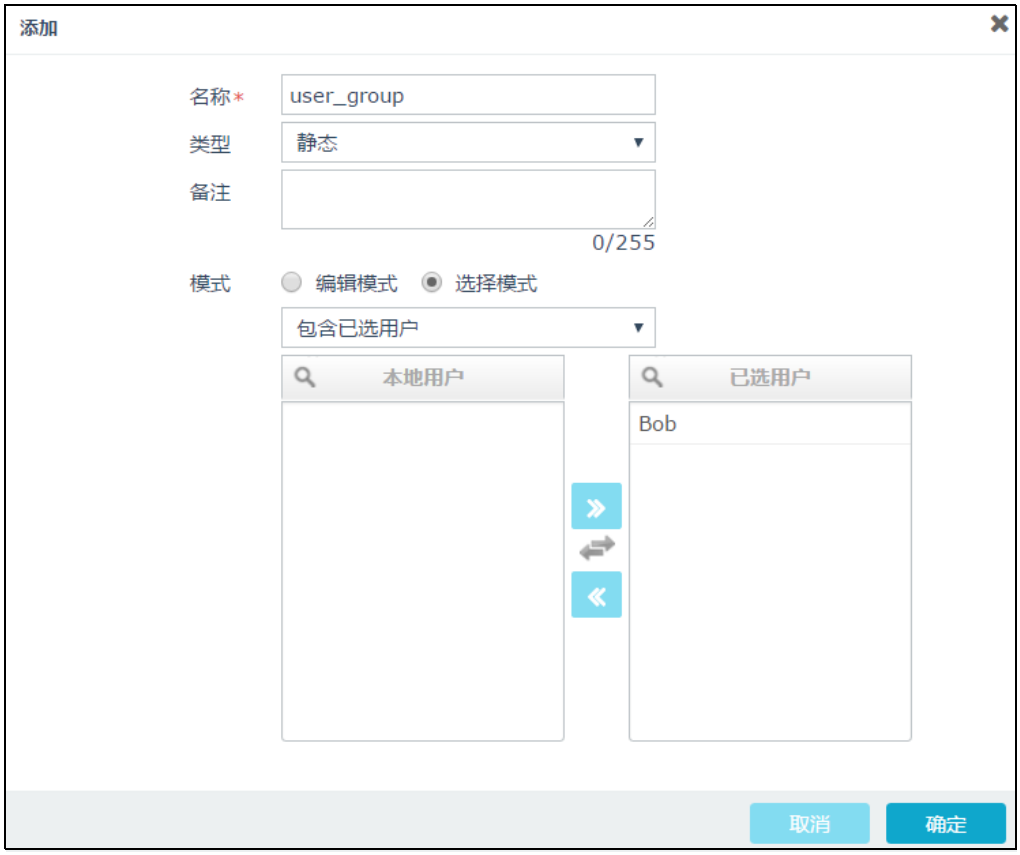
配置用户和用户组

1. 选择**基础功能 > 用户**。
2. 点击**添加**，创建名为 Bob 的用户并将密码设置 123456。



3. 点击**确定**。

4. 选择**基础功能 > 用户组**。
5. 点击**添加**，添加用户组。设置用户组名称，将允许访问资源的用户添加到用户组中。



6. 点击**确定**。

配置 VPN 策略

1. 选择**基础功能 > VPN 策略**。
2. 点击**添加**。
3. 在**基础配置**页签配置策略基本信息。

4. 在**用户组**页签选择策略应用于的用户组。

5. 在**资源组**页签选择策略应用于的资源组。

6. 点击**确定**。

添加 CA 证书和本地证书

1. 选择**系统管理 > 证书**。
2. 点击**添加**，选择**根 CA 证书**，添加根 CA 证书。

3. 点击**确定**。
4. 点击**添加**，选择**本地证书**，添加服务器证书和个人证书。

5. 点击**确定**。

配置远程访问 IPSec VPN

1. 选择**基础功能 > IPSec VPN**。在隧道列表中，可以看到系统默认提供的远程访问 IPSec VPN 隧道 （RemoteAccess）。

2. 点击 配置隧道和远程用户信息。
   a. 在**基础配置**页签，启用隧道，启用记录日志功能，配置证书认证方式。

   b. 点击**本地配置**页签，配置本端 IP 地址。

   输入的 ID 信息与前面创建本地证书时输入的证书主题信息应保持一致。
   c. 点击**对端配置**页签，配置客户端虚拟地址池。VPN 网关从地址池中选取 IP 地址并将其分配给 VPN 客户端。

   d. 点击**确定**。

配置出口防火墙 DNAT

由于 VPN 网关接在内网，需要通过前置防火墙将 VPN 服务 IP 映射到公网，所以需要在前置防火墙上做 TCP/UDP 标准端口 500 和 4500 的映射：

- DNAT1：172.16.2.200:500->192.168.2.200:500
- DNAT2：172.16.2.200:4500->192.168.2.200:4500

由于各个厂家设置方法有所不同，以上配置此处不截图说明。

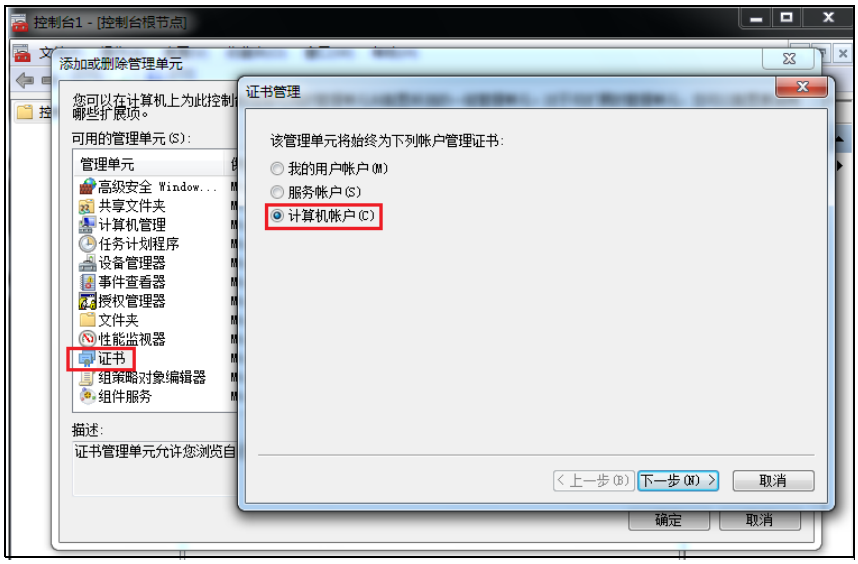
配置 Windows 内置 IPSec VPN 客户端

IPSec VPN 远程访问用户可以使用 Windows 系统 （以 Win7 为例）内置的 VPN 客户端连接到 VPN 网关。请预先从 VPN 网关上下载 CA 证书并导入远程用户 PC。

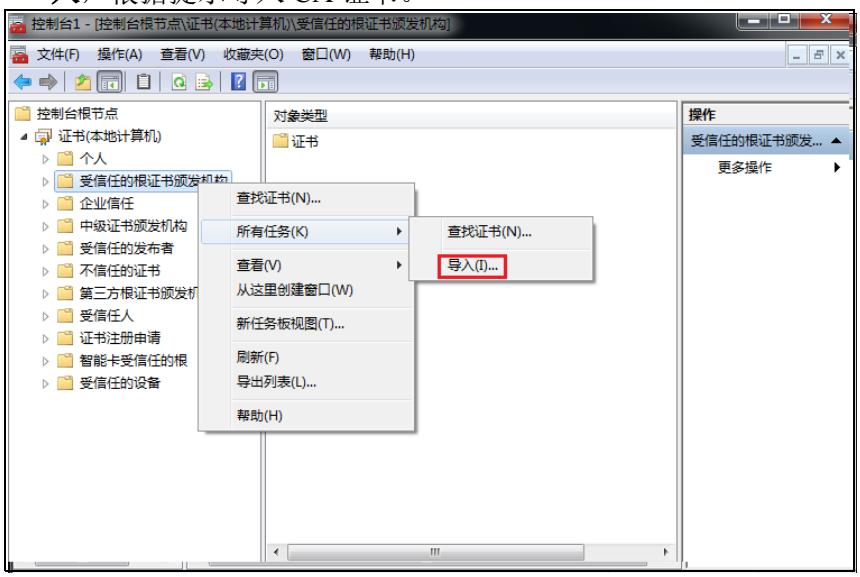
- 导入 CA 证书
- 创建 VPN 连接
- 修改 VPN 客户端配置

导入 CA 证书

1. 点击**开始** > **运行**，输入 **mmc** 命令。
2. 选择**文件** > **添加 / 删除管理单元**。点击**证书** > **添加**，选择**计算机帐户**，点击**下一步**。



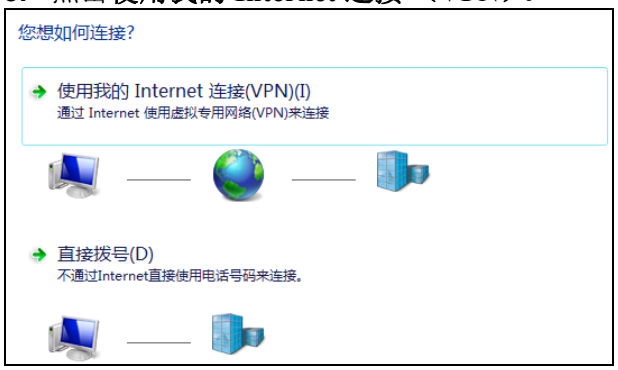
3. 点击**本地计算机**，点击**完成**，点击**确定**。
4. 在左侧**控制台根节点**，展开**证书**节点，选择**受信任的根证书颁发机构** > **所有任务** > **导入**，根据提示导入 CA 证书。



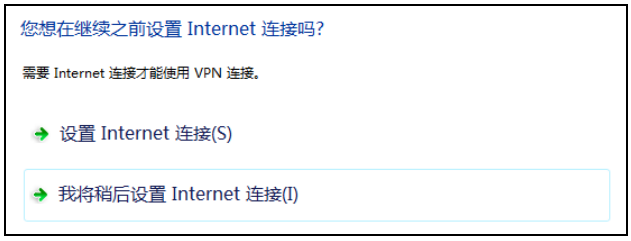
创建 VPN 连接

1. 打开网络和共享中心，点击**设置新的连接或网络**。
2. 点击**连接到工作区**，点击**下一步**。

3. 点击**使用我的 Internet 连接 （VPN）**。

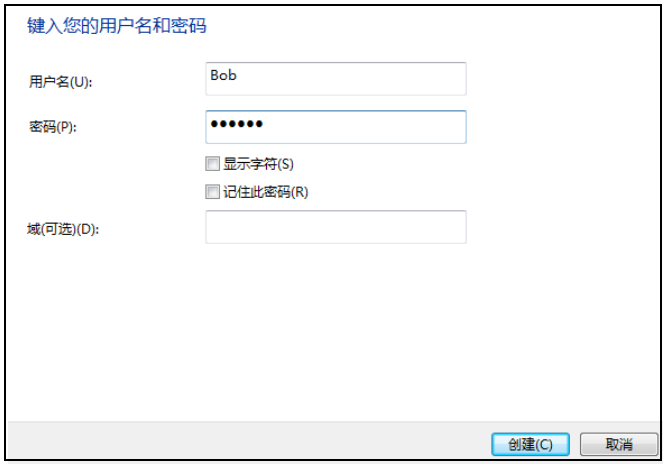


4. 点击**我将稍后设置 Internet 连接**。



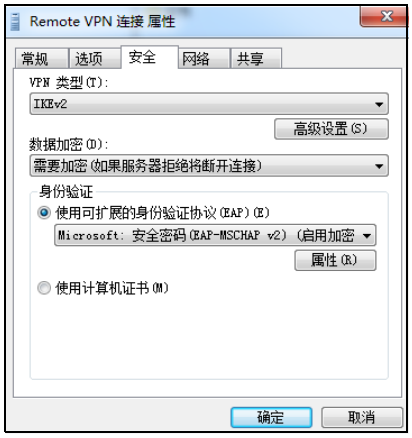
5. 在 **Internet 地址**文本框中，填写 VPN 网关的 IP 地址。在**目标名称**文本框中，添加 VPN 连接的名称。点击**下一步**。

6. 输入远程用户的名称和密码 （Bob 和 123456）。点击**创建**。



7. 点击**关闭**，继续配置 VPN 连接的详细信息。
8. 找到已创建的 VPN 连接，双击打开连接窗口，输入用户名和密码。

9. 点击**属性**，点击**安全**，配置安全选项。

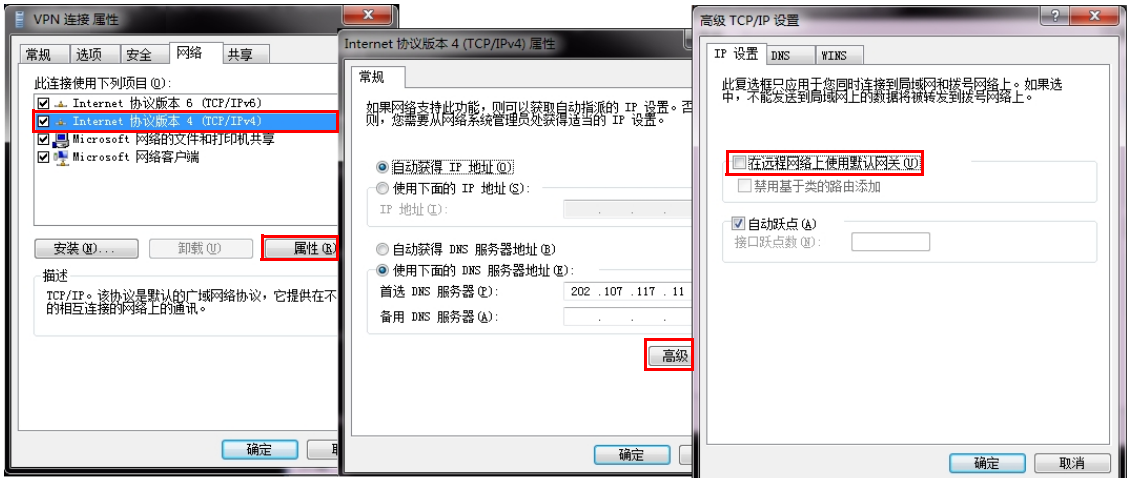


10. 点击**确定**。点击**连接**。待成功连接后，用户即可访问内网资源。

修改 VPN 客户端配置

如果想在远程访问 IPSec VPN 资源的同时不断开互联网和局域网连接，可通过以下方式实现：

1. 在连接属性窗口点开**网络**选项卡，选中 **Internet Protocol Version 4 (TCP/IPv4)**，点击**属性**，点击**高级**，取消勾选**使用远程网络的默认网关**。



2. 在终端运行中输入 cmd，然后通过 **`ipconfig /all`** 命令查看分配的 IPSec VPN 客户端地址，通过 **`route add`** 命令添加到目标资源的路由。

```
PPP adapter IPSecVPN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : IPSecVPN
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 9.9.0.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
C:\Windows\system32>route add 172.16.2.0 mask 255.255.255.0 9.9.0.1
 OK!
```

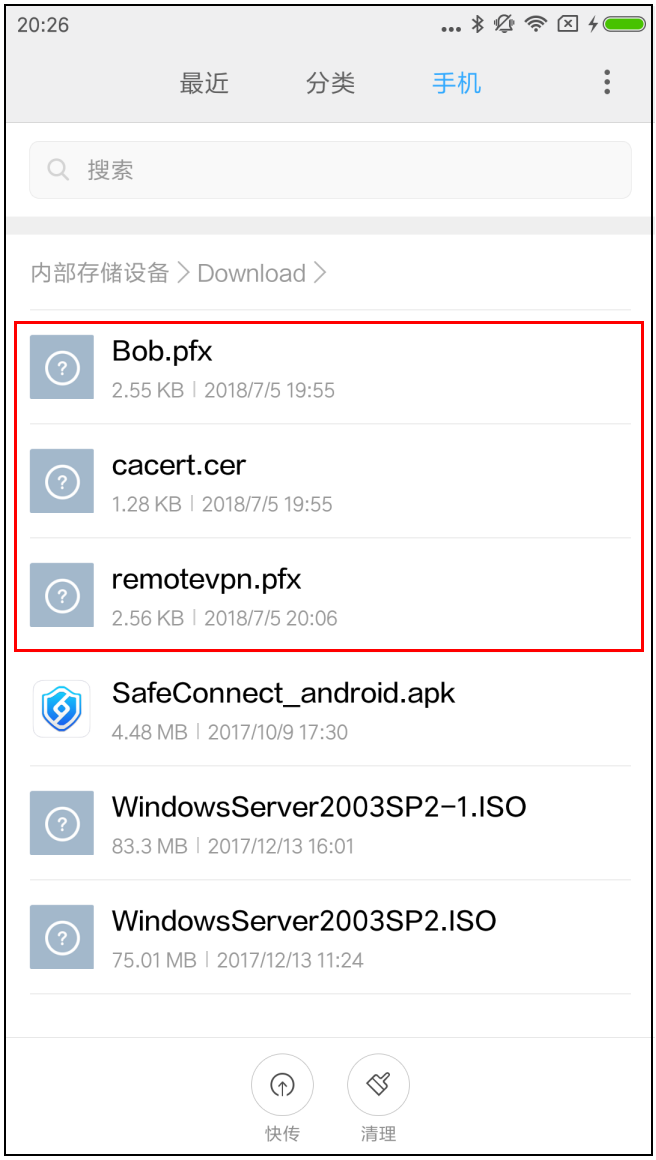
配置 Android 内置 IPSec VPN 客户端

导入和安装证书

1. 管理员将 CA 证书和远程用户个人证书发送给远程用户。
2. 远程用户将证书导入 Android 手机并安装。
   a. 连接手机和电脑，设置 USB 用途为**传输文件 （MTP）**。

