Neusoft

东软 NetEye VPN 网关 V3.0

用户使用指南

版本 1.0

2018 年 12 月

联系信息

网站：http://www.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。

文档内容包括：

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 SSL VPN Portal 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 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*
- *Window 内置 IPSec VPN 客户端接入指南.pdf*
- *Android 内置 IPSec VPN 客户端接入指南.pdf*
- *iOS 内置 IPSec VPN 客户端接入指南.pdf*
- *macOS 内置 IPSec VPN 客户端接入指南.pdf*

第1章 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

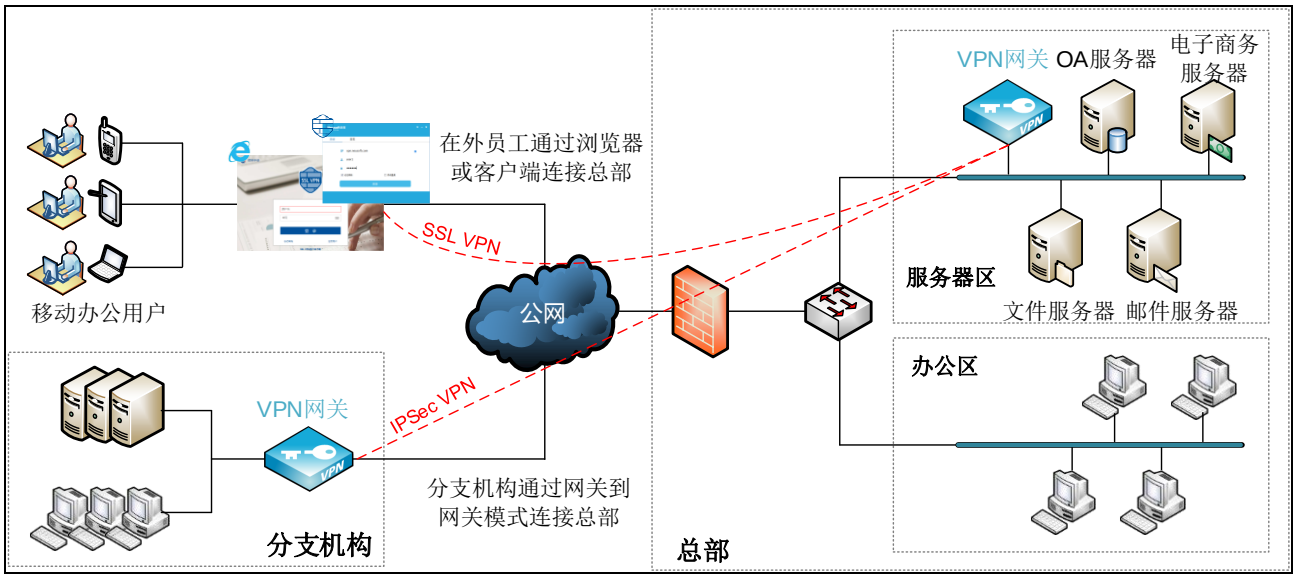
功能模块	功能特性
SSL VPN	• 支持隧道模式 SSL VPN，对客户端到网关的网络传输数据进行加密。 • 支持 Web 模式 SSL VPN，对 HTTP、HTTPS、FTP、RDP、SSH、Telnet 等协议基于流式的 html 替换以及缓存压缩提升了替换的准确率和速度。 • 支持 AES、DES、3DES、MD5、RC4、RSA 等加密算法，支持加载扩展安全算法模块。 • 支持与现有用户数据库的快速结合，支持 RADIUS、LDAP、Active Directory、eDirectory 等第三方认证方式以及组合认证。 • 支持 LDAP 动态组和安全组，直接复用 LDAP 服务器的安全策略，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

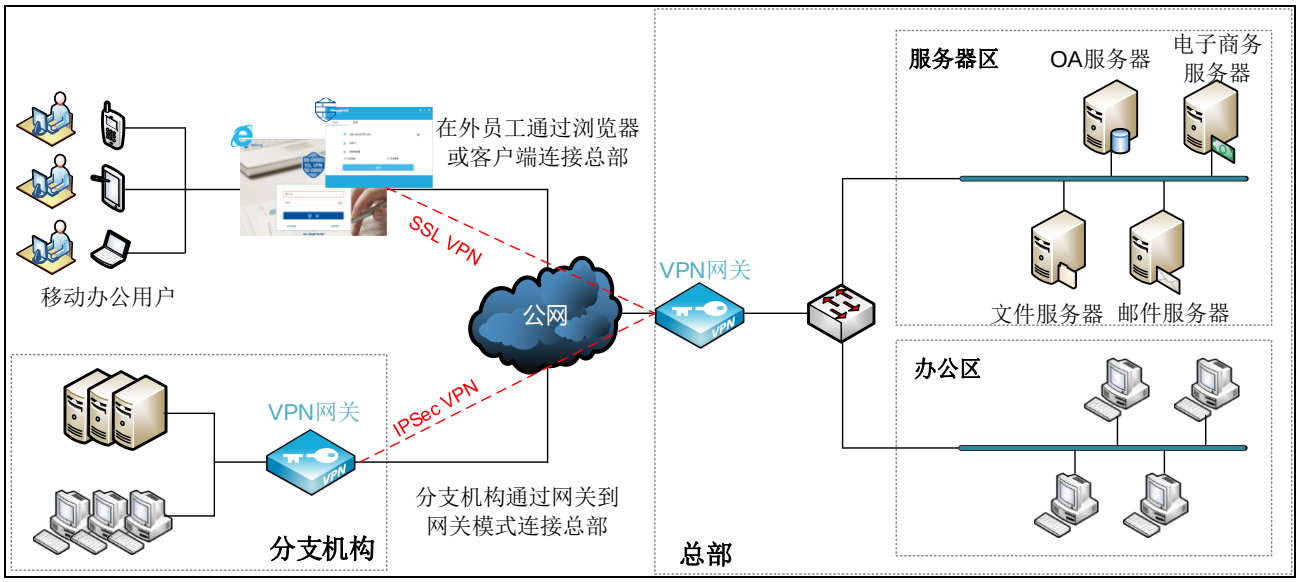
请在使用本产品前，对网络进行必要的规划，确定产品部署方式。如不是全新网络，需考虑部署本产品对原有网络规划及编址的影响。

VPN 网关支持单臂和网关两种部署方式：

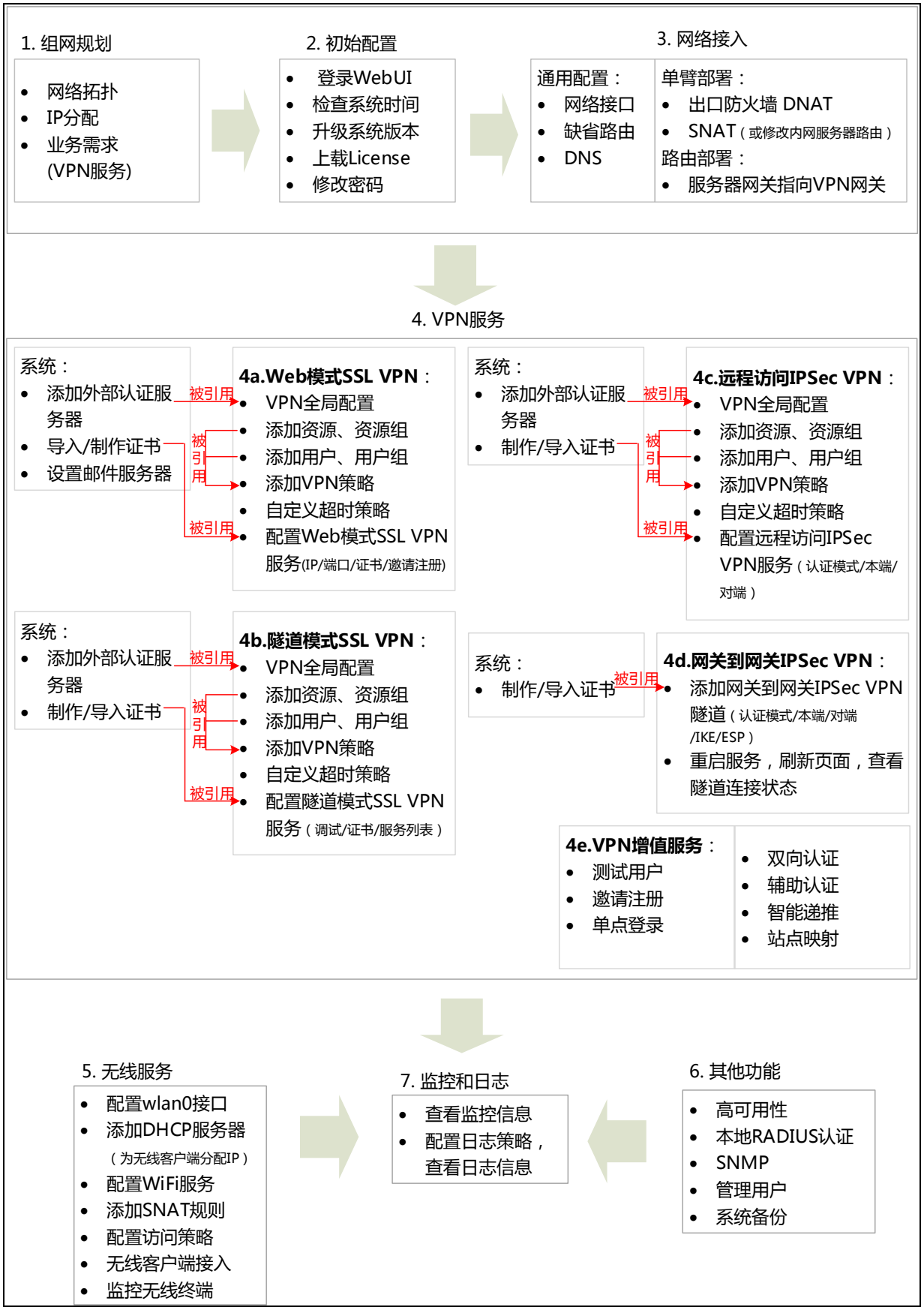
- 单臂模式



- 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

1.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**。 • SSH 管理密码：可在控制台通过 passwd 命令进行修改。

2a.单臂模式部署

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。

2b.网关模式部署

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。

3. Web 模式 SSL VPN

1.配置外部认证服务器（可选）	认证配置>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，然后在全局配置或者缺省认证服务器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）；认证配置>缺省认证服务器（选择缺省的认证服务器） **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（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	认证配置>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。

4.隧道模式 SSL VPN

1.配置外部认证服务器（可选）	认证配置>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，然后在全局配置或者缺省认证服务器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）；认证配置>缺省认证服务器（选择缺省的认证服务器） **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	认证配置>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）。

5a.远程访问 IPSec VPN

1.配置外部认证服务器（可选）	认证配置>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，然后在全局配置或者缺省认证服务器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）；认证配置>缺省认证服务器（选择缺省的认证服务器） **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）	认证配置>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。

5b.网关到网关 IPSec VPN

1.制作/导入证书（可选）	认证配置 > 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

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。

6. 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。
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。

7.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

8.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	认证配置>外部认证服务器页面右上角的本地 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

第2章 系统主页

本章介绍系统登录、WebUI 布局以及系统主页的相关信息。

2.1.登录 WebUI

安装好硬件设备后，首次登录请执行以下操作：

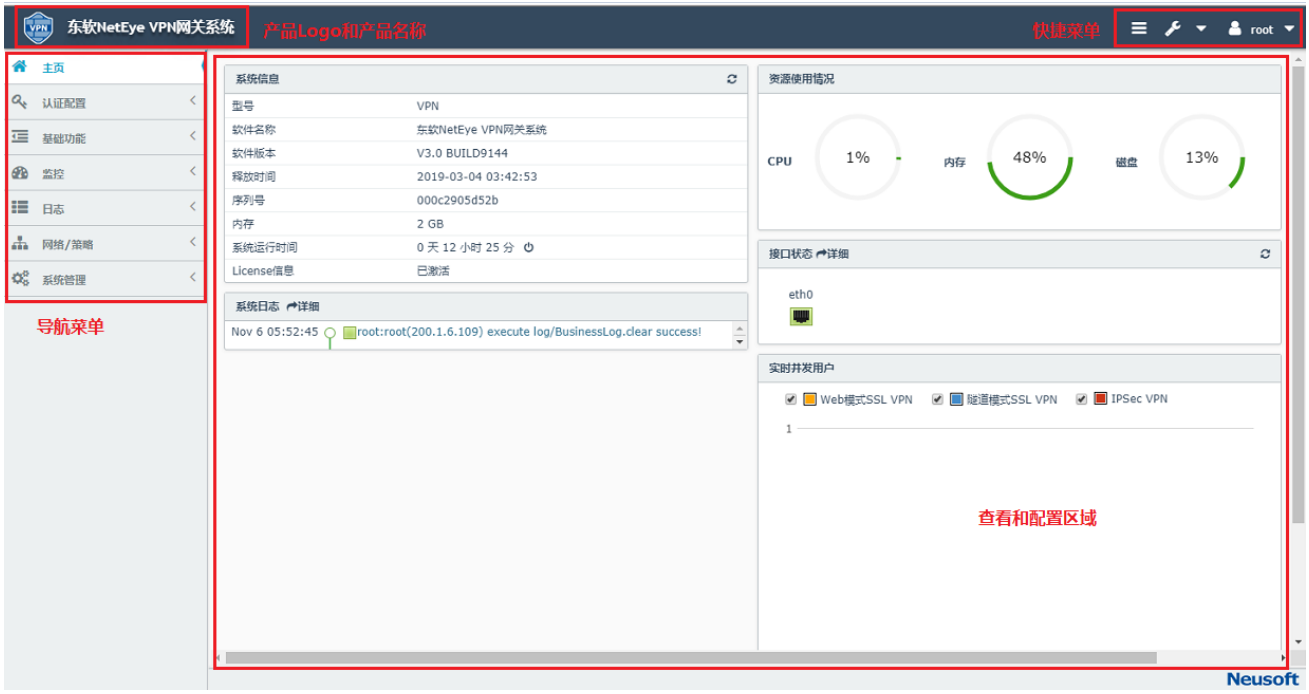
连接设备的管理接口至管理 PC，或直接连接设备的管理接口到 LAN。请使用带有 RJ-45 接头的超 5 类或 6 类的非屏蔽双绞线或屏蔽双绞线连接设备。

1. 在管理 PC 上添加 IP 地址 192.168.1.200，掩码为 255.255.255.0。
2. 打开管理 PC 中的浏览器，输入 https://192.168.1.100:10443。出现一个证书错误提示页面，点击“继续浏览此网站（不推荐）”。

3. 在登录页面输入缺省用户名/密码：root/neteye，点击登录按钮，登录 WebUI。

2.2.WebUI 界面布局

VPN 网关提供简单易用的 Web 管理界面，界面布局如下图所示：

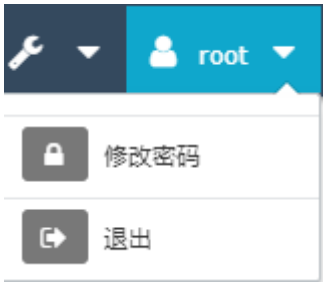


- 点击  隐藏或展开界面左侧导航菜单。
-  工具，点击右侧的向下箭头，可以选择更多菜单：

  - 点击测试用户，输入用户名和密码，测试 VPN 用户名和密码是否匹配。此功能支持本地和外部用户。
  - 点击基础功能分页设置，可以设置每页显示的记录条数。

- 

用于显示当前登录用户名称，点击右侧的向下箭头，可以选择更多菜单：



  - 点击修改密码，修改当前登录用户的密码。
  - 点击退出，退出系统。

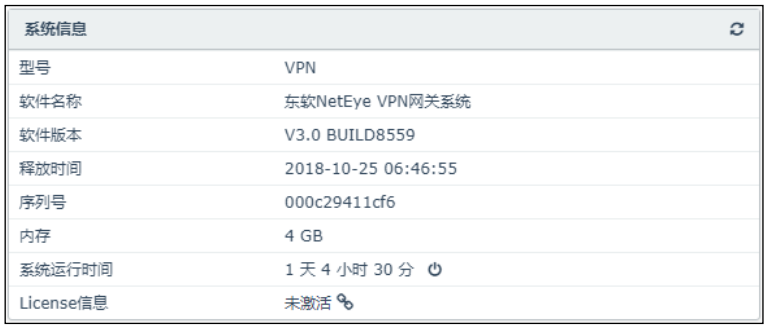
2.3.查看系统主页

登录 WebUI 后将进入系统主页，通过主页可查看系统信息、资源使用情况、接口状态、系统日志、隧道模式在线用户和 Web 模式在线用户等信息。

用鼠标按住并拖拽主页各显示区域，可自定义主页布局。

2.3.1. 查看系统信息

在系统信息区域，可以查看以下信息：产品型号、软件名称、软件版本、释放时间、序列号、内存大小、系统运行时间和 License 激活状态。



- 申请或更新 License 时，需要提供序列号信息。
- 点击系统运行时间后的图标，重启或关闭 VPN 网关。
- 如果 License 未激活，可以点击图标跳转到 License 配置页面上传 License。
- 点击右上角的图标可以刷新系统信息。

2.3.2. 查看资源使用情况

在资源使用情况区域，可以查看 CPU、内存和磁盘利用率。

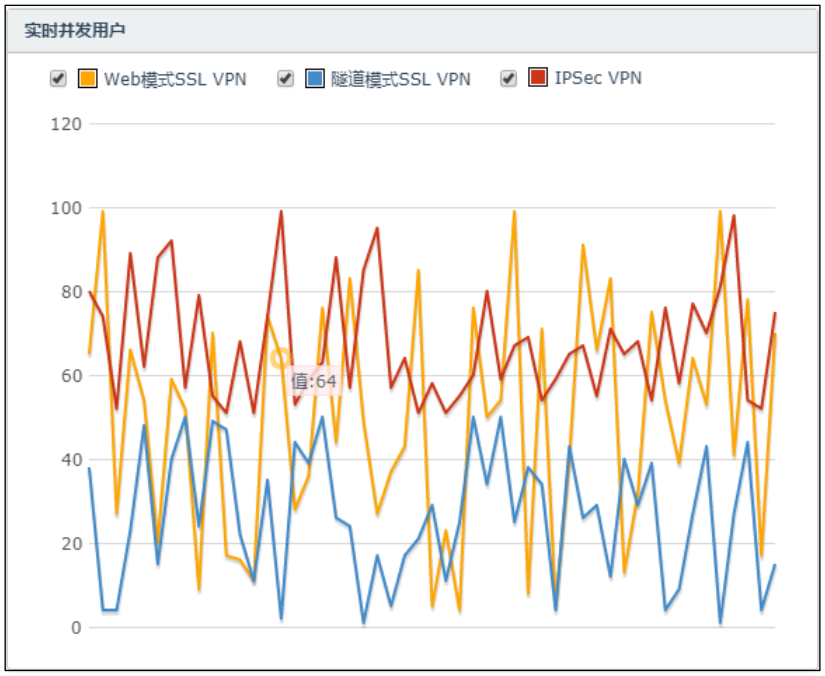
2.3.3. 查看接口状态

在接口状态区域，可以查看所有以太网接口的链路状态和配置信息。

- 绿色表示接口链路处于连通状态，灰色表示链路断开。
- 鼠标指向接口时，系统会弹出接口的 IP 地址信息。
- 点击**详细**链接，可以跳转到**接口监控**页面查看接口详细信息。
- 点击右上角的图标可以刷新接口状态。

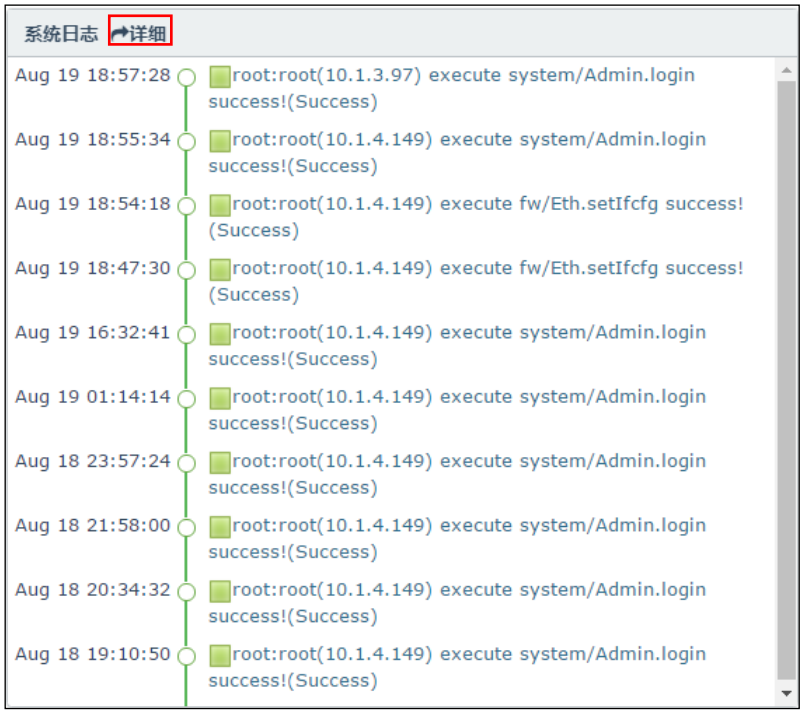
2.3.4. 查看实时并发用户

在实时并发用户区域，可以查看所有用户的实时信息。鼠标移到曲线上时，可查看具体数值（用户个数）。



2.3.5. 查看系统日志

在系统日志区域，可以查看最近的 10 条系统管理日志。



点击**详细**链接，可以跳转到**管理日志**页面查看全部管理日志信息。

第3章 认证配置

本章介绍缺省认证服务器、外部认证服务器、辅助认证以及证书。

3.1.缺省认证服务器

当配置了一些外部认证服务器时，可以选择缺省的认证服务器，然后提交，也可以选择多服务器认证。

1. 选择**认证配置>缺省认证服务器**。

2. 点击**提交**。

3.2.外部认证服务器

VPN 网关可以与网络中现有的用户数据库快速结合，实现用户认证，大大节省系统管理员的配置维护负担。系统支持 RADIUS、LDAP、Active Directory、eDirectory 等第三方认证服务器以及组合认证。

3.2.1. 外部认证服务器

1. 选择**认证配置>外部认证服务器**。
2. 点击**新建**，在下拉列表中选择要添加的服务器类型，设置相关信息，点击**确定**。

- 添加 RADIUS 服务器时，填写如下信息：

如果想使用VPN网关的本地RADIUS服务器对VPN用户进行认证，可以创建一个外部RADIUS认证服务器，IP地址和端口设置为本地RADIUS服务器地址和端口，然后在认证配置缺省认证服务器中将该外部RADIUS认证服务器设为缺省认证服务器。

- 添加其余三种服务器时，填写如下信息：

如果认证过程需要使用 SSL 加密，则需启用安全连接，包括 SSL/TLS 和 STARTTLS。启用安全连接时，需指定用于安全连接的 SSL 证书，推荐使用系统自带的本地证书 Test。

如果填写公共名标识符、识别名称、管理员识别名称和密码，需要与添加的外部认证服务器保持一致。注意 AD 服务器的管理员识别名称与 LDAP 的格式不同：

3. 选择认证服务器

- 选择**认证配置>缺省认证服务器**，在缺省认证服务器下拉列表中选择一种外部认证服务器或多服务器认证。
- 如果在**基础功能>全局设置**中选择了 LDAP 认证服务器，则认证时可在外部 LDAP 服务器上认证，同时可设置 LDAP 安全组，方便管理员添加授权用户。选择**基础功能> VPN 策略**，添加 VPN 策略，选择用户组，通过安全组选择用户。
- 如果安全组包含的用户是动态变化的（比如员工离职或新员工入职），可通过添加 LDAP 动态组添加授权用户。选择**基础功能>用户组**，点击**添加**，在**类型**下拉列表中选择 **LDAP 动态组**，添加 LDAP 用户组。

3.2.2. 本地 RADIUS 认证服务

VPN 网关可以作为 RADIUS 服务器提供认证服务。

1. 选择**认证配置>外部认证服务器，**点击页面右上角的**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，添加认证客户端的子网范围和共享密钥。共享密钥用于 RADIUS 客户端与服务器之间的用户密码传输加密。

3. 设置认证协议，保证 VPN 网关与 RADIUS 客户端之间的通信安全。

4. 选择认证模式，包括：

   - **本地**：使用本地数据库认证。

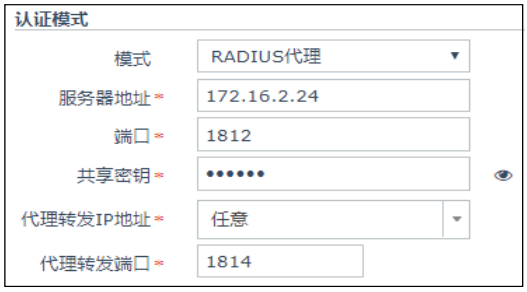
   - **LDAP**：使用外部 LDAP 数据库认证。

参数	说明
IP 地址/域名	外部 LDAP 服务器的 IP 地址或域名。
端口	外部 LDAP 服务器提供认证服务的端口。

Base DN	LDAP 根目录识别名，如 DC=neusoft,DC=com。
管理员信息	管理员识别名，如 cn=admin,ou=users,dc=neusoft,dc=com。
密码	管理员密码。
公共名标识符	LDAP 目录树中用于标识用户名的标识符。即，在 LDAP 服务器的数据库中查询用户名时，通过什么符号进行索引。
成员属性	LDAP 目录树中用于标识用户所属关系的标识符。
密码类型	LDAP 服务器返回用户密码的格式，包括： • **Cleartext-Password**：明文密码。 • **Password-With-Header**：带头部信息的明文密码。 • **NT-Password**：加密后的密码。

此处所填写的LDAP参数信息应与外部LDAP认证服务器的配置信息保持一致。

- **RADIUS 代理**：作为 RADIUS 认证服务器的代理，将认证请求转发给真正的 RADIUS 服务器进行认证。



参数	说明
服务器地址	VPN 网关代理的 RADIUS 服务器的 IP 地址或域名。
端口	VPN 网关代理的 RADIUS 服务器提供代理认证服务的端口。
共享密钥	用于 VPN 网关与代理的 RADIUS 服务器之间的通信加密。
代理转发 IP 地址	VPN 网关用于转发认证请求的接口 IP 地址，即 VPN 网关从哪个接口将用户认证请求转发给真正的 RADIUS 服务器。
代理转发端口	VPN 网关转发认证请求的端口。

5. 点击**提交**。

3.3.辅助认证

VPN 网关支持短信认证、OTP 动态令牌认证和硬件特征码认证三种辅助认证方式。

三种认证方式的区别如下：

认证方式	适用场景	服务类型	客户端类型
短信认证	对多数用户进行认证	Web 模式 SSL VPN 隧道模式 SSL VPN	Portal Android
OTP 认证	对少数用户进行认证	Web 模式 SSL VPN 隧道模式 SSL VPN	Portal Android
硬件特征码认证	对多数用户进行认证	隧道模式 SSL VPN	Windows Android

短信认证配置步骤：

1. 选择**系统管理>短信服务**，选择一个短信服务平台，查看需要哪些认证参数；
2. 到短信服务平台注册用户，获取认证相关参数信息；
3. 选择**系统管理>短信服务**，完成短信平台相关参数的配置；
4. 选择**认证配置>辅助认证>短信认证**，开启短信认证，添加认证用户。
5. SSL VPN 用户输入用户名和密码登录后，根据提示获取短信验证码，完成认证。

OTP 认证配置步骤：

1. 选择**系统管理>系统时间**，查看系统时间是否正确。

VPN 网关的系统时间如果不正确，可能会导致 OTP 认证失败。

2. 管理员选择**认证配置>辅助认证> OTP 认证**，开启 OTP 认证，添加认证用户，并为用户绑定 OTP 设备。
3. SSL VPN 用户输入用户名和密码登录后，根据提示输入 OTP 设备上显示的一次性动态口令，完成认证。

硬件特征码认证的配置步骤：

1. 选择**认证配置>辅助认证>硬件特征码认证>通用配置**，开启硬件特征码认证，设置特征码收集策略和审批策略。
2. 通知 SSL VPN 用户输入用户名和密码登录，配合服务端完成硬件特征码的收集。
3. 选择**认证配置>辅助认证>硬件特征码认证>用户配置**，查看收集到的用户及硬件特征码信息。

如果设置了收集特征码后待审批，需要对收集到的用户特征码进行审批，允许或拒绝其访问。

本节内容包括：

3.3.1. 短信认证

短信认证要求在创建用户账号之初就绑定用户的手机号码。用户登录时，VPN 网关会通过短信方式发送一个校验码到用户的手机上，用户必须输入该校验码才能登录成功。

使用短信认证服务需要事先指定使用的短信平台及相关参数。详情参见短信服务。

1. 选择**认证配置>辅助认证>短信认证**。
2. 在**通用配置**页面进行如下配置：

启用短信认证并选择启用短信认证的服务类型，包括 Web 模式 SSL VPN 和隧道模式 SSL VPN。

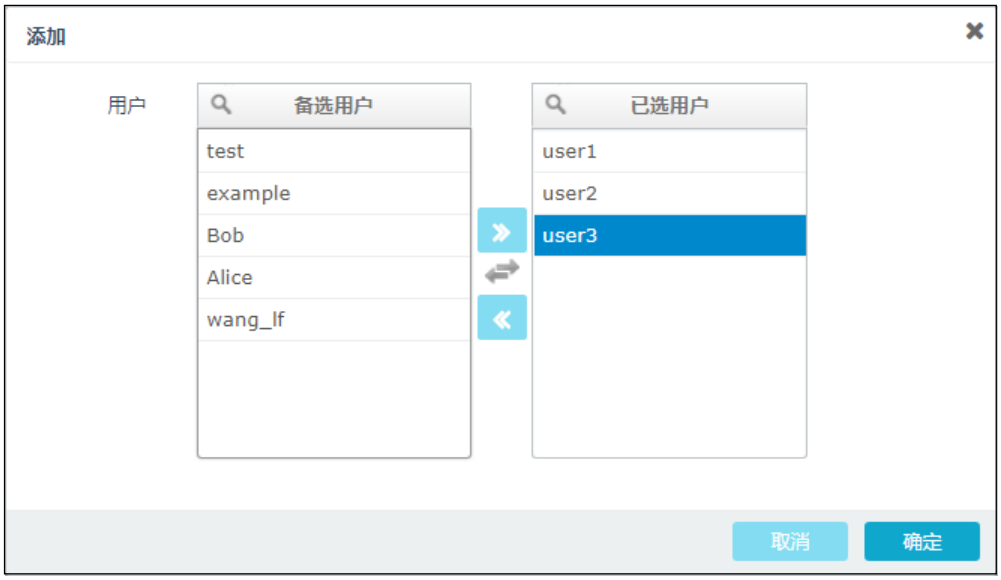
勾选**强制启用**后还可以配置例外用户，表示除例外用户，所有用户都必须进行短信认证。此时需要到用户配置页面添加需要认证的用户到用户列表并绑定电话号码。

如果不勾选**强制启用**，则只需将少数需要短信认证的用户添加到用户配置页面的用户列表中，其他用户无需进行短信认证。

3. 点击**提交**。

4. 在**用户配置**页面添加需要进行短信认证的用户：

- 点击**添加>本地用户**，选择要进行短信认证的本地用户，点击**确定**。



- 点击**添加>外部用户**，添加要进行短信认证的外部用户及电话号码，点击**确定**。

对于列表中的用户，管理员可进行编辑、删除、启用/禁用、导入/导出等操作。

3.3.2. OTP 认证

开启 OTP 认证的 VPN 用户在拨号登录时，除了输入用户名和密码，还需要输入 OTP 设备上显示的动态密码才能登录成功。

VPN 网关基于系统时钟与 OTP 令牌种子，通过特定算法计算出一个密码，然后与 OTP 设备端的密码进行匹配：如果一致，则认证通过；否则，认证失败。

1. 选择**认证配置>辅助认证>OTP 认证**。
2. 在**通用配置**页面进行如下配置：

启用 OTP 认证并选择服务类型，包括 Web 模式 SSL VPN 和隧道模式 SSL VPN。

OTP 设备和 VPN 网关之间通常存在时间误差。为了解决时间误差导致的 OTP 认证失败问题，VPN 网关允许管理员设置误差时间。

OTP 认证缺省误差时间为 10 分钟，表示 OTP 认证过程中，VPN 网关将计算当前系统时间前后 5 分钟内的所有密码，与 OTP 设备上的密码进行匹配。

为保证 OTP 认证成功，请确保 VPN 网关的系统时间正确。

勾选**强制启用**后还可以配置例外用户，表示除例外用户，所有用户都必须进行 OTP 认证。此时需要到用户配置页面添加需要认证的用户到用户列表并绑定 OTP 设备。

如果不勾选**强制启用**，则只需将少数需要 OTP 认证的用户添加到用户配置页面的用户列表中。

3. 点击**提交**。

4. 打开**用户配置**页面，点击**添加**，添加新的用户并绑定 OTP 设备。

OTP 令牌密钥用于计算 OTP 口令，为 OTP 设备出厂自带的一个唯一标识字符串，如：

ll037B4ECE09A5C9C4696A2134269D16F37FAD0F8D24CD38C0。

5. 点击**确定**。

6. 查看添加的用户和 OTP 令牌绑定信息。

7. 点击**设备同步**，输入 OTP 设备上连续两次出现的口令，点击**确定**，可以同步 VPN 网关和 OTP 设备的时间。

8. 点击**确定**。

3.3.3. 硬件特征码认证

硬件特征码是根据硬件设备的硬件特征（如网卡 MAC、硬盘等信息）按一定算法生成的唯一标识。通过将硬件特征码与用户账号一一绑定，从而达到仅允许指定硬件设备接入授权网络的目的。

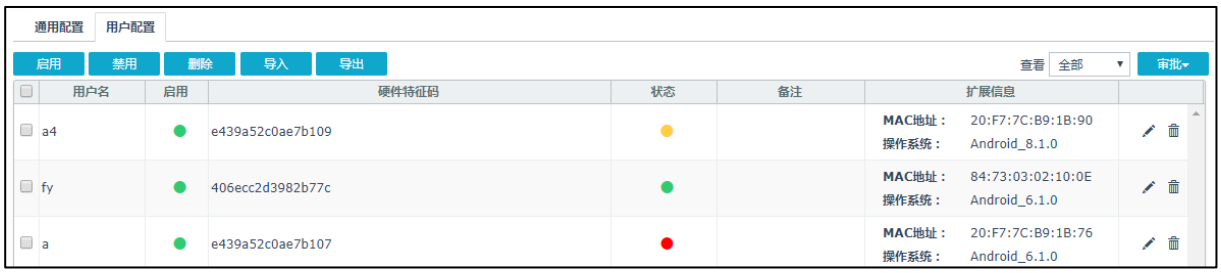
一个用户账号可以绑定一个或多个硬件特征码。如果一个用户想通过手机、平板、PC 等多种终端接入授权网络，则需要为其账号绑定多个硬件特征码。

1. 选择**认证配置>辅助认证>硬件特征码认证**。
2. 在**通用配置**页面进行如下配置：

参数	说明
启用	勾选启用硬件特征码认证。
服务类型	目前仅隧道模式 SSL VPN 服务支持硬件特征码认证。
强制启用	勾选表示强制使用硬件特征码认证。 需要结合例外用户和用户特征码绑定列表一起达到认证用户身份的目的： 如果多数用户需要进行硬件特征码认证，推荐强制使用，表示所有用户默认必须进行硬件特征码认证才能登录成功。 此时可以添加例外用户，除指定的例外用户，其他所有用户都必须添加到用户列表并绑定硬件特征码。 如果只有少数用户需要进行硬件特征码认证，推荐不强制，只需将少数需要认证的用户添加到用户列表并绑定硬件特征码即可。
例外用户	强制启用硬件特征码认证的情况下，用于指定哪些用户可以例外放行。

每个用户拥有的特征码数	指定每个用户最多允许使用几台设备接入授权网络。
收集特征码	是否收集用户接入网络所使用设备的硬件特征码。
收集特征码后的状态	收集特征码后是否需要管理员审批才允许接入网络。
收集阶段忽略特征码认证	设置收集阶段是否允许用户无需通过硬件特征码认证也可以登录。

3. 启用硬件特征码认证并收集硬件特征码后，还需要到用户配置页面进行审批：



参数	说明
用户名	需要进行硬件特征码认证的用户的名称。
启用	该条目启用或禁用状态。 禁用状态相当于没有将该条目添加到列表中，但是占用该用户所拥有的特征码个数。
硬件特征码	用户接入网络时所使用客户端的硬件特征码。
状态	用户策略的审批状态，即收集到该用户的硬件特征码后，是否允许其访问通过。 • 绿色表示审批通过。 • 红色表示拒绝。 • 黄色表示待审批。
备注	用户策略的备注信息。
扩展信息	用户所使用客户端设备的硬件信息，包括 MAC 地址和操作系统版本。

对于列表中的用户，管理员可以进行启用/禁用、删除、导入/导出和审批操作。通过查看来查看部分条目。

3.3.4. 验证结果

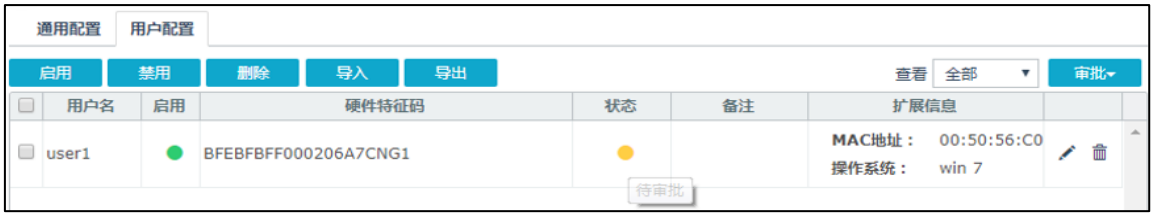
以 SSL VPN 用户身份登录，可验证辅助认证的配置结果：

- 通过 Portal 登录的 SSL VPN 用户：
  - 短信认证：

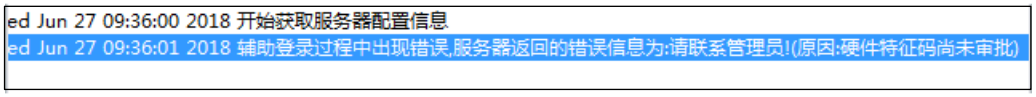
  - OTP 辅助认证：

- 同时开启短信认证和 OTP 认证：

- 通过 Windows 版 SSL VPN 客户端登录的 SSL VPN 用户仅支持硬件特征码辅助认证：
  - 如果设置收集特征码后待审批且收集阶段忽略特征码认证，用户首次接入时客户端不会有任何提示，直接认证通过。但是，服务端收集到的用户信息是待审批状态，需要管理员进行审批，否则过了收集阶段该用户将不能正常访问。