提示：也可以通过邮件导入证书。

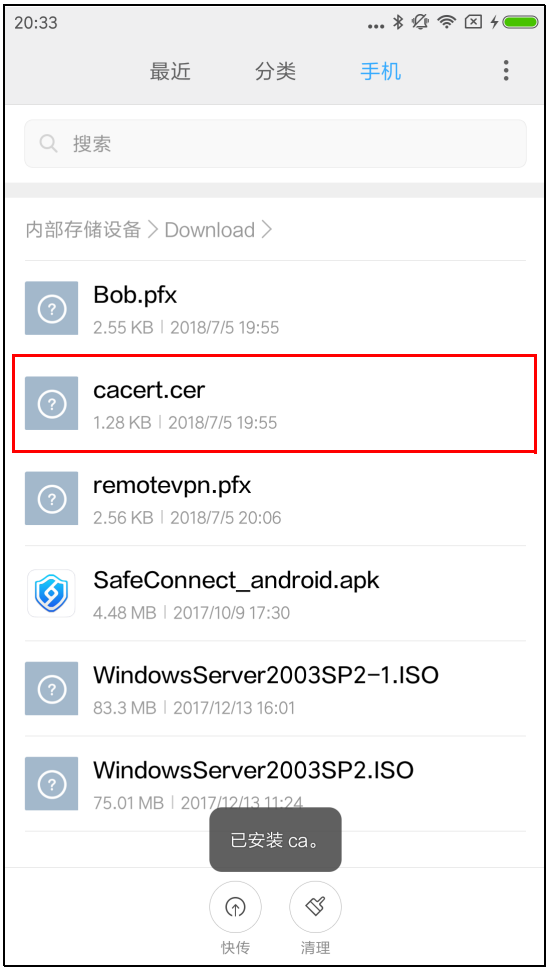
b. 将证书导入手机 Download 文件夹。



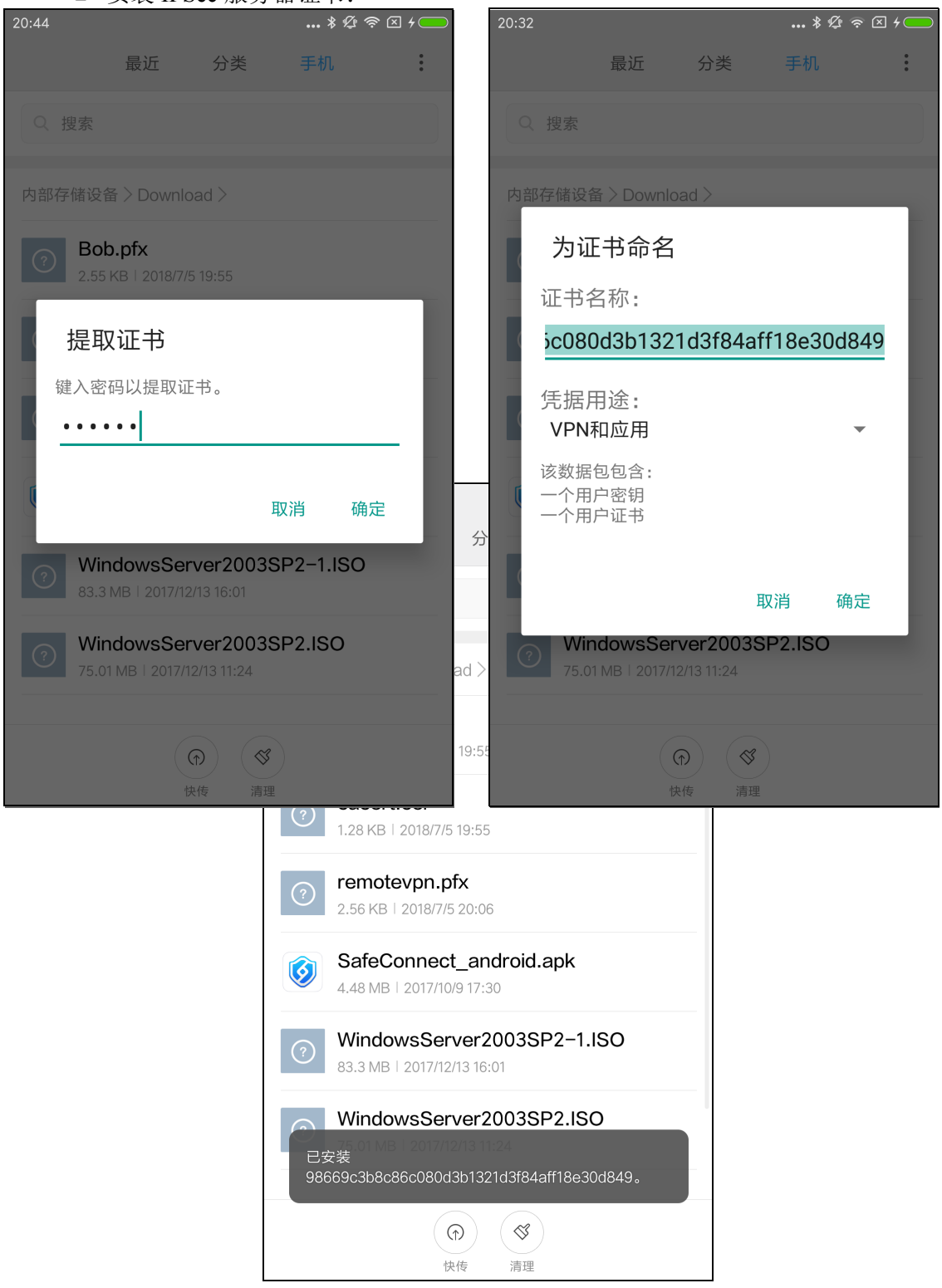
c. 点击证书文件进行安装。

- 安装 CA 证书：

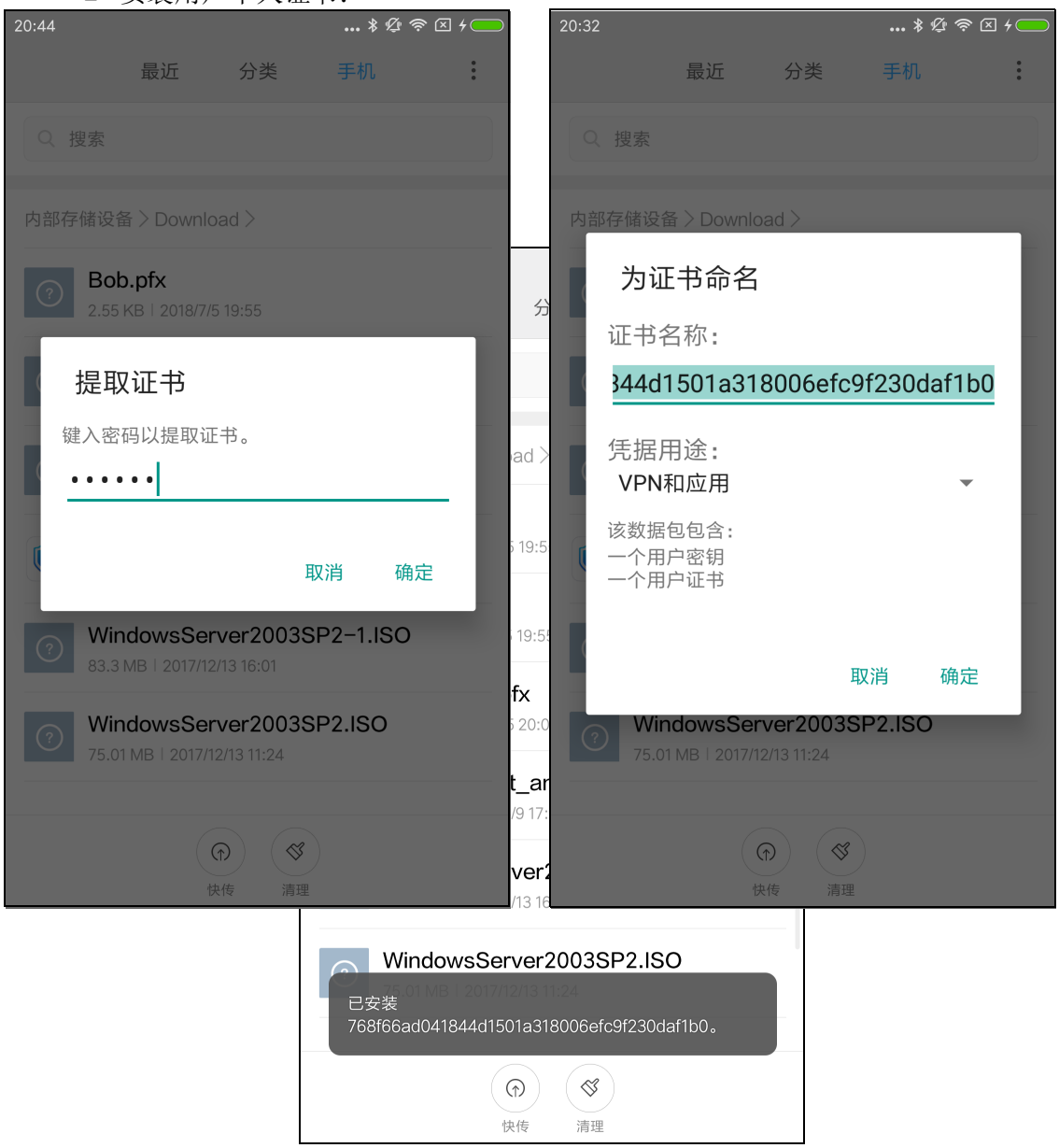

20:33
最近
分类
手机
搜索
内部存储设备 > Download >
为证书命名
证书名称：
ca
凭据用途：
VPN和应用
该数据包包含：
1个CA证书
取消
确定
WindowsServer2003SP2.ISO
75.01 MB | 2017/12/13 11:24
快传
清理


20:33
最近
分类
手机
搜索
内部存储设备 > Download >
Bob.pfx
2.55 KB | 2018/7/5 19:55
cacert.cer
1.28 KB | 2018/7/5 19:55
remotevpn.pfx
2.56 KB | 2018/7/5 20:06
SafeConnect_android.apk
4.48 MB | 2017/10/9 17:30
WindowsServer2003SP2-1.ISO
83.3 MB | 2017/12/13 16:01
WindowsServer2003SP2.ISO
75.01 MB | 2017/12/13 11:24
已安装 ca。
快传
清理

- 安装 IPSec 服务器证书：

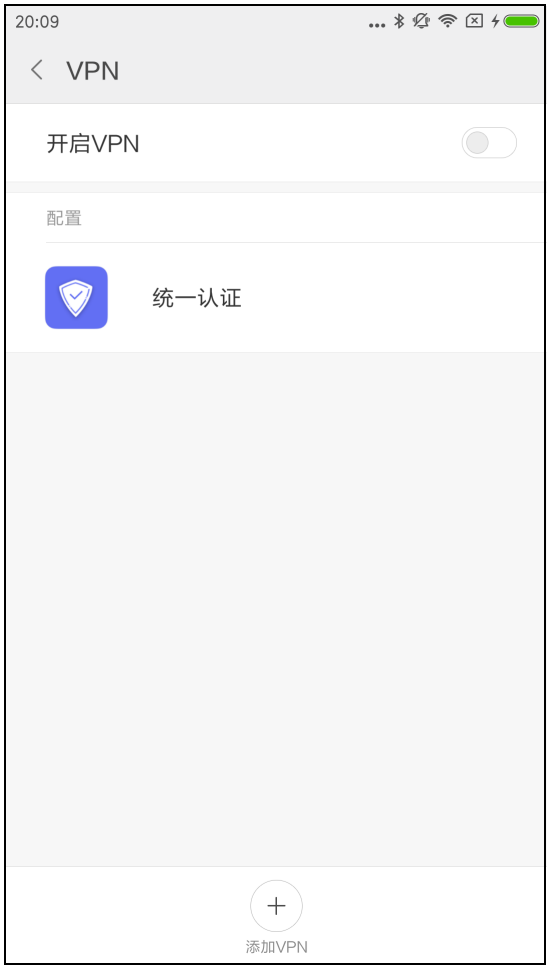


- 安装用户个人证书：


20:44
最近
分类
手机
搜索
内部存储设备 > Download >
Bob.pfx
2.55 KB | 2018/7/5 19:55
提取证书
键入密码以提取证书。
取消
确定
WindowsServer2003SP2-1.ISO
83.3 MB | 2017/12/13 16:01
WindowsServer2003SP2.ISO
75.01 MB | 2017/12/13 11:24
快传
清理
20:32
为证书命名
证书名称：
344d1501a318006efc9f230daf1b0
凭据用途：
VPN和应用
该数据包包含：
一个用户密钥
一个用户证书
取消
确定
已安装
768f66ad041844d1501a318006efc9f230daf1b0。