  - 如果设置收集特征码后待审批但收集阶段不忽略特征码认证，则用户首次接入时无法认证通过，客户端日志中将提示“请联系管理员!(原因:硬件特征码尚未审批)”。



此外，服务端收集到的用户信息是待审批状态，需要管理员手动审批后该用户方可进行访问。

  - 如果设置收集特征码后自动审批通过，则用户首次接入时客户端不会有任何提示，直接认证通过，管理员也无需做任何操作。

- 通过 Android 版 SSL VPN 客户端登录的 SSL VPN 用户：

短信认证：

OTP 认证：

同时开启短信和 OTP 认证：

硬件特征码认证（特征码未审批提示）：

3.4.证书

VPN 网关内置 CA 服务器，可本地生成 CA 证书、服务器证书和个人证书。

系统默认提供一组 Test 证书用于测试：一个 CA 证书 Test、一个服务器证书 Test、两个用户证书 Test_a 和 Test_b。

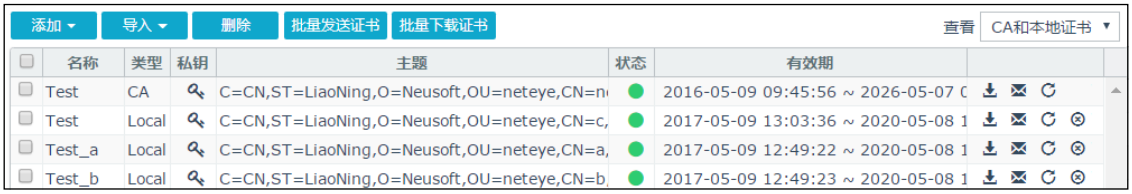
- 测试 Web 模式 SSL VPN 隧道时，可以使用服务器证书 Test 作为 SSL VPN 服务器的本地证书进行隧道协商。
- 测试隧道模式 SSL VPN 隧道时，可以使用 CA 证书 Test 来验证客户端证书、使用服务器证书 Test 作为 SSL VPN 服务器的本地证书进行隧道协商。
- 测试网关到网关的 IPSec VPN 隧道时，可以使用 Test_a 和 Test_b 作为两端的本地证书进行隧道协商。

系统自带的证书仅供测试使用。企业用户请自行申请或制作证书，并导入系统供使用。

本节介绍以下内容：

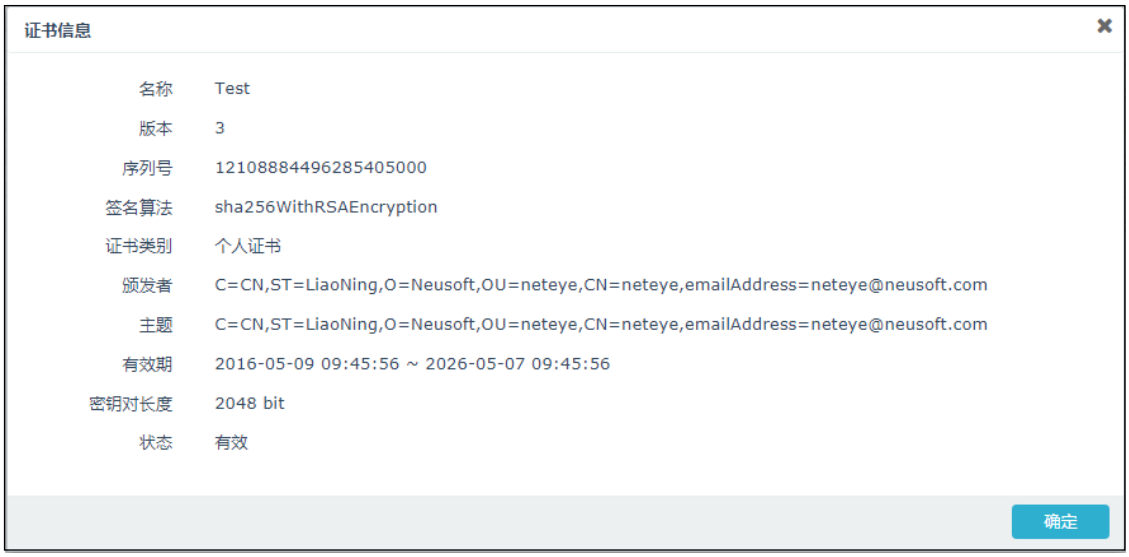
3.4.1. 查看证书

1. 选择**认证配置>证书**，查看系统自带的证书信息。



2. 通过右上角的**查看**下拉菜单，可选择要查看的证书类型。

- 点击 查看证书详细信息。



- 点击 下载证书到本地。

  如需批量下载证书，选中证书条目后，点击**批量下载证书**。

  下载本地证书时，需要输入证书访问密码，重新导入该证书时需要输入该密码。

- 点击证书条目对应的，设置收件人地址，邮件发送该证书。

  要邮件发送证书，需要到**系统管理>邮件服务器**页面设置邮件服务器和发件人信息。系统默认使用证书主题信息中的电子邮件地址作为收件人地址，用户可自行修改。邮件附件包含.pfx 格式的本地证书和关联的 CA 证书，邮件内容包含.pfx 格式本地证书的导出密码。

  如需批量发送证书，设置证书收件人地址后，选中证书条目，点击**批量发送证书**。

- 点击 续订证书。设置新的有效期和密钥对，点击**确定**。

- 点击 吊销证书。

3.4.2. 添加证书

1. 选择**认证配置>证书**。
2. 点击**添加**，选择根 CA 证书、从属 CA 证书、本地证书或本地证书（批量）。

- 添加根 CA 证书：

- 添加从属 CA 证书：

- 添加本地证书：

- 创建服务器证书时，公共名必须填写真实服务器的IP地址或域名，且生成的证书会带有服务器属性；创建个人证书时，公共名一般填写用户名。

- 批量添加本地证书：

参数	说明
证书名称	长度 1～63 字节，只能由字母、数字和特殊字符组成，空格及?,'"\<>&#=除外。 批量生成本地证书时，多个证书名称之间用逗号分隔。
证书名称前缀	设置要批量生成的证书的名称前缀。
有效期	证书的有效期。
哈希算法	支持 SHA-1 和 MD5 算法。
证书类别	支持服务器证书和个人证书。
密钥对选项	密钥对选项包括： • **类型**：包括 RSA、DSA 和 ECDSA，自动注册证书只能选择 RSA 算法。 • **密钥对长度**：密钥越长，越安全，但加密和解密速度越慢。密钥对长度可以为 768、1024、1536 和 2048。
证书主题信息	证书主题信息包括： • **国家代码（2 字母）**：代表 VPN 网关**设备所在的国家。**

- **省份**：UTF-8 字符。不能输入以下字符：`^?,='"\/<>&
- **城市**：**UTF-8 字符。不能输入以下字符：`^?,='"\/<>&**
- **公司**：**UTF-8 字符。不能输入以下字符：`^?,='"\/<>&**
- **部门**：**UTF-8 字符。不能输入以下字符：`^?,='"\/<>&**
- **公共名**：**UTF-8 字符。不能输入以下字符：`^?,='"\/<>&**

  服务器证书的公共名为使用该证书的 VPN 网关的公网 IP 地址或域名，个人证书的公共名为用户名称。
- **邮件地址**：对证书负责的联系人的邮件地址。

  如果取消勾选**高级**选项，则可以手动输入所需证书主题参数信息，参数之间用逗号隔开，如：

  C=CN,ST=Liaoning,L=Shenyang,O=Neusoft,OU=NSD,CN=NetEye123,emailAddress=neteye123@neusoft.com

3. 点击**确定**。

3.4.3. 导入证书

导入证书时，先导入 CA 证书再导入本地证书，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。

1. 选择**认证配置>证书**。
2. 点击**导入**，选择 **CA 证书**或**本地证书**，导入证书。导入本地证书时需输入证书访问密码。

第4章 VPN 基础功能

本章介绍如何配置 VPN 基础功能，内容包括：

- VPN 基本配置：
  - 全局配置
  - 资源
  - 资源组
  - 用户
  - 用户组
  - VPN 策略
  - 快速运维
  - 超时策略
- Web 模式 SSL VPN
- 隧道模式 SSL VPN
- IPSec VPN

VPN 基本配置主要用于指定允许哪些 VPN 用户访问哪些资源。其中，资源被资源组引用，用户被用户组引用，资源组和用户组被 VPN 策略引用。此外，还可以设置用户认证方式、超时时间、Web 缓存压缩等全局配置信息。

VPN 网关支持网关到网关和远程访问两种类型的 IPSec VPN。要使用远程访问 IPSec VPN、Web 模式 SSL VPN 以及隧道模式 SSL VPN，必须配置 VPN 基本信息。

4.1.全局配置

全局配置中可以对 VPN 用户使用的 LDAP 认证服务器进行统一配置。如果使用外部 LDAP 认证服务器，需要提前配置，详细步骤请参见外部认证服务器。

如果配置了 LDAP 外部认证服务器，还可以配置 LDAP 安全组，从而可以通过 LDAP 安全组添加 VPN 用户，减轻管理员配置负担。

针对 Web 模式 SSL VPN，还可以对资源的缓存和压缩策略进行统一配置。

1. 选择**基础功能>全局设置**。
2. 可选择 LDAP 认证服务器，如果系统已经关联 LDAP 服务器，还可根据需要配置 LDAP 安全组。设置资源缓存/压缩全局策略以及会话超时提醒时机。

参数	说明
LDAP 认证服务器	对 SSL VPN 用户或远程访问 IPSec VPN 用户进行身份认证的认证服务器。 如果添加了 LDAP 外部认证服务器，此处可以选择其中一种认证服务器。
LDAP 安全组	请根据要使用的 LDAP 服务器上的配置填写安全组根识别名称（Base DN）和安全组成员属性标识，可在 VPN 策略中引用。

Gzip 压缩	是否对资源文件进行 Gzip 压缩传送。
HTML/JS/CSS 缓存	是否缓存 HTML/JS/CSS 文件，以提升访问速度。如果启用，还可以指定要缓存的 HTML/JS/CSS 文件后缀，后缀名之间用逗号分隔。
HTML/JS/CSS 缓存过期时间	HTML/JS/CSS 缓存过期时间。
非 HTML/JS/CSS 快速代理	对于非 HTML/JS/CSS 文件，是否进入快速代理模式。
非 HTML/JS/CSS 缓存	是否缓存非 HTML/JS/CSS 文件。如果启用，还可以指定要缓存的非 HTML/JS/CSS 文件后缀，后缀名之间用逗号分隔。
非 HTML/JS/CSS 缓存过期时间	非 HTML/JS/CSS 缓存过期的时间。
会话超时提醒	VPN 会话超时前多长时间进行提醒。

3. 点击**提交**。

4.2.资源

配置 SSL VPN 或远程访问 IPSec VPN 服务之前，需要事先指定用户可以访问的资源，包括 HTTP、HTTPS、子网、远程桌面、远程 Web 应用、FTP、SSH、TELNET 等类型。

- Web 模式 SSL VPN 支持的资源类型包括 HTTP、HTTPS、远程桌面、FTP、SSH、TELNET，且所有资源支持在 SSL VPN 客户端以资源列表的形式展现；
- 隧道模式 SSL VPN 支持所有资源类型，但仅 HTTP、HTTPS 和远程桌面类型的资源支持在 SSL VPN 客户端以资源列表形式展现；
- 远程访问 IPSec VPN 支持所有资源类型，但不提供统一的 IPSec VPN 客户端，所以也不支持资源列表。

本节介绍如下内容：

4.2.1. 查看资源

1. 选择**基础功能>资源**。
2. 查看已配置资源：

名称	显示名称	类型	地址	自动登录	归属者	授权职能	引用
ProcessBase	东软日报系统	HTTP	192.168.10.10:80	SSO	-	func01	
EHR	东软人力资源管理系统	HTTPS	192.168.2.12:443	SSO	-	func01	
IPM	IPM	SSH	192.168.5.10:22		-	func01	
Customer		子网	192.168.6.0/24		-	func01	
NSD		子网	192.168.3.0/24		-	func01	

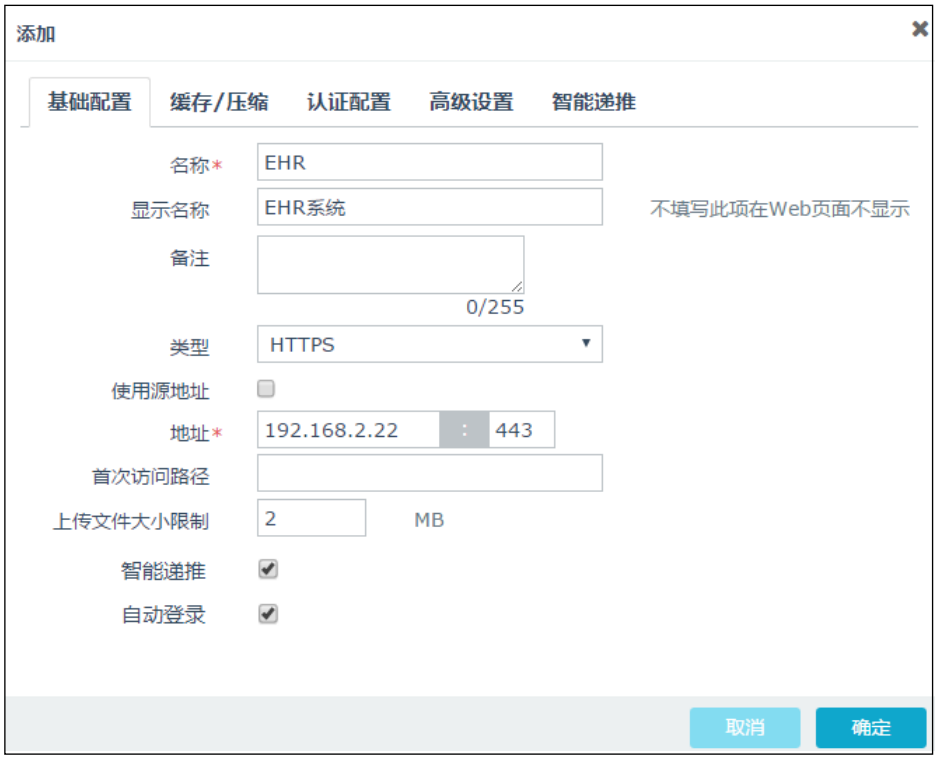
   归属者表示此资源是由哪个分级管理员创建的，如果是由系统管理员（Root、管理员）创建的，则归属者显示“-”，授权职能表示该资源都被分配给了哪些分级管理职能。
3. 点击**测试资源匹配**按钮，可以根据 IP 地址查询资源是否已经添加。
4. 在页面右上角的**查看**下拉列表中，可以选择要查看的资源类型。
5. 如果资源启用了自动登录并启用了 SSO，自动登录列会显示 SSO；如果启用了自动登录并使用资源系统账号，则会显示 图标。

4. 如果资源被资源组引用，引用列会出现一个图标。点击该图标，可查看资源被哪些资源组引用了。

点击图标，可跳转到资源组页面。

4.2.2. 添加 HTTP/HTTPS 资源

1. 选择**基础功能>资源**，点击**添加**。
2. 在**基础配置**页签的**类型**下拉框中选择 **HTTP** 或 **HTTPS**，设置资源的基本参数，点击**确定**。



参数	说明
名称	资源名称。
显示名称	Web 资源的显示名称，配置后将显示在客户端资源列表中。
备注	资源的备注信息。

使用源地址	勾选表示用户访问资源时不走 VPN 网关代理，系统返回用户的地址为内部服务器的真实地址，否则为通过系统代理转换后的地址。推荐不勾选此选项。 勾选后不能进行自动登录和缓存/压缩配置。
地址	资源的内部 IP 地址/域名和端口号。 如果资源地址填写域名，点击查看页面的**更新 Hosts 文件**按钮可将域名对应的 IP 关系更新到 hosts 文件中， 以提高访问性能。
首次访问路径	不填表示根路径。
上传文件大小限制	限制 SSL VPN 用户或远程访问 IPSec VPN 用户上传文件的大小。
智能递推	勾选表示启用智能递推，目前仅支持 HTTP 和 HTTPS 资源。 对于嵌套了其他服务器或数据库链接的网站资源，管理员只需添加网站主页资源到 SSL VPN 资源池并指定递推范围，即可实现用户对这些嵌套链接资源的访问，而无需将这些嵌套的资源链接也逐一添加到 SSL VPN 资源池。 启用智能递推后，需要在**智能递推**页面指定递推范围。对于访问速度较慢的网页，还可以为其添加优化策略。
自动登录	勾选表示启用自动登录，用户访问该资源时无需输入用户名和密码等参数即可登录。勾选后出现**认证配置**和**高级设置**页签，需要根据实际情况配置自动登录所需参数信息。

3. 点击**缓存/压缩**页签，配置资源的缓存和压缩策略，点击**确定**。

勾选**全局设置**，表示使用全局设置中的缓存/压缩策略设置；不勾选则需自定义缓存/压缩策略，参数含义同全局设置。

4. 如果在**基础配置**页签勾选了**自动登录**，则需要点击**认证配置**页签，进行认证相关的配置，然后点击**确定**。

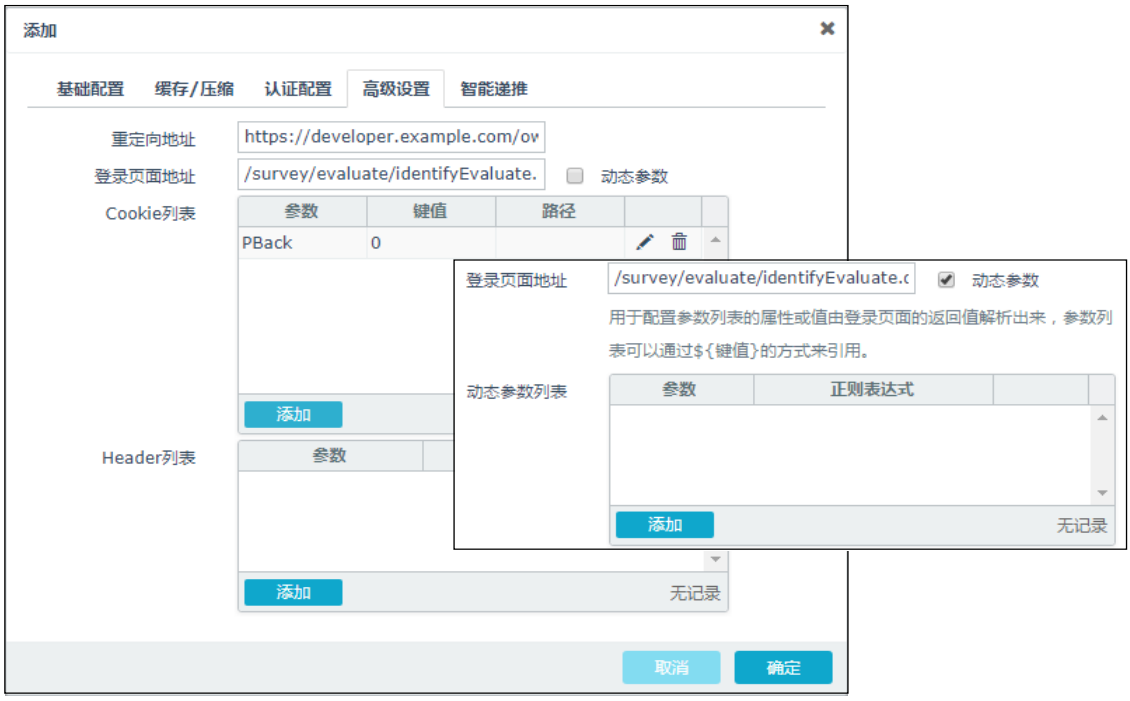
参数	说明
SSO	即单点登录（Single Sign On），表示在多个相互信任（使用同一个认证服务器或使用相互信任的认证服务器）的应用资源中，用户只需要登录一次，就可以访问所有应用资源。目前仅支持 Web 模式 SSL VPN。 如果勾选，SSL VPN 用户登录 Portal 后，无需再次登录即可访问资源列表中的应用资源。
使用资源系统账号	SSL VPN 用户使用独立的账号访问目标资源。 如果勾选，SSL VPN 用户登录 Portal 后，首次访问该资源时须输入访问该资源所使用的独立用户名和密码。 如果使用资源系统账号，**高级配置**中的**登录页面地址**不能为空。
用户可编辑	勾选表示允许 SSL VPN 用户登录 Portal 后自行修改资源账号密码。 仅当开启**使用资源系统账号**时可配。
认证地址	资源服务器上存储用户认证信息的 URL 地址。 启用自动登录时必须填写认证地址。
参数列表	用户自动登录所需参数，缺省为 username 和 password，需要设置键值，即用户名和密码。 如果勾选 SSO，则无需设置此两项参数，其键值将被 Portal 登录时提供的值所替代。

提示：SSO和使用资源系统账号一般不同时启用。如果同时勾选，表示默认使用SSO的用户名和密码访问目标资源，用户可登录Portal进行修改。

如果使用资源系统账号，用户登录 Portal 后，在资源列表中可以看到资源后面有个图标。首次登录，可以点击该图标，设置访问该资源所使用的用户名和密码。VPN 网关将自动学习该用户名和密码，用户后续登录 Portal 后即可直接访问该资源。用户访问该资源的用户名和密码发生变更

时，还可以点击图标进行修改，更换 VPN 网关上存储的用户名和密码信息。

5. 如果在**基础配置**页签勾选了**自动登录**，则可以点击**高级设置**页签，对相关内容进行配置，然后点击**确定**。



参数	说明
重定向地址	登录成功后重定向到的网页地址。有些网站登录后需要重定向才能继续访问。
登录页面地址	用于输入认证信息的登录网页地址。有些网站需要先访问登录页面才能完成认证。
动态参数	如果认证参数中包含动态变化的内容，可以通过指定动态参数来完成认证。 勾选后需要设置动态参数列表。
动态参数列表	包括键值和正则表达式。 定义完动态参数后，可以在**认证配置**的**参数列表**中通过${参数键值}的方式来引用。

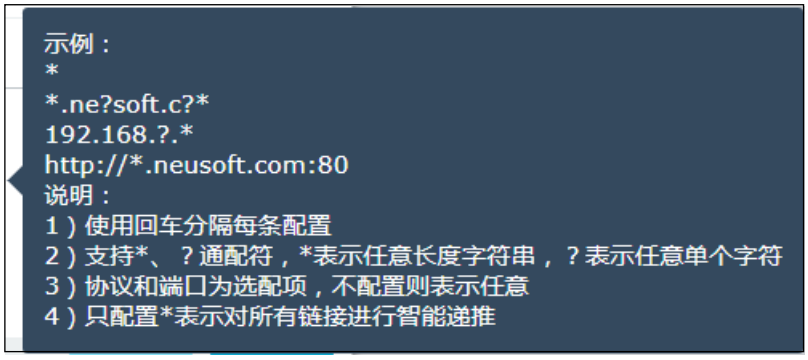
Cookie 列表　　进行后续访问时的必要 Cookie。

Header 列表　　有些站点需要特定的 Header 字段才能完成登录，请填入所需字段。

6. 如果在**基础配置**页签勾选了**智能递推**，则可以点击**智能递推**页签，点击**添加**，添加智能递推的 URL 地址范围，点击**确定**。

对于个别访问慢的 URL，还可以点击高级，设置页面优化策略。

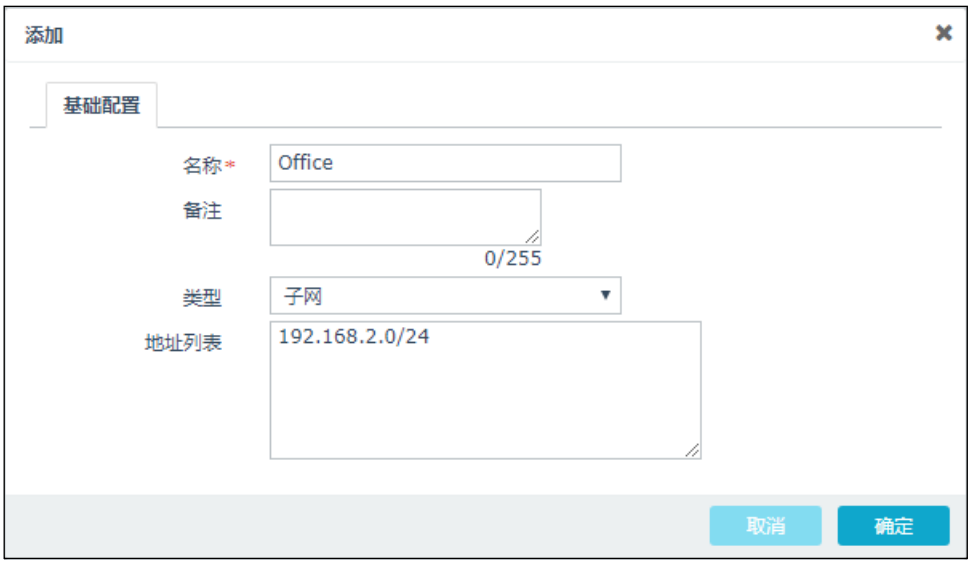
鼠标指向**智能递推**文本框时，系统会提示 URL 地址的格式：



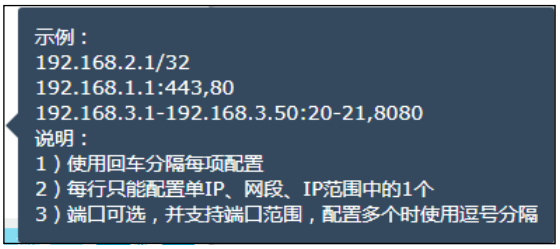
7. 点击**确定**，完成资源的添加。

4.2.3. 添加子网资源

1. 选择**基础功能>资源**，点击**添加**。
2. 在**基础配置**页签的**类型**下拉框中选择**子网**，设置资源的基本参数。



鼠标指向地址列表文本框时，系统会提示子网地址的格式：



3. 点击**确定**。

4.2.4. 添加远程桌面/远程 Web 应用/FTP/SSH/TELNET 资源

1. 选择**基础功能>资源**，点击**添加**。
2. 在**基础配置**页签的**类型**下拉框中选择**远程桌面**、**远程 Web 应用**、**FTP**、**SSH** 或 **TELNET**，设置资源的基本参数。

如果添加远程桌面、SSH 或 TELNET 资源，需要填写连接的远程主机地址和端口号，以及远程登录使用的账号和密码。

如果添加远程 Web 应用资源，需要指定 Web 应用基于的远程桌面资源和应用服务器地址。访问远程 Web 应用时，需要先登录远程桌面。

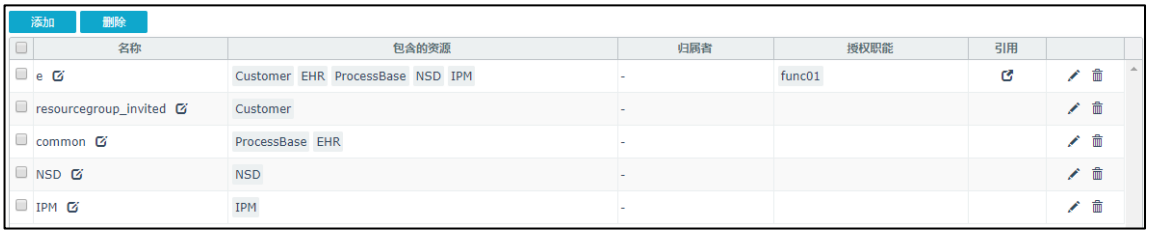
如果添加 FTP 资源，还可以填写根路径。

3. 点击**确定**。

4.3.资源组

SSL VPN 用户或远程访问 IPSec VPN 用户可访问的资源可以划分为不同的组，并在 VPN 策略中引用。

1. 选择**基础功能>资源组**。
2. 查看已创建的资源组。

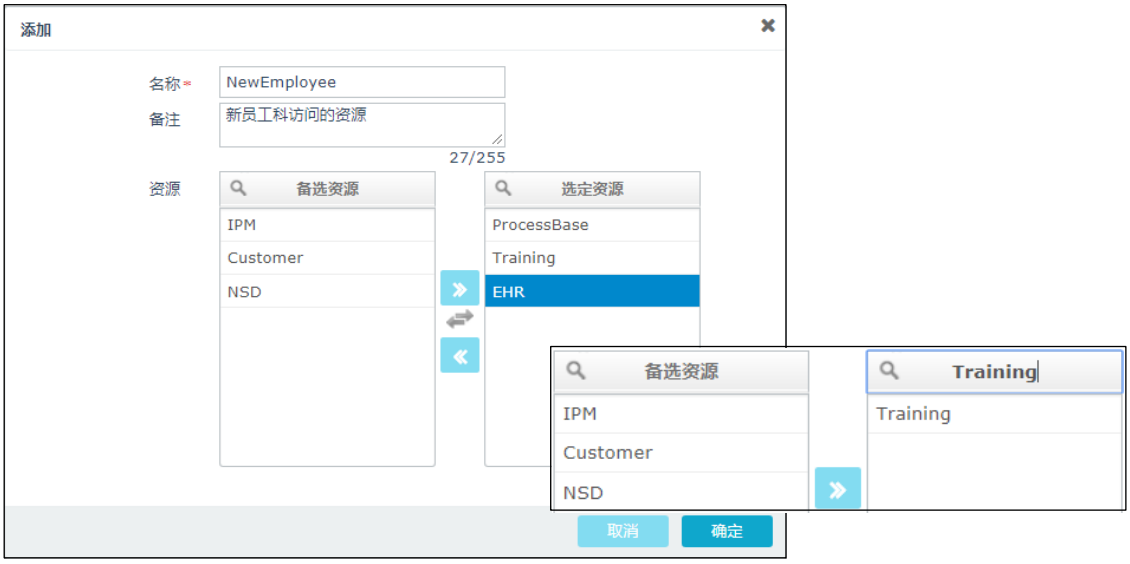


归属者表示此资源组是由哪个分级管理员创建的，如果是由系统管理员（Root、管理员）创建的，则归属者显示“-”，授权职能表示该资源组都被分配给了哪些分级管理职能。

如果资源组被 VPN 策略引用，引用列将出现一个 图标。点击该图标，可查看该资源组被哪些 VPN 策略引用了。

点击 图标，可跳转到 VPN 策略页面。

3. 点击**添加**，添加资源组，选择允许访问的资源。



添加资源时可以通过列表表头的搜索功能查找要选定或取消选定的资源条目。

4. 点击**确定**。

4.4.用户

配置 SSL VPN 隧道或远程访问 IPSec VPN 隧道之前，需要事先添加 VPN 用户。

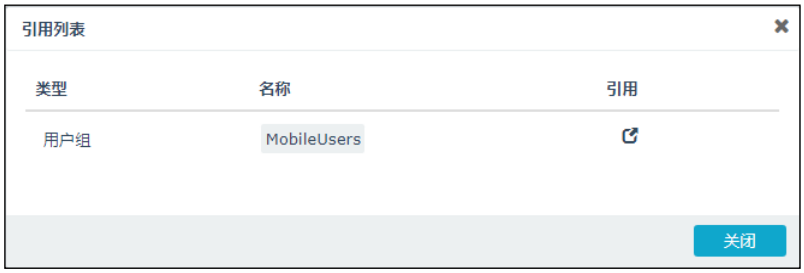
本节介绍如下配置：

- 查看/创建 VPN 用户
- 配置密码策略

4.4.1. 查看/创建 VPN 用户

1. 选择**基础功能>用户**。
2. 查看已创建的 VPN 用户。

如果用户被用户组引用，引用列将出现一个图标。点击该图标，可查看用户被哪些用户组引用了。



点击图标，可跳转到用户组页面。

3. 点击**添加**，在弹出的对话框中输入用户信息。

勾选用户详细信息时，可设置用户的姓名、公司、部门、职务、备用号码、办公号码、备注等信息。

取消勾选永不过期，可点击有效期到文本框，通过弹出的时间控件选择具体到期时间。

4. 点击**确定**。以同样方式创建更多用户。
5. 如果想批量编辑用户详细信息，可将当前用户信息导出，编辑后再导入。
   a. 点击**导出**按钮，导出当前用户信息为 csv 文件。
   b. 新建 excel 文件，选择**数据>自文本**，导入已导出 csv 文件中的用户信息。注意文件原始格式选择 UTF-8，分隔符号选择逗号。
   c. 编辑用户信息，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。

4.4.2. 配置密码策略

1. 选择**基础功能>用户**，点击**配置密码策略**。
2. 根据信息安全等级要求设置密码策略。

3. 点击**提交**。

4.5.用户组

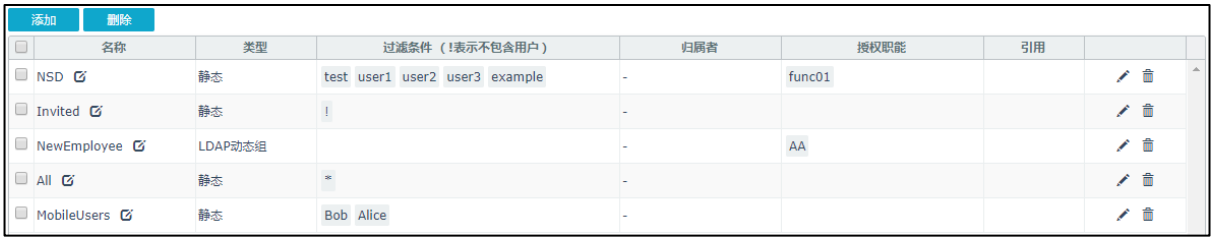
为了方便管理，可将具有相同属性或访问需求的用户划分为一个用户组。用户组分为静态和 LDAP 两种类型：

- 静态用户组用于精确控制具体用户权限的情况。
- LDAP 用户组用于通过某些条件控制一类用户权限的情况，还可以结合筛选条件进行进一步的权限控制。

本节介绍如下配置：

4.5.1. 查看用户组

1. 选择**基础功能>用户组**。
2. 查看已创建的用户组。



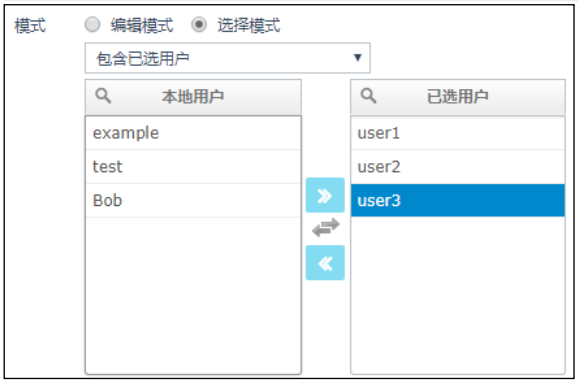
归属者表示此用户组是由哪个分级管理员创建的，如果是由系统管理员（Root、管理员）创建的，则归属者显示“-”，授权职能表示该用户组都被分配给了哪些分级管理职能。

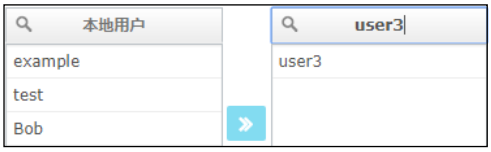
3. 如果用户组被 VPN 策略引用，引用列将出现一个图标。点击该图标，可查看该用户组被哪些 VPN 策略引用了。

点击图标，可跳转到 VPN 策略页面。

4.5.2. 添加静态用户组

1. 选择**基础功能>用户组**。
2. 点击**添加**，输入用户组名称，在**类型**下拉框中选择**静态**，并通过编辑或选择的方式将用户添加到用户组中。





为用户组指定用户时，可以指定要包含的用户，也可以指定不包含的用户。

使用编辑模式时，需要手动输入用户名称，多个用户名称之间用逗号分隔。

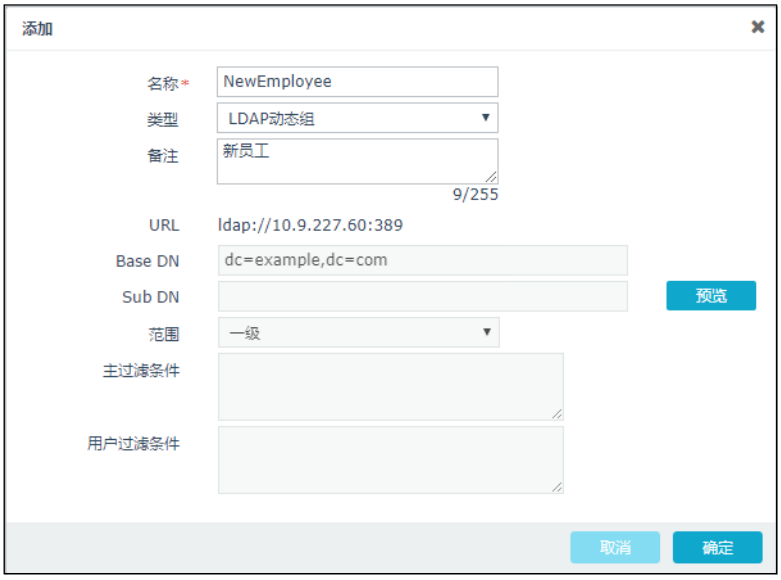
使用选择模式时，可以通过列表表头的搜索功能查找要选定或取消选定的用户。

3. 点击**确定**。

4.5.3. 添加 LDAP 动态用户组

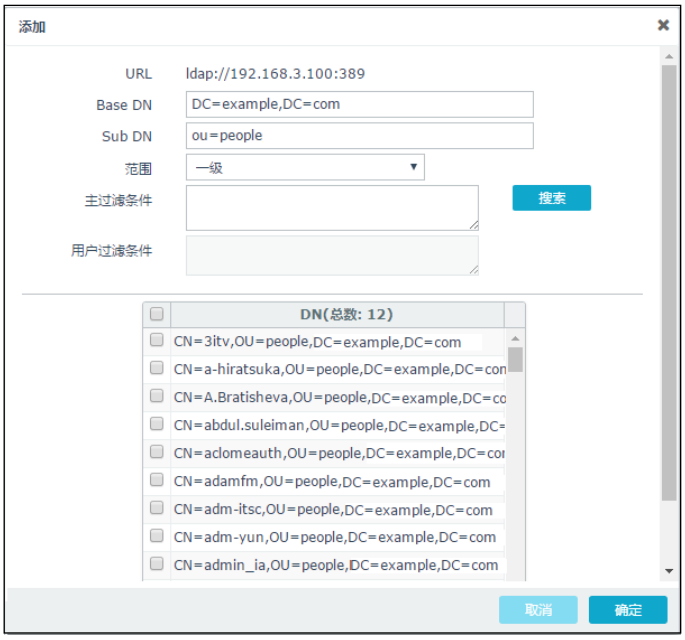
如果使用 LDAP 服务器作为缺省认证服务器且用户组成员是动态变化的（如员工离职或新员工入职），可以通过添加 LDAP 动态组减轻管理员的配置负担。

1. 选择**基础功能>用户组**。
2. 点击**添加**，输入用户组名称，在**类型**下拉框中选择 **LDAP 动态组**。



提示：需要提前添加LDAP认证服务器，并在全局设置中选择LDAP认证服务器，同时要保证VPN网关与LDAP服务器可以正常通信。

3. 点击**预览**，输入过滤条件并点击**搜索**，可以查看符合条件的用户信息。



4. 在打开的对话框中依次点击**确定**。

4.6.VPN 策略

配置 SSL VPN 隧道或远程访问 IPSec VPN 隧道之前，可事先配置 VPN 策略。通过配置 VPN 策略，可限制用户对资源的访问权限。

VPN 策略遵从拒绝优先原则。例如，如果策略 A 中用户组 1 可以访问资源组 1 和资源组 2，但策略 B 中用户组 1 不可以访问资源组 2 和资源组 3，则用户组 1 中的用户不能访问资源组 2。

此外，为了方便管理员查询用户权限，VPN 网关还提供了测试用户匹配的功能。

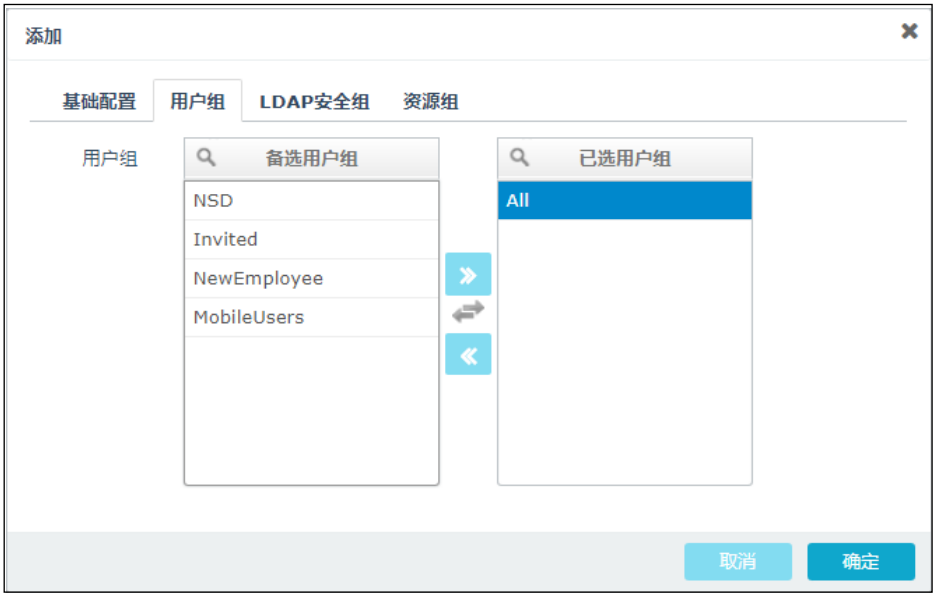
本节介绍如下内容：

4.6.1. 创建 VPN 策略

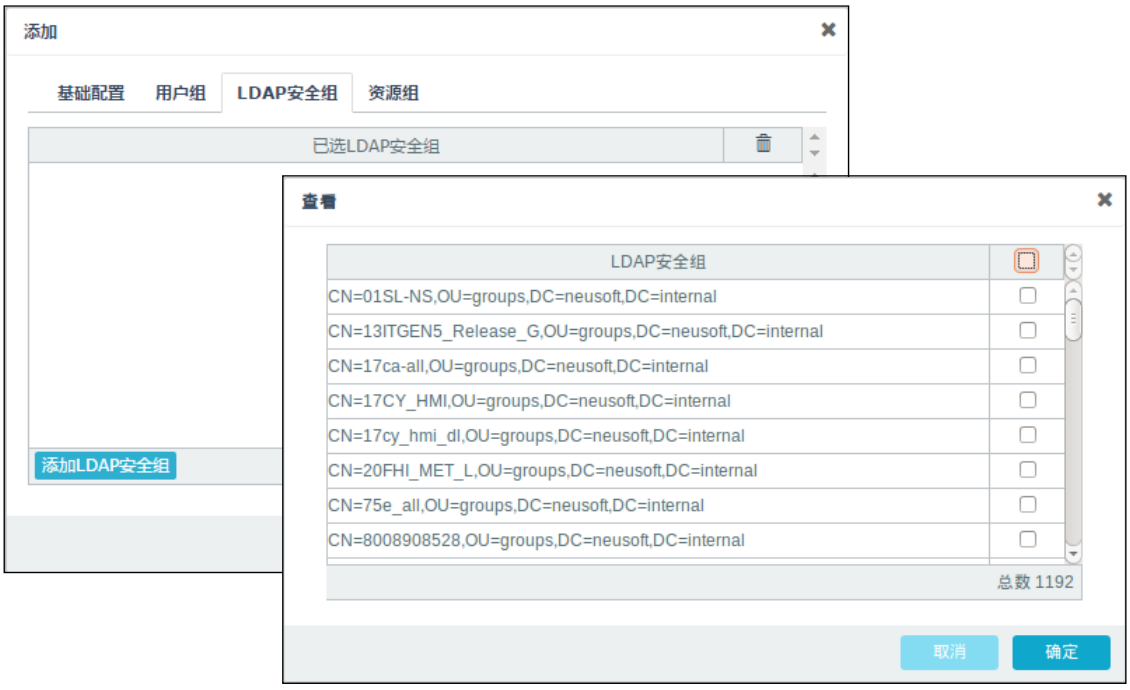
1. 选择**基础功能> VPN 策略**。
2. 点击**添加**，在**基础配置**页签进行相关配置。

勾选**时间表**时，需要设置策略生效时间，包括单次生效和循环生效两种。

3. 点击**用户组**页签，选择允许访问资源的静态用户组。



4. 也可点击 **LDAP 安全组**页签，通过选择事先配置的 LDAP 安全组来添加授权用户。



如果选择安全组，VPN 网关将使用 LDAP 服务器上已配置的安全组控制用户访问，而无需管理员事先添加用户和用户组。要使用安全组，需要具备两个前提条件：

- **系统管理>认证服务器**：已正确配置 LDAP 服务器。
- **基础功能>全局设置**：已选 LDAP 认证服务器，已正确配置 LDAP 安全组信息。

5. 点击**资源组**页签，选择允许用户访问的资源组。

6. 点击**确定**。

7. 查看创建的 VPN 策略。

归属者表示此 VPN 策略是由哪个分级管理员创建的，如果是由系统管理员（Root、管理员）创建的，则归属者显示“-”。

8. 点击**名称**右侧图标，可以按字母顺序（升序降序）对 VPN 策略排序。

9. 点击**单次有效时间**右侧图标，可以按时间顺序（升序降序）对 VPN 策略排序。

10. 点击列表右侧操作区域中的图标，可以对此条 VPN 策略进行**克隆**操作。

11. 点击列表中的策略名、用户组/安全组名、资源组名，可以对此条 VPN 策略进行**一键跳转**操作。

    a. 点击列表中策略名，可以跳转至**快速运维**界面，即可实现策略名的快速搜索。

    b. 点击列表中用户组/安全组名，可以跳转至**用户组**编辑界面，即可实现用户组的快速编辑。

    c. 点击列表中资源组名，可以跳转至**资源组**编辑界面，即可实现资源组的快速编辑。

4.6.2. 快速创建 VPN 策略

1. 选择**基础功能>VPN 策略**。

2. 点击**添加**，在**基础配置**页签中选中**快速新建**，可以快速新建 VPN 策略、资源组、用户组。

3. 可在**用户**页签中，快速配置用户组。
4. 可在 **IP** 页签中，快速配置资源组及子网资源。
5. 其他配置请参考 4.6.1，进行相关配置。

4.6.3. 测试用户权限匹配

1. 选择**基础功能> VPN 策略**。
2. 点击列表上方的**测试用户匹配**按钮，可测试 VPN 策略是否生效。

- 具备 Web 资源访问权限时：

- 用户不存在或没有资源访问权限时：

4.7.快速运维

快速运维功能可以快速的查看 VPN 策略、用户组、资源组、资源等信息，并且可以对 VPN 策略、用户组、资源组、资源等信息进行快速编辑操作。

1. 选择**基础功能>快速运维**。
2. 在列表上方的输入框中，输入相应的搜索条件，再点击**搜索**按钮，可查看到与输入条件相匹配的策略、用户组、用户、资源组、资源等信息。
3. 可以通过点击列表中的策略名、用户组名、资源组名、资源名，进行快速编辑操作。

4. 点击**导出**按钮，可将当前列表中显示的数据保存到本地。

4.8.超时策略

配置 VPN 隧道之前，可针对不同的用户配置不同的超时策略，包括 Web 模式超时时间、隧道模式超时时间和会话超时时间。系统自带一条 Default 策略，如果对用户没有配置其他超时策略，系统将对所有 VPN 用户执行此缺省策略。

1. 选择**基础功能>超时策略**。
2. 查看缺省超时策略。

3. 点击**添加**，在弹出对话框中设置策略名称、超时时间和要应用该超时策略的用户。

参数	说明
Web 模式超时时间	Web 模式下，SSL VPN 用户不进行操作后，连接能够保持的时间。0 表示永不超时。 系统会在超时前 5 分钟进行提醒，用户可以通过刷新页面等操作刷新超时时间。
隧道模式超时时间	隧道模式下，SSL VPN 用户不进行操作后，连接能够保持的时间。0 表示永不超时。 达到超时时间后，连接直接断开，客户端用户可以重新连接或开启自动重连功能。
会话超时时间	VPN 连接能够保持的时长。0 表示永不超时。 不管 VPN 用户是否进行操作，达到会话超时时间后，连接都会断开。 会话超时时间针对所有类型的 VPN 隧道都生效。
模式	可以通过编辑模式或选择模式指定要应用超时策略的用户。
包含的用户	要应用超时策略的用户。多个用户名称之间用逗号分隔。

4. 点击**确定**。

4.9.Web 模式 SSL VPN

如果用户要访问的资源都是 Web 应用，推荐使用 Web 模式 SSL VPN。通过配置 Web 模式 SSL VPN，SSL VPN 用户无需安装任何软件即可在 Windows、Linux、Mac OS、Android、iOS 等主流操作系统登录 SSL VPN Portal 来访问 HTTP 或 HTTPS 资源。

提示：Web模式SSL VPN可以代理仅使用HTML、CSS、Javascript开发的网站。对于采用其他技术（如flash、activeX、VBScript）开发的网站，并且网站涉及到URL，不推荐使用Web模式SSL VPN。

Web 模式 SSL VPN 通过统一的 Portal 入口页面为用户提供资源访问链接，VPN 网关支持自定义 Web 模式 SSL VPN 的 Portal 入口页面。

为方便用户使用，VPN 网关还提供了邀请码和系统通知功能。如果配置了邀请码，管理员和已注册 SSL VPN 用户可以邀请其他用户注册。如有需要，管理员可以通过 Portal 入口页面统一发布通知消息。

本节介绍如下内容：

4.9.1. 配置 Web 模式 SSL VPN 隧道

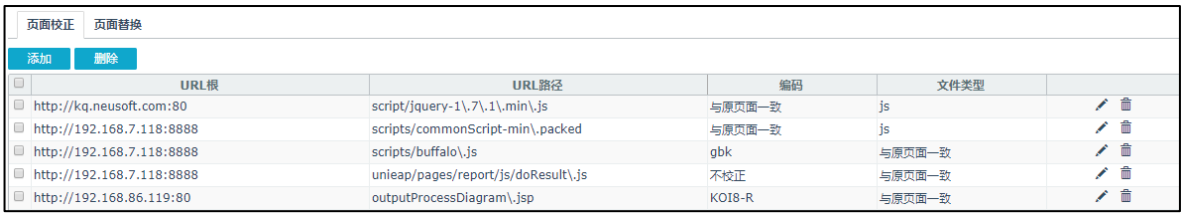
1. 选择**基础功能> Web 模式 SSL VPN > Portal**。
2. 启用 Web 模式 SSL VPN 以及访问日志功能，设置服务 IP 及端口，选择本地证书，其他参数使用默认配置。

参数	说明
IP 地址	SSL VPN Web 入口页面的 IP 地址及端口号，缺省为 0.0.0.0:443，表示所有接口的所有 IP 地址都可做为用户访问地址。
本机域名	如果设置 SSL VPN 服务对应的域名，用户也可通过域名访问该服务。
HTTP 重定向到 HTTPS	勾选表示开启重定向，SSL VPN 用户访问 Portal 时发起的 HTTP 访问会重定向为 HTTPS 访问。
本地证书	SSL VPN 服务器向客户端浏览器证明自身身份的数字证书，建议使用权威 CA 机构颁发的服务器证书。
页面模板	可选择缺省的 Web 页面模板，也可点击**配置模板**按钮，自行创建新的模板。
登录验证码	用户登录时，在 Web 上是否需要填写验证码。
邀请码	点击**配置邀请码**按钮配置邀请码，用于邀请用户注册成为 SSL VPN 系统的网络用户。需要事先创建用户组和 VPN 策略，控制被邀请人的资源访问权限。
页面校正	（可选）点击**配置页面校正**按钮配置页面校正，用于对特殊的 URL 路径的编码格式、文件类型进行配置，以及配置一些特殊的页面替换规则，详见本节第 7 点中的描述。

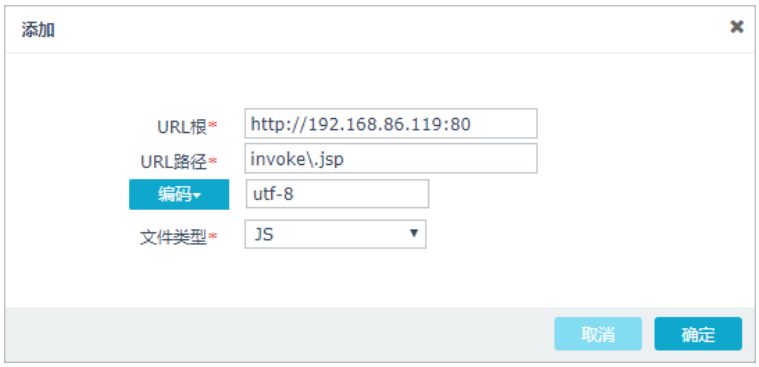
3. 点击**提交**。
4. 仅当启用或禁用 Web 模式 SSL VPN 服务时，才需点击**重启服务**。
5. 在调试阶段，可点击**清空缓存**更新 VPN 网关上的缓存内容。
6. 如果正确配置了用户、用户组、资源、资源组和 VPN 策略，已授权 SSL VPN 用户可在浏览器中输入 Portal 入口页面地址 **https://portal-IP/domain:port**（如 https://vpn.neusoft.com:443），登录后访问授权资源。

提示：如果服务端口使用缺省端口号443，访问Portal时可以不输入端口号。

7. 点击**配置页面校正**按钮可以配置页面校正。包括页面校正和页面替换，可以更换标签页查看。



点击**页面校正 > 添加**，可以添加页面校正配置。



参数	说明
URL 根	URL 的协议、域名、端口部分
URL 路径	URL 的子路径
编码	当 URL 路径的实际编码格式和访问 URL 得到的响应中不一致时，在此处可以配置 URL 路径的实际编码格式，保证 Web 模式 SSLVPN 页面显示正常
文件类型	当 URL 路径的实际文件类型和访问 URL 得到的响应中不一致时，在此处可以配置 URL 路径的实际文件类型，保证 Web 模式 SSLVPN 页面显示正常

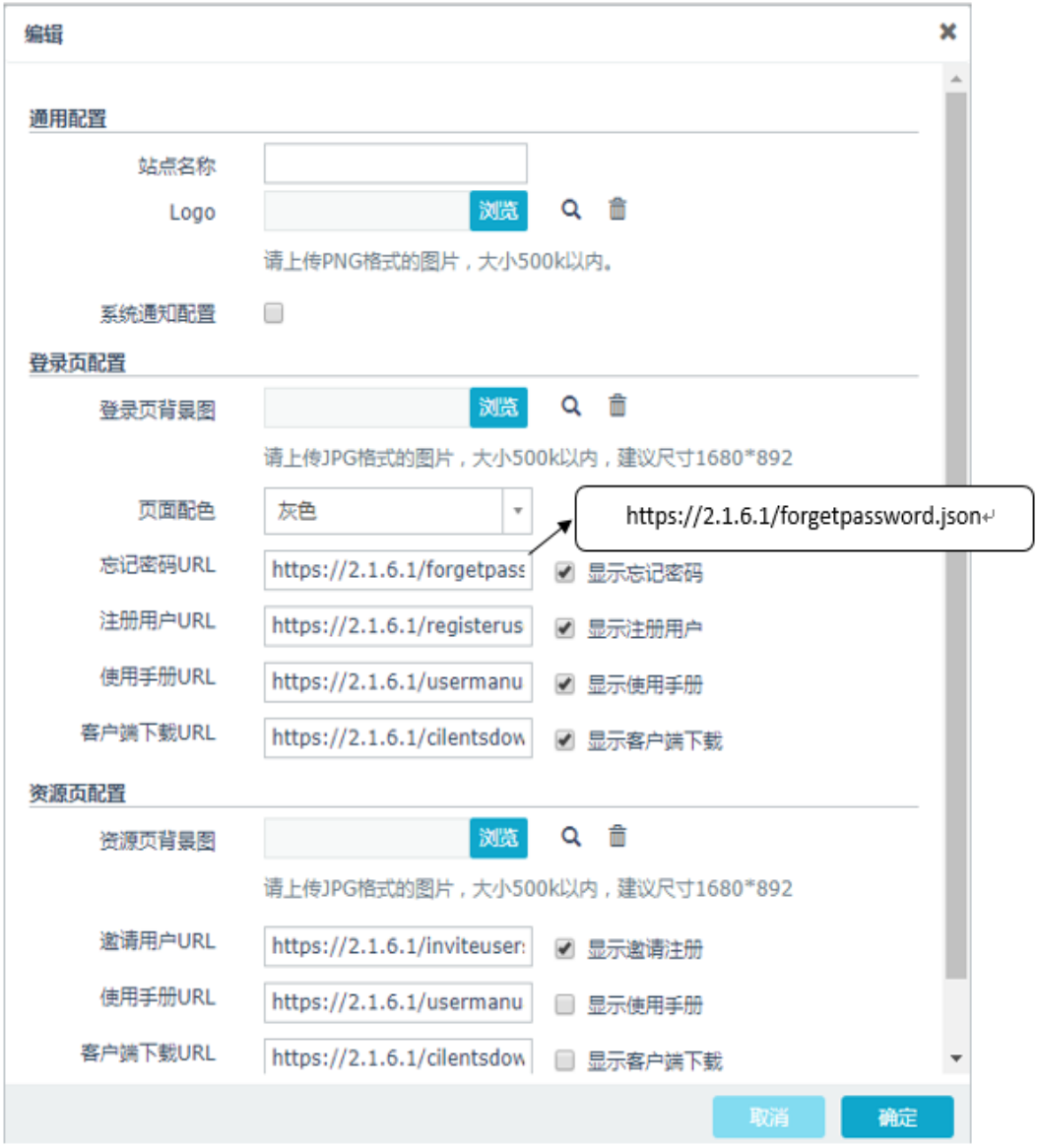
点击**页面替换 > 添加**，可以添加页面替换配置。

参数	说明
URL 根	URL 的协议、域名、端口部分
URL 路径	URL 的子路径
替换前	指定要进行替换的页面中的标签
替换后	表示将替换前的标签替换成此形式

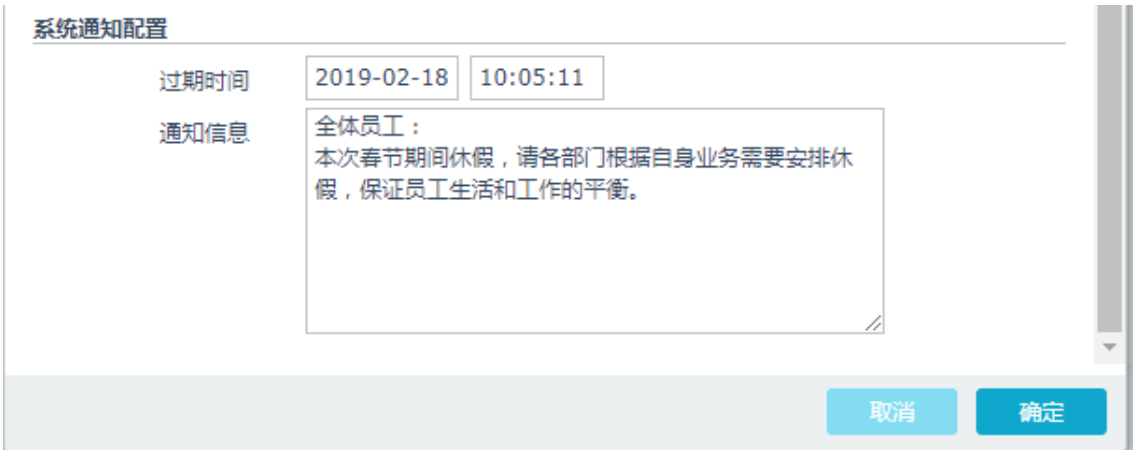
4.9.2. 配置页面模板

1. 选择**基础功能> Web 模式 SSL VPN**。
2. 点击**页面模板**后面的**配置模板**按钮，进入页面模板配置页面。

- 点击 GridView 对应的 图标，编辑页面模板的配置信息，设置站点名称、上传背景图片、根据需要设置 URL（也可以不设置）等等。

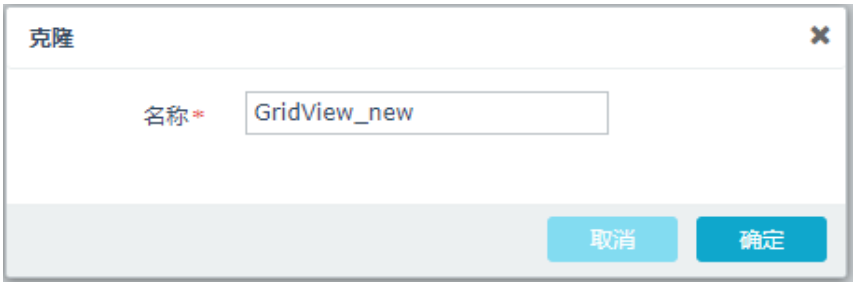


- 勾选**通用配置**中的**系统通知配置**，在**资源页配置**下面的**系统通知配置**中配置要下发的通知内容和通知的过期时间。



点击确定后，如果此模板正在使用，SSL VPN用户在浏览器中输入Portal入口页面地址https://portal-IP/domain:port（如https://portal.neusoft.com:443），登录Portal后可见通知消息。

- 点击 GridView 对应的，下载模板基础代码。
- 点击 GridView 对应的，设置克隆页面模板的名称，克隆新的模板。



点击 **导入**，可导入之前导出的页面模板或者自定义的符合规则的模板。

- 点击 GridView_new 对应的，可以删除未使用的非默认模板。

点击**页面模板**后面的图标，可预览默认的页面模板的界面风格。

3. 点击**确定**。
4. 如果新添加页面模板，点击左侧目录树 **Web 模式 SSL VPN**，返回主配置页面，选择新添加的页面模板，点击**提交**。
5. SSL VPN 用户在浏览器中输入 Portal 入口页面地址 **https://portal-IP/domain:port**（如 https://portal.neusoft.com:443），登录 Portal 后可见新页面模板效果。

4.9.3. 配置邀请码

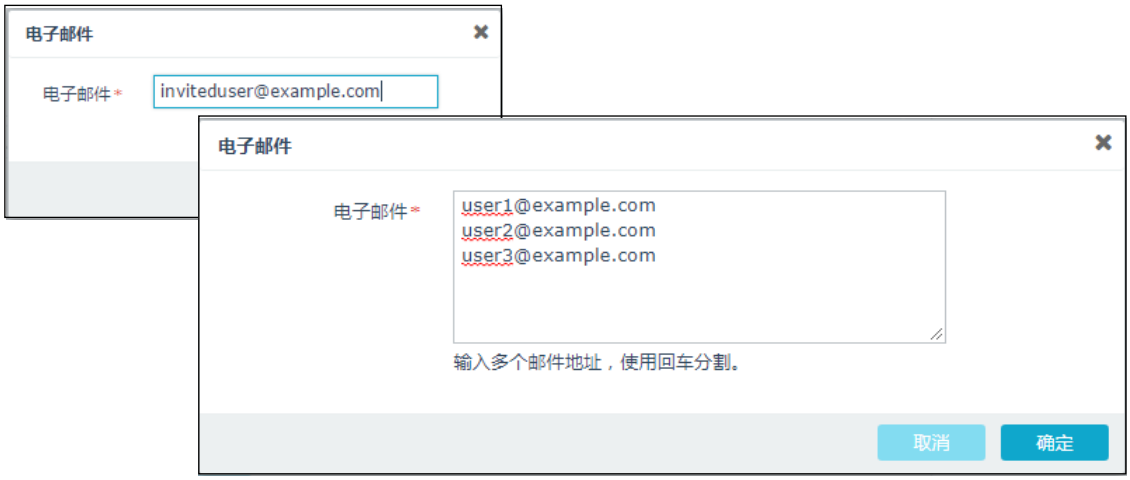
1. 选择**基础功能> Web 模式 SSL VPN**。
2. 点击**邀请码**后面的**配置邀请码**按钮，配置邀请码相关选项。
3. 启用邀请功能，设置可邀请用户数以及默认用户组，点击**提交**。

提示：需要在**基础功能>用户组**中事先创建一个空用户组，并在**基础功能>VPN策略**中为其指定资源访问权限。

4. 在邀请码列表中点击**创建**，创建邀请码。

5. 点击电子邮件列中邀请码对应的图标，输入被邀请人用于接收邀请码的邮件地址，然后点击**确定**，可将该邀请码发送给指定的被邀请人。

点击表头的图标，可批量发送邀请码。



提示：需要事先在**系统管理>邮件服务器**中设置发送邮件使用的邮件服务器地址和发件人信息，同时保证VPN网关与被邀请人使用的邮件服务器可以通信。

6. 点击邮件模板区域的，编辑发送邮件邀请码时使用的邮件正文，点击**提交**。

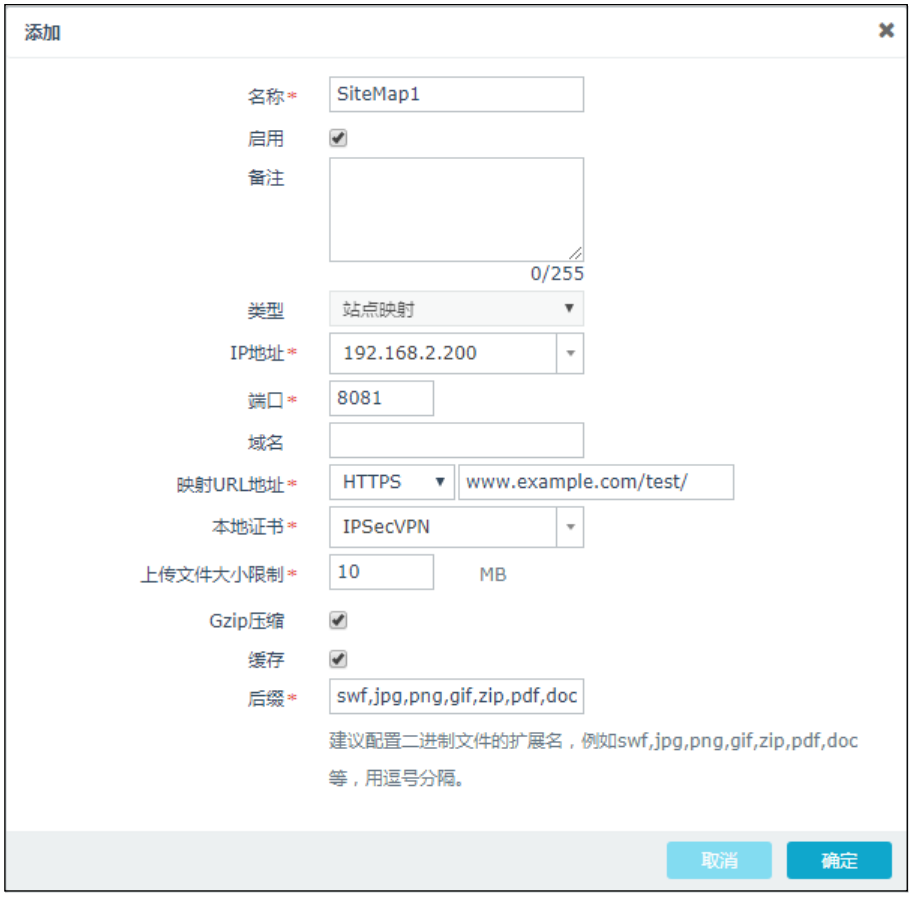
7. SSL VPN 用户在浏览器中输入 **https://portal-IP/domain:port**（如 https://portal.neusoft.com:443），登录 Portal 后可见**邀请注册**按钮，点击该按钮可邀请他人注册成为 SSL VPN 用户。

8. 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。

4.9.4. 配置站点映射

某些企业 OA 系统逻辑复杂，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 OA 系统的 Web 应用。这样，用户就可以通过访问 VPN 网关的指定 IP 和端口直接访问 OA 系统应用了。

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。



参数	说明
IP 地址	VPN 网关提供站点映射的服务接口 IP 地址。
端口	VPN 网关提供站点映射的服务端口。
域名	为站点映射服务配置的域名（选填）。
映射 URL 地址	映射的内网资源 URL 地址。
本地证书	VPN 网关作为 SSL VPN 服务器向客户端浏览器证明自身身份的数字证书，建议使用权威 CA 机构颁发的服务器证书。
上传文件大小限制	允许用户上传到映射站点的文件大小。

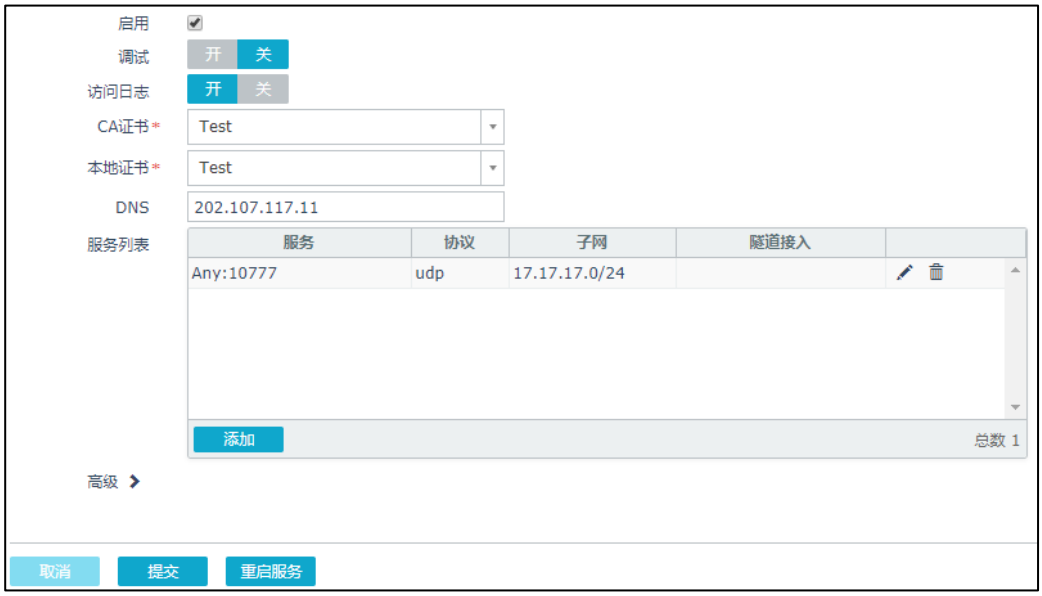
Gzip 压缩	是否对用户下载文件进行 Gzip 压缩传输。
缓存	是否缓存用户下载的文件。
后缀	通过文件后缀指定缓存的文件类型。

3. 点击**确定**。

4.10.隧道模式 SSL VPN

如果用户要访问的资源除了 Web 应用，还有其他如 FTP、SSH、Telnet、RDP 等协议类型的应用，推荐使用隧道模式 SSL VPN。隧道模式 SSL VPN 需要用户安装客户端软件，但操作简单、使用方便。

1. 选择**基础功能> 隧道模式 SSL VPN**，启用隧道模式 SSL VPN 并进行相关配置。



参数	说明
调试	开启调试功能后，可在**日志>调试>隧道模式调试信息**页面查看隧道调试信息。
访问日志	开启 SSL VPN 访问日志记录功能。
CA 证书	企业 CA 证书，用于颁发 SSL VPN 服务器和客户端证书。 协商隧道时，该 CA 证书将被推送给客户端，用于客户端验证 SSL VPN 服务器证书。 启用双向认证时，该 CA 证书还将用于验证 SSL VPN 客户端证书。
本地证书	SSL VPN 服务器证书，用于向客户端证明自身身份的数字证书。
DNS	推送给客户端的 DNS 服务器 IP 地址。
服务列表	要提供的 SSL VPN 服务。

2. 点击**高级**，配置以下信息：

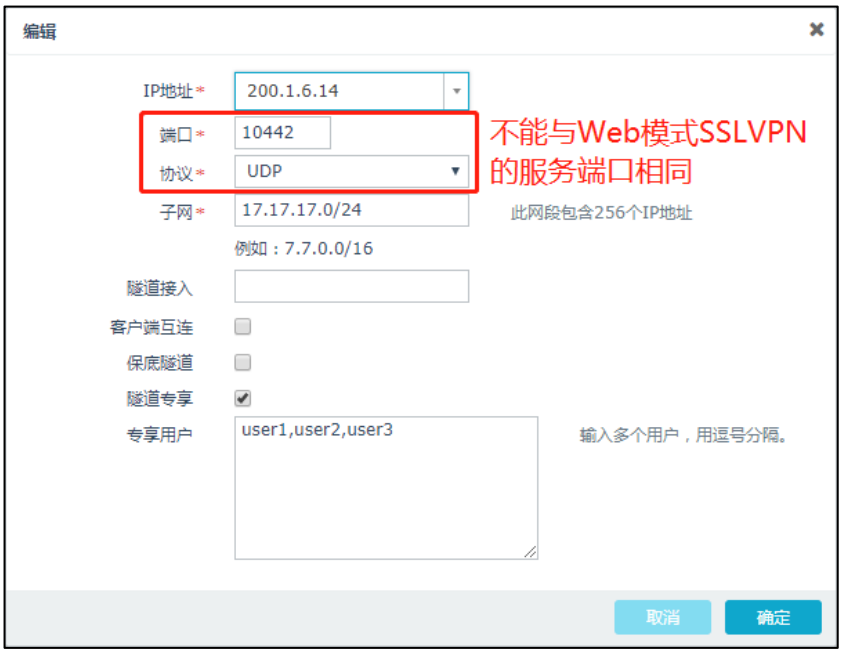
参数	说明
双向认证	勾选启用双向认证。仅 E-Key 版 Windows SSL VPN 客户端支持双向认证。
推送网关	勾选后，客户端所有流量都走 SSL VPN 隧道。
数据压缩	对隧道数据进行压缩。
摘要算法	管理员可以根据需要选择摘要算法。
加密算法	管理员可以根据需要选择加密算法。
多点登录	勾选后，允许同一用户在多个终端同时登录，但会占用多条并发。启用后，用户绑定 IP 将失效。
用户 IP 绑定	指定为用户客户端分配的 IP 地址。指定不在服务列表 > 子网中的 IP 绑定不会生效，启用多点登录也将导致绑定失效。
推送 Hosts	勾选后，在客户端登录后，服务器会将**网络/策略> Hosts > Hosts 文件**中配置的 Hosts 文件推送给客户端，客户端会根据服务器推送的 Hosts 文件进行域名解析。
主页地址	（可选）配置在客户端连接成功后默认打开的网页地址。目前只有 Windows 客户端支持此功能。

提示：同时开启数据压缩、SHA1&BF-CBC算法以及10442端口服务，iOS客户端才能连接成功。

3. 可以点击 配置用户IP绑定 进行用户 IP 绑定的配置。

点击**提交**后，会提示需要重启隧道模式 SSLVPN 服务，点击**确定**即可。

4. 在**服务列表**中点击**添加**，添加服务和虚拟子网，点击**确定**。



参数	说明
IP 地址	提供 SSL VPN 服务的接口 IP 地址。
端口	提供 SSL VPN 服务的端口。
协议	提供 SSL VPN 服务的协议。
子网	用于为客户端分配虚拟 IP 地址的地址池，可以是任意网段，但是不能和真实子网相同，不同服务的子网也不能相同。

隧道接入	发布给 SSL VPN 用户的最终访问地址。 当 VPN 网关工作在单臂模式且映射到出口防火墙的服务端口有变化时，需要填写隧道接入地址，即 SSL VPN 服务映射后的 IP 地址和端口号。
客户端互联	勾选后，访问同一服务的 VPN 客户端之间可以互相访问。
隧道专享	勾选后，该隧道仅供指定的专享用户使用。不勾选，则允许任意用户使用。
专享用户	指定专享隧道的 SSL VPN 用户。
保底隧道	勾选后，表示此条服务为保底隧道，客户端连接时，服务器除了推送其他的服务，最后还会默认推送此条保底隧道。客户端在连接时，会在最后尝试连接保底隧道。

如果用户网络出口有端口限制，建议添加一条 TCP 443 服务。当服务端口被阻断时，保证客户端用户可以通过 443 端口访问服务。不过，该服务的 IP 地址不能与 Web 模式 SSL VPN 服务的 IP 地址相同。

如果 VPN 网关和内网服务器之间存在路由设备，还需要添加源地址转换规则，将客户端子网地址转换为 VPN 网关内网口的 IP 地址。

5. 点击**提交**。如果遇到问题，可点击**重启服务**，重启 SSL VPN 服务。
6. 东软 NetEye SSL VPN 客户端支持 Windows、MacOS、iOS 和 Android 四种操作系统。如需使用 SSL VPN 客户端访问 VPN 资源，请在 SSL VPN Portal 登录页面下载相应操作系统的客户端软件，解压后安装使用。

4.11.IPSec VPN

系统支持以下两种模式的 IPSec VPN：

- 网关到网关：用于公司总部与分支机构/合作伙伴以及分支机构之间的安全互连。
- 远程访问：用于远程用户的安全移动办公。需要用户在设备上配置 IPSec VPN 连接。远程访问 IPSec VPN 适用于 Windows 7 及以上版本、macOS、iOS 和 Android 系统。

针对各操作系统客户端，IPSec VPN 连接的配置要求如下：

<table>
<tr><th rowspan="2">客户端系统</th><th colspan="2">是否导入证书</th><th rowspan="2">IPSec VPN 连接的配置要求</th></tr>
<tr><th>使用第三方证书</th><th>自己制作证书</th></tr>
<tr><td>Windows 7
及以上</td><td>---</td><td>导入 CA 证书</td><td>IPSec VPN 连接>属性>安全
• VPN 类型：IKEv2
• 数据加密：需要加密（如果服务器拒绝将断开连接）
• 身份验证：使用可扩展的身份验证协议（EAP）Microsoft：安全密码(EAP-MSCHAP v2)（启用加密）</td></tr>
<tr><td>macOS</td><td>---</td><td>导入 CA 证书</td><td>系统偏好设置>网络
新建 VPN 连接：
• 接口：VPN
• VPN 类型：IPSec 上的 L2TP
编辑 VPN 连接：
• 服务器地址：要连接的 VPN 服务器地址
• 账户名称：用户名
• 加密：自动
• 鉴定设置>用户鉴定：密码</td></tr>
<tr><td rowspan="2">iOS</td><td rowspan="2">---</td><td>方法 1：
使用 IKEv2
导入 CA 证书</td><td>设置>通用> VPN >添加 VPN 配置
• 类型：IKEv2
• 服务器/远程 ID：要连接的 VPN 服务器地址
• 用户鉴定：用户名/密码</td></tr>
<tr><td>方法 2：
使用 IKEv1
导入 CA 证书
和个人证书</td><td>设置>通用> VPN >添加 VPN 配置
• 类型：IPSec（IKEv1）
• 服务器：要连接的 VPN 服务器地址
• 账户：用户名
• 密码：用户密码
• 使用证书：勾选
• 证书：选择事先导入的用户个人证书</td></tr>
</table>

Android	导入个人证书	导入 CA 证书、服务器证书和个人证书	**设置>网络和连接>添加 VPN 网络** • 类型：IPSec Xauth RSA • 服务器地址：要连接的 VPN 服务器地址 • 证书：选择已安装的 CA 证书、IPSec 服务器证书和用户个人证书 • 用户认证：用户名/密码 如果不验证服务器证书，则只需导入个人证书。

如需使用自己申请或制作的证书认证，请选择**认证配置>证书>导入**，导入事先申请的 CA 证书和本地证书。如需在 VPN 网关上制作证书，请选择**认证配置>证书>添加**。