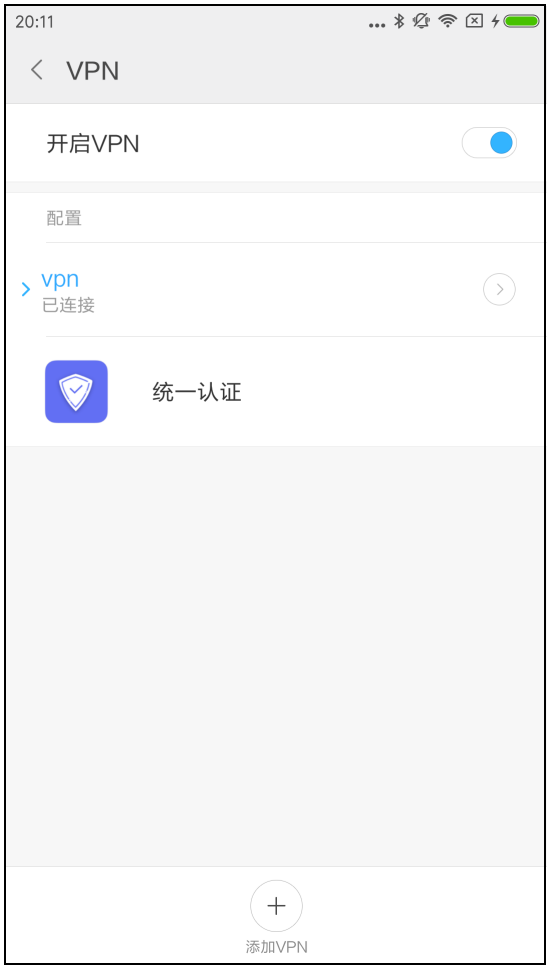
添加和建立 VPN 连接

1. 选择**设置 > VPN**，点击**添加 VPN**，添加 VPN 连接。



提示：如果选择不验证服务器证书，则只需导入用户个人证书。

2. 返回 VPN 连接界面，开启 VPN 连接。



3. 待连接成功后，用户即可访问内网资源。

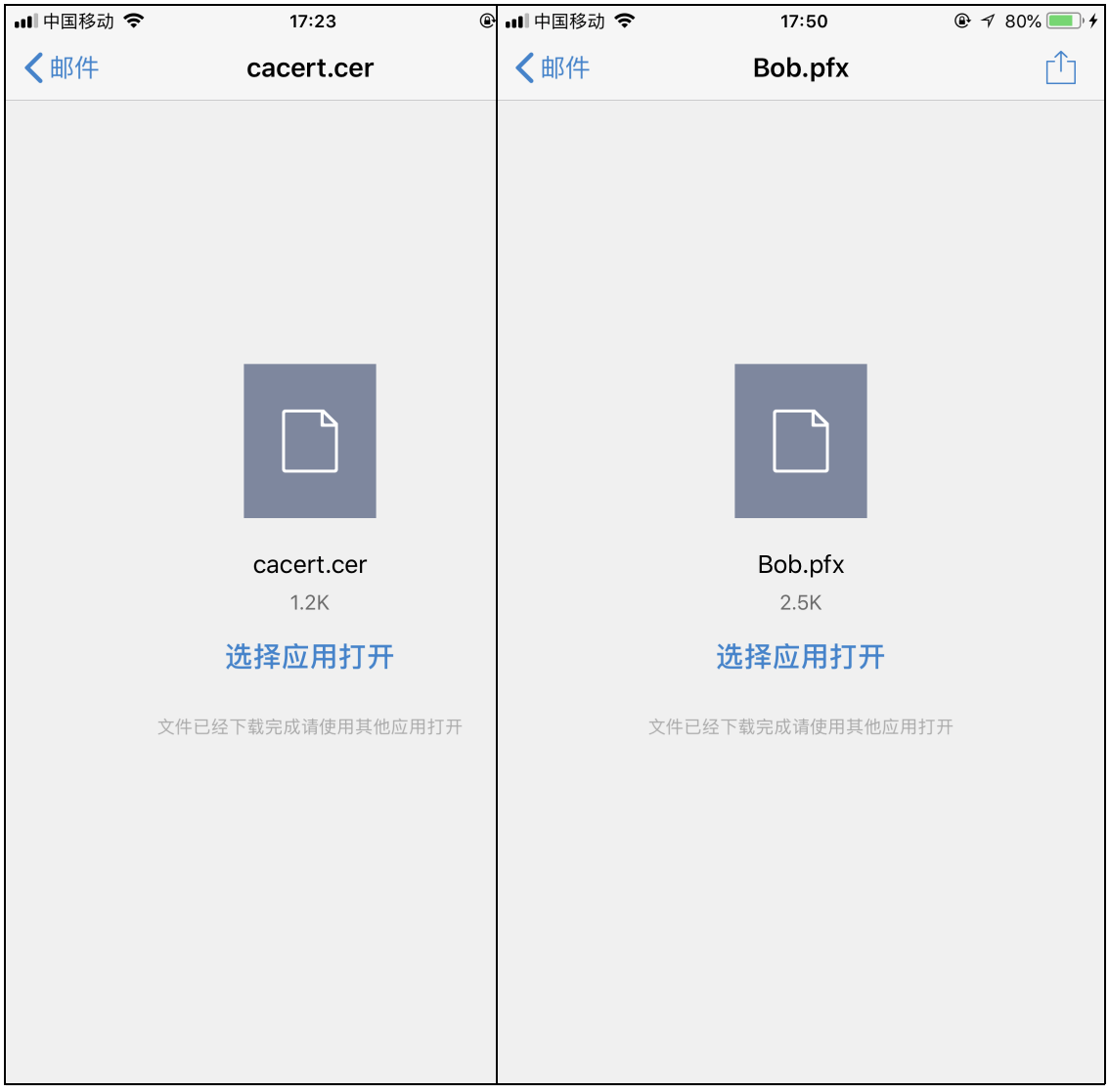
配置 iOS 内置 IPSec VPN 客户端

导入和安装证书

- 如果远程用户使用 IKEv2 类型接入，只需要导入和安装 CA 证书。
- 如果远程用户使用 IPSec （IKEv1）类型接入，则 CA 证书和个人证书都需要安装。

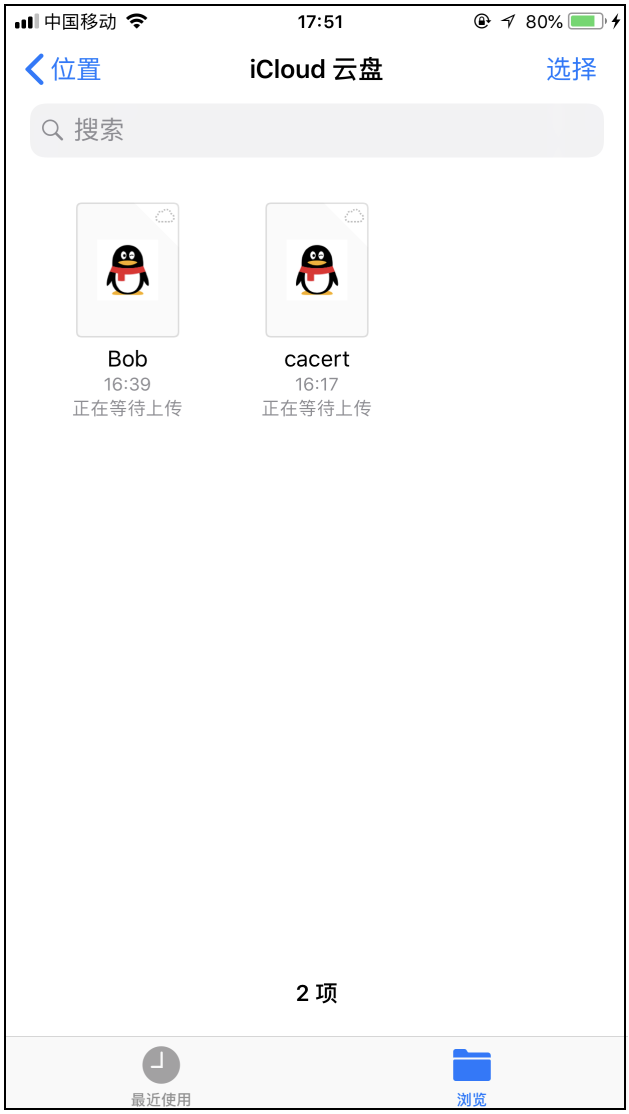
提示：由于 iOS 系统导入证书步骤复杂，本范例以 IKEv1 接入为例，说明客户端配置方法。

1. 从 VPN 网关上下载证书到本地，并通过邮件发送给远程用户。
2. 远程用户通过 iPhone 手机接收邮件，将证书存储到 iCloud 云盘。
   a. 点击证书附件。



b. 之后，依次点击**选择应用打开 > 存储到 “ 文件 ”> iCloud 云盘 > 添加**。

3. 打开 iOS 系统文件，进入 iCloud 云盘目录，点击证书文件，根据提示完成证书安装。



- 安装 CA 证书：


文件
17:51
80%
取消
安装描述文件
安装
CACenter
签名者 CACenter
尚未验证
包含 证书
更多详细信息
文件
17:51
80%
取消
警告
安装
未受管理的根证书
若安装证书“CACenter”，此证书将被添加到 iPhone 上被信任的证书列表中。只有在“证书信任设置”中启用，网站才会信任此证书。
未验证的描述文件
不能验证“CACenter”的真实性。
文件
17:51
80%
已安装描述文件
完成
CACenter
签名者 CACenter
已验证
包含 证书
更多详细信息

- 安装个人证书：


文件 17:52 80%
取消
安装描述文件
安装
身份证书
签名者 未签名
包含 证书
更多详细信息
文件 17:53 80%
取消
警告
安装
未签名的描述文件
此描述文件未签名。
文件 17:53 80%
取消
输入密码
下一步
输入证书“身份证书”的密码
应“身份证书”描述文件要求
1 2
- /
#+=
ABC
文件 17:53 80%
已安装描述文件
完成
身份证书
签名者 未签名
包含 证书
更多详细信息

添加和建立 VPN 连接

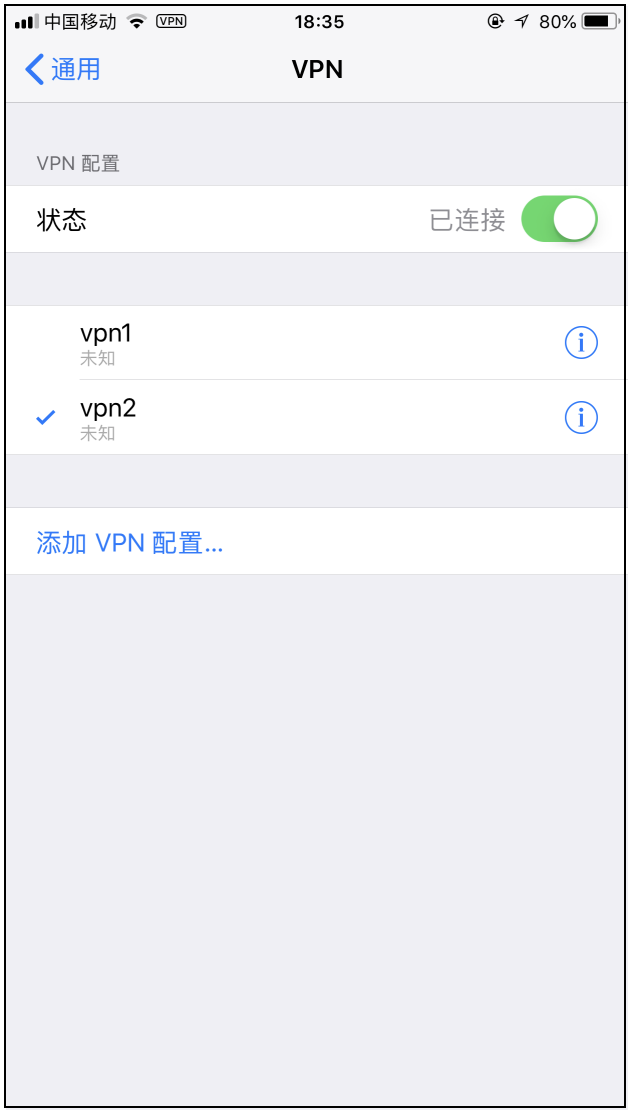
1. 选择**设置 > 通用 > VPN**。
2. 点击**添加 VPN 配置**，添加 VPN 连接，添加 VPN 连接。