注意事项：

- 为 VPN 网关制作服务器证书时，公共名应该为 VPN 服务器的公网 IP 或域名；为远程用户制作个人证书时，公共名需要为该用户的用户名。
- 往 iOS 系统中导入证书时，CA 证书的后缀名.pem 需要改为.cer。如果是通过邮件导入，需要先将证书存储到 iCloud 再到文件夹中点击该证书进行安装。

4.11.1. 配置远程访问 IPSec VPN 隧道

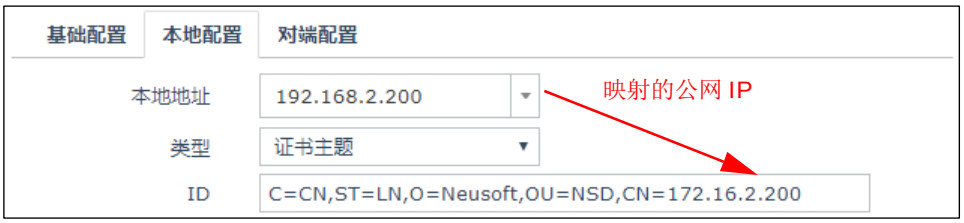
1. 选择**基础功能> IPSec VPN**。
2. 在隧道列表中，可以看到系统默认的远程访问 IPSec VPN 隧道（RemoteAccess）。

3. 点击 编辑隧道配置信息。
   a. 在**基础配置**页签，启用/禁用隧道、启用/禁用记录日志功能、填写备注信息并配置认证方式。

参数	说明

认证模式	支持证书认证和预共享密钥认证两种模式： • 选择证书认证模式时，需要指定本端使用的本地证书。 • 选择预共享密钥认证模式时，需要指定预共享密钥。用鼠标点住后面的眼睛图标可以明文显示预共享密钥。

b. 点击**本地配置**页签，配置本端 IP 地址、ID 类型和本端 ID。



参数	说明
本地地址	本端出口接口的 IP 地址，可以为指定 IP 地址，也可以为任意。
类型	本端认证类型，推荐使用 IPv4 地址。 • **IPv4 地址**：指本端网关的出口接口 IP。当出口接口配置了多个 IP 地址时，可以指定为任意，表示可以使用任意出口接口的任意 IP 地址和对端网关协商隧道。 • **域名**：主要用于出口接口有多个 IP 或 IP 不固定时的场景。使用证书认证时，域名需要与本地证书中的公共名 CN 字段保持一致。 • **邮件地址**：主要用于证书认证方式，需要与本地证书中的 emailAddress 字段保持一致。 • **证书主题**：即本地证书的证书主题，主要用于证书认证方式。 • **字符串**：当以上方式都不适用时，可以使用字符串认证，即随机输入的一串字符串，长度 1-1023 字节，只能由字母、数字和特殊字符组成，空格及?,'"\<>&#=除外。需要注意两端网关的字符串必须保持一致。

提示：类型选择**证书主题**时，ID应与所使用本地证书的主题信息一致；对于iOS用户，推荐本地地址选择一个接口IP，否则类型应选择IPv4地址，ID应设为本端地址。

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**。

4. 勾选 RemoteAccess 连接，点击**重启服务**。
5. 在终端设备下载并安装通用的 IPSec VPN 客户端，输入用户名和密码登录。

6. VPN 用户登录成功后，管理员可点击 RemoteAccess 连接后面的图标，跳转到 **IPSec VPN 在线用户监控**页面，查看在线用户信息。
7. 隧道协商成功后，系统将自动生成访问策略，可选择**网络/策略>访问策略>配置 IPSec VPN 访问策略**查看自动生成的访问策略。

4.11.2. 添加网关到网关 IPSec VPN 隧道

1. 选择**基础功能> IPSec VPN**，点击**添加**。
2. 在**基础配置**页签配置隧道名称、启用/禁用隧道、启用/禁用记录日志功能并配置相关信息。

参数	说明
主动协商	勾选表示 VPN 网关主动发起隧道协商。本端和对端网关只允许一端启用此功能。 由于在一端网关启用主动协商功能后，网关会立即向对端发起协商，因此，请先完成不启用主动协商功能网关端的配置，然后再设置启用主动协商功能的网关端，以保证隧道成功建立。
IKE 版本	支持 ikev1 和 ikev2 两个版本，推荐使用 ikev2 版本。ikev2 对 ikev1 进行了优化，兼容 NAT 设备，即使在 VPN 网关之间存在 NAT 设备时也可以协商成功。 如需使用国密办加密算法，请选择 ikev2。
认证方式	支持证书认证和预共享密钥认证两种模式： 选择证书认证模式时，需要指定本端使用的本地证书。 选择预共享密钥认证模式时，需要指定预共享密钥。用鼠标点住后面的眼睛图标可以明文显示预共享密钥。

加速卡	插入硬件加速卡时，可以选择是否开启硬件加速；未插卡时，则提示未发现加速卡。

3. 点击**本地配置**页签，配置本端 IP 地址、ID 类型、本端 ID 和本地子网。

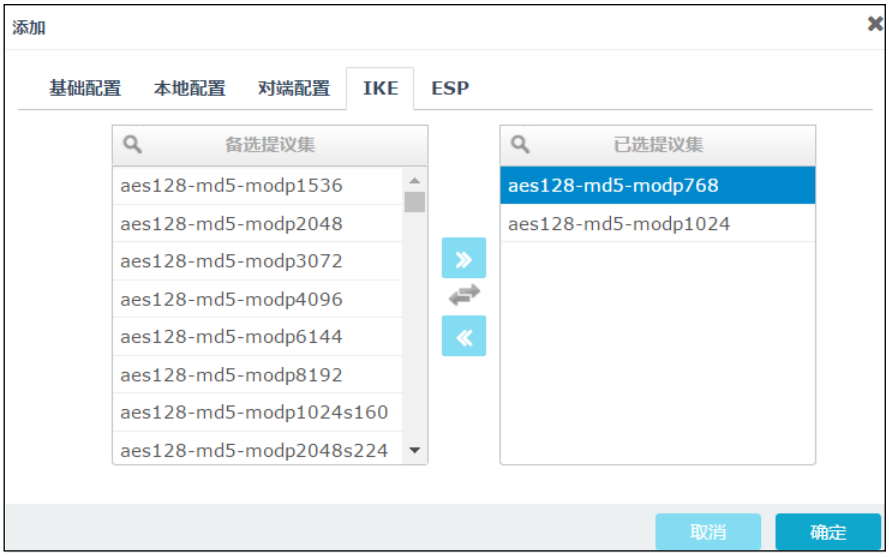
本端网关的本地配置和对端网关的对端配置需要一一对应。例如，本端网关的本地地址选择指定的 IP 地址时，则对端网关的对端地址也要输入该指定 IP 地址。

参数	**说明**
本地地址	本端出口接口的 IP 地址，可以为指定 IP 地址，也可以为任意。
类型	本端认证类型。当选择预共享密钥认证方式时，ID 类型建议选择 IPv4 地址、域名或字符串；当选择证书认证方式时，ID 类型建议选择域名、邮件地址或证书主题。 • **IPv4 地址**：指本端网关的出口接口 IP。当出口接口配置了多个 IP 地址时，可以指定为任意，表示可以使用任意出口接口的任意 IP 地址和对端网关协商隧道。 • **域名**：主要用于出口接口有多个 IP 或 IP 不固定时的场景。使用证书认证时，域名需要与本地证书中的公共名 CN 字段保持一致。 • **邮件地址**：主要用于证书认证方式，需要与本地证书中的 emailAddress 字段保持一致。 • **证书主题**：即本地证书的证书主题，主要用于证书认证方式。 • **字符串**：当以上方式都不适用时，可以使用字符串认证，即随机输入的一串字符串，长度 1-1023 字节， 只能由字母、数字和特殊字符组成，空格及?,'"\<>&#=除外。需要注意两端网关的字符串必须保持一致。
本地子网	即本端网关连接的子网，要与对端子网通过隧道进行通信的子网。当 IKE 版本设置为 ike1 时，允许添加一个子网。当 IKE 版本设置为 ike2 时，允许添加多个子网；最多支持 32 个子网。

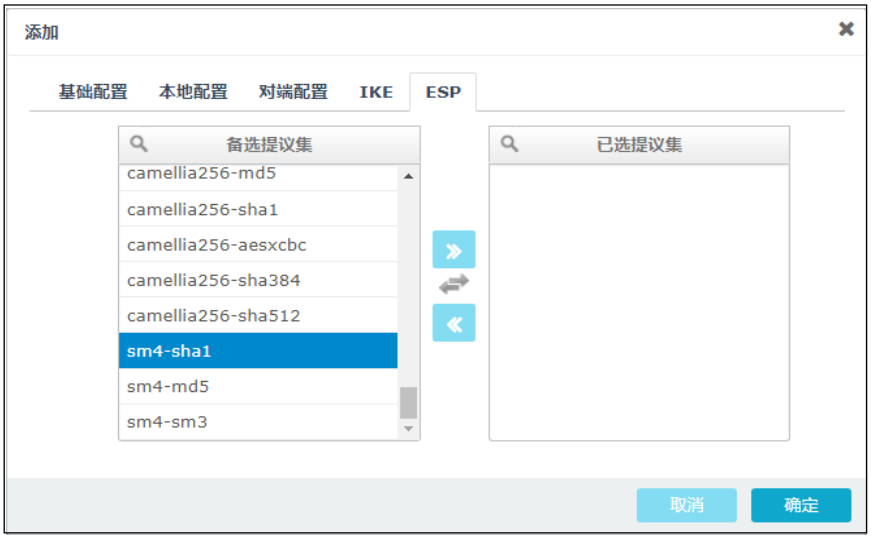
4. 点击**对端配置**页签进行相关配置。

参数	说明
IP 地址/域名	可以填写对端出口接口的 IP 地址，也可以填写其对应的域名。
类型	对端认证类型。相关参数信息同**本地配置**页签。
对端子网	即对端网关连接的子网，要与本端子网通过隧道进行通信的子网。当 IKE 版本设置为 ike1 时，允许添加一个子网。当 IKE 版本设置为 ike2 时，允许添加多个子网；最多支持 32 个子网。

5. （可选）点击 **IKE** 页签并选择第一阶段提议集。



6. （可选）点击 **ESP** 页签并选择第二阶段提议集。



如果在**基础配置**页面选择了 **ikev2**，备选提议集中将出现如下国密办加密算法：sm4-sha1、sm4-md5、sm4-sm3。

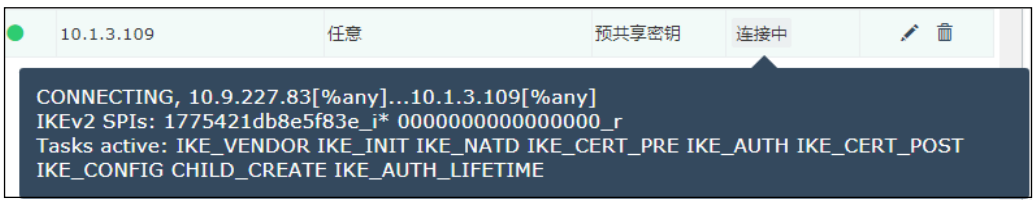
7. 点击**确定**。

8. 点击**重启服务**。

提示：配置完成后，两端网关都要重启服务，隧道才能协商成功。

9. 刷新页面后，如果查看隧道状态为已连接，则说明隧道协商成功。

- 网关到网关的 IPSec VPN 连接名称后面如果有 图标，表示启用了主动协商。
- 网关到网关的 IPSec VPN 连接状态包括未连接和连接中，鼠标指向连接状态时，界面会提示当前连接信息。



10. 隧道成功建立后，系统会自动生成访问策略。可选择**网络/策略>访问策略**，点击配置 IPSec VPN 访问策略，查看自动生成的 IPSec VPN 访问策略。

11. 如果隧道显示未连接，可以选择**日志> 调试> IPSecVPN 协商日志**，查看调试信息，查找协商失败的原因。

12. 当配置的网关到网关模式的 IPSec VPN 的本端子网和对端子网发生地址重叠时，为了保证 VPN 和本端子网中的设备通信正常，需要为本地子网配置直通路由。可以点击 **配置直通路由** 来查看和配置直通路由。

将受影响的本端子网配置在**子网**文本框中点击**确定**即可。

提示：目前不支持32位掩码的子网配置。

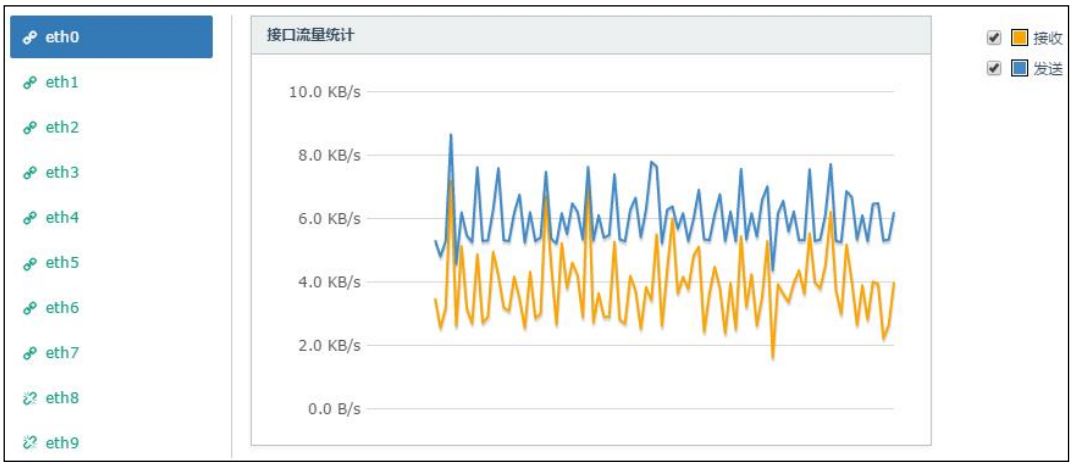
第5章 监控

本章介绍 VPN 网关的监控功能，内容包括：

5.1.系统监控

系统提供以太网接口的实时流量统计信息，并以折线图的形式直观地显示出来。

1. 选择**监控>系统监控>接口流量统计**。
2. 点击接口名称，查看接口实时流量信息。



纵坐标轴表示接口流量大小，单位为 B/s、KB/s、MB/s 或 GB/s，系统可根据实际流量的大小进行自适应调节。例如，缺省情况下为字节（B/s），当达到 1024 字节时则变为 KB/s，以此类推。

可通过折线图右上方的复选框设置要显示的内容，包括接收流量和发送流量。

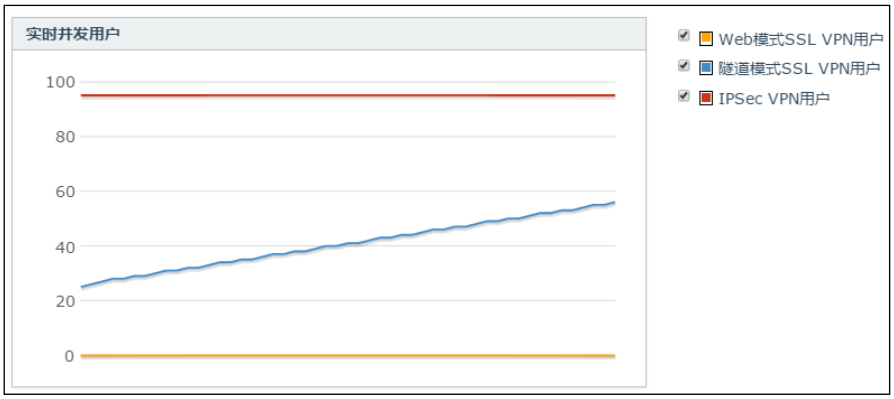
鼠标指向折线图时，可以查看到具体时间点的接收和发送速率。

接口名称前面的图标表示该接口物理连接状态， 表示接口处于连接状态， 表示接口未连接任何网络。

5.2.在线用户

5.2.1. 实时并发用户

1. 选择**监控>在线用户>实时并发用户**。
2. 查看实时并发用户信息，包括 Web 模式 SSL VPN 用户、隧道模式 SSL VPN 用户和 IPSec VPN 用户。



5.2.2. Web 模式在线用户

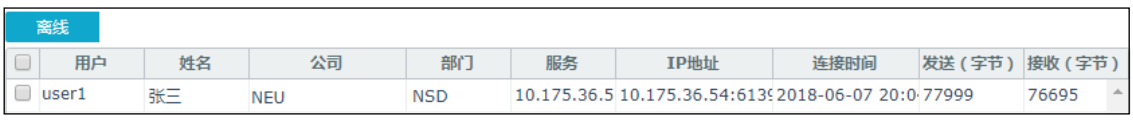
1. 选择**监控> 在线用户> Web 模式在线用户**。
2. 查看 Web 模式 SSL VPN 在线用户信息。

提示：为保证响应速度，默认不显示用户流量。管理员可通过页面右上角的流量开关开启流量监控。

3. 可勾选用户，点击**离线**按钮，强制其离线。

5.2.3. 隧道模式在线用户

1. 选择**监控>在线用户>隧道模式在线用户**。
2. 查看隧道模式 SSL VPN 在线用户信息。可勾选用户，点击**离线**按钮，强制其离线。



5.2.4. IPSec VPN 在线用户

1. 选择**监控> 在线用户> IPSec VPN 在线用户**。
2. 查看远程访问 IPSec VPN 在线用户信息。

用户	姓名	公司	部门	IKE版本	源地址	在线时间	发送	接收
u1				ikev1	9.8.0.34	46 minutes ago	37107456	797646684
u10				ikev1	9.8.0.59	46 minutes ago	38303083	793127421
u11				ikev1	9.8.0.16	46 minutes ago	37542862	780331590
u12				ikev1	9.8.0.4	46 minutes ago	37134046	769545213
u13				ikev1	9.8.0.29	46 minutes ago	37945118	786486827
u14				ikev1	9.8.0.21	46 minutes ago	36889822	743539772
u15				ikev1	9.8.0.31	46 minutes ago	37572460	768620968
u16				ikev1	9.8.0.27	46 minutes ago	37529764	767455803

提示：为保证响应速度，默认不显示用户流量。管理员可通过页面右上角的流量开关开启流量监控。

3. 可勾选用户，点击**离线**按钮，强制其离线。

5.3.历史监控

5.3.1. 并发用户趋势图

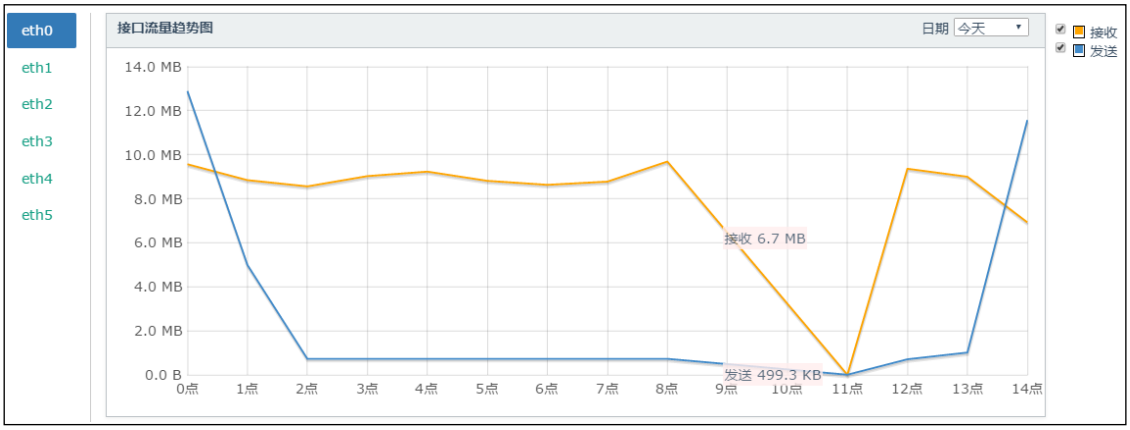
1. 选择**监控>历史监控>并发用户趋势图**。
2. 查看最近一段时间内并发在线用户的统计数据。

可在折线图右上角选择显示时间区间，包括今天、昨天、最近一周、最近一月。

可通过折线图右上方的复选框设置要显示的内容，包括 Web 模式 SSL VPN 用户和隧道模式 SSL VPN 用户。

5.3.2. 接口流量趋势图

1. 选择**监控>历史监控> 接口流量趋势图**。
2. 点击接口名称，查看该接口最近一段时间内接收和发送流量的统计数据。



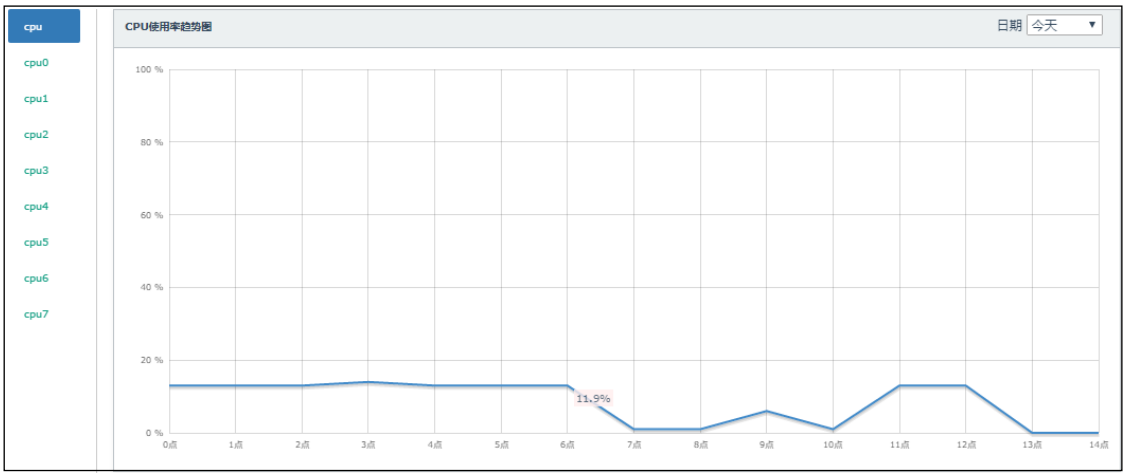
可在折线图右上角选择显示时间区间，包括今天、昨天、最近一周、最近一月。

可通过折线图右上方的复选框设置要显示的内容，包括接收和发送流量。

将鼠标放置坐标图上时，可显示鼠标所在位置的具体流量值。

5.3.3. CPU 使用率趋势图

1. 选择**监控> 历史监控> CPU 使用率趋势图**。
2. 查看最近一段时间内的 CPU 使用情况。

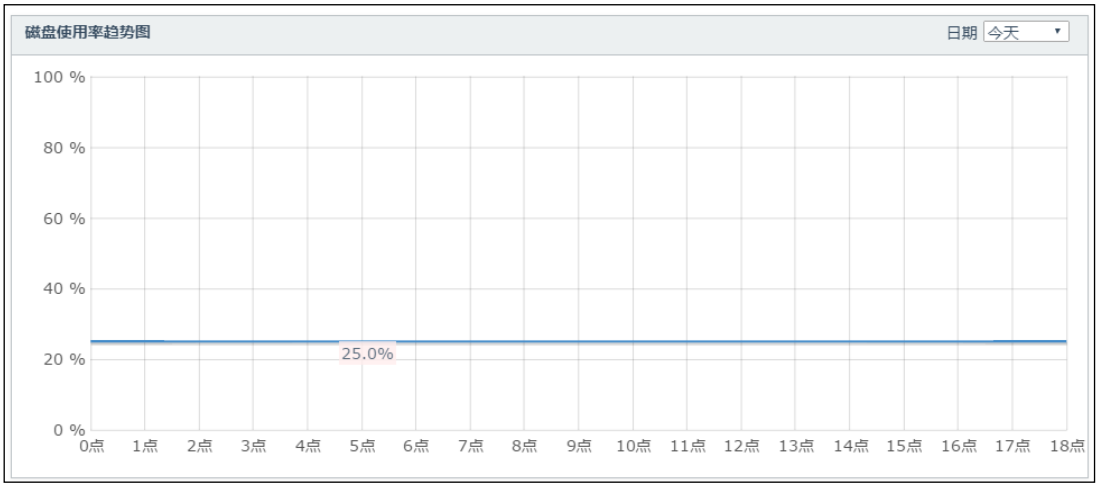


点击左侧 CPU 编号，可查看各个 CPU 的使用情况。无编号 CPU 表示所有 CPU 的综合使用情况。

在折线图的右上角可选择显示时间区间，包括今天、昨天、最近一周、最近一月。将鼠标放置坐标图上时，可显示鼠标所指位置的具体使用率数值。

5.3.4. 磁盘使用率趋势图

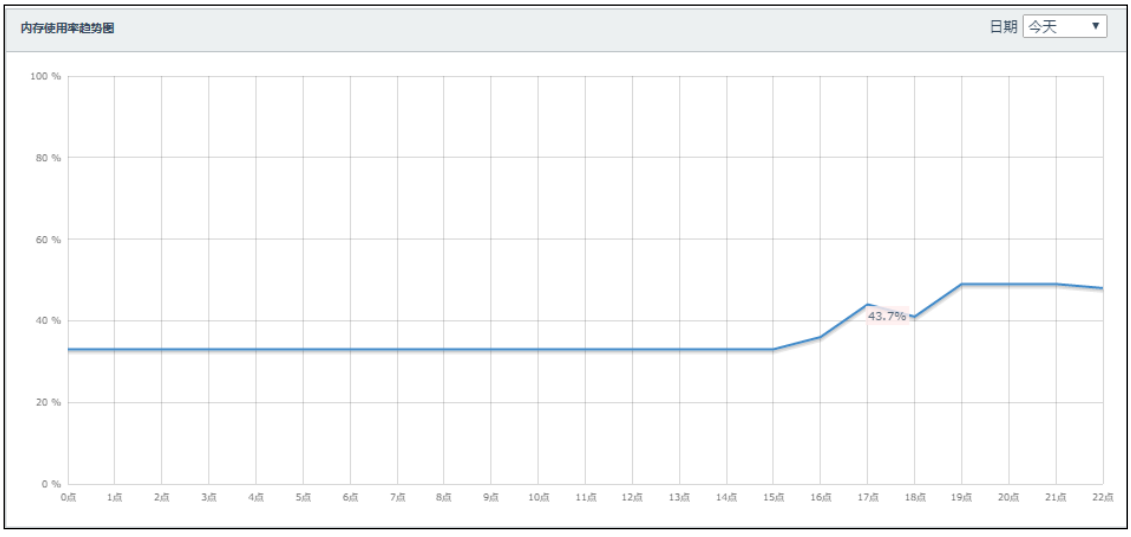
1. 选择**监控>历史监控>磁盘使用率趋势图**。
2. 查看最近一段时间内磁盘的使用情况。



在折线图的右上角可选择显示时间区间，包括今天、昨天、最近一周、最近一月。将鼠标放置坐标图上时，可显示鼠标所指位置的具体磁盘使用率数值。

5.3.5. 内存使用率趋势图

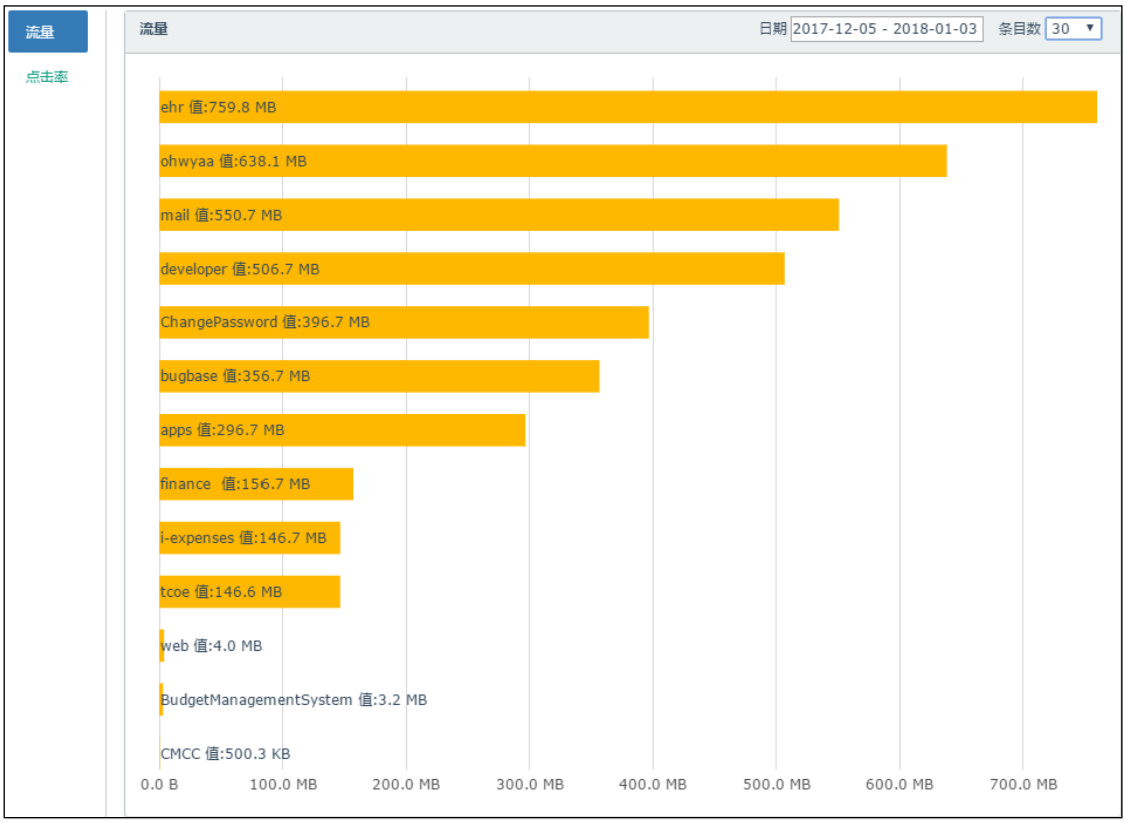
1. 选择**监控>历史监控> 内存使用率趋势图**。
2. 查看最近一段时间内的内存使用情况。



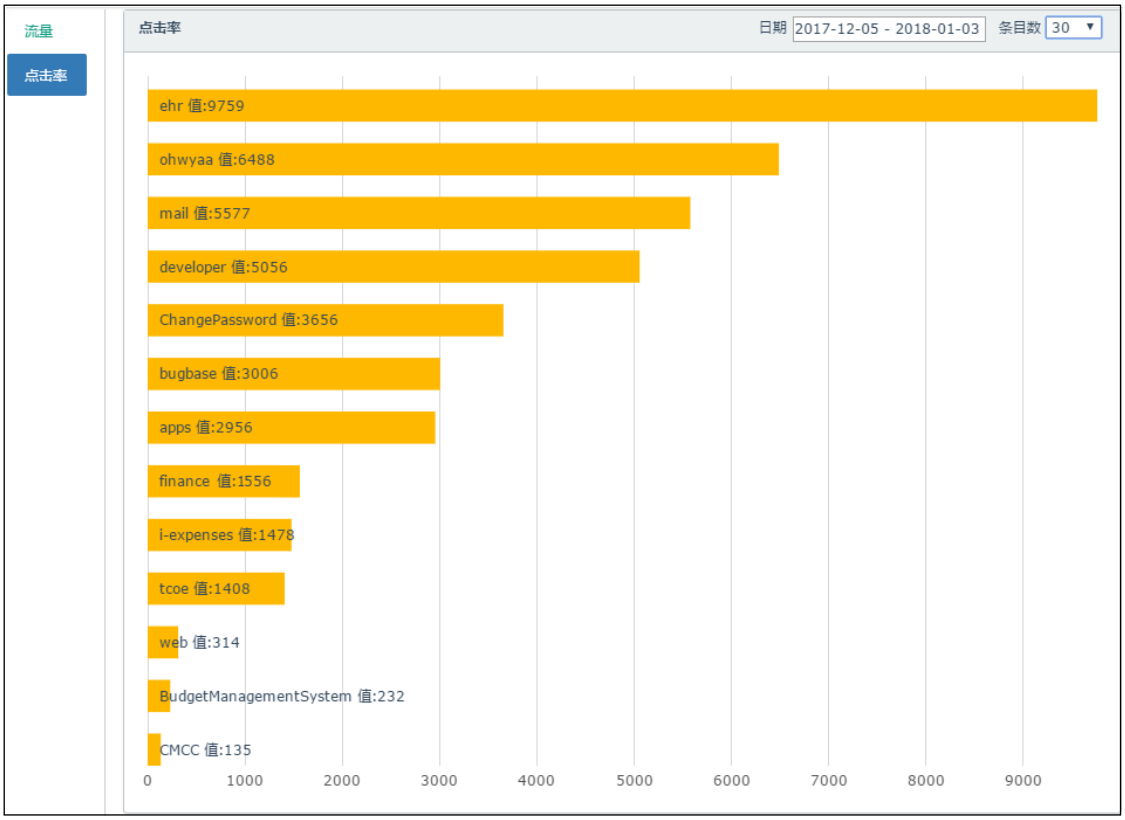
在折线图的右上角可选择显示时间区间，包括今天、昨天、最近一周、最近一月。将鼠标放置坐标图上时，可显示鼠标所指位置的具体内存使用率数值。

5.3.6. 应用排行

1. 选择**监控>历史监控>应用排行**。
2. 查看用户访问流量或点击率排名靠前的应用。可在页面右上角选择显示时间区间和显示条目数，查询指定日期区间的 Top 10、30、50 或 100 个应用。

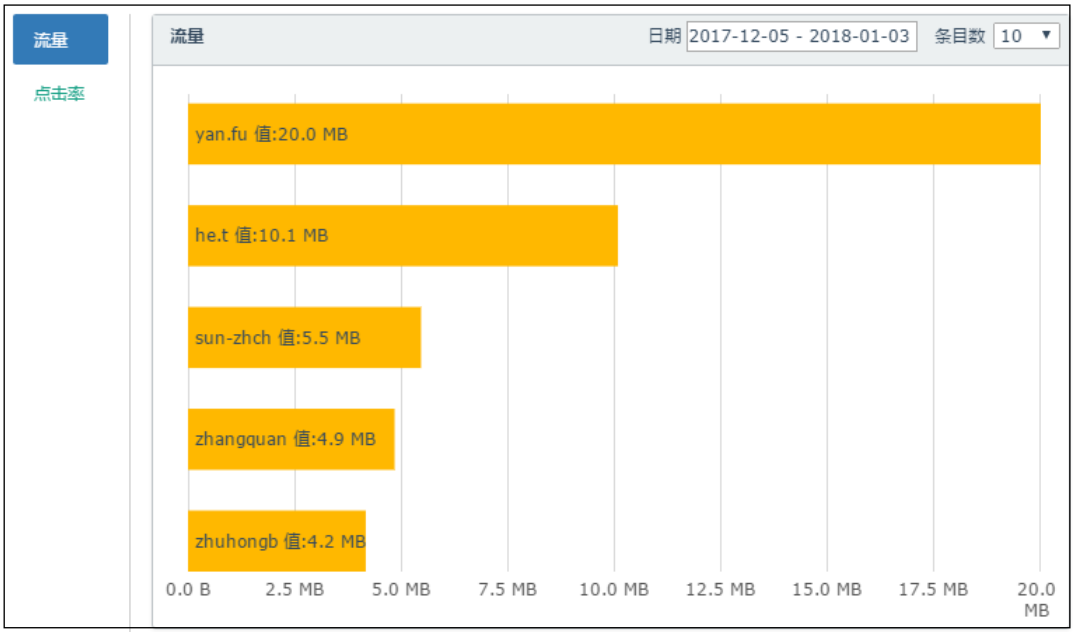


3. 点击左侧流量和点击率，可切换显示内容，按照流量或点击率显示排名。

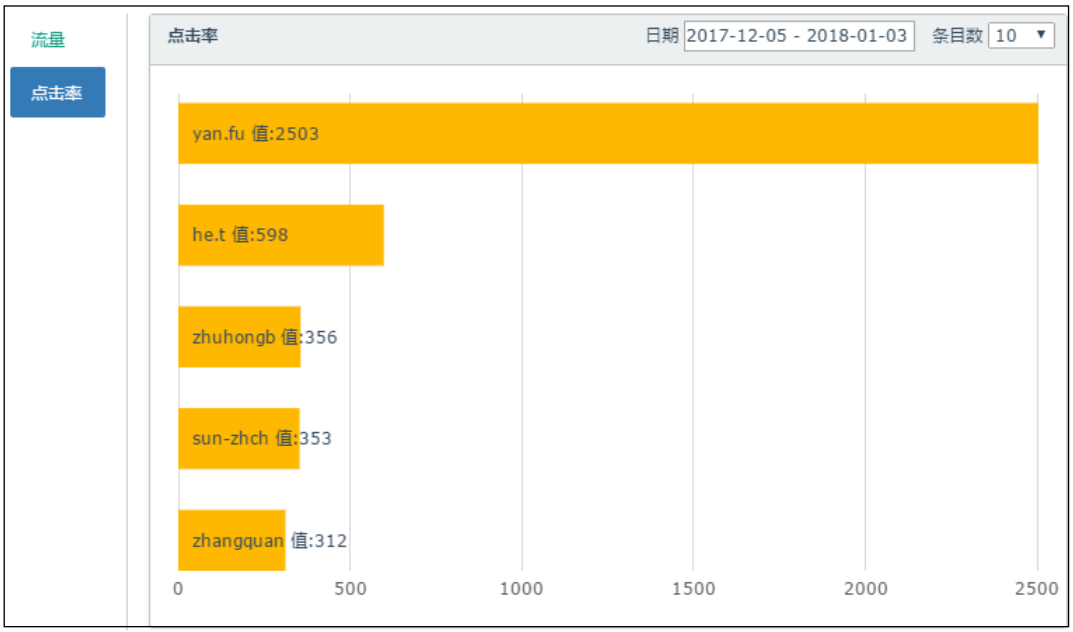


5.3.7. 用户排行

1. 选择**监控>历史监控>用户排行**。
2. 查看流量或者点击率排名靠前的用户。可在页面右上角选择显示时间区间和显示条目数，查询指定日期区间的 Top 10、30、50 或 100 个用户。



3. 点击左侧**流量**和**点击率**，可切换显示内容，按照流量或者点击率显示排名。



第6章 日志管理

本章介绍 VPN 网关的日志管理功能，内容包括：

6.1.日志配置

VPN 网关支持本地查看日志和将日志发送到 Syslog 日志服务器。如果配置了日志报警策略，当有事件发生时，VPN 网关将根据策略配置将日志发送到对应的日志服务器。

1. 选择**日志>日志配置**。
2. 配置 Syslog 日志服务器。点击**添加**，添加 Syslog 日志策略，点击**确定**。

3. 设置本地日志存储策略。

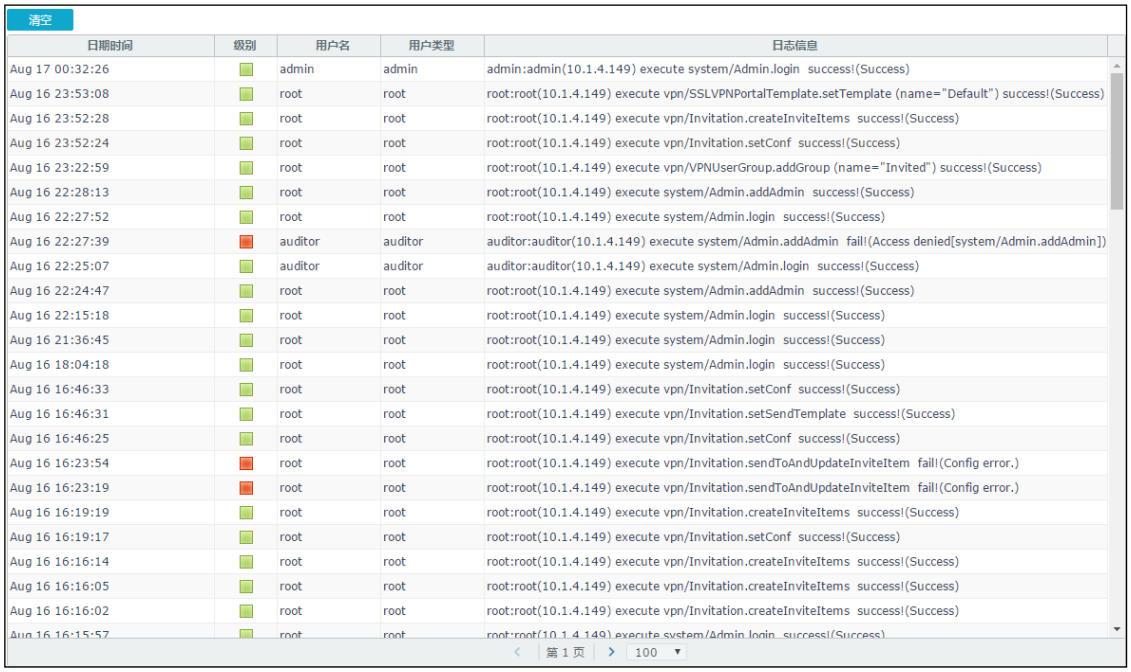
本地日志策略默认启用，不可禁用。日志存储于磁盘上，管理员可根据实际情况调整磁盘剩余空间。当剩余磁盘空间小于设置的限值时，较早生成的日志会被删除。

4. 点击**提交**。

6.2.管理日志

管理日志默认开启，记录系统管理相关的日志信息。

1. 选择日志>管理日志。
2. 查看系统管理日志。



参数	说明
日期时间	执行操作的具体时间。
级别	日志的级别，有 Info 和 Error 两种，分别以绿色和红色方框表示。 Info 表示执行操作成功，Error 表示执行操作失败。
用户名	执行操作的管理用户名称。
用户类型	用户类型，包括 Root、Administrator、Auditor 和 High Availablity。
日志信息	记录用户名、操作内容和执行结果的详细日志信息。

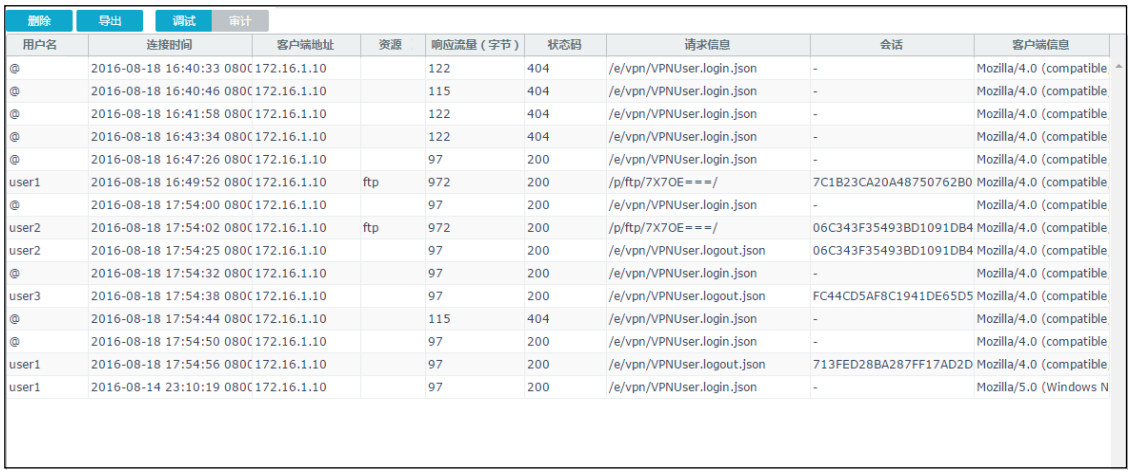
3. 点击**清空**按钮，可以清空管理日志。
4. 日志超过 100 条时会分页显示，通过列表下方的页码可翻页查看日志信息。

6.3.访问日志

6.3.1. Web 模式访问日志

Web 模式 SSL VPN 访问日志分为调试日志和审计日志：调试日志按从新到旧的顺序显示最近 1000 条，审计日志按日志产生时间（从旧到新）显示所有日志。

1. 选择**日志> 访问日志> Web 模式访问日志**。
2. 查看用户通过 Web 模式访问 SSL VPN 资源的调试日志信息。

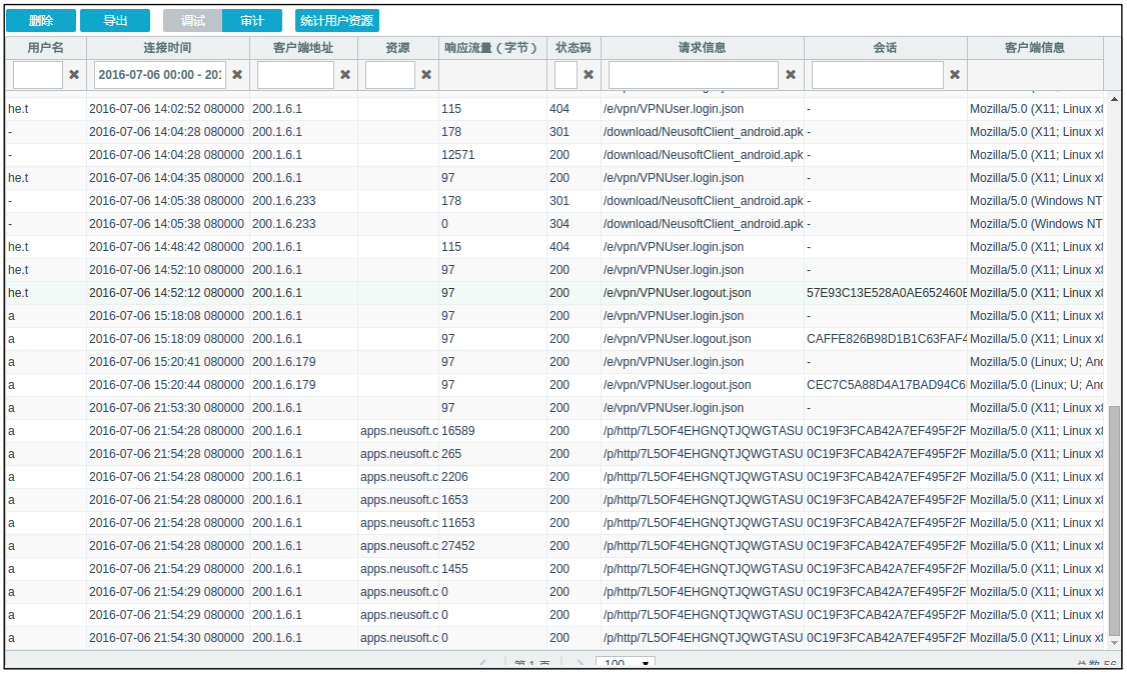


用户名	连接时间	客户端地址	资源	响应流量（字节）	状态码	请求信息	会话	客户端信息
@	2016-08-18 16:40:33 080(	172.16.1.10		122	404	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
@	2016-08-18 16:40:46 080(	172.16.1.10		115	404	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
@	2016-08-18 16:41:58 080(	172.16.1.10		122	404	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
@	2016-08-18 16:43:34 080(	172.16.1.10		122	404	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
@	2016-08-18 16:47:26 080(	172.16.1.10		97	200	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
user1	2016-08-18 16:49:52 080(	172.16.1.10	ftp	972	200	/p/ftp/7X7OE===/	7C1B23CA20A48750762B0	Mozilla/4.0 (compatible
@	2016-08-18 17:54:00 080(	172.16.1.10		97	200	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
user2	2016-08-18 17:54:02 080(	172.16.1.10	ftp	972	200	/p/ftp/7X7OE===/	06C343F35493BD1091DB4	Mozilla/4.0 (compatible
user2	2016-08-18 17:54:25 080(	172.16.1.10		97	200	/e/vpn/VPNUser.logout.json	06C343F35493BD1091DB4	Mozilla/4.0 (compatible
@	2016-08-18 17:54:32 080(	172.16.1.10		97	200	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
user3	2016-08-18 17:54:38 080(	172.16.1.10		97	200	/e/vpn/VPNUser.logout.json	FC44CD5AF8C1941DE65D5	Mozilla/4.0 (compatible
@	2016-08-18 17:54:44 080(	172.16.1.10		115	404	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
@	2016-08-18 17:54:50 080(	172.16.1.10		97	200	/e/vpn/VPNUser.login.json	-	Mozilla/4.0 (compatible
user1	2016-08-18 17:54:56 080(	172.16.1.10		97	200	/e/vpn/VPNUser.logout.json	713FED28BA287FF17AD2D	Mozilla/4.0 (compatible
user1	2016-08-14 23:10:19 080(	172.16.1.10		97	200	/e/vpn/VPNUser.login.json	-	Mozilla/5.0 (Windows N

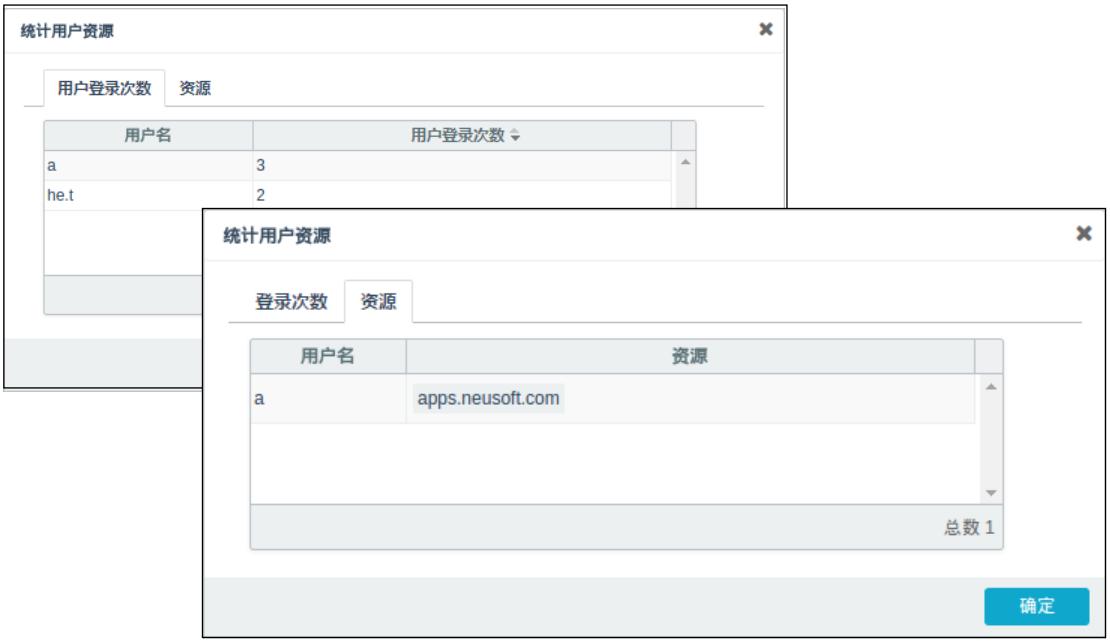
参数	说明
用户	SSL VPN 用户名称。
连接时间	建立 SSL VPN 连接的具体时间。
客户端地址	用户访问 SSL VPN 资源使用的客户端 IP 地址。
资源	用户访问的资源名称。
响应流量（字节）	服务器端响应流量的大小。单位是 bps。
状态码	HTTP 状态码。
请求信息	客户端发送的 HTTP 请求信息。
会话	客户端与服务器端建立连接的会话 ID。
客户端信息	客户端浏览器的相关信息。

可通过用户名、连接时间、客户端地址、状态码、请求信息和会话等参数筛选日志信息。

3. 点击列表上方的**审计**，查看用户通过隧道模式访问 SSL VPN 资源的审计日志信息。



4. 点击统计用户资源，查看用户登录次数以及访问的资源，可按登录次数进行排序。



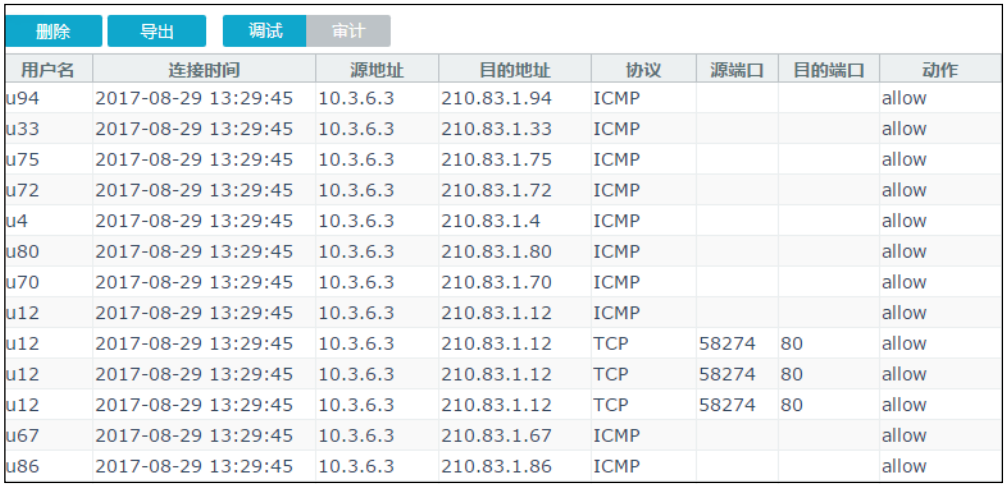
提示：如果用户登录次数过大，可能出现频繁掉线的情况，管理员可据此对用户进行进行排查。

5. 点击**删除**按钮，可设置时间区间，删除指定时间范围内的日志信息。
6. 点击**导出**按钮，可下载日志信息到本地。
7. 日志超过 100 条时会分页显示，通过列表下方的页码可翻页查看日志信息。

6.3.2. 隧道模式访问日志

隧道模式 SSL VPN 访问日志分为调试日志和审计日志：调试日志按从新到旧的顺序显示最近 1000 条，审计日志按日志产生时间（从旧到新）显示所有日志。

1. 选择**日志>访问日志>隧道模式访问日志**。
2. 查看用户通过隧道模式访问 SSL VPN 资源的调试日志信息。



用户名	连接时间	源地址	目的地址	协议	源端口	目的端口	动作
u94	2017-08-29 13:29:45	10.3.6.3	210.83.1.94	ICMP			allow
u33	2017-08-29 13:29:45	10.3.6.3	210.83.1.33	ICMP			allow
u75	2017-08-29 13:29:45	10.3.6.3	210.83.1.75	ICMP			allow
u72	2017-08-29 13:29:45	10.3.6.3	210.83.1.72	ICMP			allow
u4	2017-08-29 13:29:45	10.3.6.3	210.83.1.4	ICMP			allow
u80	2017-08-29 13:29:45	10.3.6.3	210.83.1.80	ICMP			allow
u70	2017-08-29 13:29:45	10.3.6.3	210.83.1.70	ICMP			allow
u12	2017-08-29 13:29:45	10.3.6.3	210.83.1.12	ICMP			allow
u12	2017-08-29 13:29:45	10.3.6.3	210.83.1.12	TCP	58274	80	allow
u12	2017-08-29 13:29:45	10.3.6.3	210.83.1.12	TCP	58274	80	allow
u12	2017-08-29 13:29:45	10.3.6.3	210.83.1.12	TCP	58274	80	allow
u67	2017-08-29 13:29:45	10.3.6.3	210.83.1.67	ICMP			allow
u86	2017-08-29 13:29:45	10.3.6.3	210.83.1.86	ICMP			allow

参数	说明
用户名	SSL VPN 用户名称。
连接时间	用户访问 SSL VPN 资源的时间。
源地址	SSL VPN 用户访问 SSL VPN 资源时发起连接的客户端源 IP 地址。
目的地址	SSL VPN 用户访问 SSL VPN 资源时访问的 SSL VPN 服务器地址。
协议	协议类型。
源端口	源端口号。
目的端口	目的端口号。
动作	系统对于 SSL VPN 用户访问的处理动作，包括 allow、deny、login success 和 login failure。

可通过用户名、日期时间、源地址、目的地址和动作等参数筛选日志信息。

3. 点击列表上方的**审计**，查看用户通过隧道模式访问 SSL VPN 资源的审计日志信息。

4. 点击**统计用户资源**，查看用户登录次数以及访问的资源，可按登录次数进行排序。

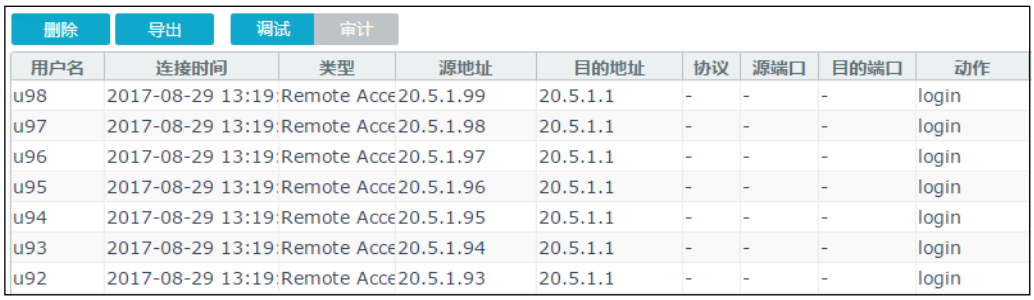
提示：如果用户登录次数过大，可能出现频繁掉线的情况，管理员可据此对用户进行进行排查。

5. 点击**删除**按钮，可设置时间区间，删除指定时间范围内的日志信息。
6. 点击**导出**按钮，可下载日志信息到本地。
7. 日志超过 100 条时会分页显示，通过列表下方的页码可翻页查看日志信息。

6.3.3. IPSec VPN 访问日志

IPSec VPN 访问日志分为调试日志和审计日志：调试日志按从新到旧的顺序显示最近 1000 条，审计日志按日志产生时间（从旧到新）显示所有日志。

1. 选择**日志>访问日志> IPSec VPN 访问日志**。
2. 查看用户通过 IPSec VPN 访问 VPN 资源的调试日志信息。



用户名	连接时间	类型	源地址	目的地址	协议	源端口	目的端口	动作
u98	2017-08-29 13:19	Remote Acce	20.5.1.99	20.5.1.1	-	-	-	login
u97	2017-08-29 13:19	Remote Acce	20.5.1.98	20.5.1.1	-	-	-	login
u96	2017-08-29 13:19	Remote Acce	20.5.1.97	20.5.1.1	-	-	-	login
u95	2017-08-29 13:19	Remote Acce	20.5.1.96	20.5.1.1	-	-	-	login
u94	2017-08-29 13:19	Remote Acce	20.5.1.95	20.5.1.1	-	-	-	login
u93	2017-08-29 13:19	Remote Acce	20.5.1.94	20.5.1.1	-	-	-	login
u92	2017-08-29 13:19	Remote Acce	20.5.1.93	20.5.1.1	-	-	-	login

参数	说明
用户名	IPSec VPN 远程用户名称。
连接时间	用户访问 IPSec VPN 资源的时间。
类型	IPSec VPN 连接类型，包括 Remote Access 和 Site-to-Site 两种类型。
源地址	IPSec VPN 远程用户访问 IPSec VPN 资源时发起连接的客户端源 IP 地址。
目的地址	IPSec VPN 远程用户访问 IPSec VPN 资源时访问的 VPN 服务器地址。
协议	协议类型。
源端口	源端口号。
目的端口	目的端口号。
动作	对于网关到网关的 IPSec VPN 隧道，动作包括 connect 和 disconnect。 对于远程访问 IPSec VPN，动作包括 login、fz_login（辅助认证登录）、logout 和 allow。

可通过用户名、日期时间、源地址、目的地址和动作等参数筛选日志信息。

3. 点击列表上方的**审计**，查看用户通过隧道模式访问 SSL VPN 资源的审计日志信息。

用户名	连接时间	类型	源地址	目的地址	协议	源端口	目的端口	动作
	2017-08-29							
u88	2017-08-29 06:55	Remote Acce	20.5.1.89	20.5.1.1	-	-	-	login
u68	2017-08-29 06:55	Remote Acce	20.5.1.69	20.5.1.1	-	-	-	login
u87	2017-08-29 06:57	Remote Acce	20.5.1.88	20.5.1.1	-	-	-	login
u8	2017-08-29 06:59	Remote Acce	20.5.1.9	20.5.1.1	-	-	-	login
u64	2017-08-29 07:01	Remote Acce	20.5.1.65	20.5.1.1	-	-	-	login
u43	2017-08-29 07:02	Remote Acce	20.5.1.44	20.5.1.1	-	-	-	login

4. 点击**统计用户资源**，查看用户登录次数以及访问的资源，可按登录次数进行排序。

提示：如果用户登录次数过大，可能出现频繁掉线的情况，管理员可据此对用户进行进行排查。

5. 点击**删除**按钮，可设置时间区间，删除指定时间范围内的日志信息。
6. 点击**导出**按钮，可下载日志信息到本地。
7. 日志超过 100 条时会分页显示，通过列表下方的页码可翻页查看日志信息。

6.4.调试

6.4.1. 隧道模式调试日志

如果在配置隧道模式 SSL VPN 时开启了调试功能，则此处可查看 SSL VPN 调试信息，帮助用户定位问题。

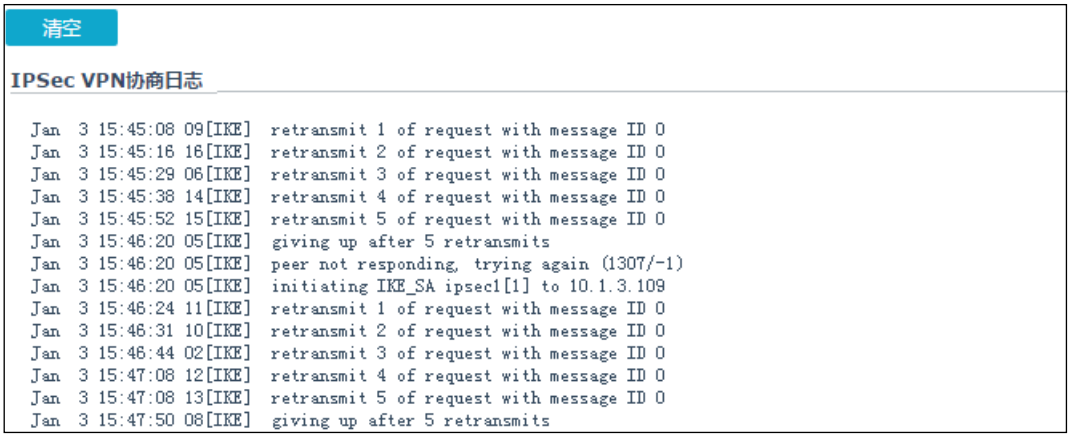
1. 选择**日志>调试>隧道模式调试信息**。
2. 查看隧道模式 SSL VPN 的调试信息。

3. 点击**清空**按钮，可清空调试日志。

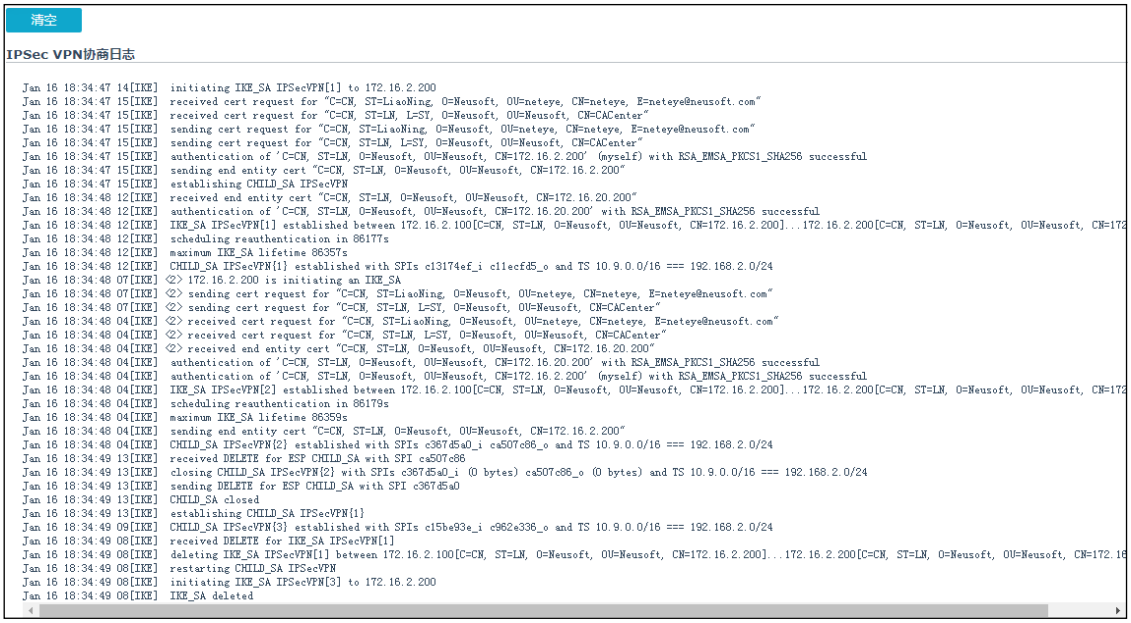
6.4.2. IPSec VPN 协商日志

系统默认开启 IPSec VPN 日志功能，记录隧道协商过程。当 IPSec VPN 隧道协商失败时，可查看协商日志查找原因。

1. 选择**日志>调试> IPSec VPN 协商日志**。
2. 查看远程访问 IPSec VPN 的协商日志。



3. 查看网关到网关 IPSec VPN 的协商日志。



4. 点击**清空**按钮，可清空协商日志。

第7章 网络/策略

本章介绍 VPN 网关的网络和策略功能，内容包括：

7.1.接口

VPN 网关的管理接口缺省为以太网接口 eth0，缺省管理 IP 地址为 192.168.1.200/24。

除了以太网接口，VPN 网关还提供以下几种逻辑接口，以满足不同用户的需求：

- Bond 接口：两个二层以太网接口作为一个逻辑接口使用，实现接口级的高可靠性。
  - 主接口：承担所有流量。
  - 备接口：没有流量通过。当主接口发生故障时，备接口自动成为主接口并接管流量。
- Bridge 接口：多个以太网接口被划分到一个 Bridge 接口中，以实现 VLAN（虚拟局域网）的作用。可以节省交换机资源。
- PPPoE 接口：VPN 网关可作为 PPPoE 客户端拨号，获取接口配置信息。

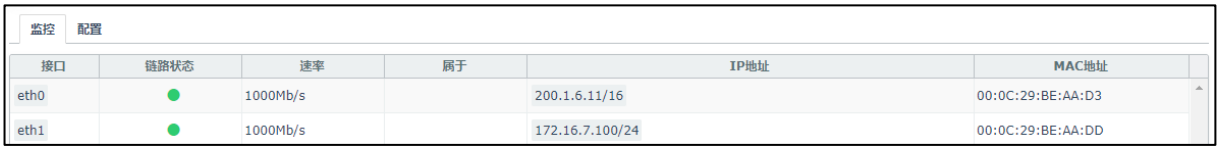
NVPN3000 机型带有一个 WLAN 接口。该机型的 VPN 网关可作为无线路由器允许内网无线客户端接入现有网络，相关配置可参考**错误!未找到引用源。**。

本节介绍以下配置：

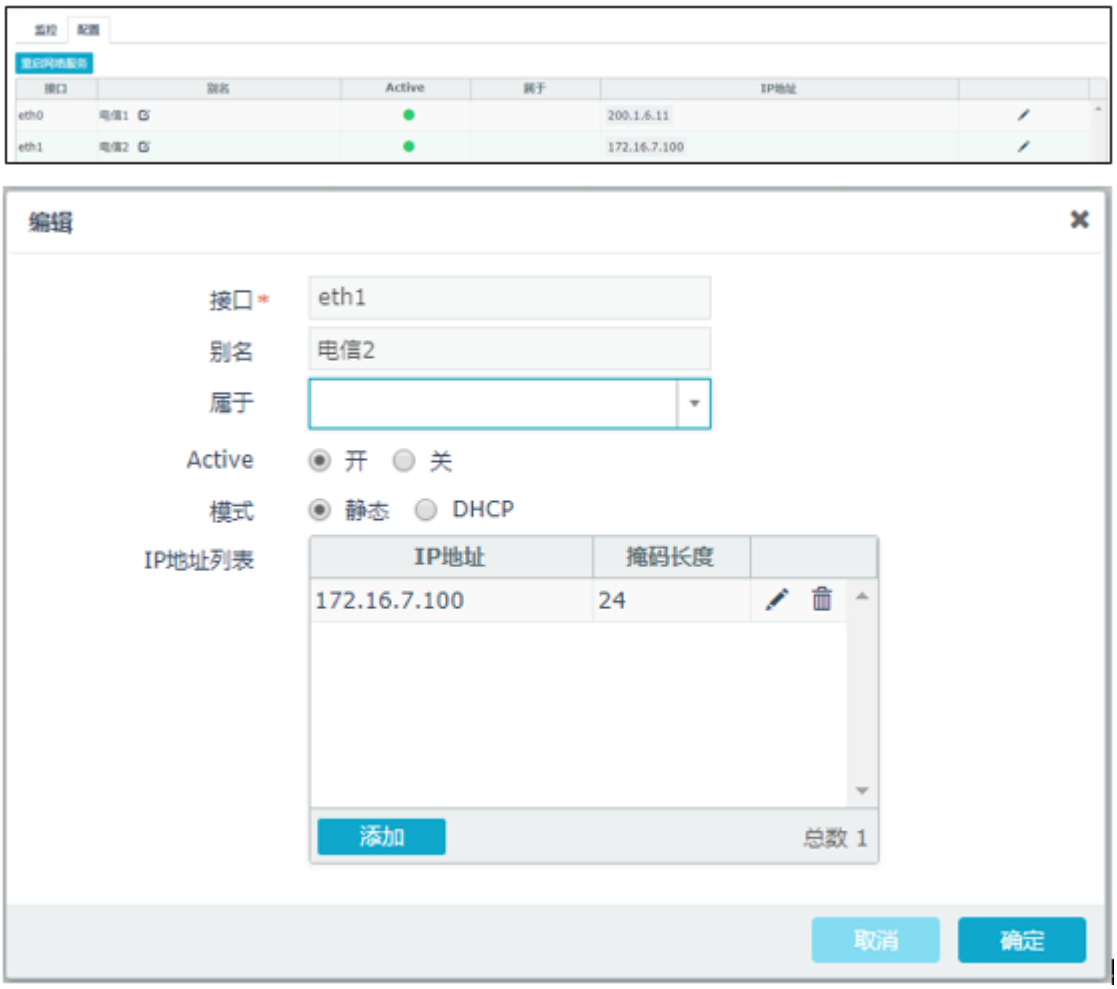
- 配置以太网接口
- 配置 Bond 接口
- 配置 Bridge 接口
- 配置 PPPoE 接口
- 配置 WLAN 接口

7.1.1. 配置以太网接口

1. 选择**网络/策略>接口**。
2. 在监控列表中，可以查看接口的概要信息。



3. 打开**配置**页签，点击别名下方的 图标进行接口别名配置，点击需要配置的接口对应的 图标，进行相关配置。



参数	说明
属于	可将接口划分给 Bond 接口（冗余接口）、Bridge 接口（VLAN 接口）或 PPPoE 接口。
模式	接口支持通过**静态**和 **DHCP** 两种方式获取 IP 地址。 • 当选择**静态**时，需要为接口手动添加 IP 地址。对于已添加的 IP 地址，可点击 进行编辑或点击 删除。 • 当选择 **DHCP** 时，DHCP 服务器会为接口分配 IP 地址。

4. 点击**确定**。
5. 当网络连接出现问题时，可点击**重启网络服务**按钮辅助问题排查。

提示：点击**重启网络服务**按钮后，网络服务会暂停一段时间。

7.1.2. 配置 Bond 接口

1. 选择**网络/策略>接口>配置**。

2. 点击需要配置的接口对应的 图标，进行相关配置。

3. 在**属于**下拉框中选取一个 Bond 接口 bond0，将以太网接口 eth1 和 eth2 划分给此 bond0 接口。

4. 点击**确定**。在接口配置列表中，可以看到 bond0 接口。

5. 点击对应的 图标，配置 bond0 接口的相关信息。

6. 点击**确定**。

7.1.3. 配置 Bridge 接口

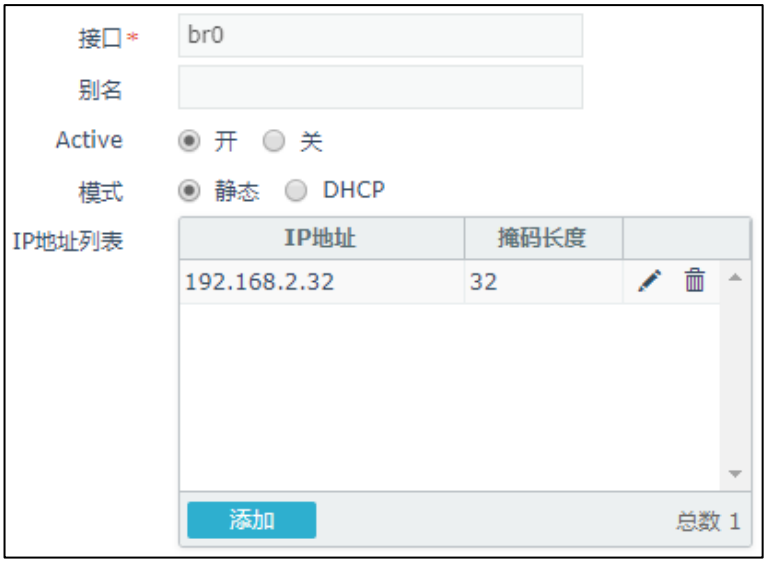
1. 选择**网络/策略>接口>配置**。

2. 点击需要配置的接口对应的 图标，进行相关配置。

3. 在**属于**下拉框中选取一个 Bridge 接口 br0，将以太网接口 eth1、eth2 划分给此 br0 接口。

4. 点击**确定**。在接口配置列表中，可以看到 br0 接口。

5. 点击对应的 图标，配置 br0 的相关信息。

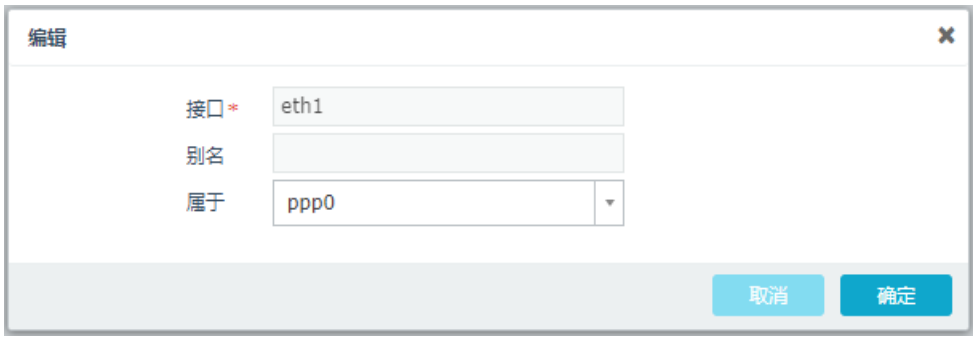


6. 点击**确定**。

7.1.4. 配置 PPPoE 接口

1. 选择**网络/策略>接口>配置**。

2. 点击 PPPoE 接口要包含的以太网接口对应的 图标，在**属于**下拉框中选取 ppp0，将以太网接口划分给此 PPPoE 接口。



3. 点击**确定**。在接口配置列表中，可以看到 ppp0 接口。

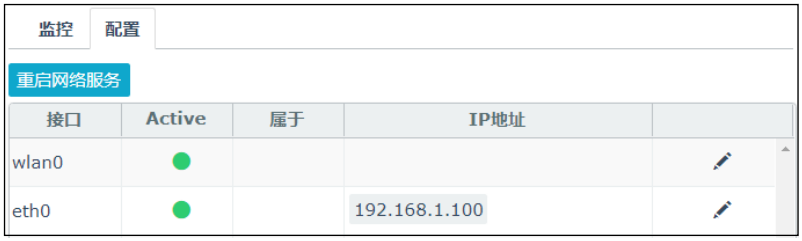
4. 点击 ppp0 对应的 图标，配置 ppp0 的相关信息。

5. 点击**确定**。

7.1.5. 配置 WLAN 接口

提示：仅NVPN3000机型支持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，进行相关配置。

   - wlan0 作为三层接口使用时，需要为其分配 IP 地址，并将其作为 DHCP 服务器接口，用于为内网无线客户端动态分配 IP 地址。

   - wlan0 作为二层接口使用时，需要将其划入 Bridge 接口，将 Bridge 接口作为 DHCP 服务器接口，用于为内网无线客户端动态分配 IP 地址。

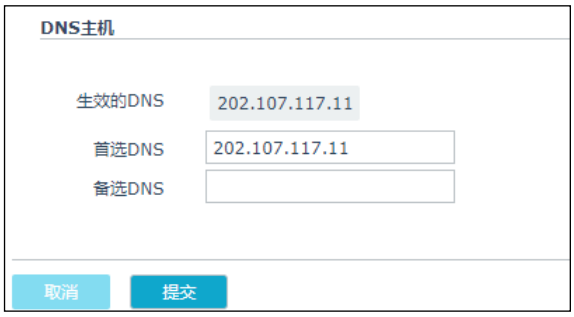
3. 点击**确定**。

提示：要允许内网无线客户端通过VPN网关接入网络，还需到**网络/策略> WiFi**页面配置无线服务。

7.2.DNS

VPN 网关可作为 DNS 客户端从 DNS 服务器获取域名解析服务，用于解析系统升级服务器、外部认证服务器等域名。

1. 选择**网络/策略> DNS**。
2. 查看当前生效的 DNS 服务器，配置首选和备选 DNS 服务器地址。



3. 点击**提交**。

7.3.Hosts

7.3.1. 修改主机名

为了方便区分设备，管理员可以修改主机名：

1. 选择**网络/策略> Hosts >主机名配置**。
2. 修改主机名。

3. 点击**提交**。

7.3.2. 更新 Hosts 配置文件

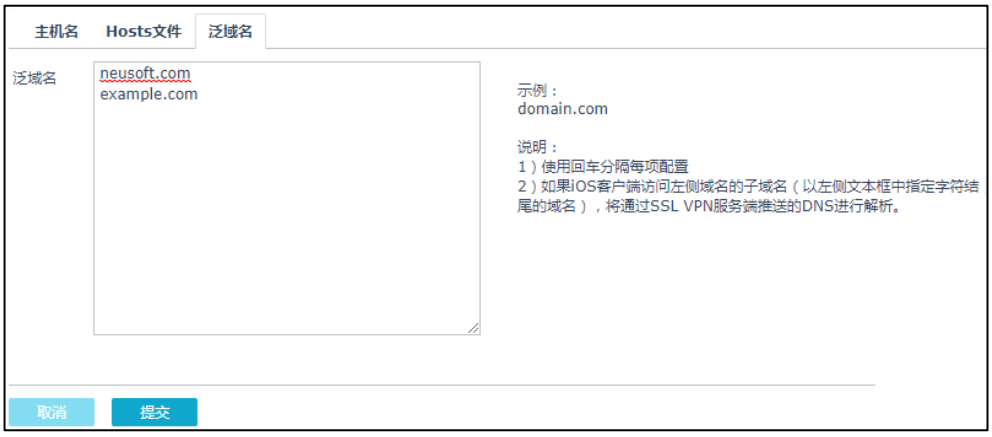
将资源域名与 IP 地址的对应关系更新到 hosts 文件中，在 VPN 网关做上静态缓存，可以大大加快内部 DNS 的解析速度，从而提升用户访问体验。