- 如果使用 IKEv2，请填写如下信息（**服务器**和**远程 ID** 均填写 VPN 服务器地址）：

- 如果使用 IPsec （即 IKEv1），请填写如下信息：

3. 点击**完成**，完成 VPN 连接的添加。

4. 回到 VPN 连接界面，选择新建的 VPN 连接，滑动**状态**按钮，建立 VPN 连接。

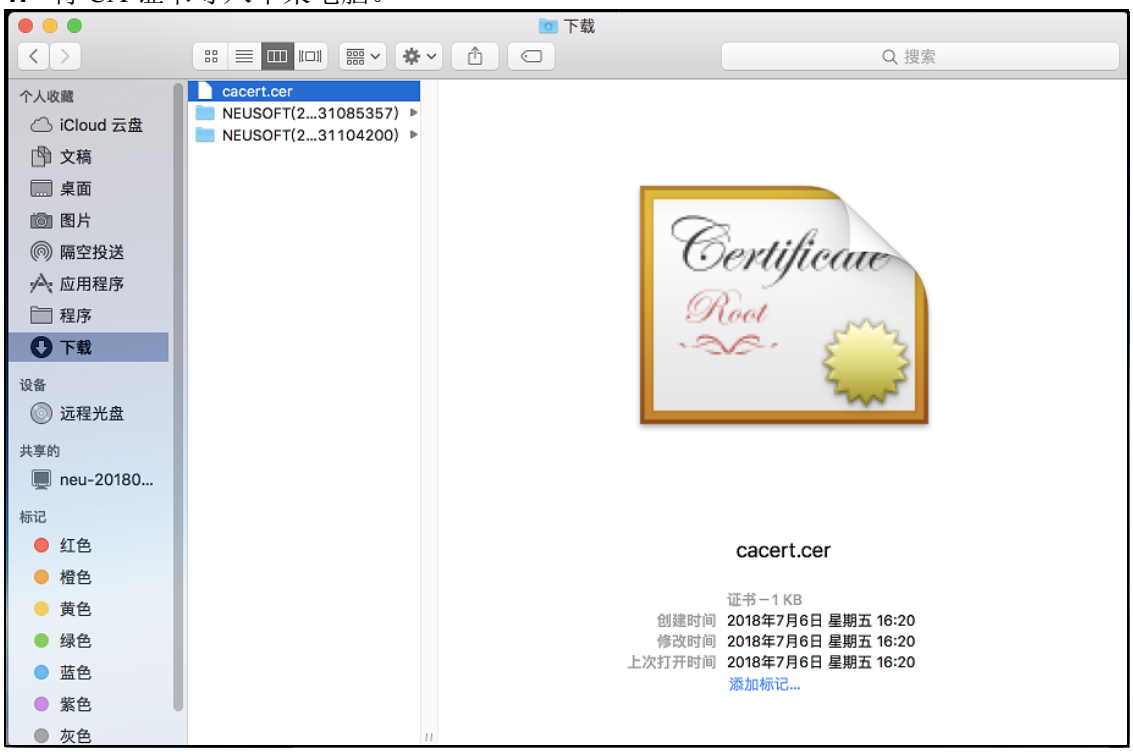


5. 待连接成功后，用户即可访问内网资源。

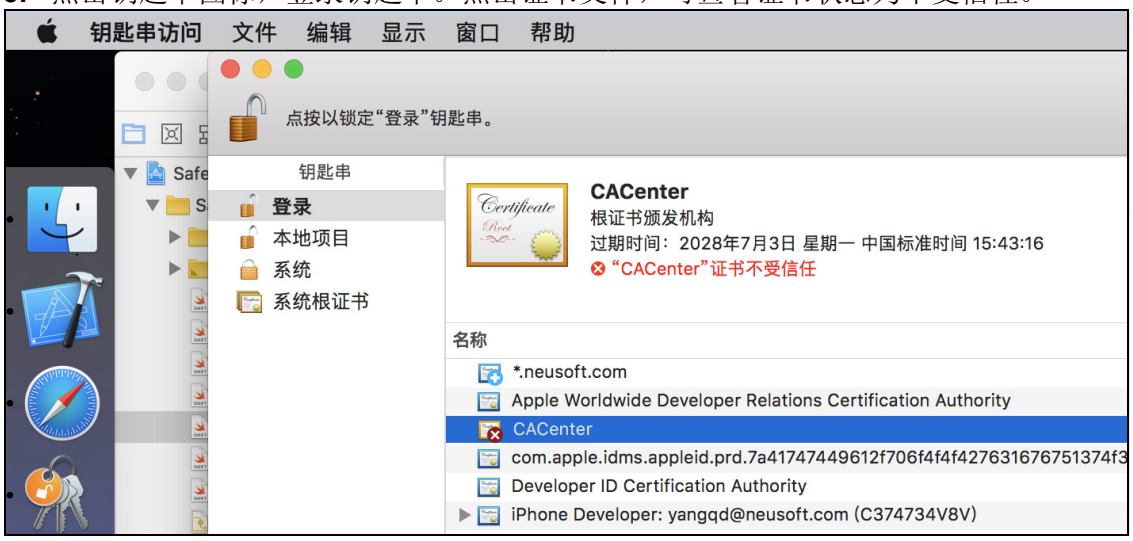
配置 macOS 内置 IPSec VPN 客户端

导入证书

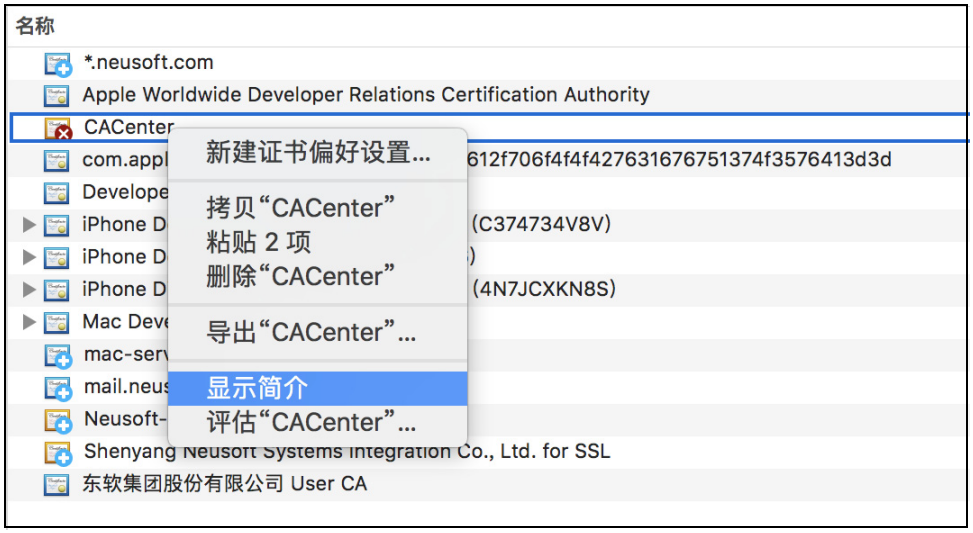
1. 将 CA 证书导入苹果电脑。



2. 双击证书文件，将证书添加进钥匙串。
3. 点击钥匙串图标，登录钥匙串。点击证书文件，可查看证书状态为不受信任。



4. 右键点击证书文件，选择显示简介。



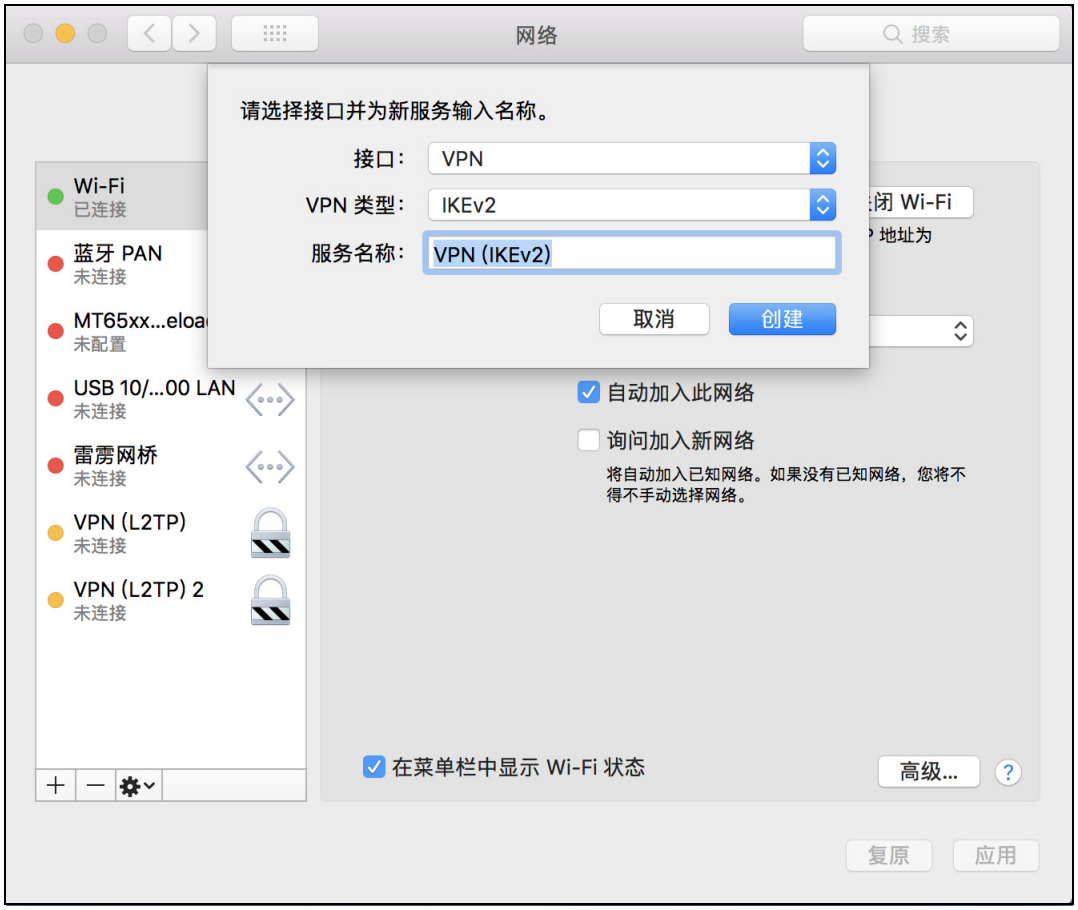
5. 在信任区域的下拉框中选择始终信任。

6. 按确认键。根据提示输入管理员用户名和密码，点击更新设置，授权信任该证书。

7. 查看证书状态，可发现证书变为受信任状态。

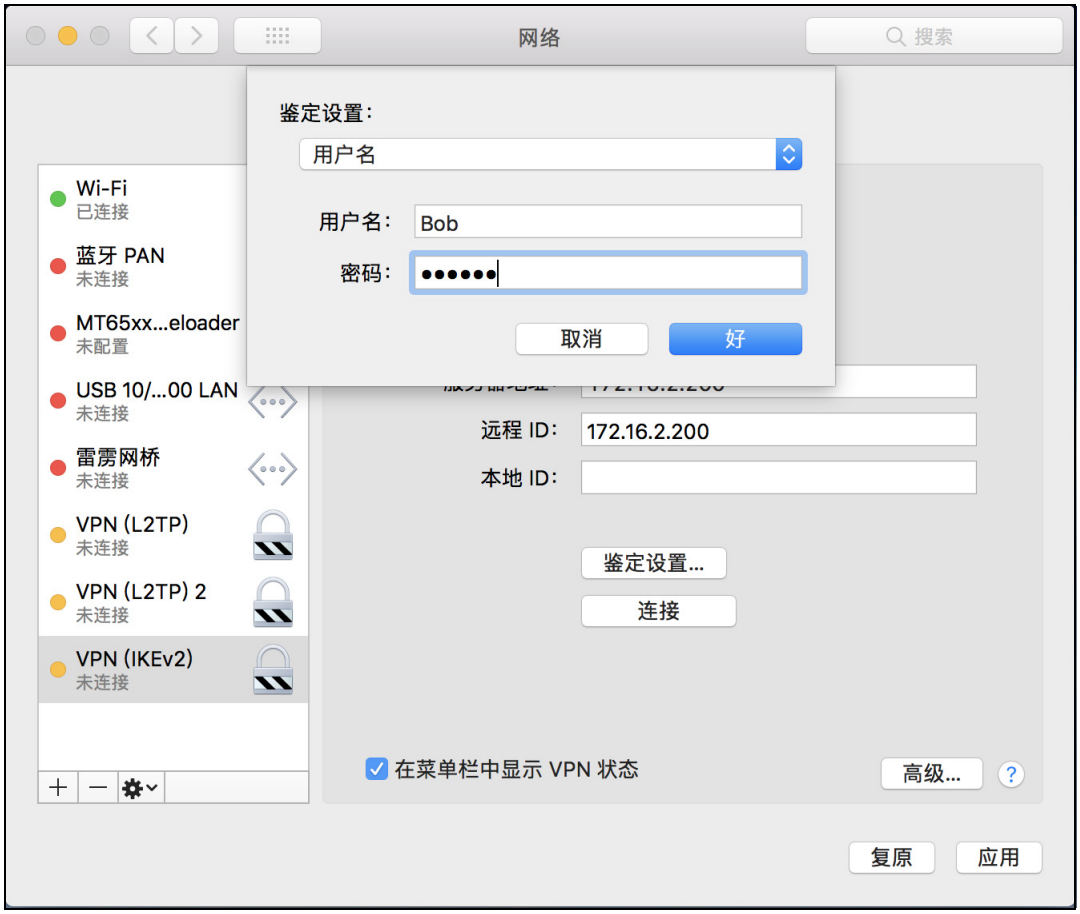
建立 VPN 连接

1. 选择**系统偏好设置 > 网络**，点击加号，创建 VPN 连接 （VPN 类型选择 IKEv2）。



2. 设置 IPSec VPN 服务器地址和远程 ID。

3. 点击**鉴定设置**，设置用户名和密码，点击**好**。



4. 点击**连接**，建立 VPN 连接。

验证结果

1. 通过客户端终端访问远程 IPSec VPN 资源。
2. 选择**监控 > 在线用户 > IPSec VPN 在线用户**，查看远程 IPSec VPN 用户在线信息。

点击右上角的流量开关，可查看在线用户在线时长和收发流量信息。

3. 可选择**网络/策略>访问策略**，点击**配置IPSec VPN访问策略**，查看是否自动生成远程访问 IPSec VPN 访问策略。
4. 如果监控不到在线用户，也查看不到自动生成的访问策略，则选择**日志>调试>IPSec VPN 协商日志**，查看远程访问 IPSec VPN 协商过程，分析连接失败原因。

   建议断开连接后先清空日志，然后重新拨号，查看完整协商过程。

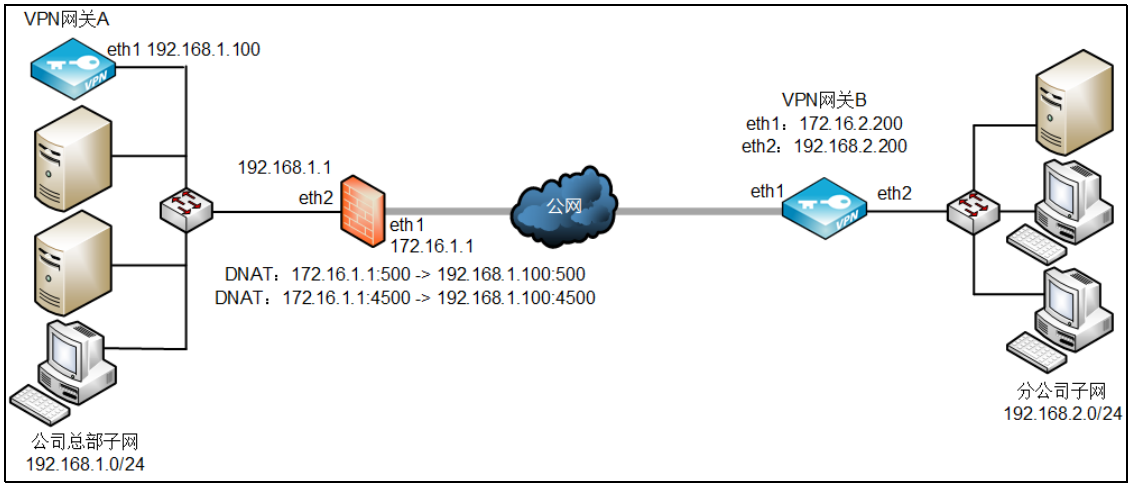
   需要事先在远程访问 IPSec VPN 中开启日志记录功能（选择**基础功能 > IPSec VPN**，点击 RemoteAccess 对应的编辑图标）。

2.6 网关到网关 IPSec VPN

基本需求

某客户网络拓扑如下图所示，总部出口处部署了防火墙，且以单臂模式部署了 VPN 网关，实现与分公司的 VPN 网关互连。分公司在网络出口以网关模式配置了 VPN 网关，实现内部员工上网，并与总部 VPN 网关进行 VPN 互连。同时，要求在公司总部和分公司之间建立一条 VPN 隧道，使公司分部的员工可以访问总部资源。为安全起见，要求隧道两端使用证书认证。

组网拓扑



配置要点

- 配置总部防火墙 DNAT
- 配置总部 VPN 网关 A
- 配置分部 VPN 网关 B
- 验证结果

配置步骤

配置总部防火墙 DNAT

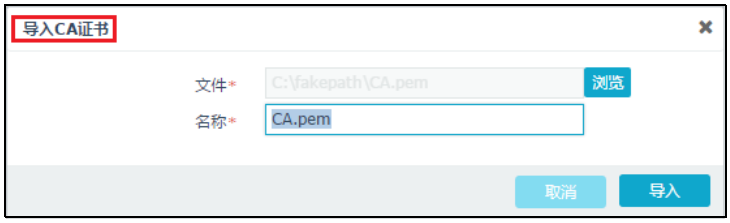
由于 VPN 网关接在内网，需要通过前置防火墙将 IP 映射到公网，与分部 VPN 网关进行隧道协商，所以需要在前置防火墙上做 TCP/UDP 标准端口 500 和 4500 的映射：

- DNAT1：172.16.1.1:500 ->192.168.1.100:500
- DNAT2：172.16.1.1:4500 ->192.168.1.100:4500

由于各个厂家设置方法有所不同，以上配置此处不截图说明。

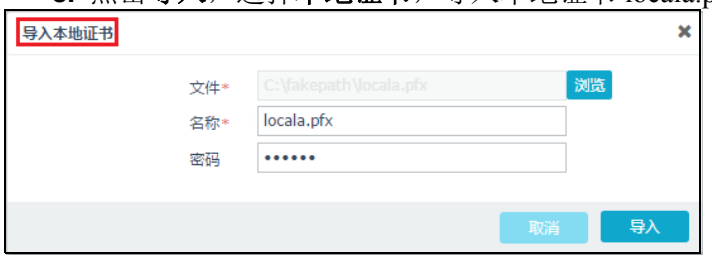
配置总部 VPN 网关 A

1. 导入证书。先导入 CA 证书再导入本地证书，步骤如下：
   a. 选择**系统管理 > 证书**。
   b. 点击**导入**，选择 **CA 证书**，导入 CA 证书。



提示：导入的 CA 证书必须是授权颁发对应本地证书的 CA 机构的 CA 证书。

   c. 点击**导入**，选择**本地证书**，导入本地证书 locala.pfx。



提示：如需自行制作服务器证书，可以选择**系统管理 > 证书**，点击**添加**并点击**本地证书**。请参见 添加 CA 证书和本地证书。

2. 单臂模式部署设备。详细配置过程参见 2.1.1 单臂模式。
   - 配置接口：配置 eth1 的 IP 地址为 192.168.1.100，掩码长度 24。
   - 配置网关：添加缺省路由，出口设置为 eth1，目的地址为 0.0.0.0/0，网关为 192.168.1.1。

3. 创建 IPSec VPN 隧道：
   a. 选择**基础功能 > IPSec VPN**。
   b. 点击**添加**，在**基础配置**页签设置隧道基础配置。

提示：为了适应 VPN 网关之间存在 NAT 设备的情况，这里推荐使用 **ikev2** 版本。基于安全目的，这里推荐使用**证书**认证模式；两端网关的本地证书和对应的 CA 证书需要提前导入。

   c. 点击**本地配置**，设置本端地址、认证类型和本地子网。

本地地址选择本端网关的外网接口 IP，认证类型选择证书主题， ID 为**基础配置**页签所选本地证书的证书主题。

d. 点击**对端配置**，设置对端地址、认证类型和对端子网。

对端的 IP 地址 / 域名请填写对端网关的外网接口 IP。本端和对端的配置信息应该是相对应的。

4. 点击**确定**。

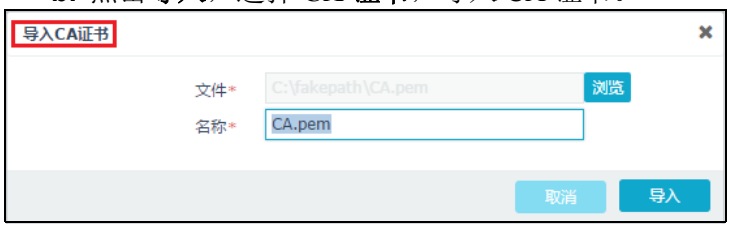
5. 在两端设备上都点击**重启服务**。稍后刷新页面。

配置分部 VPN 网关 B

1. 导入证书。先导入 CA 证书再导入本地证书，步骤如下：

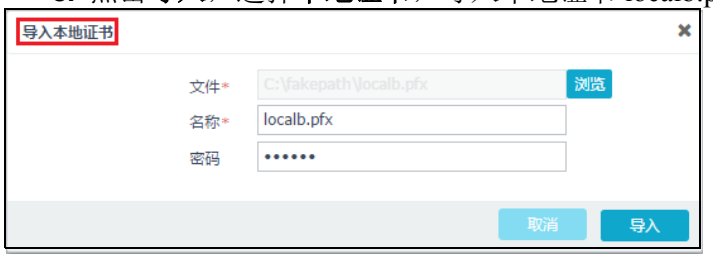
a. 选择**系统管理 > 证书**。

b. 点击**导入**，选择 **CA 证书**，导入 CA 证书。



提示：导入的 CA 证书必须是授权颁发对应本地证书的 CA 机构的 CA 证书。

c. 点击**导入**，选择**本地证书**，导入本地证书 localb.pfx。



提示：如需自行制作服务器证书，可以选择**系统管理 > 证书**，点击**添加**并点击**本地证书**。请参见 添加 CA 证书和本地证书。

2. 网关模式部署设备。详细配置过程参见 2.1.2 网关模式。

- 配置接口：分别配置 eth1 和 eth2 的 IP 地址为 172.16.2.200、192.168.2.200，掩码长度均为 24。
- 配置缺省路由：出口为 eth1，目的地址为 0.0.0.0/0，网关设置为 172.16.2.1。

3. 创建 IPSec VPN 隧道：
   a. 选择**基础功能 > IPSec VPN**。
   b. 点击**添加**，在**基础配置**页签设置隧道基础配置，勾选**主动协商**。

提示：为了适应 VPN 网关之间存在 NAT 设备的情况，这里推荐使用 **ikev2** 版本。基于安全目的，这里推荐使用**证书**认证模式；两端网关的本地证书和对应的 CA 证书需要提前导入。

   c. 点击**本地配置**，设置本端地址、认证类型和本地子网。

本地地址选择本端网关的外网接口 IP，认证类型选择证书主题， ID 为**基础配置**页签所选本地证书的证书主题。

d. 点击**对端配置**，设置对端地址、认证类型和对端子网。

对端的 IP 地址 / 域名请填写对端网关的公网 IP。本端和对端的配置信息应该是相对应的。

4. 点击**确定**。

5. 在两端设备上都点击**重启服务**。稍后刷新页面。

验证结果

1. 当隧道状态变为**已连接**时，说明隧道协商成功。

- 总部 VPN 网关 A：

- 分部 VPN 网关 B：

2. 此时，公司分部的客户端主机应该可以成功访问公司总部的服务资源。

3. 如果隧道状态显示为**未连接**，则可以选择**日志 > 调试 > IPSec VPN 协商日志**，查看隧道协商信息，查找协商失败的原因。

2.7 使用外部 LDAP 认证

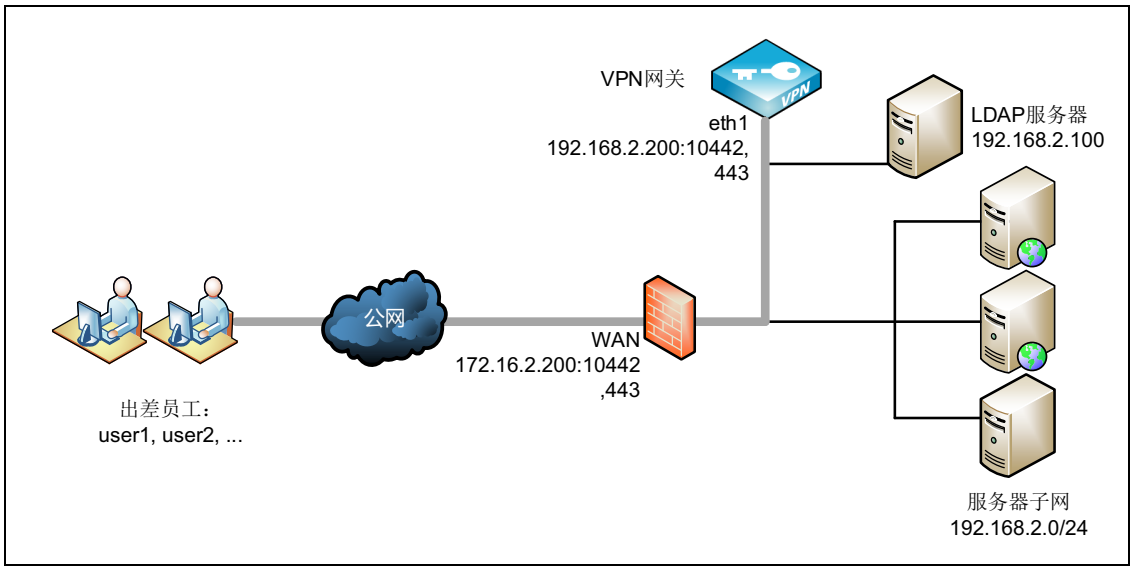
基本需求

某公司部署东软 NetEye VPN 网关后，想配合已有的 LDAP 服务器进行用户认证。LDAP 服务器上配置的安全组结构如下：

dc=com
  dc=example
    ou=people
      cn=admin
      cn=user1
      cn=user2
      cn=user3
      ...
    ou=groups
      cn=depart1 (member=[cn=user1])
      cn=depart2 (member=[cn=user2, cn=user3, ...])