1. 选择**网络/策略> Hosts > Hosts 文件**。
2. 点击**更新 Hosts 文件**，可将资源中配置的域名和 IP 对应关系更新到 Hosts 文件中，可在上方文本框中查看更新结果。
3. 也可以手动添加资源域名与 IP 地址的映射关系，点击**提交**。

7.3.3. 泛域名

可以通过配置泛域名来指定 iOS 客户端访问某些域名时，使用 SSL VPN 服务端推送的 DNS 进行域名解析。

1. 选择**网络/策略> Hosts > 泛域名**。
2. 在**泛域名**文本框添加要配置的域名后缀，点击**提交**即可。

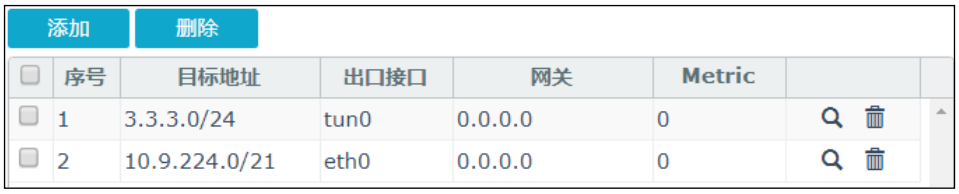


7.4.路由

管理员可以在 VPN 网关上配置静态路由和策略路由。

7.4.1. 配置静态路由

1. 选择**网络/策略>路由>静态路由**。
2. 查看系统自动探测到的路由信息：
   - VPN 隧道协商成功时自动添加的路由：目标地址为 VPN 隧道连接的虚拟子网的地址，出口接口为隧道出口接口。
   - 物理网络的直连路由：目标地址为 VPN 网关连接的物理网络的子网地址，出口接口为连接目标网络的以太网接口。



点击 查看路由信息。点击 删除路由条目。

3. 点击**添加**按钮，手动添加路由条目。
   - 添加缺省路由：

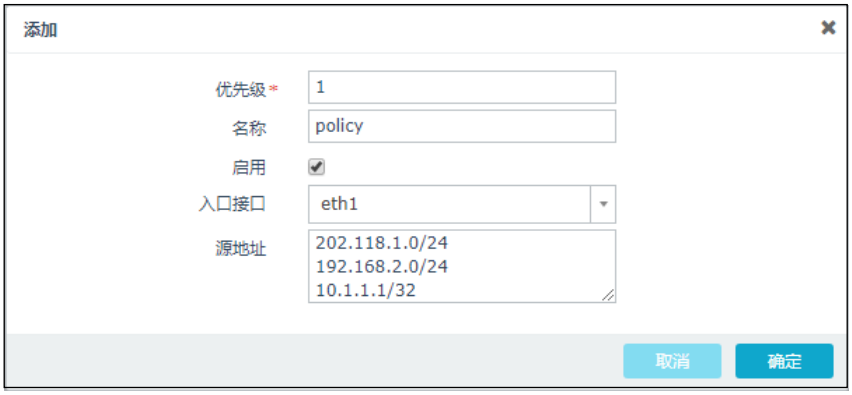
- 添加自定义静态路由：

提示：如果添加路由条目时，指定的网关不可达，路由条目将不能成功添加。

4. 点击**确定**。

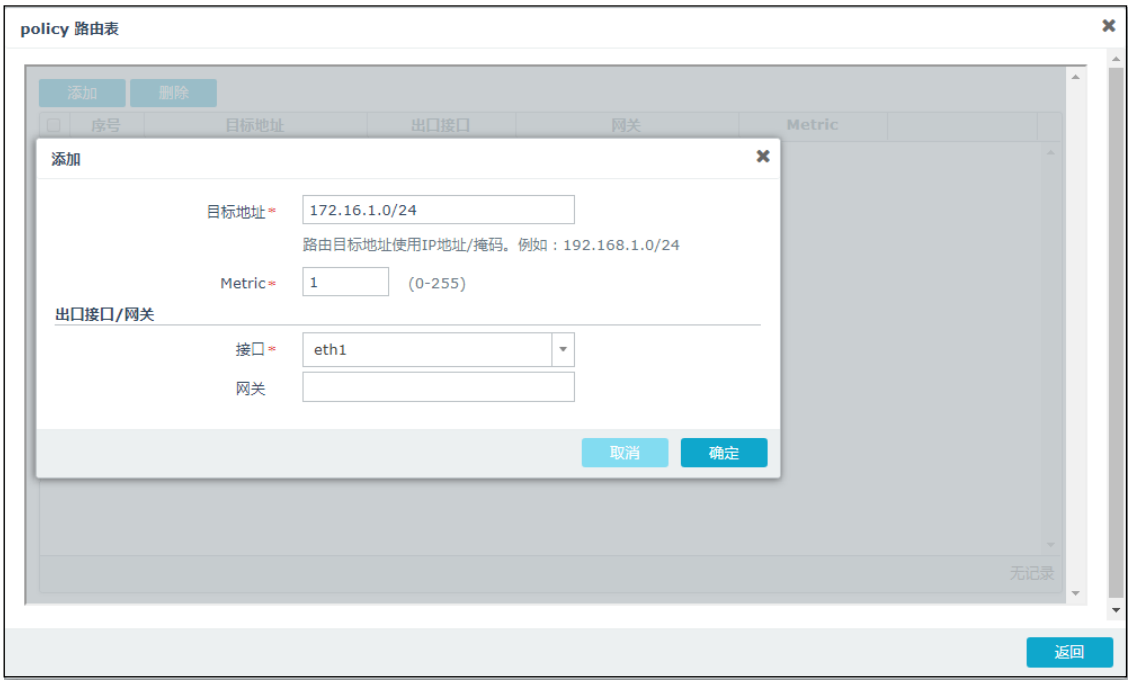
7.4.2. 配置策略路由

1. 选择**网络/策略>路由>策略路由**。
2. 点击**添加**按钮，手动添加路由的匹配策略。



3. 在策略路由列表中，点击策略对应的，为其配置路由表。

4. 在 policy 路由表中，点击**添加**，添加路由条目。



当数据包匹配以上策略时，VPN 网关会继续匹配其对应的路由表，最终根据匹配的路由将其转发出去。

5. 点击**确定**。
6. 点击**返回**，返回到策略路由页面。

7.5.智能选路

为了提高业务交付效率和用户访问体验，企业通常会架设多条线路。此时，可以通过启用 VPN 网关的智能选路功能，为用户自动选择最佳线路接入 SSL VPN。

VPN 网关内置运营商 IP 地址库，可自动更新。

1. 选择**网络/策略>智能选路**。
2. 启用智能选路功能，添加不同运营商的链路信息。

每种运营商仅允许添加一条链路。VPN 网关根据源地址将不同运营商用户的访问请求通过对应运营商的链路转发给内网服务器，然后将服务器应答返回给用户。

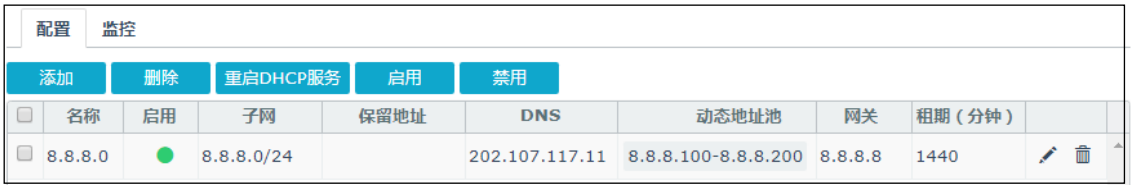
勾选**智能链路探测**，可实时探测链路健康状态，在链路故障时及时切换线路，在故障恢复后还原选路策略。

3. 点击**提交**。

7.6.DHCP 服务器

VPN 网关可以充当 DHCP 服务器，为内网客户端动态分配 IP 地址。

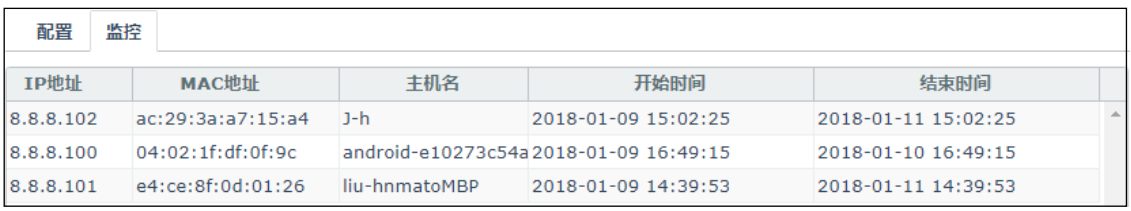
1. 选择**网络/策略> DHCP 服务器**。



2. 在**配置**页面点击**添加**，添加 DHCP 服务器。

3. 点击**确定**。点击**重启 DHCP 服务**。

4. 点击**监控**页签，查看 DHCP 地址分配情况。



7.7.WiFi

VPN 网关可以提供无线接入服务，允许内网无线客户端接入网络。

1. 选择**网络/策略>接口>配置**，为 WLAN 接口配置 IP 地址。
2. 选择**网络/策略> DHCP 服务器**，创建 DHCP 服务器，为内网无线客户端分配 IP 地址。
3. 选择**网络/策略> WiFi >配置**，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。点击**提交**。

参数	说明
启用	启用无线接入服务。
名称	无线服务的名称。
安全类型	无线服务的安全类型，固定为 WPA2 PSK（保护无线访问的一种）。
加密类型	无线服务使用的加密算法，包括 CCMP 和 TKIP 两种。
密码	无线客户端接入无线服务时需要输入的密码。
高级	点击展开或隐藏以下高级配置项： **连接数**：允许接入的最大无线客户端数。 **开启广播**：启用或禁用无线服务广播。 **MAC 过滤**：启用或者禁用 MAC 过滤功能。 选择**启用白名单**，可以设置允许接入无线网络的客户端 MAC 地址； 选择**启用黑名单**，可以设置禁止接入无线网络的客户端 MAC 地址。

如果使用过程中修改了 WiFi 服务配置，可点击**重启服务**，重启 WiFi 服务。

4. 选择**网络/策略>地址转换>源地址转换**，添加源地址转换规则，将内网无线子网地址转换为 VPN 网关外网接口的 IP 地址，使得内网无线客户端可以访问外网。

5. 选择**网络/策略>访问策略**，添加访问策略，允许内网无线客户端访问外网。
6. 当有无线客户端接入时，可点击**监控**页签，查看接入的无线客户端信息。

7.8.访问策略

本节介绍以下内容：

7.8.1. 配置全局访问策略

访问策略根据数据包的源、目的 IP 地址等特征限制数据包的转发，从而达到控制用户访问的目的。

1. 选择**网络/策略>访问策略**。
2. 查看访问策略配置信息。

- 在页面上方缺省访问控制区域，查看缺省访问控制动作，包括允许和拒绝。

  缺省访问控制表示当数据包未匹配到已配置的访问策略时，系统如何处理该数据包。缺省情况下，系统会拒绝未匹配策略的数据包通过。

- 在访问策略列表中查看系统中已经配置的访问策略。

  如果开启了隧道模式 SSL VPN 服务且隧道协商成功，系统会自动生成一条隧道访问策略“tun0”。

- 支持导入、导出访问策略。

3. 点击**添加**，手动添加访问策略。

访问策略的动作包括允许和拒绝。

- **允许**：表示系统将转发符合策略条件的数据包，并更新会话表。
- **拒绝**：表示系统将丢弃符合策略条件的数据包。

4. 点击**确定**。

7.8.2. 配置 IPSec VPN 访问策略

当网关到网关的 IPSec VPN 隧道建立成功后，系统会自动生成动作为“允许”的 IPSec VPN 访问策略。管理员可以根据需要手动添加动作为“拒绝”的策略，以限制特定隧道的数据包转发。

1. 选择**网络/策略> 访问策略**。
2. 点击配置 IPSec VPN 访问策略。
3. 查看系统自动生成的 IPSec VPN 访问策略。

- 网关到网关：

序号	名称	动作	入口接口	源地址	出口接口	目的地址	方向	协议	端口
1		LOG	eth1	192.168.2.0/24	任意	192.168.1.0/24	In	任意	
2		ACCEPT	eth1	192.168.2.0/24	任意	192.168.1.0/24	In	任意	
3		LOG	任意	192.168.1.0/24	eth1	192.168.2.0/24	Out	任意	
4		ACCEPT	任意	192.168.1.0/24	eth1	192.168.2.0/24	Out	任意	

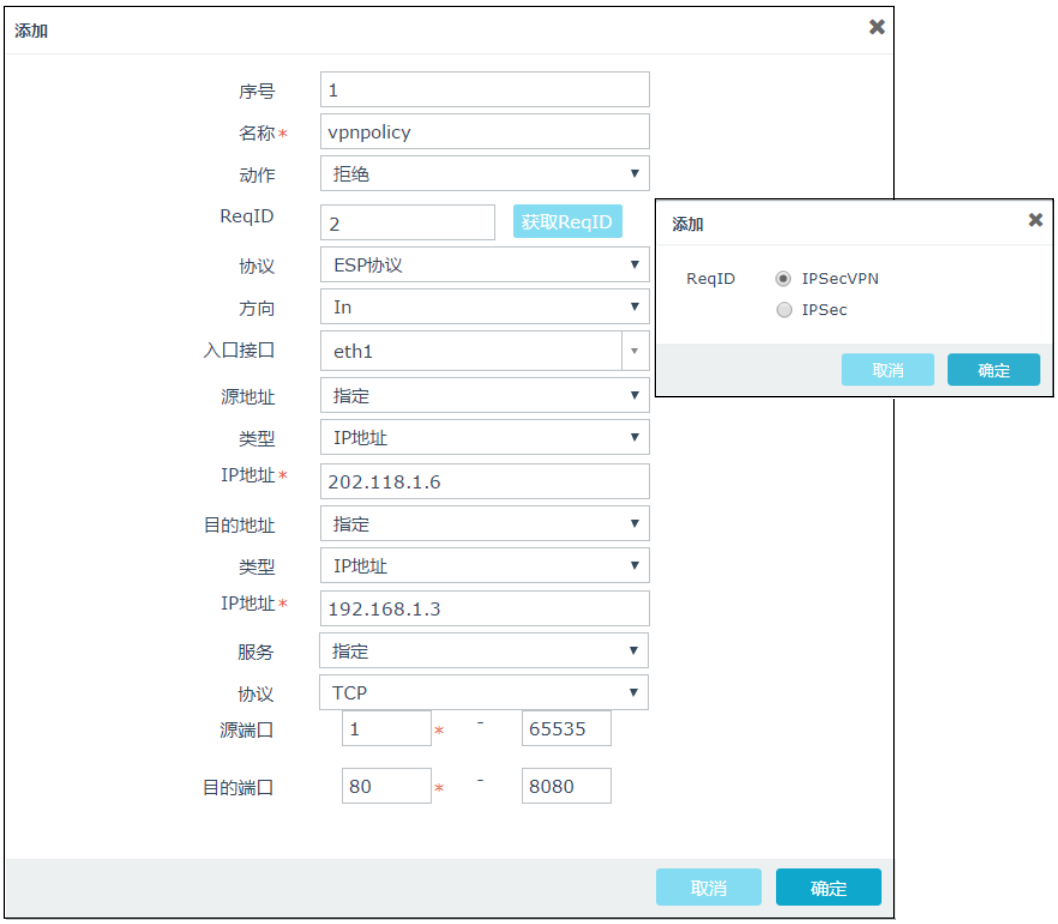
  - 如果配置 IPSec VPN 隧道时为两端网关分别指定了一个本地子网和一个对端子网，则在本端和对端网关分别生成两条反方向的访问策略。
  - 如果配置 IPSec VPN 隧道时指定了多个本地子网和对端子网，则按照本端和对端的子网组合在本端和对端网关分别生成双向的访问策略。
  - 如果配置 IPSec VPN 隧道时启用了日志功能，则针对每对子网间的访问策略再分别生成一条日志访问策略。

- 远程访问：

序号	名称	动作	入口接口	源地址	出口接口	目的地址	方向	协议	端口
1	test	LOG	eth0	9.9.0.1/32	任意	192.168.2.100/32	In	UDP	
2	test	ACCEPT	eth0	9.9.0.1/32	任意	192.168.2.100/32	In	UDP	
3	test	ACCEPT	eth0	9.9.0.1/32	任意	192.168.2.100/32	In	TCP	
4	test	LOG	任意	192.168.2.100/32	eth0	9.9.0.1/32	Out	UDP	
5	test	ACCEPT	任意	192.168.2.100/32	eth0	9.9.0.1/32	Out	UDP	
6	test	ACCEPT	任意	192.168.2.100/32	eth0	9.9.0.1/32	Out	TCP	

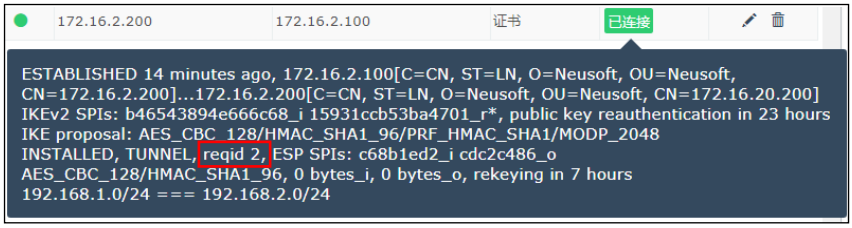
  - 远程用户一旦拨号成功，VPN 网关将根据为其授权的资源范围自动生成访问策略，针对每个资源分别生成两对进出向访问策略，一条 TCP，一条 UDP。
  - 如果远程访问 IPSec VPN 开启了日志记录功能，还将针对每个资源分别生成双向的日志访问策略。

4. 点击**添加**，针对指定隧道添加访问策略，进一步限制用户对 IPSec VPN 资源的访问。



点击**获取 ReqID**，选取已建立的隧道名称，点击**确定**，系统会自动添加获取到的隧道 ID 信息。

管理员也可以选择**基础功能> IPSec VPN**，鼠标指向已连接隧道的连接状态获取 ReqID 信息。

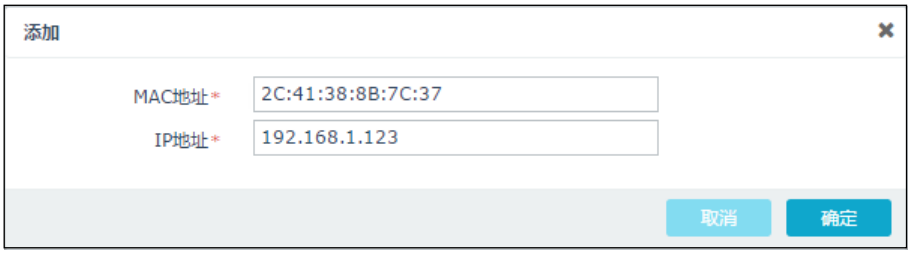


5. 点击**确定**。

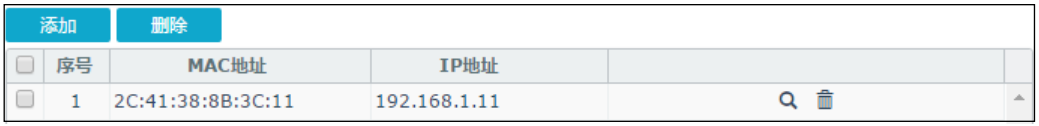
7.9.IP-MAC 绑定

VPN 网关可以将主机的 IP 地址及其网卡的 MAC 地址绑定到一起，防止非法主机冒用合法主机的 IP 地址。

1. 选择**网络/策略> IP-MAC 绑定**。
2. 点击**添加**，添加 IP-MAC 绑定策略。



3. 查看已添加的 IP-MAC 绑定策略。



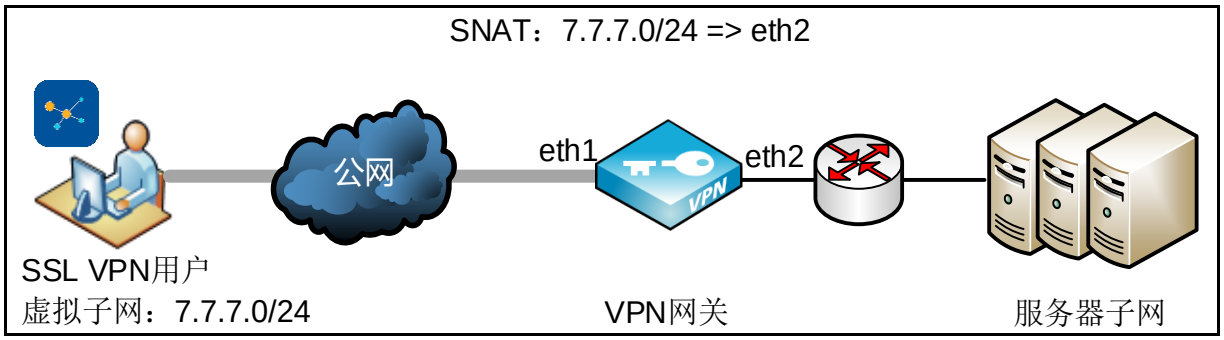
7.10.地址转换

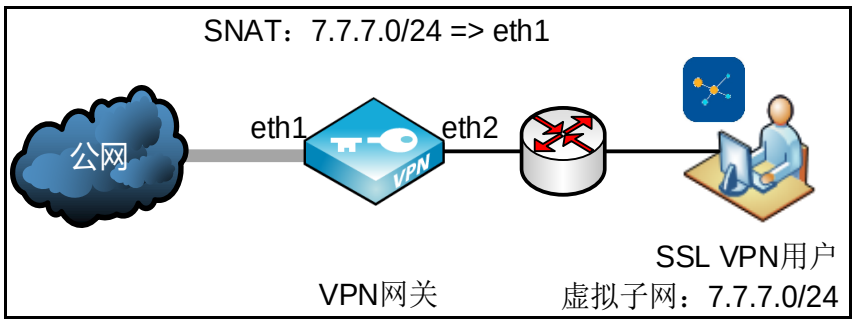
VPN 网关支持源地址转换和目的地址转换，作用如下：

- 源地址转换能够帮助网络用户通过很少的公网 IP 地址接入到互联网中。
- 目的地址转换能够隐藏内部主机的 IP 地址及网络拓扑，一定程度上避免遭受外部攻击，保证内部网络安全。

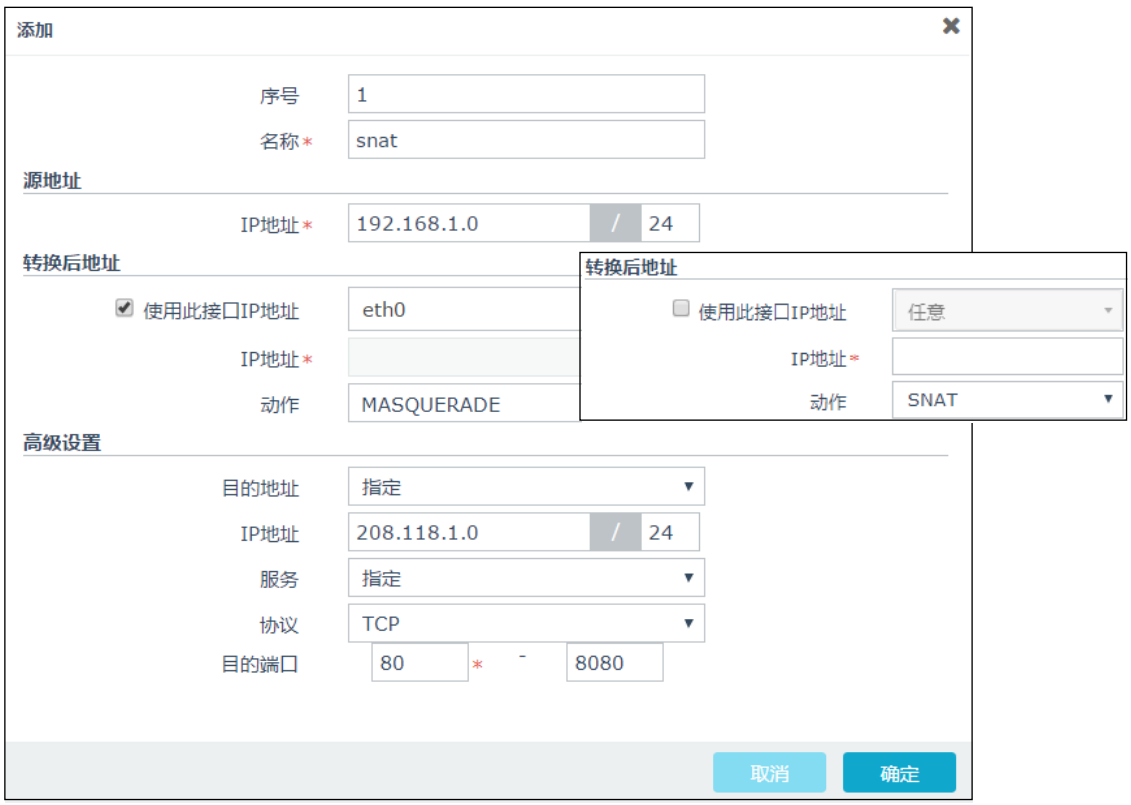
以下两种情况也需要配置源地址转换规则，使返回的数据包可以送达目的地：

- SSL VPN 用户从外网访问内网服务器，内网服务器和 VPN 网关之间存在路由设备，内网服务器的网关指向路由设备。
- SSL VPN 用户从内网访问 Internet，用户客户端和 VPN 网关之间存在路由设备，用户客户端的网关指向路由设备。





1. 选择**网络/策略>地址转换**。
2. 在源地址转换页签点击添加，在弹出的对话框中填入所需内容，点击确定。



参数	说明
源地址	一般是允许访问外网的内网子网的 IP 地址。 使用隧道模式 SSL VPN 服务时添加的源地址转换规则中，源地址为系统分配给 SSL VPN 客户端的虚拟子网 IP 地址。

转换后地址	一般是外网接口 IP 地址或指定公网 IP 地址。
	• **使用此接口 IP 地址**：适用于拨号网络或是使用 DHCP 获取 IP 地址的情况。只需选择接口而无需设置固定 IP 地址，此接口动态获取的 IP 地址将作为转换后的 IP 地址。
	VPN 网关对数据包的处理动作可以设置为 MASQUERADE（将源地址转换为接口 IP 地址后继续与其他策略进行匹配）或 ACCEPT（不转换直接允许数据包通过）。
	• **IP 地址**：将源 IP 转换为该指定 IP 地址。
	VPN 网关对数据包的处理动作为 SNAT（直接将源地址转换为指定 IP 地址）。
	使用隧道模式 SSL VPN 服务时添加的源地址转换规则中：
	  • 如果 SSL VPN 用户从外网访问内网，转换后地址为连接目标服务器的内网接口 IP 地址。
	  • 如果 SSL VPN 用户从内网访问外网，转换后地址为 VPN 网关外网接口的 IP 地址。

高级设置	可以指定过滤条件，只有符合过滤条件的数据包才进行地址转换。

3. 点击**目的地址转换**页签，点击**添加**，在弹出的对话框中输入所需内容，点击**确定**。

参数	说明
入口接口	连接外网的接口。
目的地址	外网用户访问的服务器公网 IP 地址和端口号。
转换后地址	外网用户访问的内网服务器的真实 IP 地址和端口号。
高级设置	可以指定过滤条件，只有符合过滤条件的数据包才进行地址转换。

7.11.攻击防御

管理员可以配置 DDoS 攻击防御和 IP 选项校验策略，以防止 VPN 网关系统或 VPN 网关后面的服务器资源遭受 DoS/DDoS 攻击。

1. 选择**策略>攻击防御**。
2. 在 **DDoS 防御**页签中，选择对**当前系统**或**后台服务器**进行保护。
   - **当前系统**：指当前配置用于保护 VPN 网关自身的系统安全。
   - **后台服务器**：指当前配置用于保护 VPN 网关后面的内部服务器。

   选择**当前系统**或**后台服务器**进行相关配置并提交后，再选择另外一种保护对象进行配置并提交，针对两种保护对象的配置将同时生效。切换回之前的保护对象时，可看到之前针对该保护对象所配置的信息。
3. 配置每类攻击数据包的阈值并勾选**丢弃**，当数据包数量达到阈值时 VPN 网关丢弃后续数据包。

4. 点击**提交**。

5. 点击 **IP 校验选项**，勾选**丢弃**。当 VPN 网关收到相应的攻击包会丢弃后续数据包。IP 校验选项适用于对后台服务器的保护。

6. 点击**提交**。

第8章 系统管理

本章介绍 VPN 网关的系统管理功能，内容包括：

8.1.管理员

系统默认存在一个超级管理员 root，可以添加管理员、审计员和 HA 用户。管理用户角色和权限划分如下表所示：

用户角色	权限
Root	系统缺省管理用户，用户名/密码为 root/neteye。全局唯一，不可删除。 具有系统配置的所有权限以及添加和管理其他角色用户的权限。
管理员	由 root 添加。能进行除管理员、认证服务器、高可用性、备份/恢复、系统升级、时间修改、管理日志清除之外的系统配置。
审计员	由 root 添加。仅具有查看以下页面的权限： • 主页 • 监控：所有页面 • 日志：所有页面 • 网络/策略：所有页面 • 系统管理：系统时间（仅能查看当前系统时间）、证书、Licenses、版权
HA 用户	由 root 添加。仅用于 HA 同步认证。 为了方便用户使用，系统默认提供一个 HA 用户，缺省用户名/密码为 ha/neteye。

1. 以 root 用户身份登录，选择**系统管理>管理员**。
2. 查看系统默认的管理用户信息。点击 图标可修改用户密码。

3. 点击**添加**，添加所需角色（管理员、审计员、HA 用户）管理用户。

4. 点击**确定**。

5. 点击右上角的**配置密码策略**，为管理用户配置密码策略。

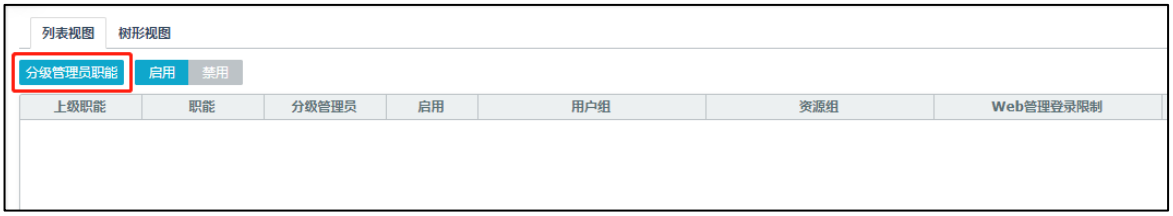
6. 点击**确定**。

8.2.分级管理员

随着用户数量、资源数量、VPN 策略数量的日益增长，系统管理员（Root、管理员）在日常管理工作中要处理大量的用户、资源、VPN 策略等的创建或划分操作，操作量大且复杂繁琐，不利于用户管理工作的进行。新增的分级管理员功能可以很好的解决这一问题，系统管理员（Root、管理员）可以按照部门、团队等组织结构来创建分级管理职能，为分级管理职能分配合适的分级管理员，然后可以把部分资源和用户划分给此分级管理员进行管理。分级管理员可以根据实际需要，针对上级划分的用户、资源，重新创建、划分用户组、资源组以及 VPN 策略，达到分担系统管理员（Root、管理员）日常管理工作的效果。要支持分级管理员功能，需要导入开启了分级管理员功能的 license，目前最多支持 16 级分级管理员。

1. 以 root（或管理员）用户身份登录，选择**系统管理 > 分级管理员**。
2. 点击**启用**，保证分级管理员功能开启，当不需要分级管理员功能时可以点击**禁用**，禁用后全部分级管理员将无法登录管理页面。

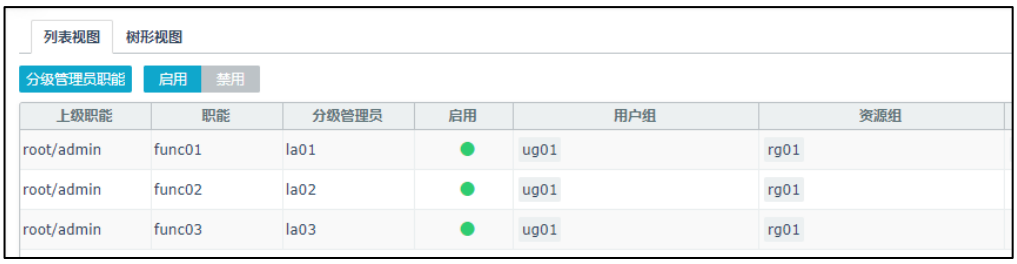
3. 点击**分级管理员职能**，添加新的分级管理职能。

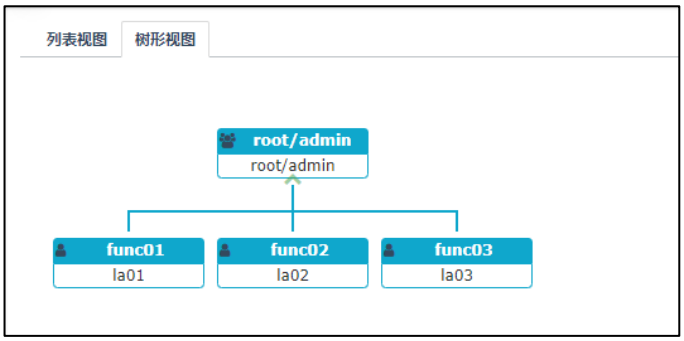


4. 根据实际需要，为分级管理职能指定分级管理员，点击**分级管理员**可以选择**选择模式**或者**编辑模式**进行分级管理员的指定。对于系统管理员（Root、管理员），在创建分级管理职能时，可以在**上级职能**选择框指定其上级职能，但是对于分级管理员，在创建分级管理职能时，上级职能默认为当前登录的分级管理职能且不可修改。可以通过**职能**文本框设置此分级管理职能的职能名称。可以通过**启用**勾选项来启用和禁用此分级管理职能，禁用后此分级管理职能的分级管理员无法登录管理页面。可以通过下面的**用户组**标签页划分想要分配给此分级管理职能管理的用户，通过**资源组**标签页划分想要分配给此分级管理职能管理的资源。在**高级设置**标签页，可以通过**添加下级管理员**勾选项来配置是否允许此分级管理职能再创建下级分级管理职能，默认为开启；可以通过

编辑本地用户属性勾选项来配置是否允许此分级管理职能编辑划分给它的本地用户的属性，默认为关闭；可以通过 **WEB 管理登录限制**文本框来配置允许哪些子网或者 IP 地址段以此分级管理职能的身份登录管理页面。

5. 可以通过点击**列表视图**选项卡或**树形视图**选项卡来切换分级管理职能的显示模式。

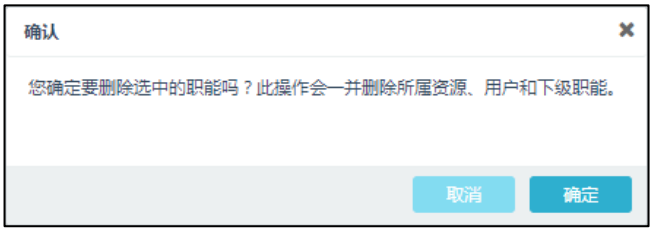




列表视图中方便进行分级管理职能的添加、编辑、删除等操作，树形视图中方便查看各分级管理职能之间的上下级关系。

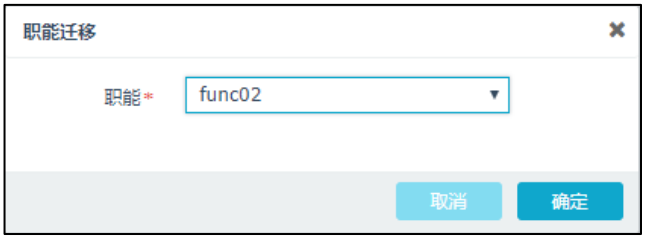
6. 在列表视图中，可以点击分级管理职能条目后的 图标对分级管理职能进行**编辑**操作。

7. 在列表视图中，可以点击分级管理职能条目后的 图标对分级管理职能进行**删除**操作。

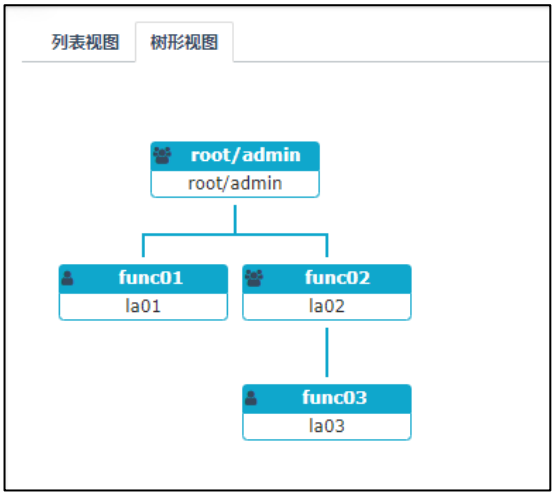


注意，删除分级管理职能会一并删除此职能下创建的资源、资源组、用户组、VPN 策略、下级职能以及所有下级职能下创建的各对象，所以请谨慎操作。

8. 在列表视图中，可以点击分级管理职能条目后的 图标对分级管理职能进行**职能迁移**操作。职能迁移操作是用于把当前职能迁移至其他职能的下级，即更换当前职能的上级职能。



例如将 5 中的 func03 职能迁移至 func02 的下级。迁移后可以在树形视图中查看迁移后的职能组织结构。



9. 在列表视图中，可以点击分级管理职能条目后的 图标对分级管理职能进行**工作移交**操作。工作移交操作是用于更换当前分级管理职能的分级管理员。

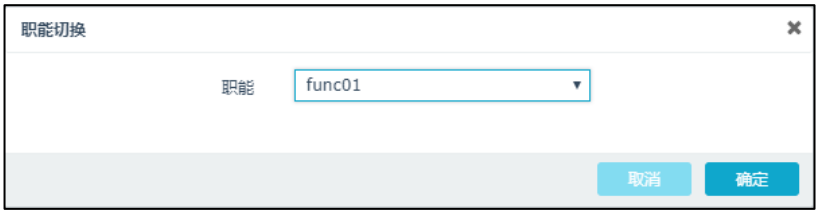
例如把 func01 职能的分级管理员由 la01 重新指定为 la03。工作移交后可以在列表视图中看到分级管理职能对应的分级管理员的变化。

10. 分级管理员的登录入口和系统管理员（Root、管理员）是一致的。对分级管理员开放的管理页面内容主要包括：主页的部分信息、基础功能->资源、基础功能->资源组、基础功能->用户、基础功能->用户组、基础功能->VPN 策略、监控->在线用户、系统管理->分级管理员。

11. 在基础功能中的资源、资源组、用户组页面中新增了归属者、授权职能 2 列，归属者表示此对象是由哪个分级管理员创建的，如果对象是由系统管理员（Root、管理员）创建的，则归属者这 1 列显示“-”，授权职能表示该对象都被分配给了哪些分级管理职能。因为目前不支持 VPN 策略的划分，所以在 VPN 策略页面中仅新增了归属者 1 列。

12. 分级管理员可以根据上级划分的资源、用户，自行创建资源、资源组、用户组、VPN 策略。但是分级管理员不应该创建超出上级划分的资源地址范围的资源，也不应该在用户组中添加不包含在上级划分的用户列表里的用户。如果分级管理员创建了超出上级划分的资源地址范围的资源，则会通过把地址栏标红并添加删除线来警告这是一条非法资源。分级管理员创建的非法资源、资源组、用户组在实际策略中不会生效。