其中， user1 可以访问整个内网资源，其他用户仅允许访问内网 Web 资源。

组网拓扑



配置要点

- 配置 LDAP 外部认证服务器
- 配置 VPN 全局设置
- 配置用户组
- 配置资源和资源组
- 配置 VPN 策略
- 配置 SSL VPN 服务

配置步骤

配置 LDAP 外部认证服务器

1. 选择**系统管理 > 认证服务器**。
2. 点击**新建**，在下拉菜单中选择 **LDAP**，添加 LDAP 认证服务器。

3. 点击**确定**。

配置 VPN 全局设置

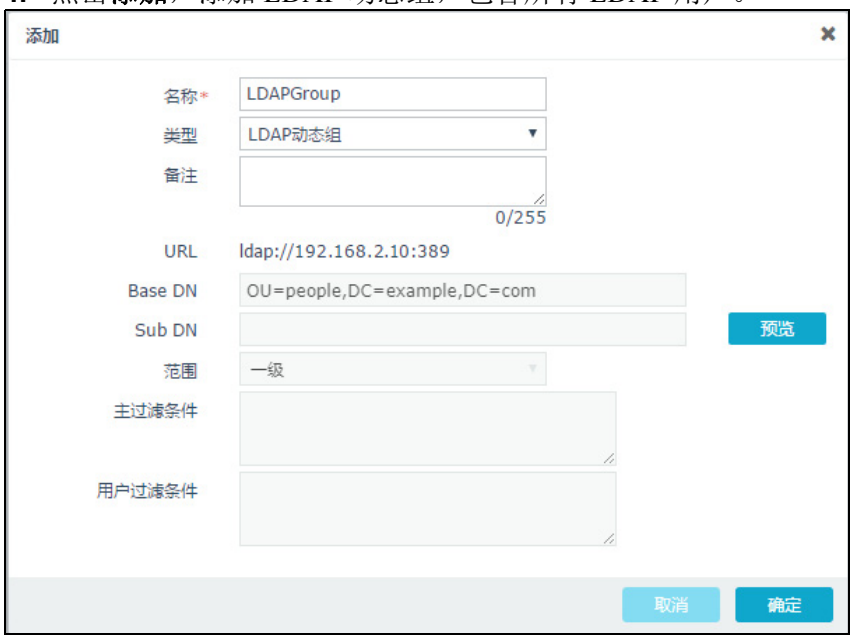
1. 选择**基础功能 > 全局设置**。
2. 认证服务器勾选 Local 和 LDAP，并配置 LDAP 安全组信息。

3. 点击**提交**。

配置用户组

1. 选择**基础功能 > 用户组**。
2. 点击**添加**，添加静态用户组，包含 user1。

3. 点击**确定**。
4. 点击**添加**，添加 LDAP 动态组，包含所有 LDAP 用户。



5. 点击**确定**。

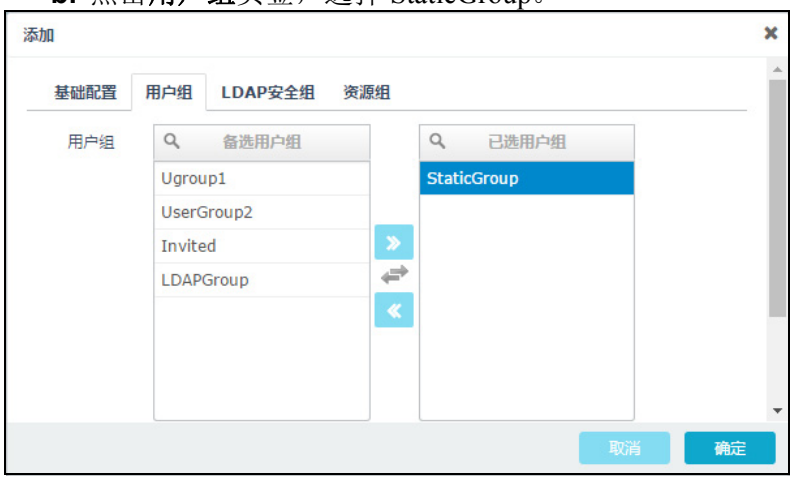
配置资源和资源组

参考 3.2 资源添加内网资源，参考 3.3 资源组添加资源组 HTTP_HTTPS 和 All_resources。HTTP_HTTPS 包含所有 HTTP 和 HTTPS 资源，All_resources 包含所有内网资源。

配置 VPN 策略

1. 选择**基础功能 > VPN 策略**。
2. 点击**添加**，添加一条隧道 SSL VPN 策略，允许 user1 访问所有内网资源。
   a. 在**基础配置**页签进行相关配置。

   b. 点击**用户组**页签，选择 StaticGroup。



也可以点击 **LDAP 安全组**页签，通过选择安全组添加用户。

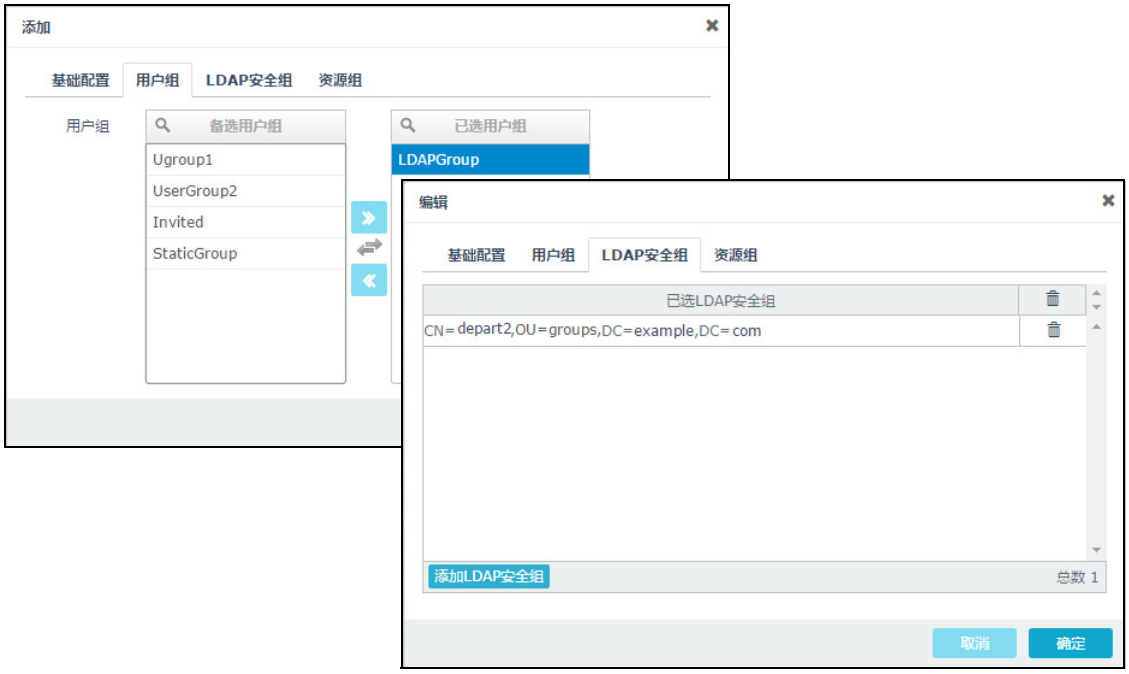
c. 点击**资源组**页签，选择资源组 All_resources。

d. 点击**确定**。

3. 点击**添加**，添加一条 Web SSL VPN 策略，允许其他用户访问 HTTP 和 HTTPS 资源。

a. 在**基础配置**页签进行相关配置。

b. 点击**用户组**页签，选择 LDAPGroup。也可以点击 **LDAP 安全组**页签，通过选择安全组添加用户。



c. 点击**资源组**页签，选择允许用户访问的资源组 HTTP_HTTPS。

d. 点击**确定**。

配置 SSL VPN 服务

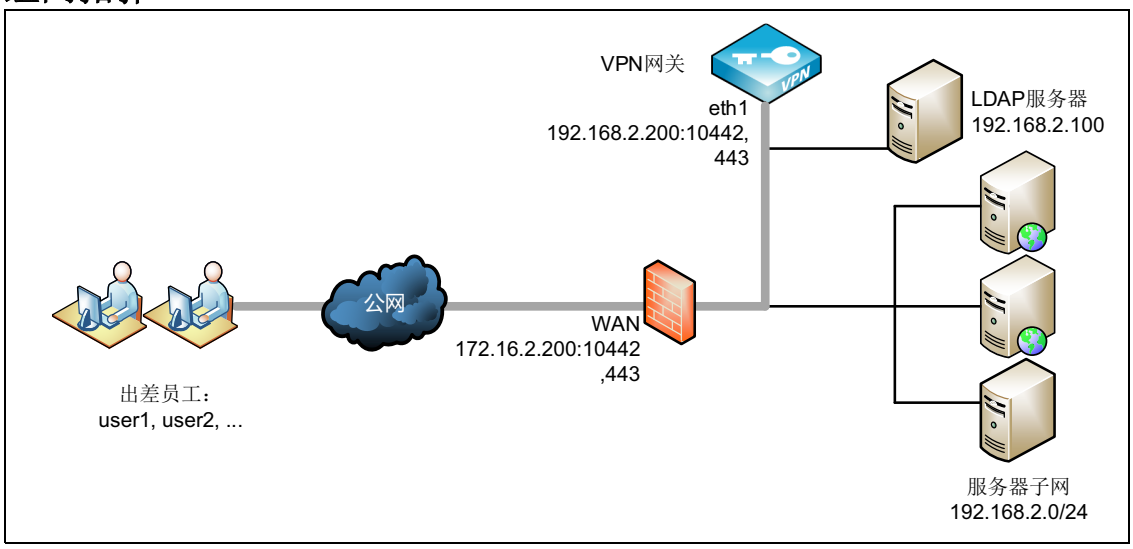
参考 3.8 Web 模式 SSL VPN 和 3.9 隧道模式 SSL VPN 配置 SSL VPN 服务。

2.8 使用本地 RADIUS 认证服务

基本需求

如果公司已有 LDAP 服务器，可将 VPN 网关作为本地 RADIUS 服务器提供认证服务，已有 LDAP 服务器作为用户数据库提供用户信息查询服务。因为本地 RADIUS 服务器支持更多认证协议，认证过程更安全。

组网拓扑



配置要点

- 配置本地 RADIUS 认证服务
- 添加外部认证服务器
- 设置缺省认证服务器
- 配置 SSL VPN 或远程访问 IPSec VPN

配置步骤

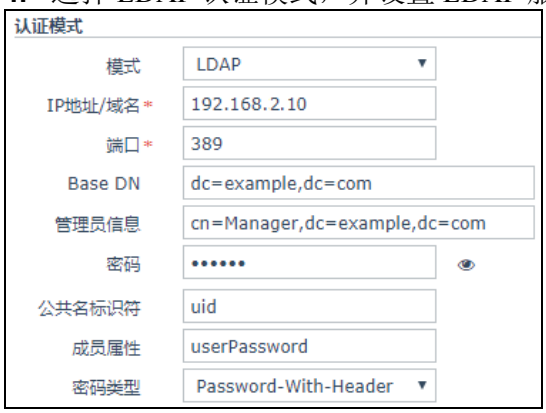
配置本地 RADIUS 认证服务

1. 选择**系统管理 > 本地 RADIUS 认证服务**。
2. 启用本地 RADIUS 认证服务，设置提供服务的 IP 和端口，添加认证服务的子网范围和共享密钥。

IP 地址选择**任意**表示监听所有接口的认证请求。服务子网设置为 127.0.0.1/32 表示该服务仅为本地 VPN 用户提供认证服务。

3. 勾选全部认证协议，保证 VPN 网关与 RADIUS 认证客户端之间的通信安全。

4. 选择 LDAP 认证模式，并设置 LDAP 服务器信息。



提示：请联系 LDAP 服务器管理员获取 LDAP 服务器信息。

5. 点击**提交**。

添加外部认证服务器

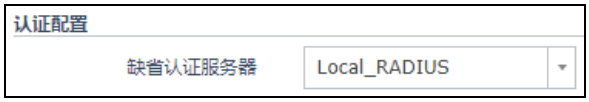
1. 选择**系统管理 > 认证服务器**。
2. 点击**新建**，在下拉菜单中选择 **RADIUS**，添加外部 RADIUS 服务器，IP 地址指向本地 RADIUS 服务器。

> **提示：**IP 地址必须为 127.0.0.1（表示本地服务），密钥必须与本地 RADIUS 认证服务添加的本地服务条目中的密钥保持一致。

3. 点击**确定**。

设置缺省认证服务器

1. 选择**基础功能 > 全局设置**。
2. 认证服务器勾选添加的指向本地 RADIUS 服务器的外部 RADIUS 服务器。



3. 点击**提交**。

配置 SSL VPN 或远程访问 IPSec VPN

具体配置步骤可参考 2.3 Web 模式 SSL VPN， 2.4 隧道模式 SSL VPN 和 2.5 远程访问 IPSec VPN。

2.9 测试用户

基本需求

为了方便管理员排查问题， VPN 网关提供了测试用户的功能，包括测试用户的账号密码是否正确和测试用户是否具有 VPN 资源访问权限。

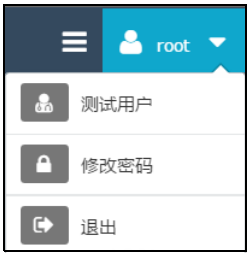
配置要点

- 测试用户账号和密码
- 测试用户资源访问权限

配置步骤

测试用户账号和密码

1. 以 root 或管理员账号登录。
2. 点击界面右上角当前登录用户名右侧的向下箭头，选择快捷菜单**测试用户**。



3. 输入用户名和密码，点击**是**，测试用户账号和密码是否匹配。

4. 如果用户账号和密码匹配，系统将提示“ 操作成功 ”；如果用户账号和密码不匹配或不存在该用户，系统将提示“Authentication failed.”（认证失败）。

测试用户资源访问权限

1. 选择**基础功能 > VPN 策略**。
2. 点击**测试用户匹配**按钮，输入用户名，选择用户类型，点击**搜索**，可查看用户是否具备 VPN 资源访问权限。例如 user1 具备 Web 模式 SSL VPN 资源的访问权限，user6 具备隧道模式 SSL VPN 资源的访问权限，测试结果如下：
   - user1 具备 Web 资源访问权限：

   - user6 具备隧道模式 SSL VPN 资源访问权限，不具备 Web 模式 SSL VPN 资源访问权限：

2.10 邀请用户注册

基本需求

为方便来宾快速接入公司内网，在 VPN 网关上开启邀请用户注册功能，使系统管理员和 SSL VPN 用户都可以邀请来宾注册成为 SSL VPN 用户，使用内网资源。

配置要点

- 创建被邀请人用户组
- 创建资源组
- 创建 VPN 策略
- 配置邮件服务器
- 配置 DNS
- 配置邀请注册功能
- 管理员发送邀请码
- SSL VPN 用户发送邀请码
- 注册成为 SSL VPN 用户

配置步骤

配置 Web 模式 SSL VPN 的步骤请参考 2.3 Web 模式 SSL VPN。

创建被邀请人用户组

创建被邀请人用户组，方便统一管理被邀请用户。

1. 选择**基础功能 > 用户组**。
2. 点击**添加**，输入被邀请人用户组名称，在**类型**下拉框中选择**静态**。

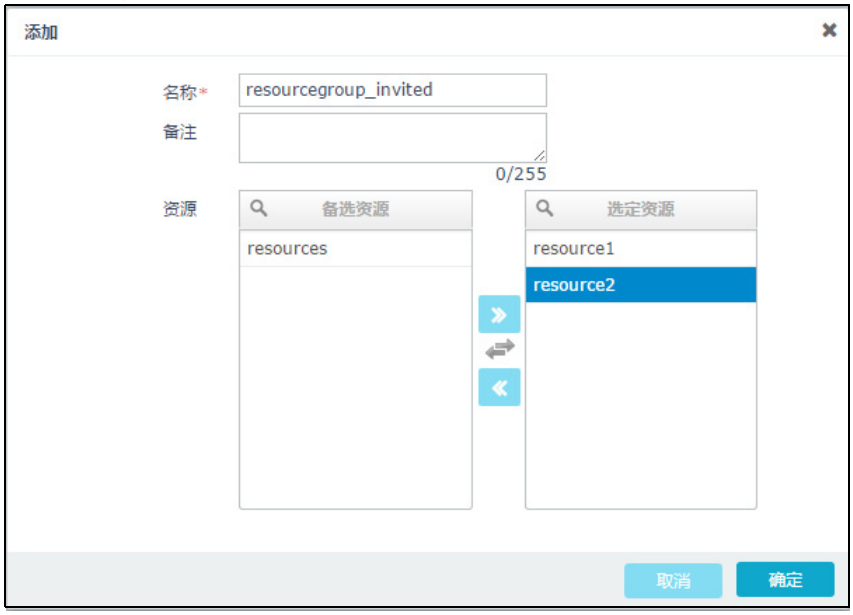
提示：创建被邀请人用户组时，包含用户应该为空。

3. 点击**确定**。

创建资源组

创建资源组，设置允许被邀请用户访问的资源。

1. 选择**基础功能 > 资源组**。
2. 点击**添加**，添加资源组，对资源组命名并选择允许被邀请用户访问的资源。



3. 点击**确定**。

创创建 VPN 策略

添加 VPN 策略，用于控制被邀请用户的访问权限。

1. 选择**基础功能 > VPN 策略**。
2. 点击**添加**，在**基础配置**页签进行相关配置。

3. 点击**用户组**页签，选择已创建的被邀请人用户组。

4. 点击**资源组**页签，选择允许被邀请用户访问的资源组。

5. 点击**确定**。

配置邮件服务器

配置邮件服务器，使系统可以对外发送包含验证码或邀请码的邮件。

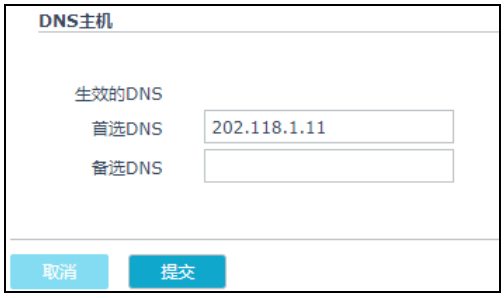
1. 选择**系统管理 > 邮件服务器**。
2. 配置邮件服务器和发件人信息。

3. 点击**提交**。

配置 DNS

配置 DNS 服务器地址，使系统可以解析用于发送邀请码 / 验证码邮件的邮件服务器的域名。

1. 选择**网络 / 策略 > DNS**。
2. 设置首选 DNS 服务器地址。



3. 点击**提交**。

配置邀请注册功能

1. 选择**基础功能 > Web 模式 SSL VPN**。
2. 点击**配置邀请码**按钮，配置邀请码相关选项。
   a. 启用邀请功能，设置可邀请用户数以及默认用户组，点击**提交**。
   b. 在**邀请码列表**中点击**创建**，创建邀请码。

管理员发送邀请码

1. 选择**基础功能 > Web 模式 SSL VPN**。
2. 点击**配置邀请码**按钮，进入邀请码配置页面。
3. 点击**电子邮件**列的邮件图标，输入被邀请人用于接收邀请码的邮件地址，然后点击**确定**。

SSL VPN 用户发送邀请码

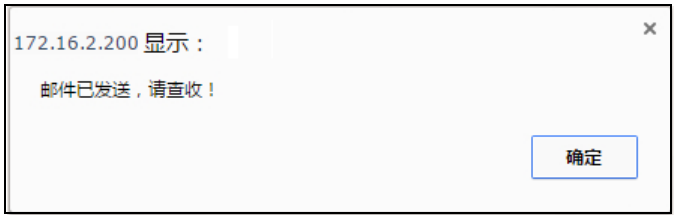
1. SSL VPN 用户可在浏览器中输入 **https://portal-IP/domain_name:port** （如 https://172.16.2.200:443），登录 SSL VPN Portal。
2. 点击**邀请注册**按钮，输入被邀请人邮件地址，邀请他人注册。

注册成为 SSL VPN 用户

被邀请人收到邀请码后，可在 Portal 登录页面点击**注册用户**按钮完成注册。

1. 在 Portal 登录页面点击**注册用户**。

2. 输入注册使用的邮箱地址，点击**获取验证码**。



3. 在新出现的文本框中输入邮箱验证码、新注册用户的账号和密码，以及之前收到的邀请码，点击**注册**，完成用户注册的操作。

4. 完成注册后，即可使用新注册的用户名和密码访问 SSL VPN 资源。

2.11 找回密码

基本需求

允许 SSL VPN 用户在忘记密码的情况下重置密码。

配置要点

- 配置邮件服务器
- 找回密码

配置步骤

配置 Web 模式 SSL VPN 的步骤请参考 2.3 Web 模式 SSL VPN。以下步骤默认已建立 Web 模式 SSL VPN 隧道。

配置邮件服务器

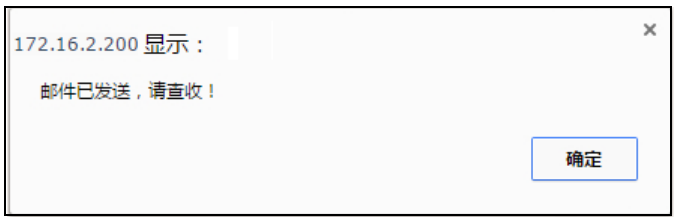
1. 选择**系统管理 > 邮件服务器**。
2. 设置邮件服务器和发件人信息。

3. 点击**提交**。
4. 点击**测试邮件服务器配置**，确保已连通邮件服务器。

找回密码

1. 登录 Portal 页面，点击**忘记密码**。

2. 输入找回密码使用的邮箱账号，点击**获取验证码**。



3. 点击**确定**，在新出现的文本框中输入邮箱验证码和新密码，点击**修改**，完成重置密码的操作。

2.12 单点登录

基本需求

某公司允许员工通过 Web 模式 SSL VPN 访问公司多种 Web 系统，这些 Web 系统均使用统一的认证服务器进行认证。

为了方便用户使用，管理员可配置单点登录功能。启用单点登录后，用户只需登录 Portal 时输入一次用户名和密码，即可访问资源列表中的所有资源。

对于个别需要使用独立账号的 Web 系统（如 EHR 系统），管理员可以使用资源系统独立账号，用户登录 Portal 后，可自行为目标资源设置独立的从属用户名和密码。

配置要点

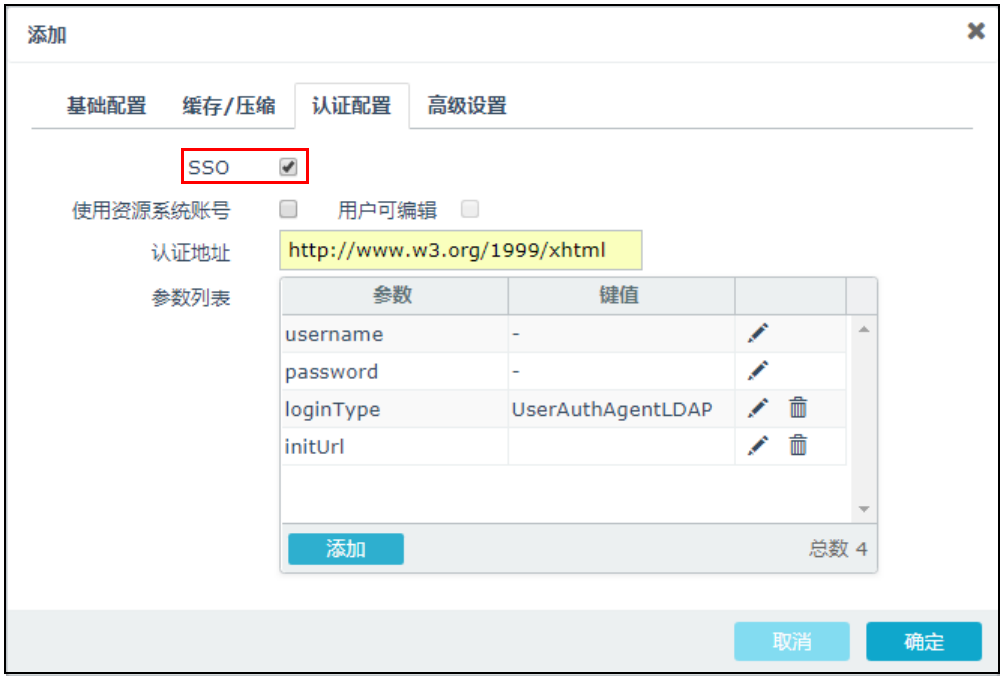
- 为资源开启单点登录
- 允许例外资源使用独立账号
- 用户登录

配置步骤

为资源开启单点登录

1. 选择**基础功能 > 资源**。
2. 点击要启用单点登录的 HTTP 或 HTTPS 资源对应的 图标，打开编辑窗口。
3. 在**基础配置**页面勾选**自动登录**。

4. 在**认证配置**页面启用 **SSO**，并配置相关参数信息。



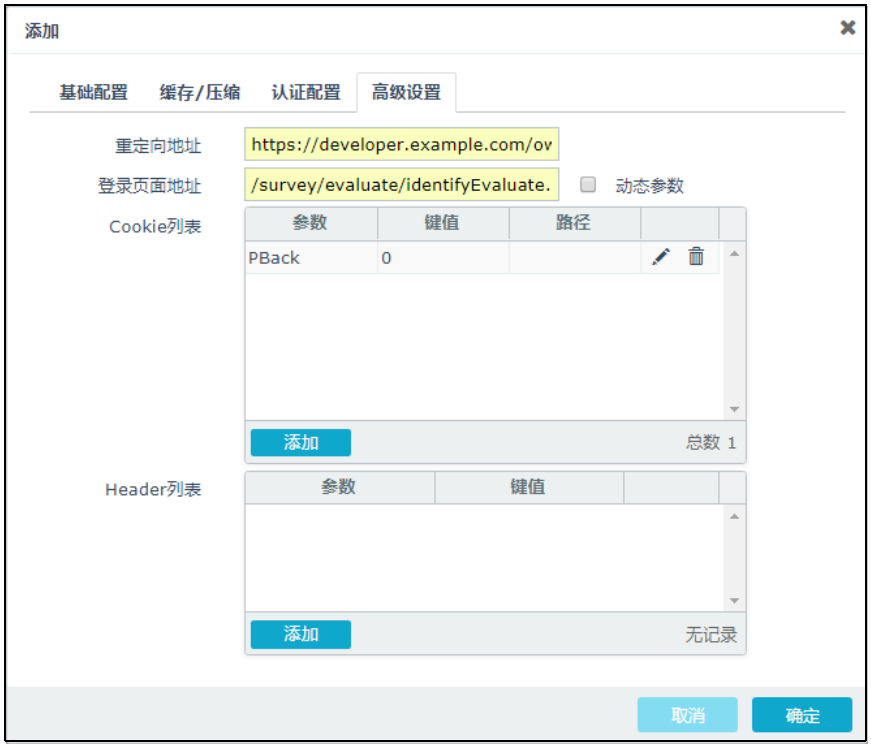
a. 认证地址是用户提交用户名、密码时，携带用户名及密码等认证信息的 URL 地址。必须填写正确的 URL 地址，才能认证通过。

b. 认证过程中至少要提供用户名和密码信息，所以用户名和密码参数也必须填写。其他参数根据网站实现填写。

c. 有些站点需要特定的 Header 字段才能完成登录，请根据需要填写所需字段。

d. 打开系统登录页面和浏览器开发者工具，根据网站实现填写相关参数信息，如：

5. 根据需要在**高级设置**页面配置相关地址及参数。



登录页面地址是用户输入用户名和密码的页面地址。

重定向地址是用户登录成功后重定向到的资源访问地址。

6. 点击**确定**。

提示：由于每个网站实现方式不同，所需参数信息也各不相同。如有需要，建议联系东软网络安全服务工程师协助您完成单点登录配置。

允许例外资源使用独立账号

1. 选择**基础功能 > 资源**。
2. 点击要使用独立账号的 HTTP 或 HTTPS 资源对应的 图标，打开编辑窗口。
3. 在**基础配置**页面勾选**自动登录**。
4. 在**认证配置**页面启用**使用资源系统账号**，并配置相关参数信息。

5. 在**高级设置**页面配置**登录页面地址**及相关参数信息。
6. 点击**确定**。
7. 点击**提交**。

用户登录

以 SSL VPN 用户 test 为例：

1. 在浏览器中输入 SSL VPN Portal 地址（如 https://172.16.2.200:443），进入登录页面。

2. 输入用户名和密码，点击**登录**。

3. 点击**资源列表**中的资源名称访问资源。
   - 当资源名称后面带有图标时，可直接进入资源访问页面。
   - 当资源名称后面带有图标时，可以设置该资源的独立账号信息才能访问资源。

2.13 智能递推

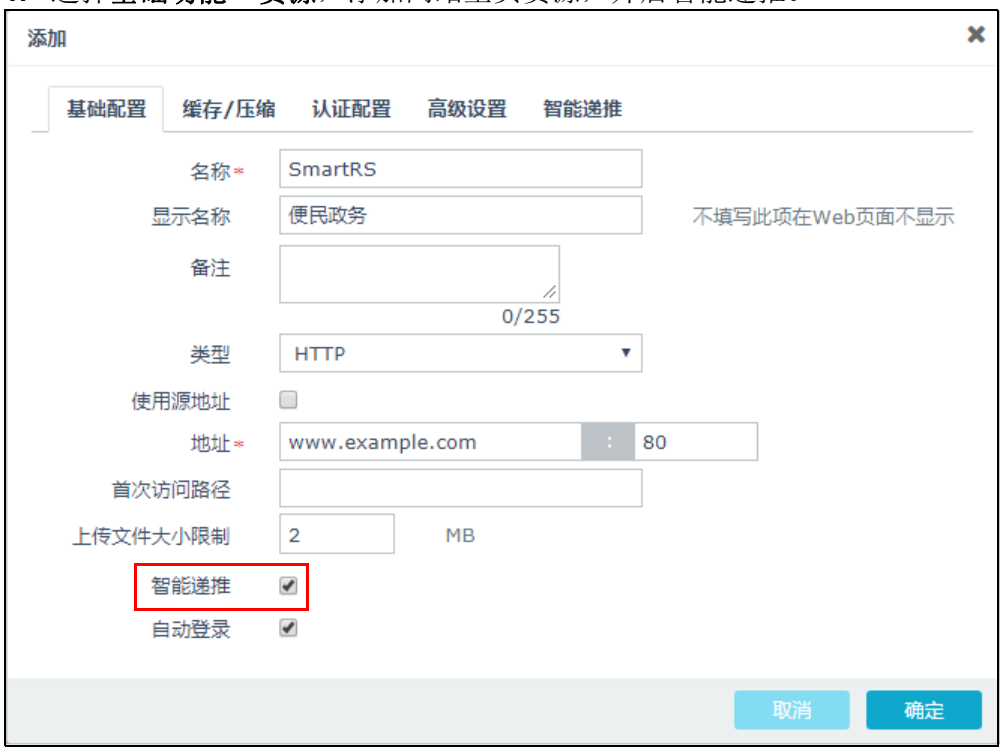
某政务网站包含大量下级机关或合作机构的网站链接。对于此类嵌套链接，逐一添加 VPN 资源不但工作量大，而且很容易漏填。此时可以开启 VPN 网关的智能递推服务，只需要添加网站主页资源和递推的 URL 范围即可，而无需逐一添加嵌套的链接资源。