13. 一个分级管理员可能对应着多个分级管理职能，分级管理首次登录时，系统会以默认的分级管理职能登入管理页面。分级管理员可以点击管理页面右上角的角色下拉选择按钮，然后点击职能切换，进行名下分级管理职能的切换。



选择要切换的职能后，点击确定，页面会自动刷新并以切换后的分级管理职能登入管理页面。

8.3.访问控制

可以通过对访问控制的配置，实现对 VPN 设备访问权限的限制，阻挡那些来自不安全、不可靠地址的访问请求，来进一步保证 VPN 的安全、稳定。

1. 选择**系统管理 > 访问控制**。
2. 目前主要支持 Web 管理页面、SSH、Ping 的访问控制。可以通过选择**允许 SSH 访问、允许 Ping 访问**后的单选项来开启和关闭 SSH 以及 Ping 服务。因为 Web 管理页面是基本的对 VPN 设备的管理途径，所以不允许关闭此服务。访问控制列表默认为空，表示全网段都可以访问。将允许访问的子网信息配置在访问控制列表，并点击**提交**即可。

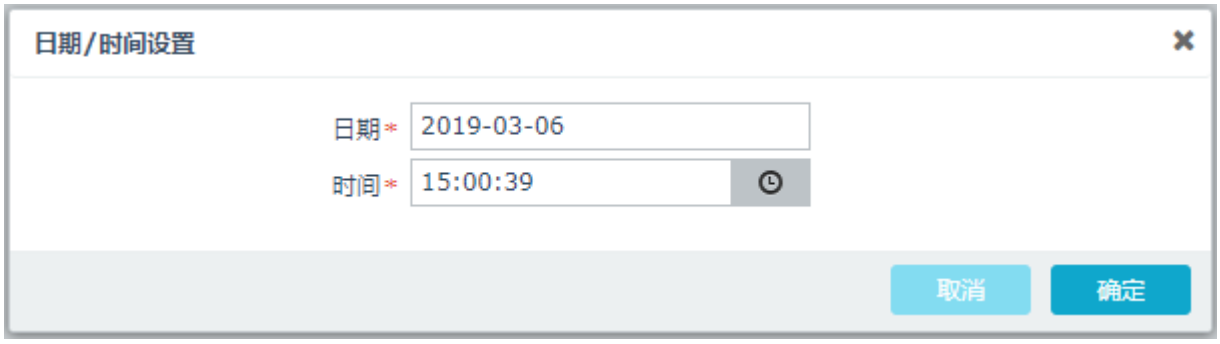
8.4.系统时间

为了能准确记录系统日志，必须保证系统时间正确。系统支持手动修改时间和通过 NTP 服务器自动同步时间。

1. 选择**系统管理>系统时间**。

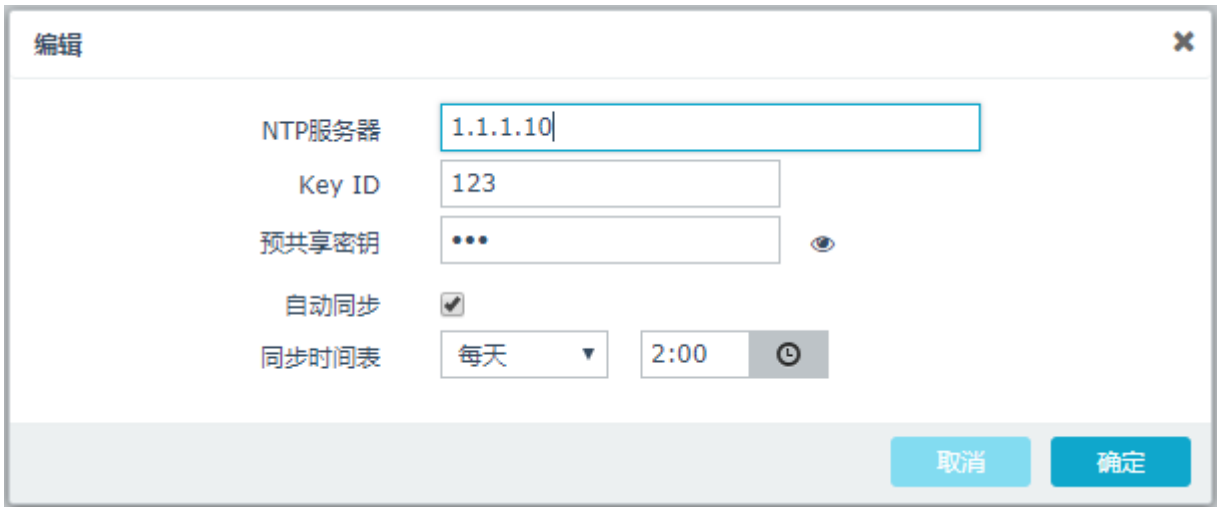
2. 点击**当前时间**对应的，手动修改系统时间。

   在弹出的对话框中点击日期和时间文本框，选择日期和时间，或根据原有格式输入日期和时间，点击**确定**。



3. 点击**同步系统时间**对应的。在弹出的对话框中填写 NTP 服务器域名或 IP 地址，Key ID 和预共享密钥如果有需要填写，勾选**自动同步**，设置同步时间表，点击**确定**，系统将周期性自动更新系统

时间。



4. 启用自动同步并设置 NTP 服务器后，点击**立即同步**按钮，可立即同步系统时间。

8.5.邮件服务器

如果在设置 Web 模式 SSL VPN 服务时启用了邀请注册功能，则需要配置邮件服务器，用于发送邀请码和验证码邮件。验证码和邀请码为注册 SSL VPN 用户时必须使用的两个字符串。

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。

参数	说明
服务器地址	用于发送邀请码和验证码邮件的邮件服务器域名或 IP 地址。 填写域名时，还需设置 DNS 服务器地址。只有
端口	邮件服务器端口号，必须和服务器端设置保持一致。
安全连接	是否使用安全连接，包括 SSL/TLS 和 STARTTLS，必须和服务器端设置保持一致。
发件人	指管理员发送邀请码时所使用的邮箱账号。
测试邮件服务器配置	测试上面配置的邮件服务器是否可达。

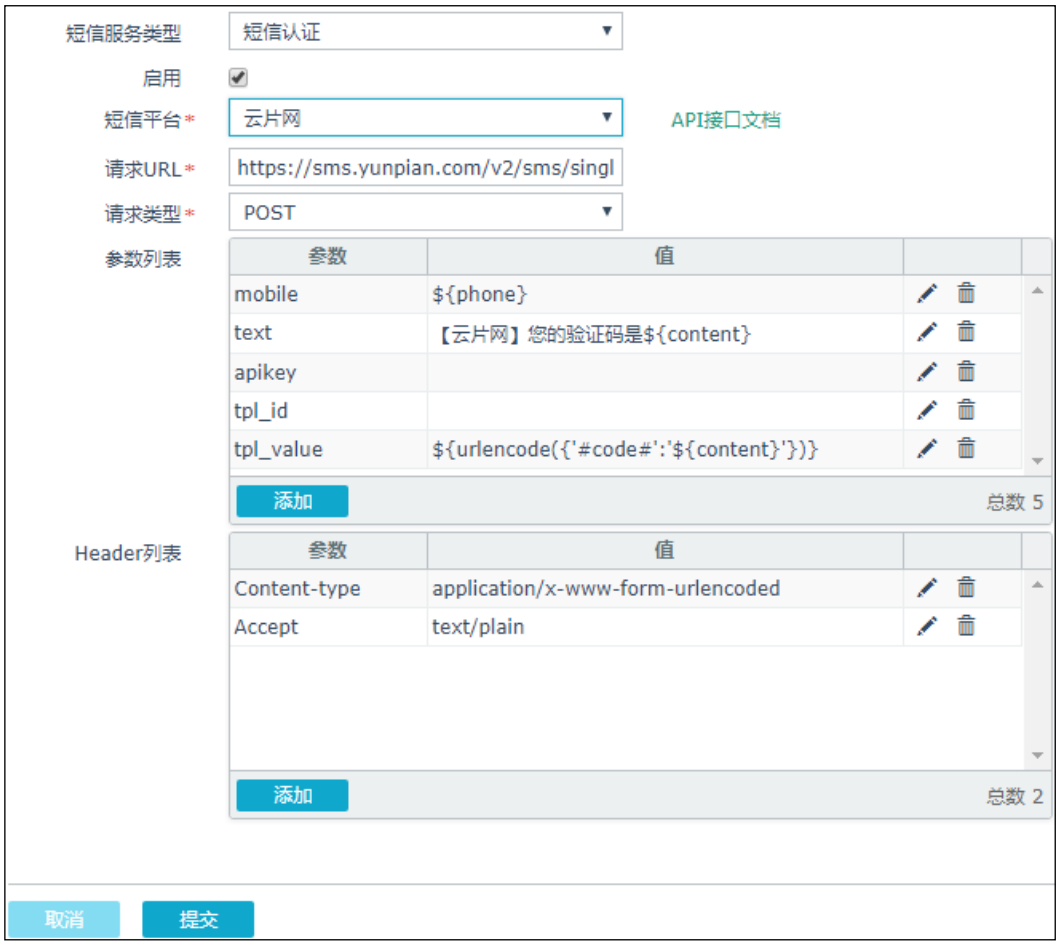
提示：使用邀请码注册的SSL VPN用户则通过注册时使用的邮箱账号发送邀请码。

3. 点击**提交**。
4. 点击**测试邮件服务器配置**，可以测试邮件服务器配置是否正确。

8.6.短信服务

如果为 SSL VPN 用户启用了短信认证服务，需要事先配置短信服务平台及相关参数。

1. 选择**系统管理>短信服务**。
2. 启用短信服务，选择短信平台，系统会提供一套缺省配置，可根据需要修改配置。



参数	说明
短信服务类型	目前仅支持短信认证一种服务，将来可能增加找回密码或注册新用户等短信服务。
启用	启用短信服务。
短信平台	目前支持云片网、云之讯、Luosimao、梦网、网易云信、阿里云、Other 几种。 VPN 网关针对每种短信平台都提供一套缺省配置，管理员可以根据实际需要进行修改。 可点击 **API 接口文档**查看每种短信平台的接口说明。
请求 URL	短信平台接收短信服务请求的 URL 地址。
请求类型	包括 POST 和 GET 两种。
参数列表	VPN 网关请求短信平台发送短信验证码所需参数。

${phone}：表示需要替换的电话号码变量，后台会自行替换，无需改动。

${content}：表示需要替换的发送内容变量，后台会自行替换，无需改动。

${urlencode()}：表示需要对()中的字符串进行 url 编码，某些短信平台有这个需求，当前各平台模板已经配置好，无需改动。

${b64encode()}：表示需要对()中的字符串进行 base64 编码，某些短信平台有这个需求，当前各平台模板已经配置好，无需改动。

${gbkencode()}：表示需要对()中的字符串进行 gbk 编码，某些短信平台有这个需求，当前各平台模板已经配置好，无需改动。

${uuid}：表示需要替换的随机数变量，后台会自行替换，无需改动。

${signature}：表示需要替换的签名，后台会根据当前短信平台以及输入参数进行构建并替换，无需改动。

${timestamp_UTC}：表示需要替换的 UTC 格式时间戳变量，后台会自行替换，无需改动。

${timestamp_GMT}：表示需要替换的 GMT 格式的时间戳变量，后台会自行替换，无需改动。

Header 列表	VPN 网关请求短信平台发送短信验证码所需的特定 Header 字段。 对于网易云信平台，需要填写 AppKey 和 AppSecret 两个 Header 参数的值。

提示：系统缺省已给出各短信平台所需参数，部分参数已给出默认值，管理员只需要设置默认值为空的参数。管理员需要到相应的短信平台上注册服务，获取相关参数信息。

3. 点击**提交**。

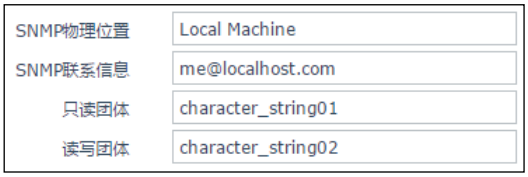
8.7.SNMP 配置

VPN 网关支持 SNMP 管理，支持 SNMPv1、v2 和 v3 版本。网络管理员可以通过 SNMP 管理站查询 VPN 网关的配置信息，但是不能修改其配置。

在 SNMPv1 和 SNMPv2 中，管理站和 VPN 网关设备之间通过团体字符串进行认证，数据通过明文传输。在 SNMPv3 中，管理站和 VPN 网关之间通过 SNMP 用户信息进行认证。VPN 网关接受管理站的访问时，会根据保存的 SNMP 用户信息对管理站进行认证。

1. 选择**系统管理> SNMP 配置**。
2. 勾选**启用 SNMP 服务**。SNMP 的通信端口号为 161。

3. 通过 SNMPv1 和 SNMPv2 通信时，填写团体字符串及必要信息。



提示：VPN网关上配置的团体字符串必须与管理站配置的团体字符串一致。

4. 当使用 SNMPv3 通信时，需要配置 SNMP 用户。
   a. 在用户列表中，点击**添加**，在弹出对话框中输入所需内容。

提示：如果配置了SNMP用户认证或加密，则管理站上也要进行相应设置。

   b. 点击**确定**。
5. 点击**提交**。

8.8.高可用性

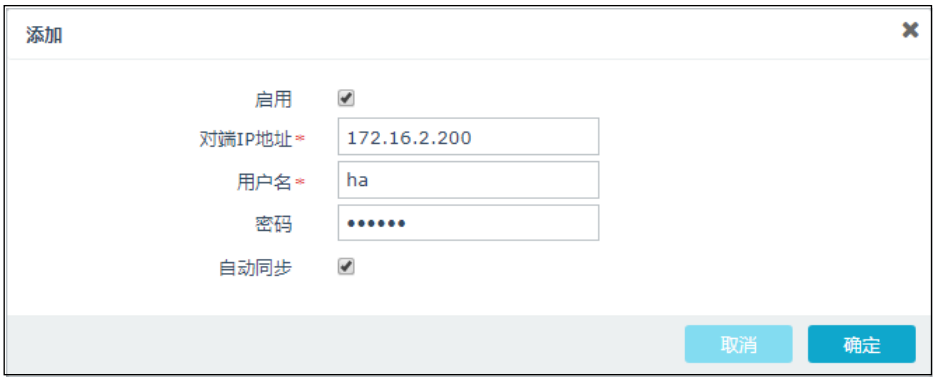
高可用性可以防止设备单点故障导致的网络中断。VPN 网关可以在多台设备间实现高可用性。高可用性配置包括：

- 配置同步
- 集群

8.8.1. 配置同步

要使用高可用性功能，需要配置对端信息，用于在 HA 设备之间同步配置信息和运行信息，保证配置一致，进行故障切换时服务不中断。

1. 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。



用户名和密码为对端设备的 HA 用户的用户名和密码，缺省为 ha/neteye。

在配置本端高可用性之前，可参照管理员在对端设备上添加 HA 用户。

3. 点击**确定**。
4. 点击**提交**。
5. 提交配置后，在提交按钮后面将出现一个**立即同步**按钮。如果对端也完成了配置同步的设置，点击该按钮，可立即同步本端配置信息到对端。

提示：高可用性配置同步功能需在两端设备上分别配置，以便配置有修改时，能够相互同步。建议在一端设备上完成所有配置后，同步到对端设备。

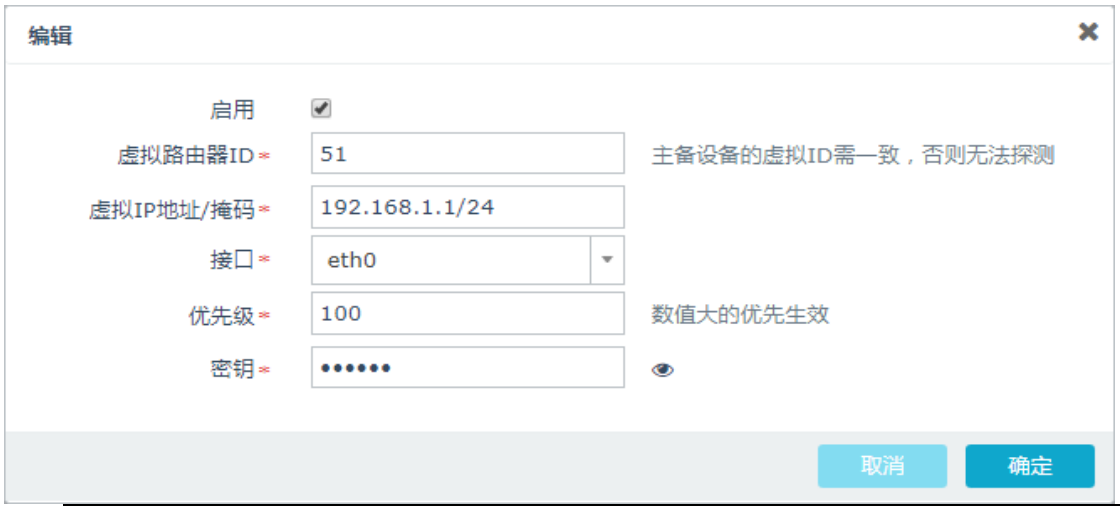
8.8.2. 集群

集群（虚拟路由器）通常由两台 VPN 网关设备组成。一台为主设备，负责转发数据包；另一台为备用设备，不转发数据包，仅负责监听主设备状态。两台 VPN 网关上运行虚拟路由冗余协议并通过此协议

选举主设备。当主设备故障时，备用设备被选举为新的主设备，接替原主设备的工作。因此，集群可以有效保障企业业务的可靠性。

1. 选择**系统管理>高可用性>集群**。
2. 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。



参数	说明
启用	勾选表示启用虚拟路由器。
虚拟路由器 ID	虚拟路由器的唯一标识，取值范围是 1～255 的整数。
虚拟 IP 地址/掩码	指虚拟路由器的备份 IP 地址。此 IP 地址用于网络通信。
接口	指转发流量的接口。
优先级	虚拟路由器的优先级，取值范围是 1～254 的整数。数值越大，优先级越高。
密钥	指对虚拟路由器内成员之间 VRRP 报文和通讯数据采用简单的明文方式的认证。 认证信息为 1～8 字节 UTF-8 字符，不能包含问号和空格。 两台成员设备之间需要配置相同的认证信息。

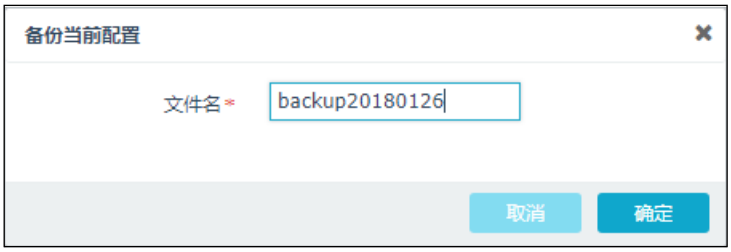
提示：单臂模式下两端网关配置一个虚拟路由器（ID须相同）即可，网关模式下则需要在两端网关上分别配置两个虚拟路由器（两端的ID也必须相同）。

4. 点击**确定**。点击**提交**。

8.9.备份/恢复

通过备份/恢复功能，用户可以备份系统配置信息，并通过备份文件恢复系统配置。系统支持手动备份和自动备份，备份文件可下载到管理 PC，也可由管理 PC 上传到系统。

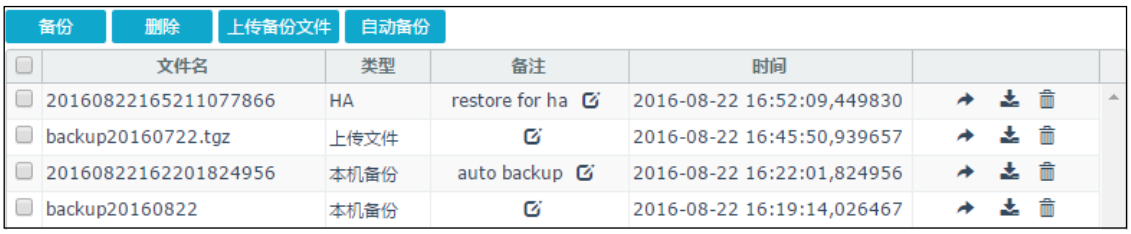
1. 选择**系统管理>备份/恢复**。
2. 点击**备份**按钮，输入备份文件名，点击**确定**。



3. 点击**自动备份**按钮，设置备份方式，点击**确定**。

   备份方式包括本地和 FTP。如果选择 FTP 备份，还需设置 FTP 服务器信息。

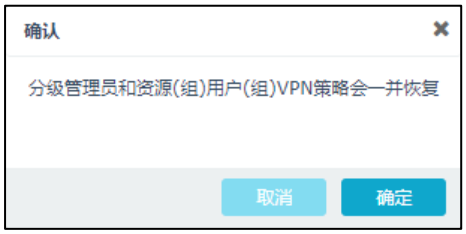
4. 点击**上传备份文件**按钮，可上传本地备份文件到系统。
5. 查看生成的备份文件。



6. 点击 图标可编辑备份文件的备注信息。
7. 点击 图标，可设置要恢复的内容，使用当前选中的备份文件恢复系统配置。

提示：以上回复配置项中，“接口”包含接口和DNS的配置信息，“访问策略”包含访问策略、IP-MAC绑定、地址转换和攻击防御的配置信息。

对于分级管理员的备份/恢复，因为分级管理员功能依托于资源(组)用户(组)VPN 策略的体系结构，当恢复分级管理员或者资源(组)用户(组)VPN 策略两者其中之一时，分级管理员和资源(组)用户(组)VPN 策略会一并恢复。



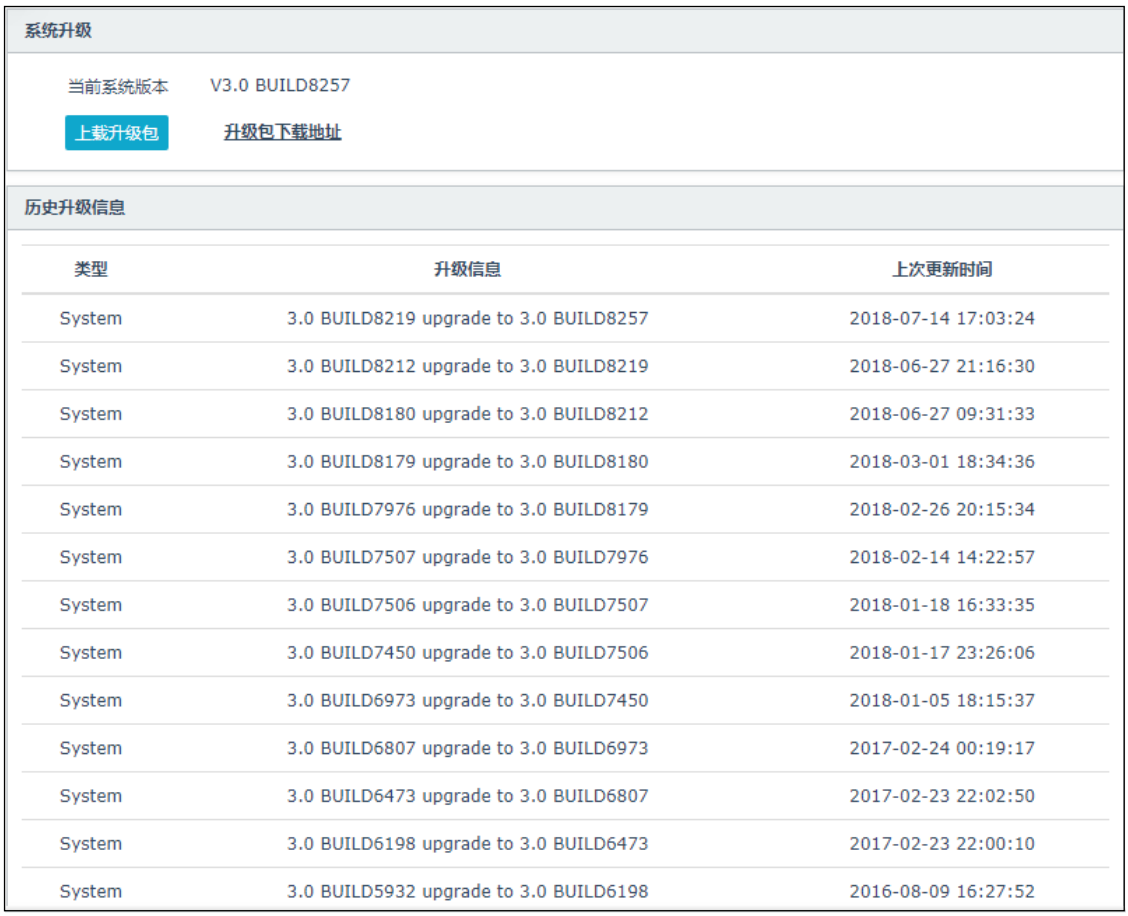
8. 点击图标，可下载备份文件到本地。

8.10.系统升级

系统升级用于修复系统缺陷或增强系统功能。

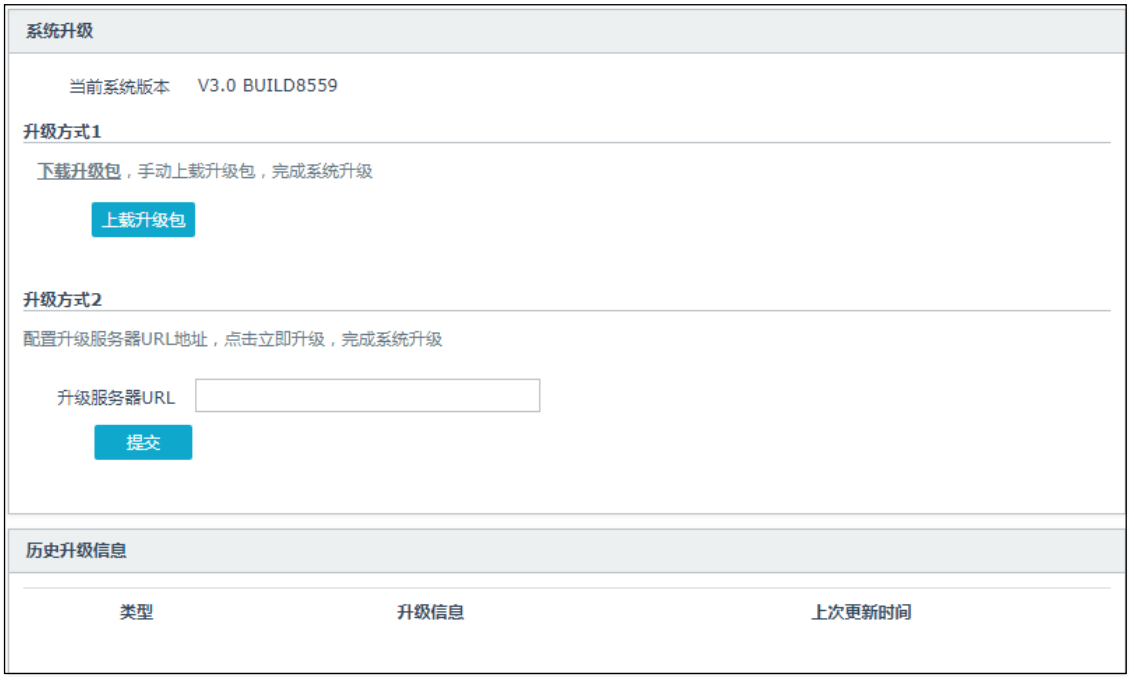
提示：系统升级可能会导致之前的备份包无法恢复，建议升级后立即执行备份。

1. 选择**系统管理>升级**。
2. 查看系统版本信息和系统升级历史信息。
   - 基于 4922 版本 ISO 安装升级包升级至 7257 版本：



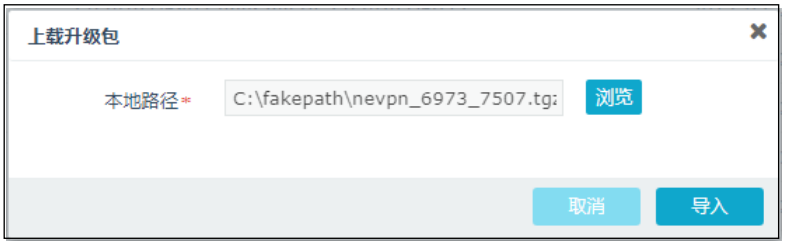
类型	升级信息	上次更新时间
System	3.0 BUILD8219 upgrade to 3.0 BUILD8257	2018-07-14 17:03:24
System	3.0 BUILD8212 upgrade to 3.0 BUILD8219	2018-06-27 21:16:30
System	3.0 BUILD8180 upgrade to 3.0 BUILD8212	2018-06-27 09:31:33
System	3.0 BUILD8179 upgrade to 3.0 BUILD8180	2018-03-01 18:34:36
System	3.0 BUILD7976 upgrade to 3.0 BUILD8179	2018-02-26 20:15:34
System	3.0 BUILD7507 upgrade to 3.0 BUILD7976	2018-02-14 14:22:57
System	3.0 BUILD7506 upgrade to 3.0 BUILD7507	2018-01-18 16:33:35
System	3.0 BUILD7450 upgrade to 3.0 BUILD7506	2018-01-17 23:26:06
System	3.0 BUILD6973 upgrade to 3.0 BUILD7450	2018-01-05 18:15:37
System	3.0 BUILD6807 upgrade to 3.0 BUILD6973	2017-02-24 00:19:17
System	3.0 BUILD6473 upgrade to 3.0 BUILD6807	2017-02-23 22:02:50
System	3.0 BUILD6198 upgrade to 3.0 BUILD6473	2017-02-23 22:00:10
System	3.0 BUILD5932 upgrade to 3.0 BUILD6198	2016-08-09 16:27:52

- 直接安装 8559 版本：



提示：低版本 VPN 网关可能没有升级包下载地址的链接，用户可到东软 NetEye 官网 http://neteye.neusoft.com的“技术支持>下载中心> VPN网关”下载升级包。

3. 点击**上载升级包**按钮，上传升级包并完成升级。



4. 点击**升级包下载地址**，可跳转到东软 NetEye 官方网站升级包下载页面。

8.11.License

系统在无 License 的状态下，可支持 5 个并发连接数和 50000 个本地用户，不支持分级管理员功能。

导入 License 之后，可支持更多用户和并发连接，可支持分级管理员功能。

1. 点击**系统管理> License**，查看 License 信息。

2. 点击**导入**按钮，在弹出的对话框中输入 License 字符串，点击**确定**。

8.12.版权信息

1. 选择**系统管理>版权**。
2. 查看版权信息。

第9章 配置范例

本章给出以下常见功能的配置范例：

9.1.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。

- 单臂模式
- 网关模式

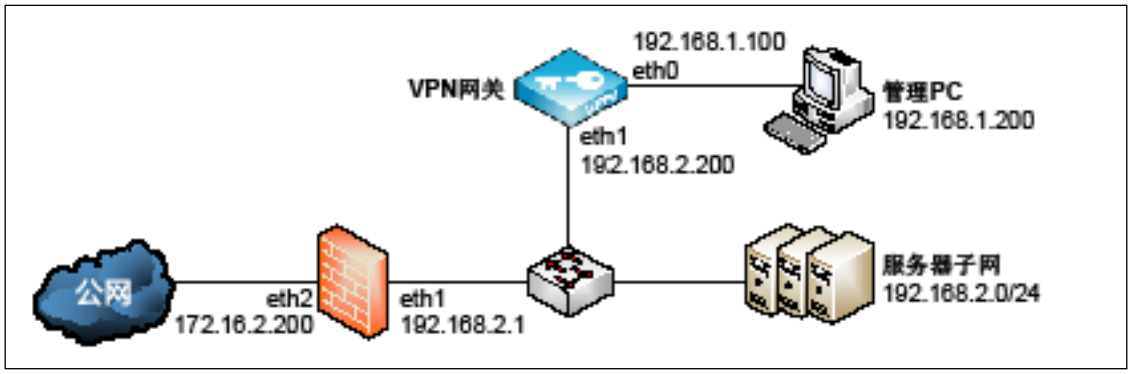
提示：推荐保留VPN网关的以太网接口eth0（缺省IP地址为192.168.1.100）作为管理接口。管理员可以在管理PC上通过eth0接口对VPN网关进行管理和配置。

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：

- Web 模式 SSL VPN
- 隧道模式 SSL VPN
- 远程访问 IPSec VPN
- 网关到网关 IPSec VPN

9.1.1. 单臂模式

组网拓扑



配置要点

- 配置接口
- 配置网关

配置步骤

9.1.1.1.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**。

9.1.1.2.配置网关

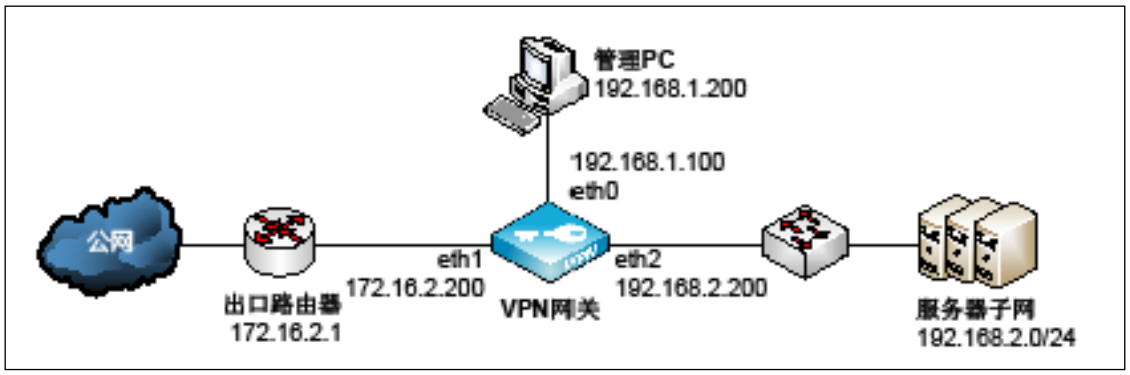
1. 选择**网络/策略>路由>静态路由**。
2. 点击**添加**，添加一条缺省路由，将出口接口设置为 eth1、网关设置为 192.168.2.1。

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。

9.1.2. 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。

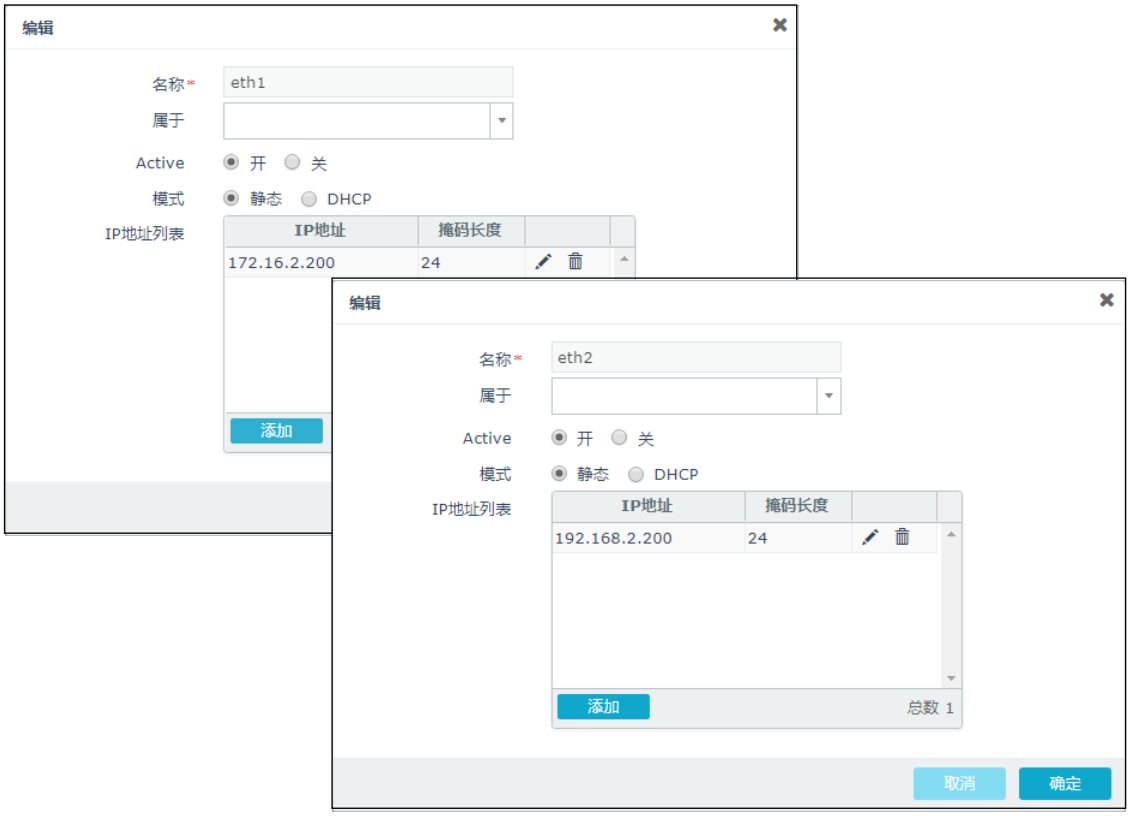
配置要点

- 配置接口
- 配置缺省路由

配置步骤

9.1.2.1.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**。

9.1.2.2.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。

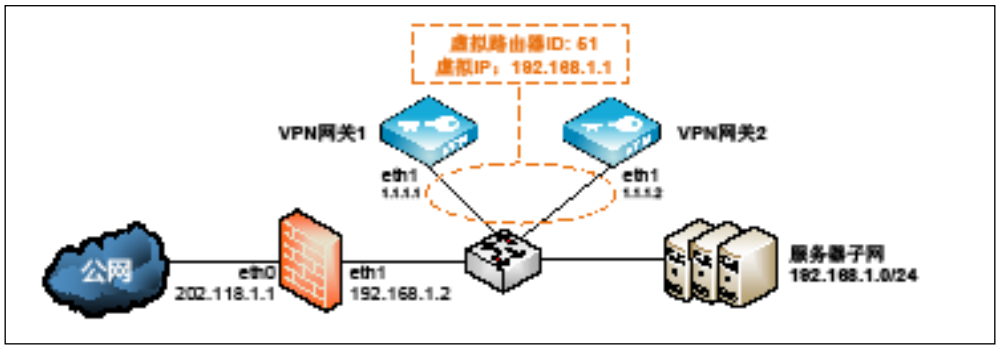
9.2.高可用性部署

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：

- 单臂模式高可用性
- 网关模式高可用性

9.2.1. 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

9.2.1.1.配置集群

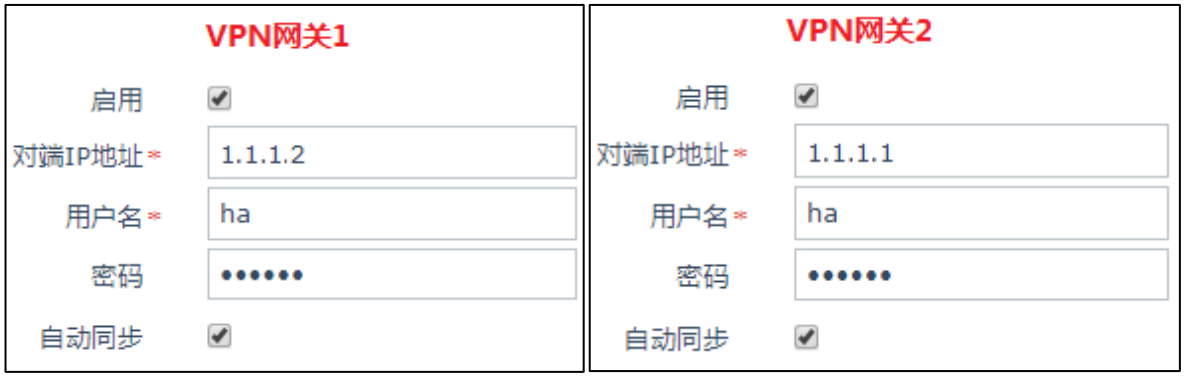
1. 假设所有配置都是在 VPN 网关 1 上进行的，在 VPN 网关 1 上选择**系统管理>高可用性>集群**。
2. 可以看到系统默认提供一个虚拟路由器 ID 为 51 的虚拟路由器配置条目。