配置要点

- 添加网站主页资源
- 启用智能递推，设置递推 URL 范围，配置递推网页优化策略
- 配置 VPN 策略，授权用户访问

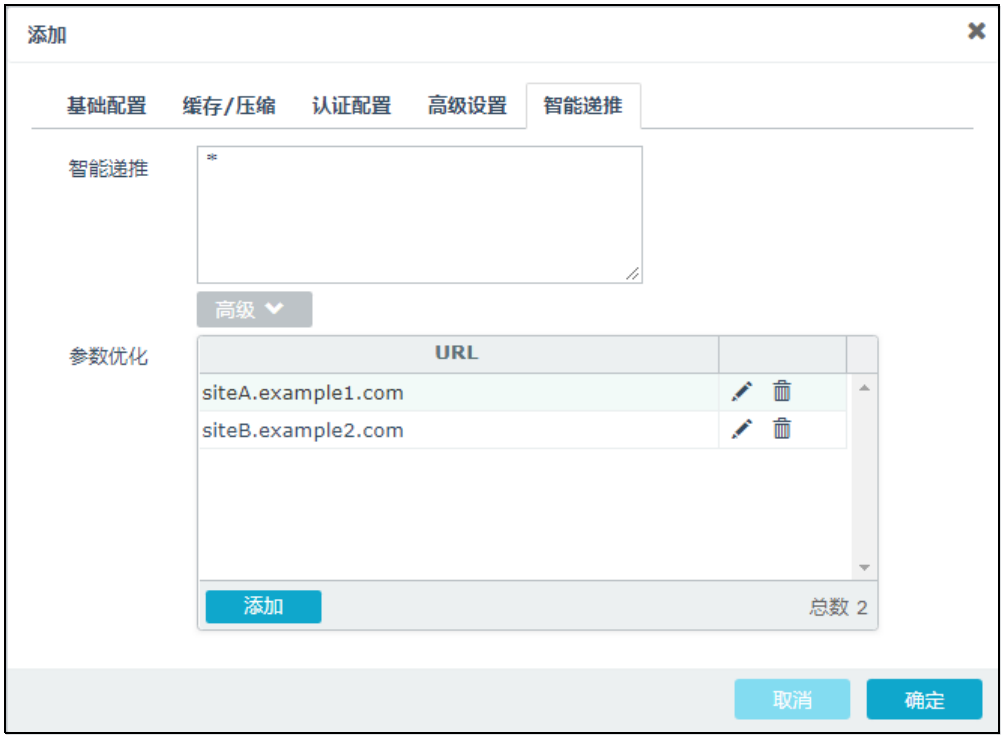
配置步骤

1. 选择**基础功能 > 资源**，添加网站主页资源，开启智能递推。

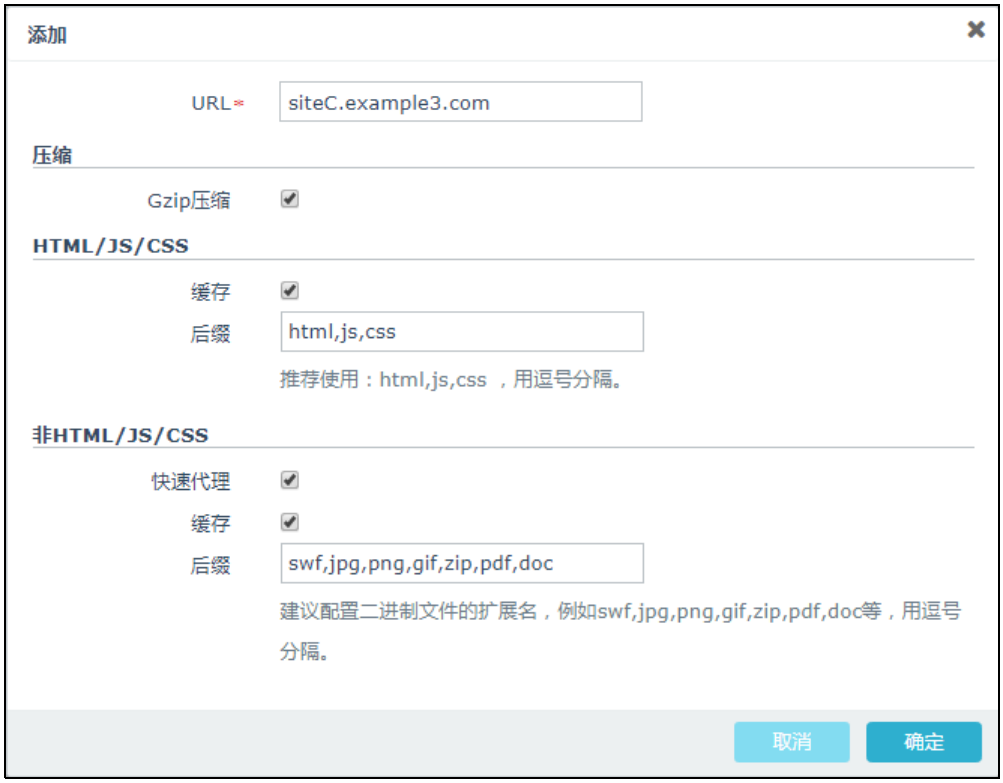


2. 在**认证配置**页面勾选 SSO，允许用户多点登录。

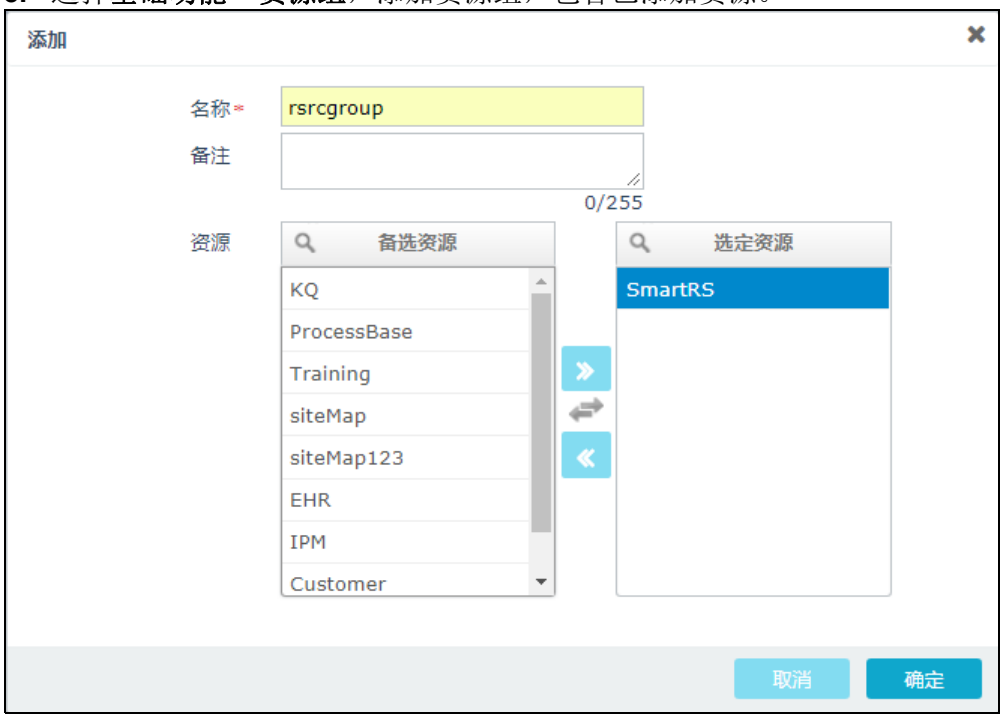
3. 打开**智能递推**页面，配置智能递推范围，添加网页访问优化策略。



点击**添加**，可添加更多需要优化的网页 URL 及优化策略。



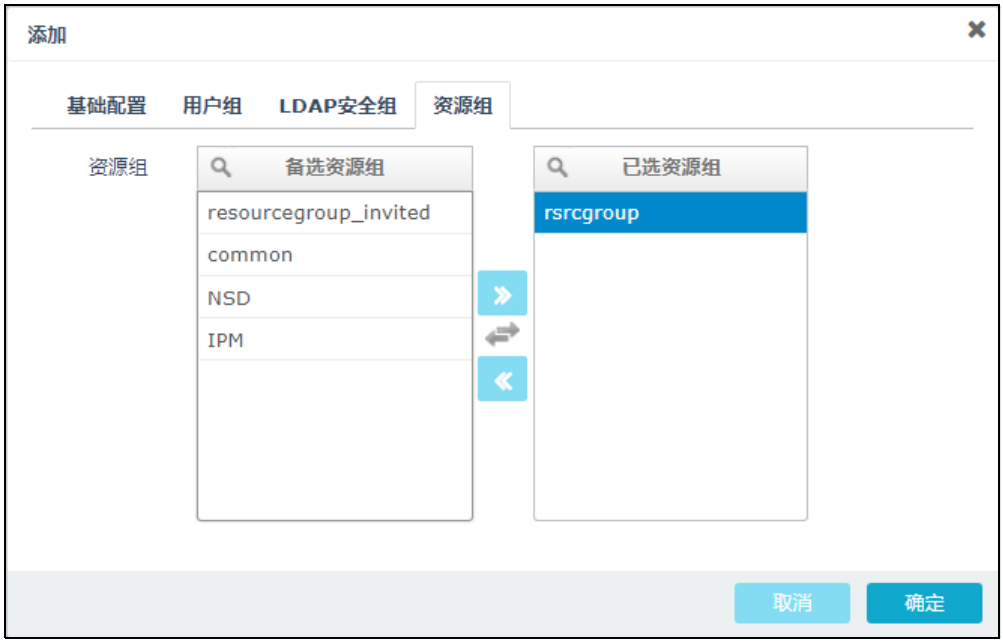
4. 点击**确定**。
5. 选择**基础功能 > 资源组**，添加资源组，包含已添加资源。



6. 选择**基础功能 > VPN 策略**，添加 VPN 访问策略，授权指定用户访问已添加资源。
   a. 添加策略，指定 VPN 服务类型。

   b. 指定授权用户。

c. 指定允许访问的资源组。



d. 点击**确定**。

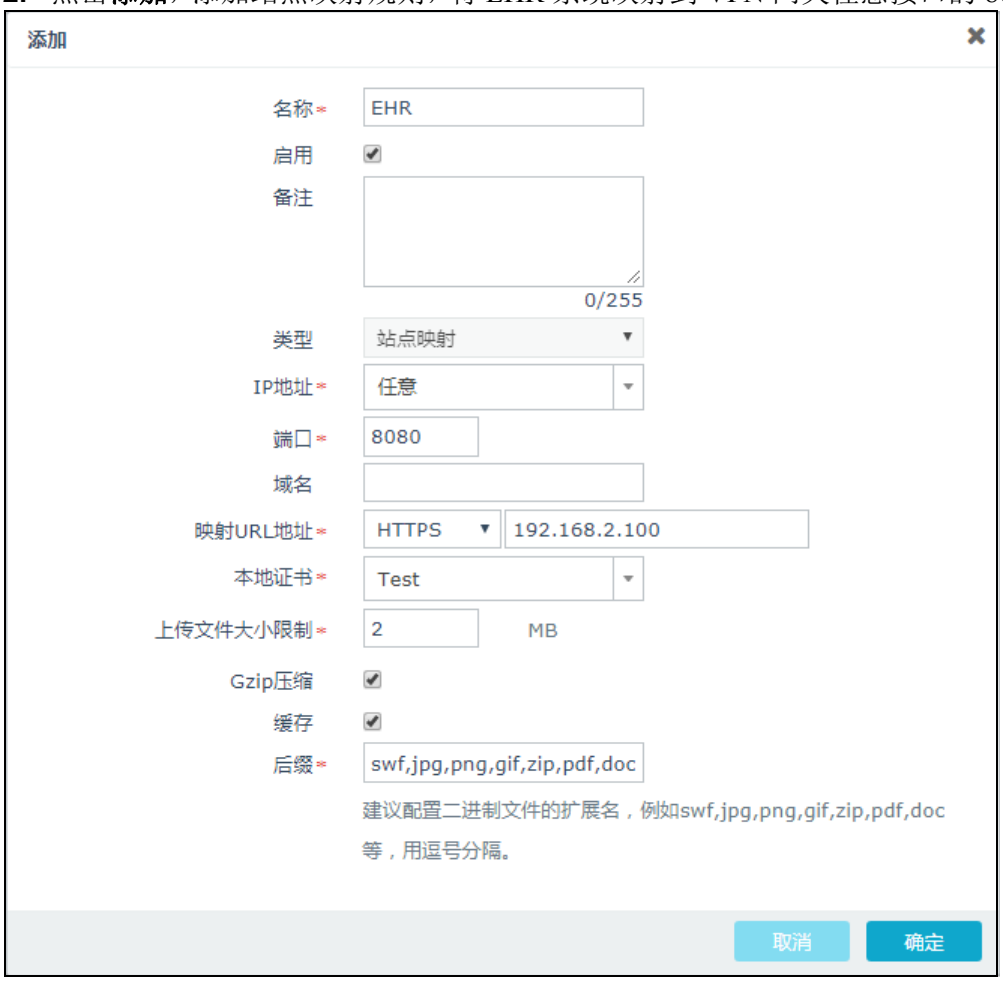
7. SSL VPN 用户可通过 Portal 方式或 SSL VPN 客户端访问该网站主页及嵌套的链接。

2.14 站点映射

某企业 EHR 系统 （192.168.2.100）逻辑复杂，并且使用了大量的 Applet 、 ActiveX 控件。为了部署方便，可以通过配置站点映射，在 VPN 网关上新开端口，直接映射到 Web 应用。这样，用户就可以通过访问 VPN 网关的映射地址和端口来访问 EHR 系统。

配置步骤

1. 选择**基础功能 > Web 模式 SSL VPN > 站点映射**。
2. 点击**添加**，添加站点映射规则，将 EHR 系统映射到 VPN 网关任意接口的 8080 端口。

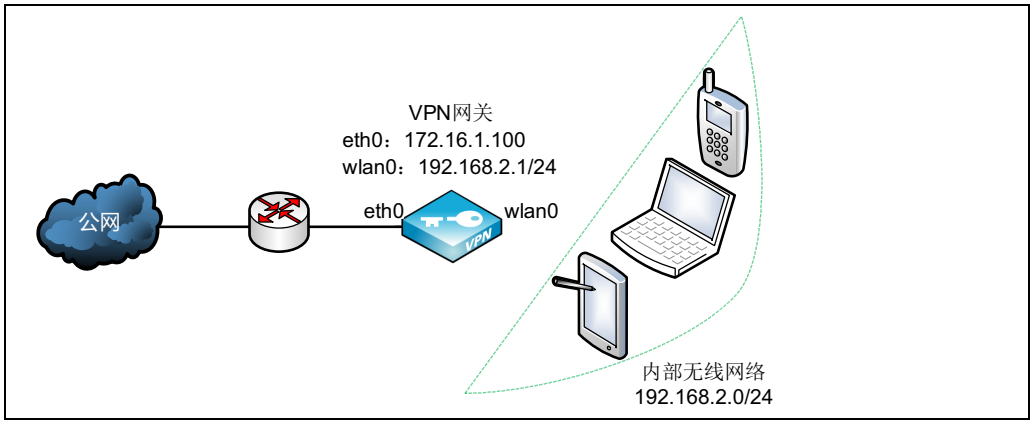


3. 点击**确定**。
4. 内网 SSL VPN 用户在浏览器中输入 https://VPN 网关地址（IP/ 域名）:8080，即可直接访问内网 EHR 系统。

2.15 WiFi 接入

为了方便在会议室等小型办公场所临时办公的员工能够方便地访问公网，可以配置 VPN 网关的无线接入功能。此时， VPN 网关相当于一个家用路由器。

组网拓扑



配置要点

- 配置 WLAN 接口
- 配置 DHCP 服务器
- 配置 WiFi 服务
- 配置源地址转换规则
- 配置访问策略
- 使用移动终端接入
- 监控无线客户端

配置步骤

配置 WLAN 接口

1. 选择**网络 / 策略 > 接口 > 配置**，可以看到接口列表中有个缺省的 WLAN 接口 wlan0。

2. 点击 wlan0 对应的 图标，配置静态 IP 地址。

3. 点击**确定**。

配置 DHCP 服务器

1. 选择**网络 / 策略 > DHCP 服务器**。
2. 在**配置**页面点击**添加**，添加 DHCP 服务器。

无线服务接口选择 wlan0，网关设置为 wlan0 接口的 IP 地址。

系统将根据 wlan0 接口的 IP 地址自动配置无线子网地址和动态地址池，无线子网默认为 wlan0 接口所在子网，动态地址池默认为所在无线子网 100-200 之间的地址。

如果要为无线客户端推送 DNS 服务器地址，请选择**网络 / 策略 > DNS** 查看当前生效的 DNS 服务器。

3. 点击**确定**。
4. 点击**重启 DHCP 服务**。

配置 WiFi 服务

1. 选择**网络 / 策略 > WiFi > 配置**。
2. 开启 WiFi 功能并配置相关信息，为内网无线客户端提供无线接入服务。

提示：如果开启广播，移动终端将能够自动搜索到该无线服务。

3. 点击**提交**。

配置源地址转换规则

1. 选择**网络 / 策略 > 地址转换**。
2. 在**源地址转换**页签点击**添加**，添加一条源地址转换规则，将无线内网地址转换到出口接口的 IP 地址，使得内网的无线客户端可以访问外网。

3. 点击**确定**。

配置访问策略

1. 选择**网络 / 策略 > 访问策略**。
2. 点击**添加**，添加一条访问策略，允许内网无线客户端访问外网。

3. 点击**确定**。

使用移动终端接入

使用移动终端接入无线网络 “VPN” （密码同上面 WiFi 服务中配置的密码）。

- 如果 WiFi 服务开启了广播，用户使用终端搜索到 VPN 无线服务后，输入密码即可接入无线网络。
- 如果 WiFi 服务未开启广播 （例如为安全起见隐藏该无线服务），用户需要手动创建一个无线服务，参数信息同 VPN 网关上的 WiFi 服务配置保持一致。

监控无线客户端

1. 选择**网络 / 策略 > WiFi > 监控**。
2. 查看接入的无线客户端信息。

提示：也可以将 wlan0 划入一个 Bridge 接口，将该 Bridge 作为 DHCP 服务器接口为内网无线客户端动态分配 IP 地址，配置访问策略时入口接口选择该 Bridge 接口。

A 常见问题

本章介绍以下内容：

通用问题排查步骤

1. 确认升级包已按如下顺序安装：

   nevpn_4922_4949.tgz

   nevpn_4949_5064.tgz

   nevpn_5064_5306.tgz

   nevpn_5306_5832.tgz

   nevpn_5832_5932.tgz

   nevpn_5932_6198.tgz

   nevpn_6198_6473.tgz

   nevpn_6473_6973.tgz

   nevpn_6973_7507.tgz

   nevpn_7507_8257.tgz

   或已安装如下镜像文件：

   NVPN_3.0_BUILD_8559.iso

2. 升级后清空缓存或重启浏览器登录。
3. 确认已上载有效许可。
4. 确认系统时间正确。
5. 确认客户端为最新版本，可登录对应的 SSL VPN Portal 站点下载最新版客户端。
6. 如客户端终端安装 360 软件，卸载客户端并重新安装。

常见问题解决方法

常见问题 1

系统升级后，登录管理页面时，页面提示无效请求。

解决办法

通过串口或 SSH 方式连到后台，执行以下命令：

service redis restart

service rsyslog restart

常见问题 2

通过 Windows 系统自带的 IPSec VPN 客户端拨号成功后，原有的网络连接断开，客户端主机无法访问互联网和本地局域网。

解决办法

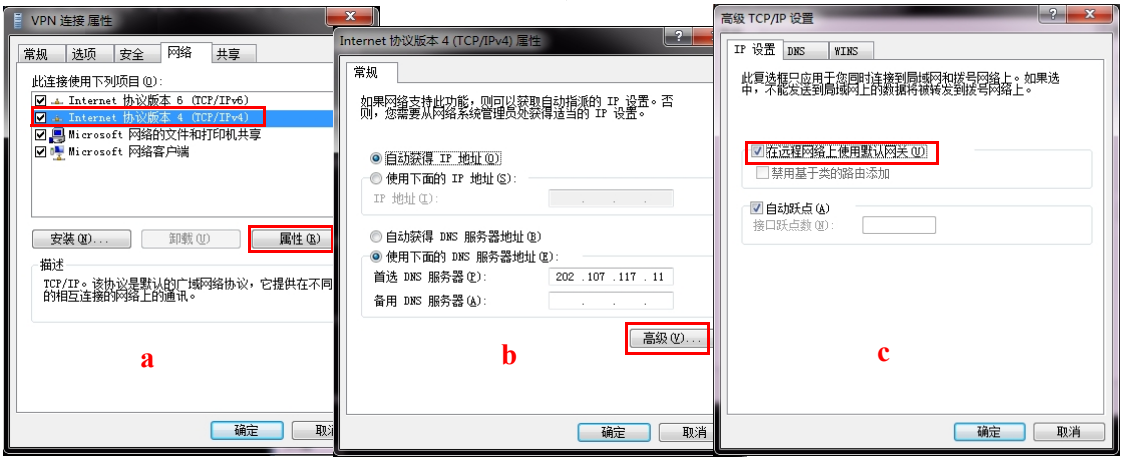
通过 IPSec VPN 连接的目的是保证通讯过程的安全。默认情况下，一旦 IPSec VPN 连接建立，所有客户端流量都走隧道，已有的互联网和局域网连接将断开。

如需同时访问 IPSec VPN 资源和互联网 / 局域网，可以通过以下方式实现：

a. 取消终端 IPSec VPN 连接中的 “ 在远程网络上使用默认网关 ” 属性。
b. 通过命令行添加到目标资源网络的路由。

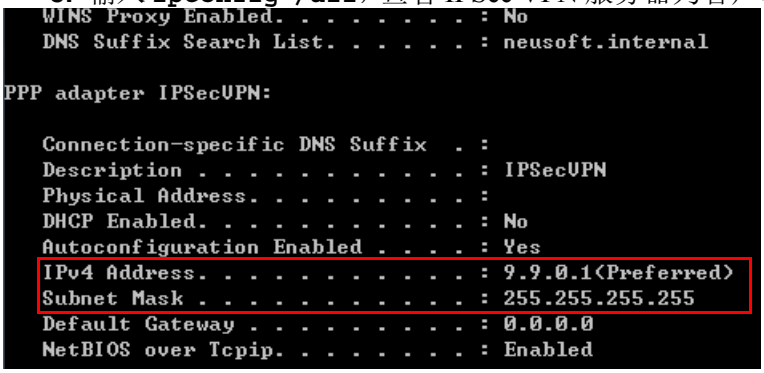
详细步骤如下：

a. 右键选择 IPSec VPN 连接，选择**属性 > 网络**。
b. 选中 **Internet Protocol Version 4 (TCP/IPv4)**，点击**属性**。
c. 点击**高级**，取消勾选**使用远程网络的默认网关**。



d. 在运行中输入 **cmd**，打开 Windows 命令行。

e. 输入 **ipconfig /all**，查看 IPSec VPN 服务器为客户端新分配的虚拟 IP 地址，如：



f. 通过 **route add** 命令，添加到 IPSec VPN 资源的路由，如：
route add 192.168.2.0 mask 255.255.255.0 9.9.0.1 -p
（192.168.2.0 是对端子网的 IP 地址段；
255.255.255.0 是对端子网掩码；
9.9.0.1 是 IPSec VPN 服务器分配给客户端的虚拟 IP ；
-p 表示永久添加该路由条目。）

常见问题 3

系统升级后，管理页面显示不正常。

解决办法

清除浏览器缓存。

常见问题 4

系统关机一段时间后， VPN 策略失效。

解决办法

更新系统时间。建议启用系统时间自动同步。

常见问题 5

VPN 用户登录时，提示认证失败。

解决办法

通过界面右上角的“ 测试用户 ”快捷菜单测试用户密码是否正确。

如果密码不正确，帮忙重置用户密码或让用户自己登录 Portal 页面修改密码。

如果密码正确，在 VPN 全局配置中将缺省认证服务器改为本地认证，使用本地用户账号登录相同资源，如果认证通过，则说明是认证服务器配置问题，请检查认证服务器配置。

常见问题 6

VPN 网关部署在出口防火墙后面时，客户端无法访问 VPN 服务。

解决办法

确认出口防火墙已添加 2 条目的地址转换规则 （服务端口 500 和 4500），将 VPN 服务的公网地址转换为 VPN 网关的地址。

确认 VPN 网关的缺省网关指向出口防火墙，或刷新 VPN 网关和出口防火墙之间的路由。

检查客户端和 VPN 网关之间是否有多条通路。当存在多条通路时，需清理并更新 VPN 网关上的 ARP 表。

常见问题 7

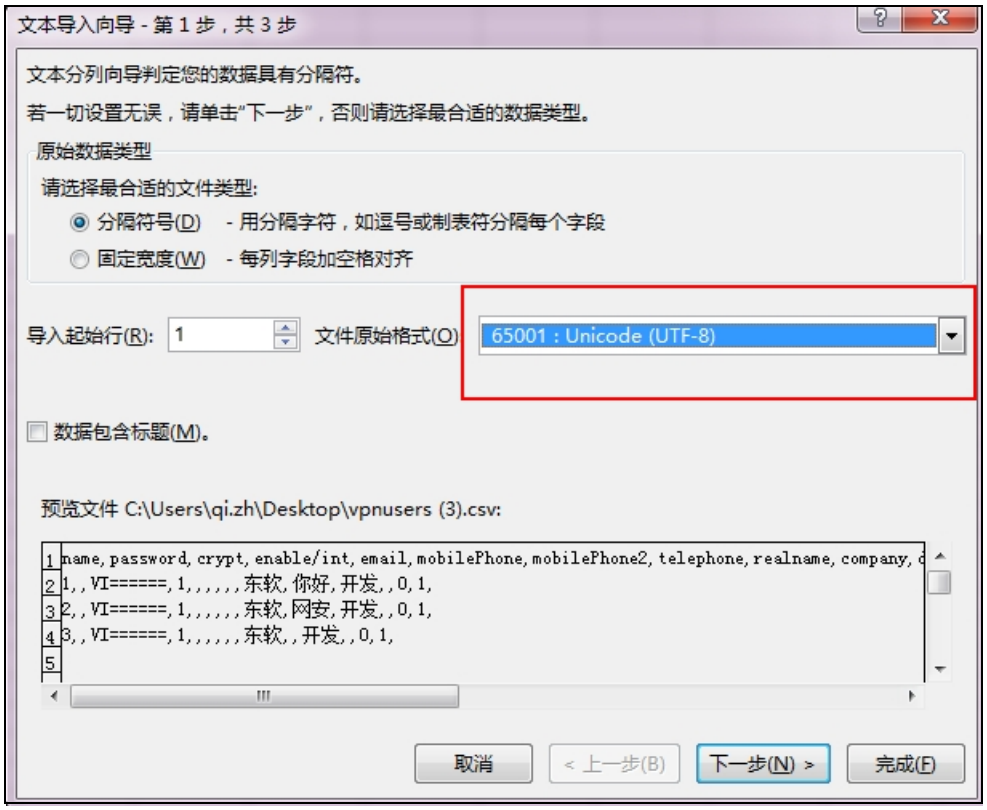
导出数据显示乱码。

解决办法

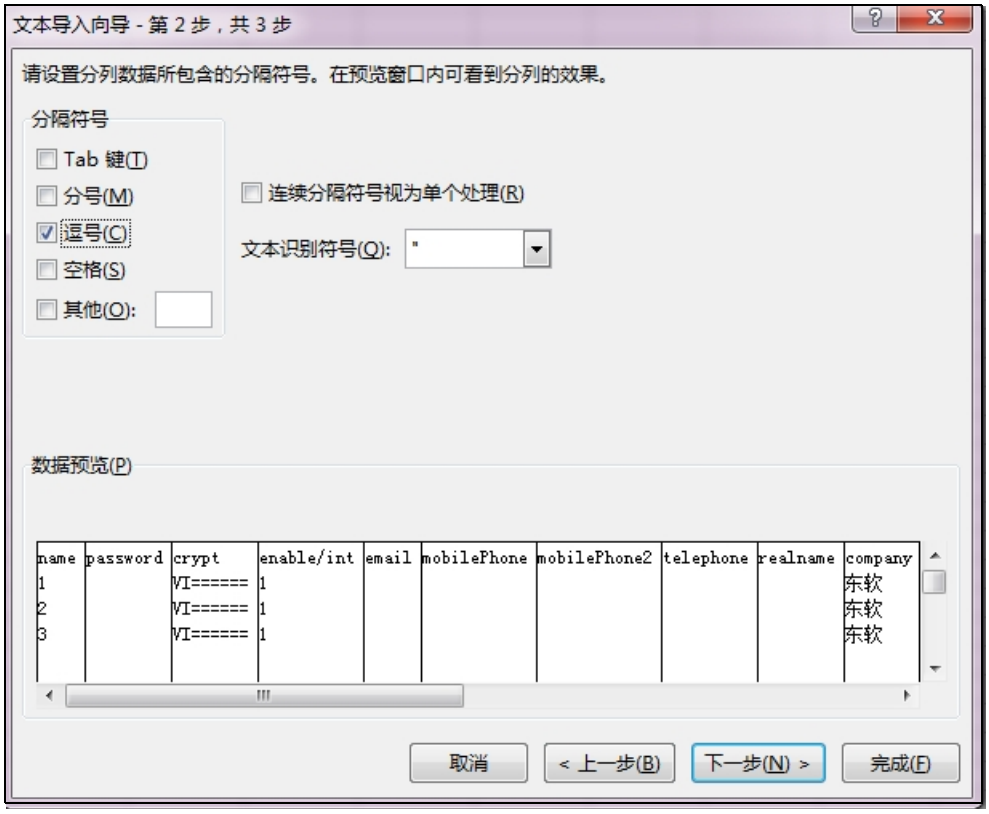
如果想批量编辑用户或策略信息，可将当前用户或策略信息导出，编辑后再导入。

a. 点击**导出**按钮，导出当前用户或策略信息为 csv 文件。

b. 新建 excel 文件，选择**数据 > 自文本**，导入已导出 csv 文件中的用户或策略信息。文件原始格式选择 UTF-8：



分隔符号选择逗号：



c. 编辑用户或策略信息，另存为 csv 格式 （逗号分隔）。

d. 备份 VPN 网关的系统信息，导入编辑后的 csv 文件。

常见问题 8

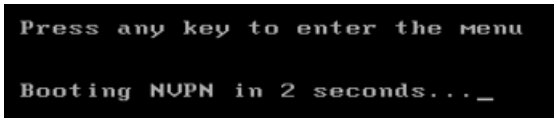
修改初始密码后，忘记密码。

解决办法

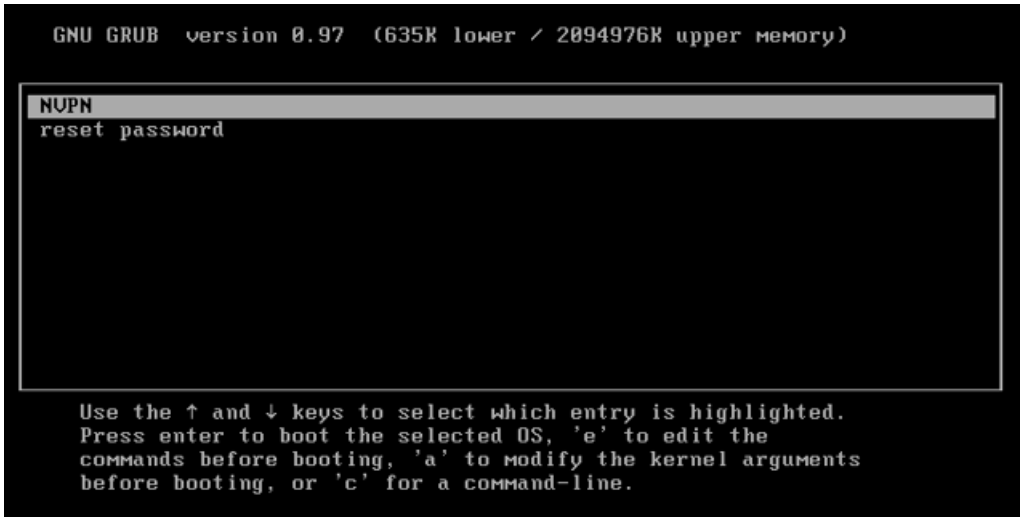
通过 Console 重置密码：

a. 将管理主机连接到设备串口。

b. 重启设备。系统启动过程中，出现如下打印时按回车键：



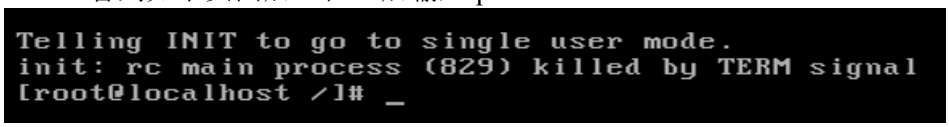
c. 之后出现如下界面：



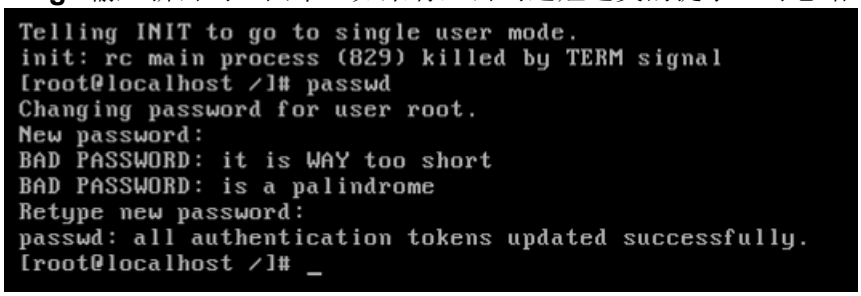
d. 选择 reset password 后回车（虚拟机需要在 reset password 上按 E，然后在 kernel 行上再按 e，然后进去把 console=ttyS0 去掉后，回车，然后按 b）。

e. 输入密码 neteye 后回车。

f. 看到如下页面后，在 # 后输入 passwd。



g. 输入新密码，回车。如果有些密码过短之类的提示，可忽略。



h. 输入 reboot 重启，采用新密码进入系统即可。

问题反馈方式

如果您在使用东软 NetEye VPN 网关、 Portal 或客户端的过程中遇到问题，请通过以下方式反馈给我们：

- 服务电话：400 655 6789
- 邮件地址：servicedesk@neusoft.com