3. 点击 对其进行修改。

4. 点击**确定**。点击**提交**。

9.2.1.2.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。

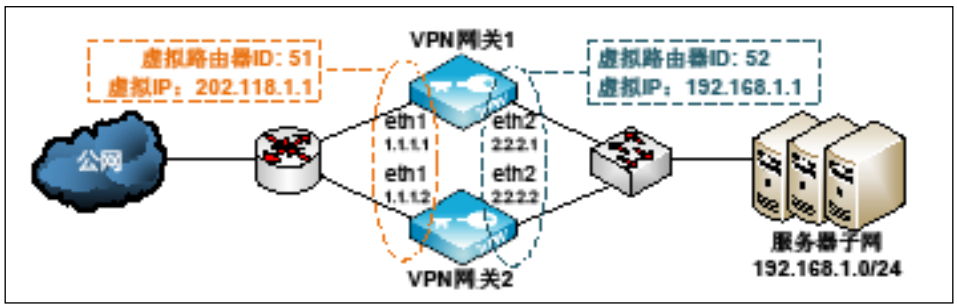


用户名和密码为对端设备的 HA 用户的用户名和密码，这里使用缺省值 ha/neteye。

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。

9.2.2. 网关模式高可用性

组网拓扑



配置要点

- 配置集群
- 配置缺省路由

配置步骤

9.2.2.1.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。

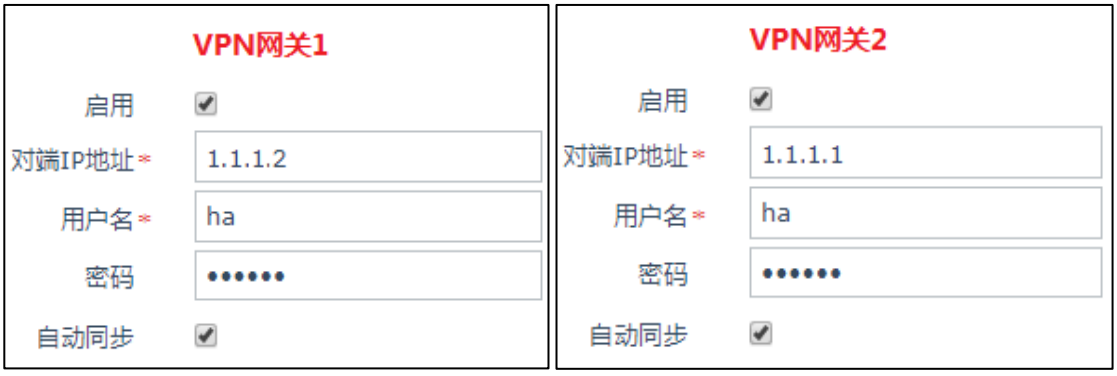
6. 点击**确定**。

7. 点击**提交**。

9.2.2.2.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。



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。

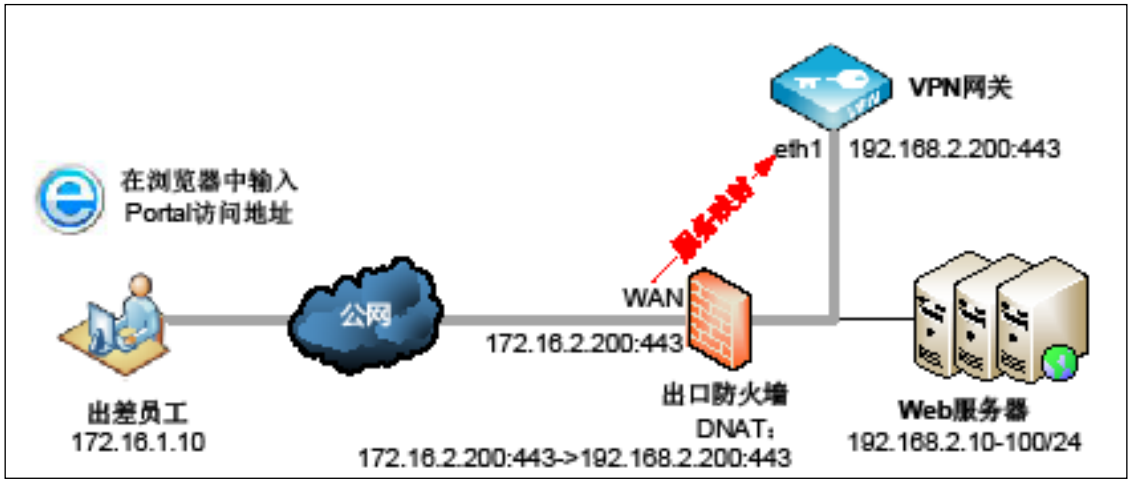
9.3.Web 模式 SSL VPN

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

9.3.1. 配置全局设置

1. 选择**认证配置>缺省认证服务器，**选择本地认证服务器。

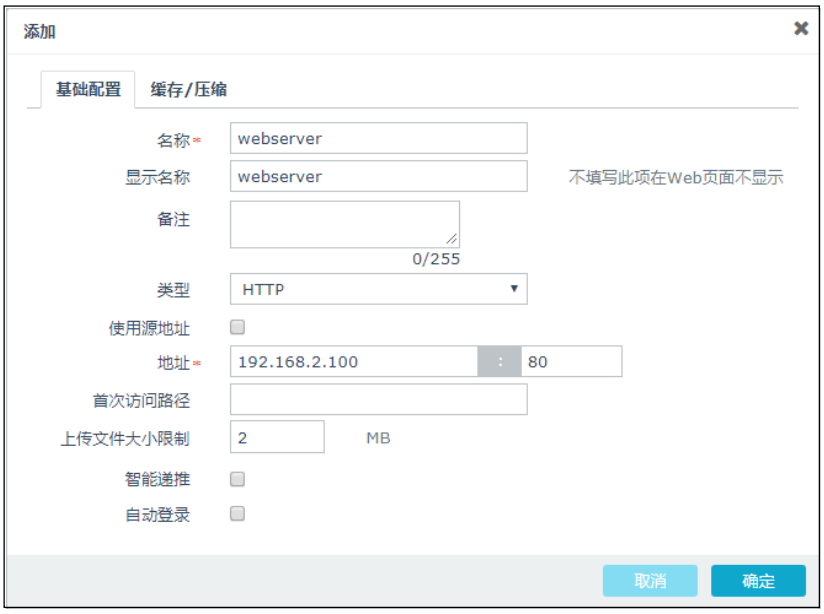
2. 选择**基础功能>全局设置**。

3. 可选择 LDAP 认证服务器，设置缓存/压缩策略和会话超时时间。

4. 点击**提交**。

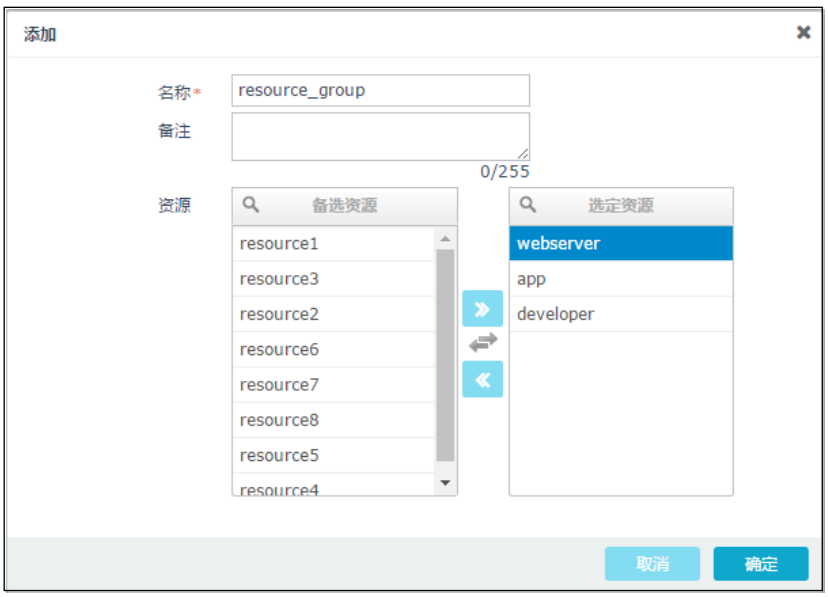
9.3.2. 配置资源和资源组

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。

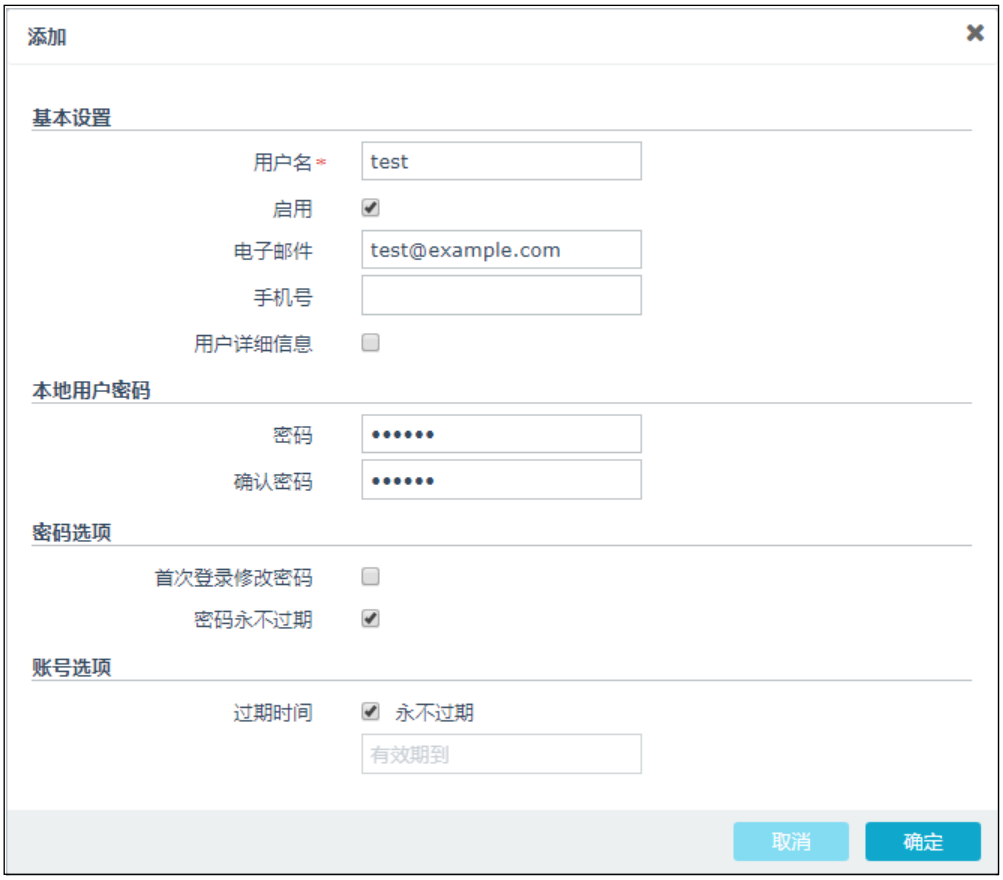
3. 点击**确定**。
4. 以同样方式添加其他资源。
5. 选择**基础功能>资源组**。
6. 点击**添加**，设置资源组名称并选择要加入资源组的资源。



7. 点击**确定**。

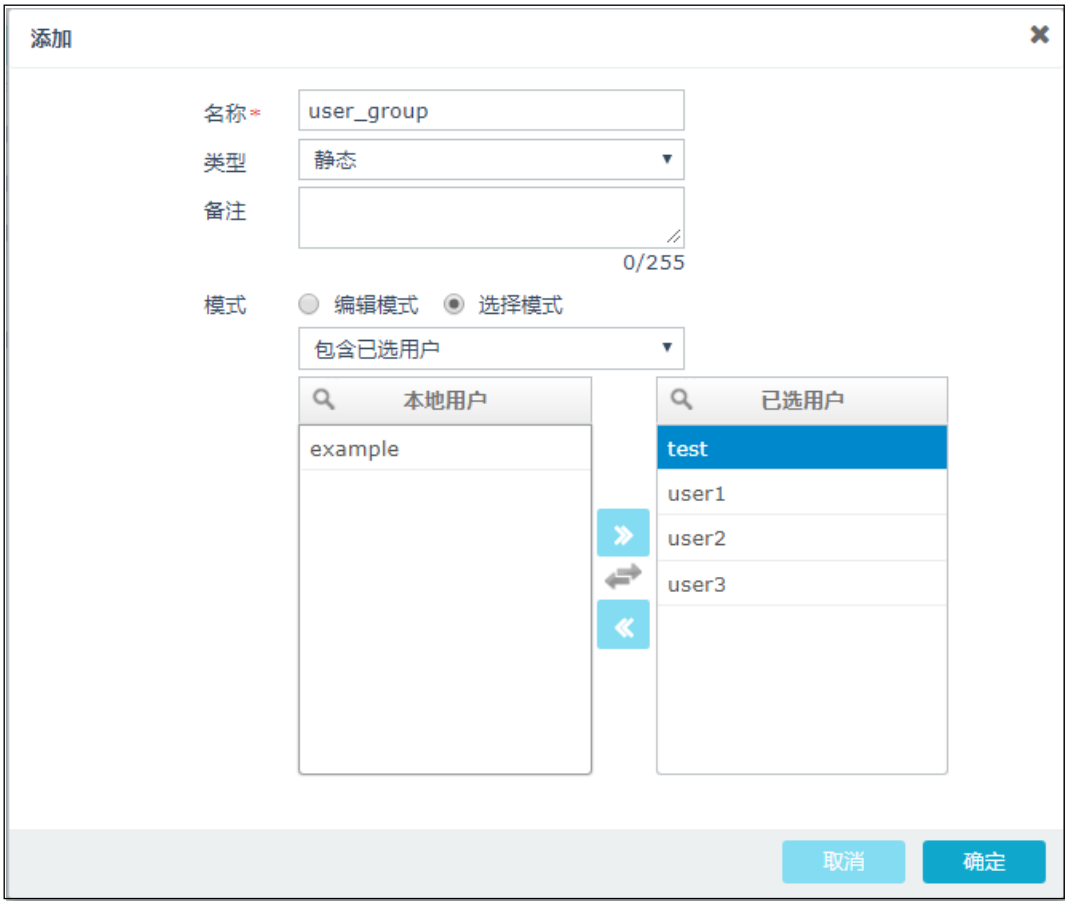
9.3.3. 配置用户和用户组

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**。

9.3.4. 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**。

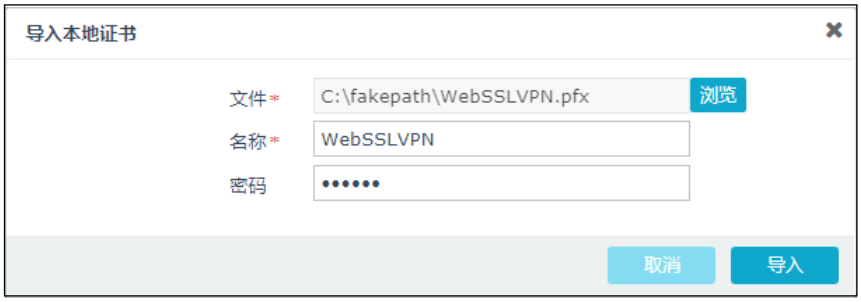
b. 在**用户组**页签选择策略应用于的用户组。

c. 在**资源组**页签选择策略应用于的资源组。

3. 点击**确定**。

9.3.5. 导入 SSL VPN 服务器证书

1. 选择**认证配置>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**。

9.3.6. 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**。

9.3.7. 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。

9.3.8. 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。

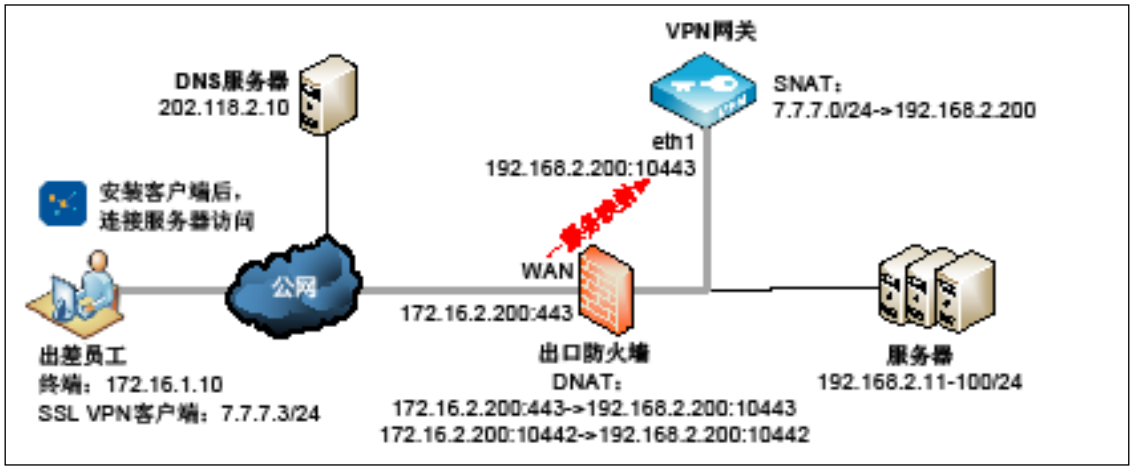
3. 如有需要，可以通过**离线**按钮强制用户下线。

9.4.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。

- 为确保 SSL VPN 客户端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

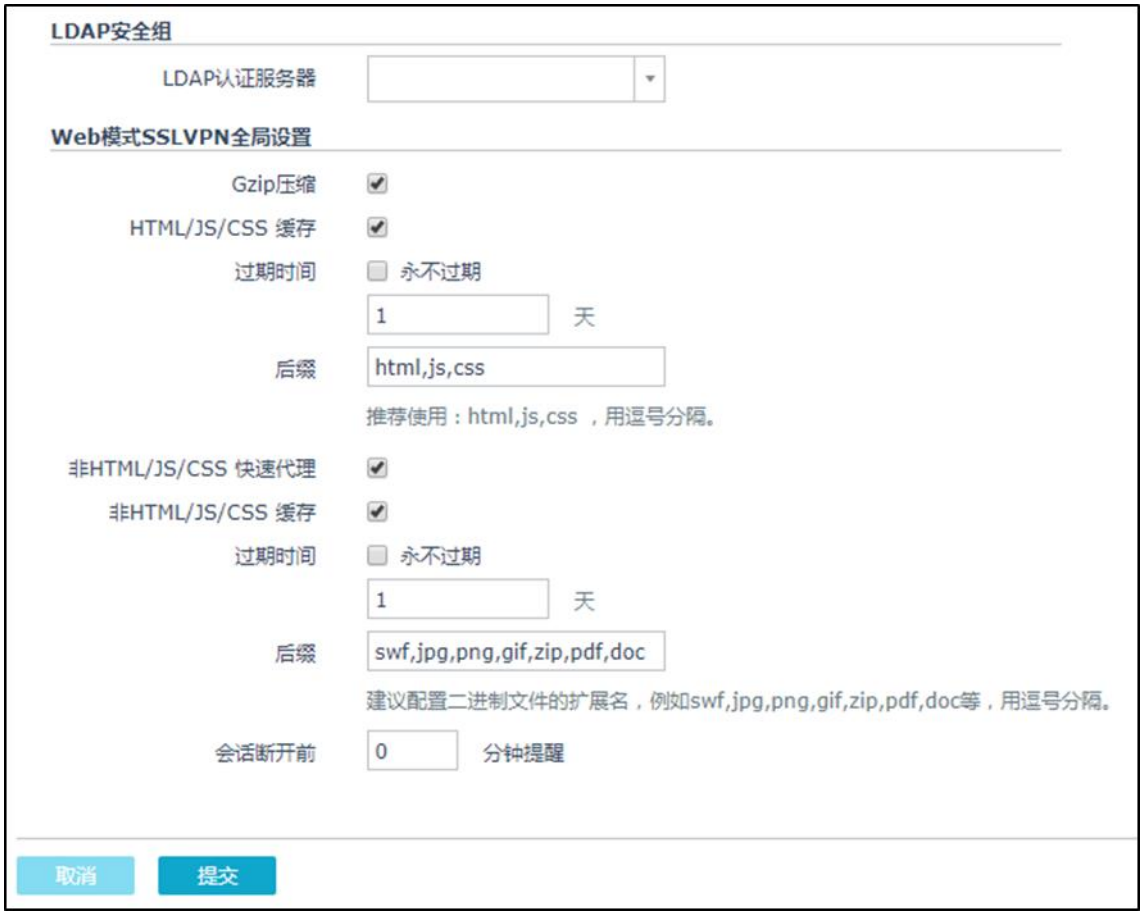
配置步骤

9.4.1. 配置全局设置

1. 选择**认证配置>缺省认证服务器**，选择本地认证服务器。

2. 选择**基础功能>全局设置**。

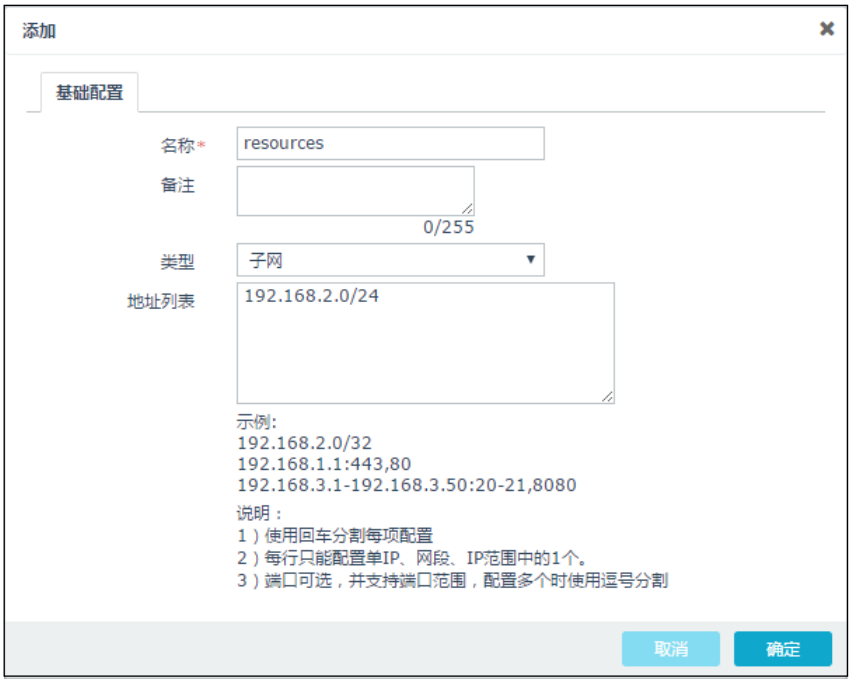
3. 可选择 LDAP 认证服务器，设置缓存/压缩策略和会话超时时间。



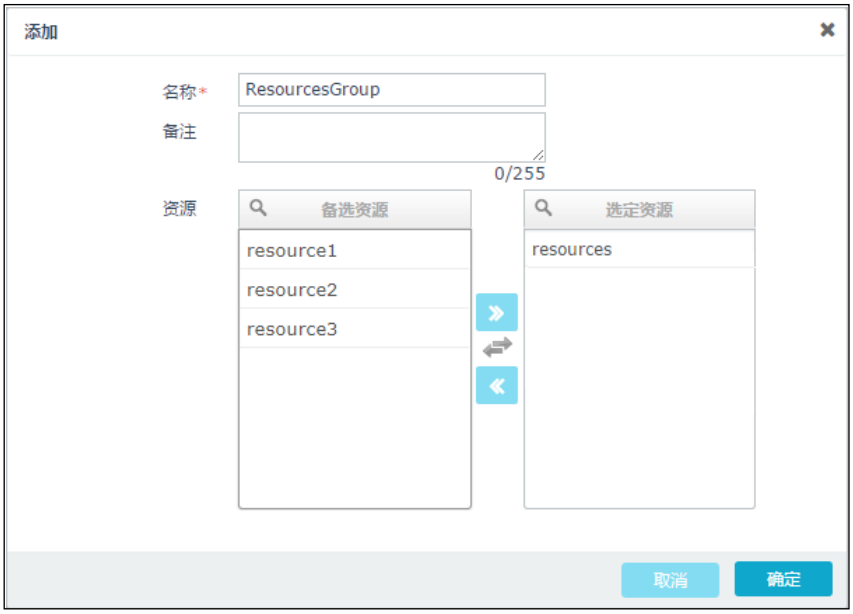
4. 点击**提交**。

9.4.2. 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。



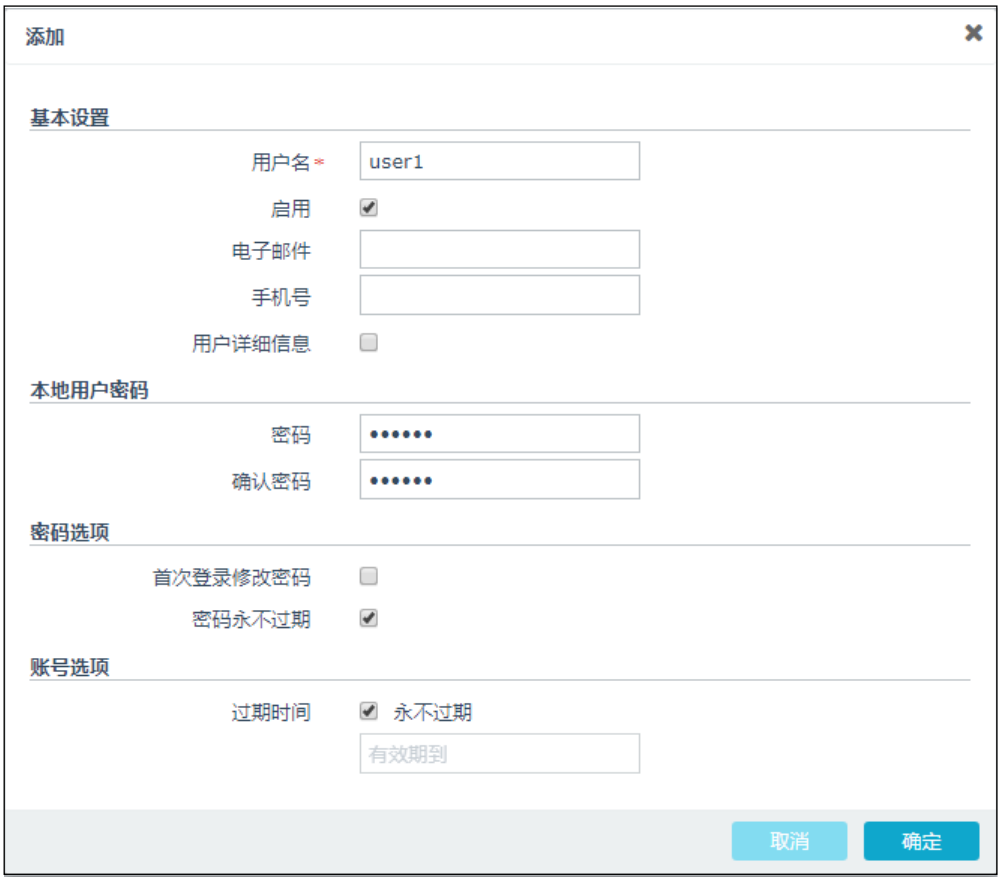
3. 点击**确定**。
4. 选择**基础功能>资源组**。
5. 点击**添加**，添加资源组，对资源组命名并选择要加入资源组的资源。



6. 点击**确定**。

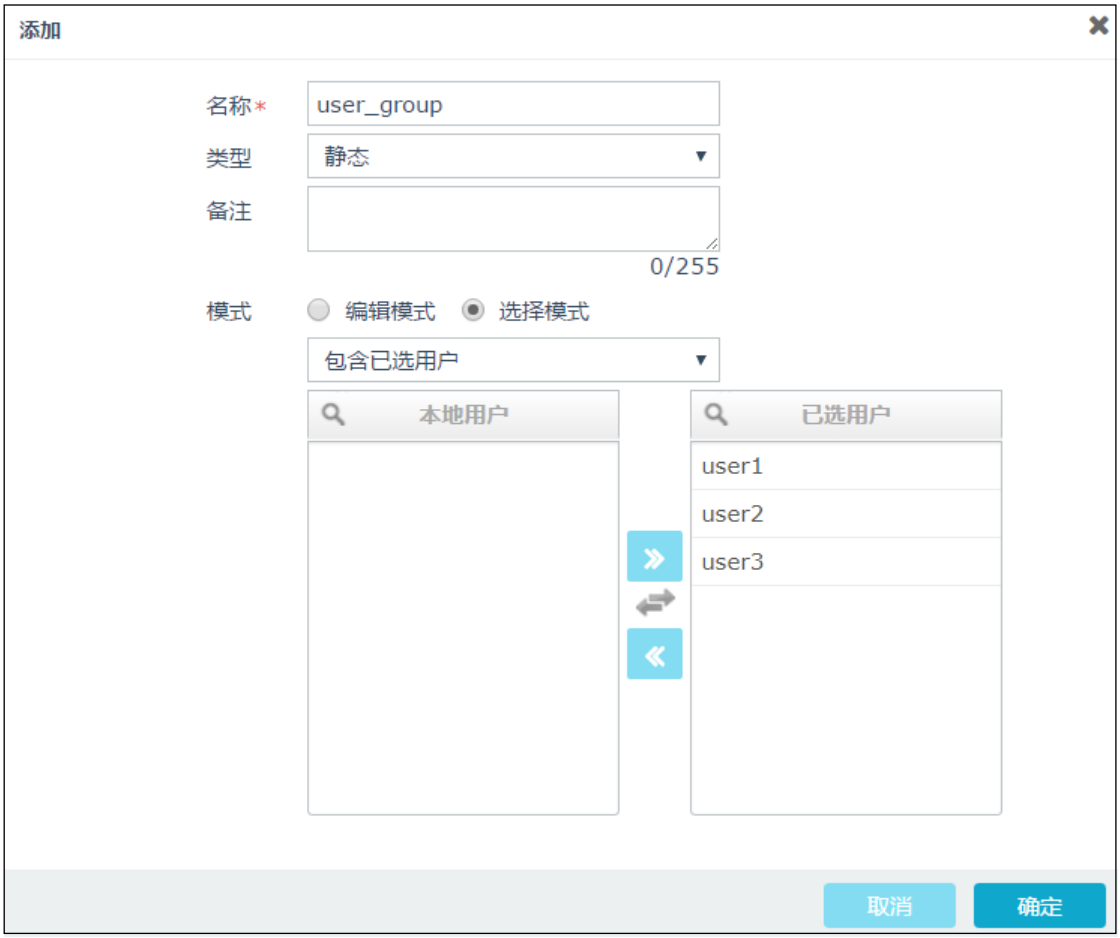
9.4.3. 配置用户和用户组

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**。

9.4.4. 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**。

9.4.5. 添加 CA 证书和本地证书

1. 选择**认证配置>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**。

9.4.6. 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**。

9.4.7. 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**。

9.4.8. 配置出口防火墙 DNAT

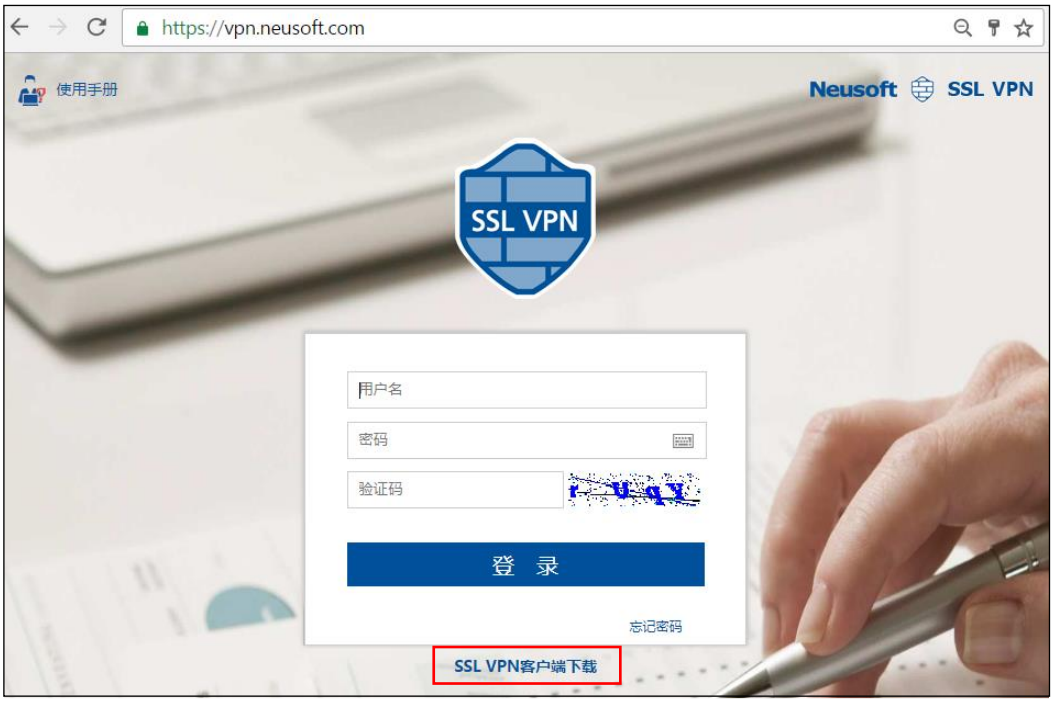
在出口防火墙上配置目的地址转换：

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。

9.4.9. 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。

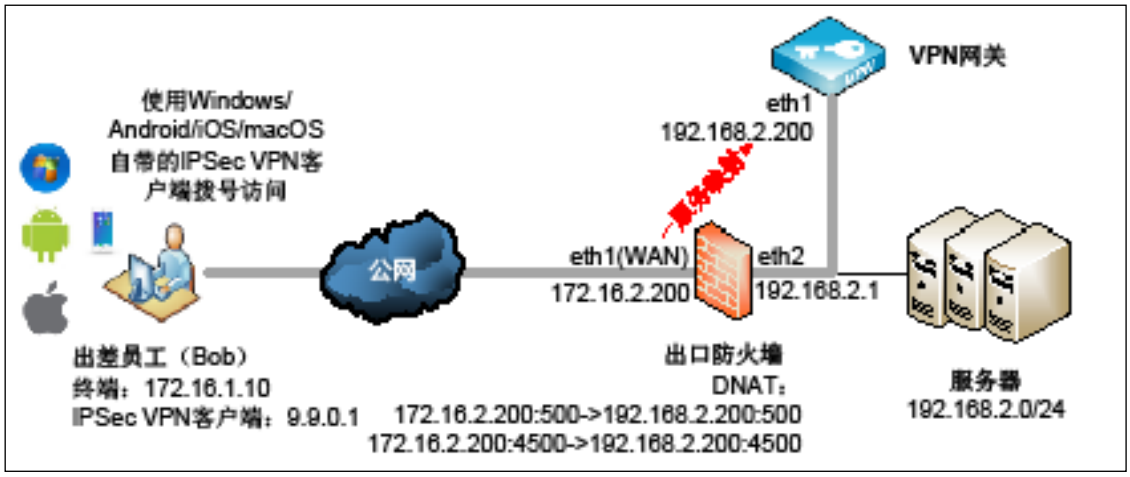
提示：如有需要，可以通过**离线**按钮强制用户下线。

9.5.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

9.5.1. 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。

9.5.2. 配置全局设置

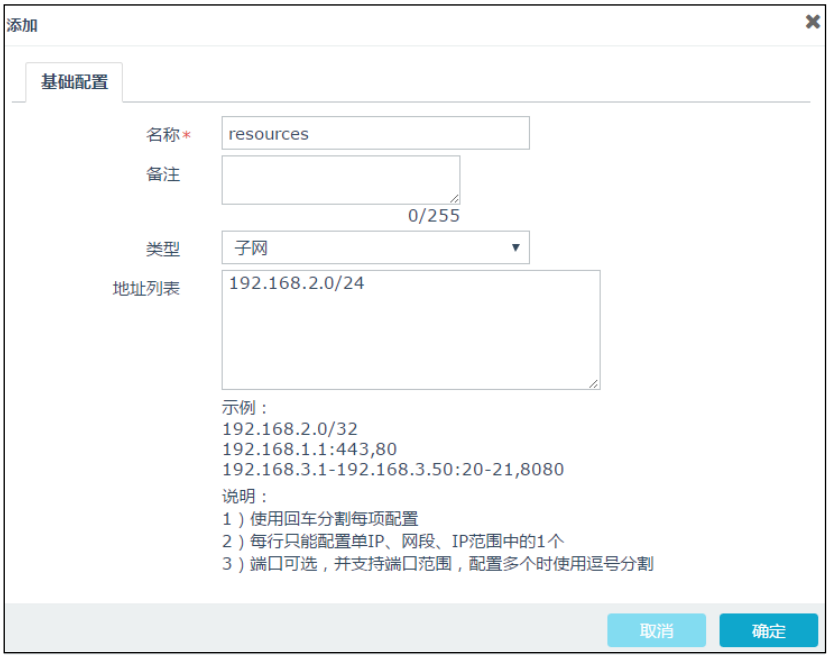
1. 选择**认证配置>缺省认证服务器**，使用本地认证服务器 Local 认证 SSL VPN 用户。

2. 选择**基础功能>全局设置**，如有需要可配置 LDAP 认证服务器。

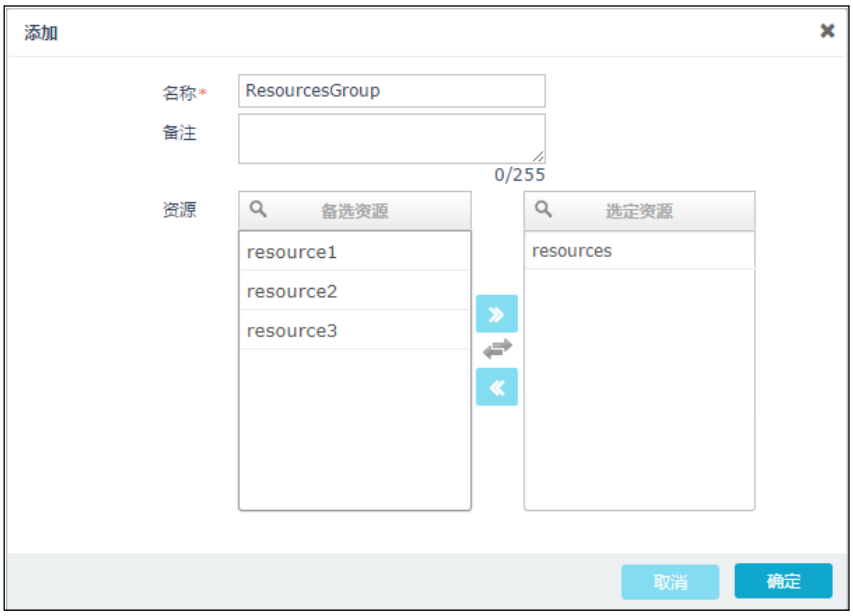
3. 点击**提交**。

9.5.3. 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。



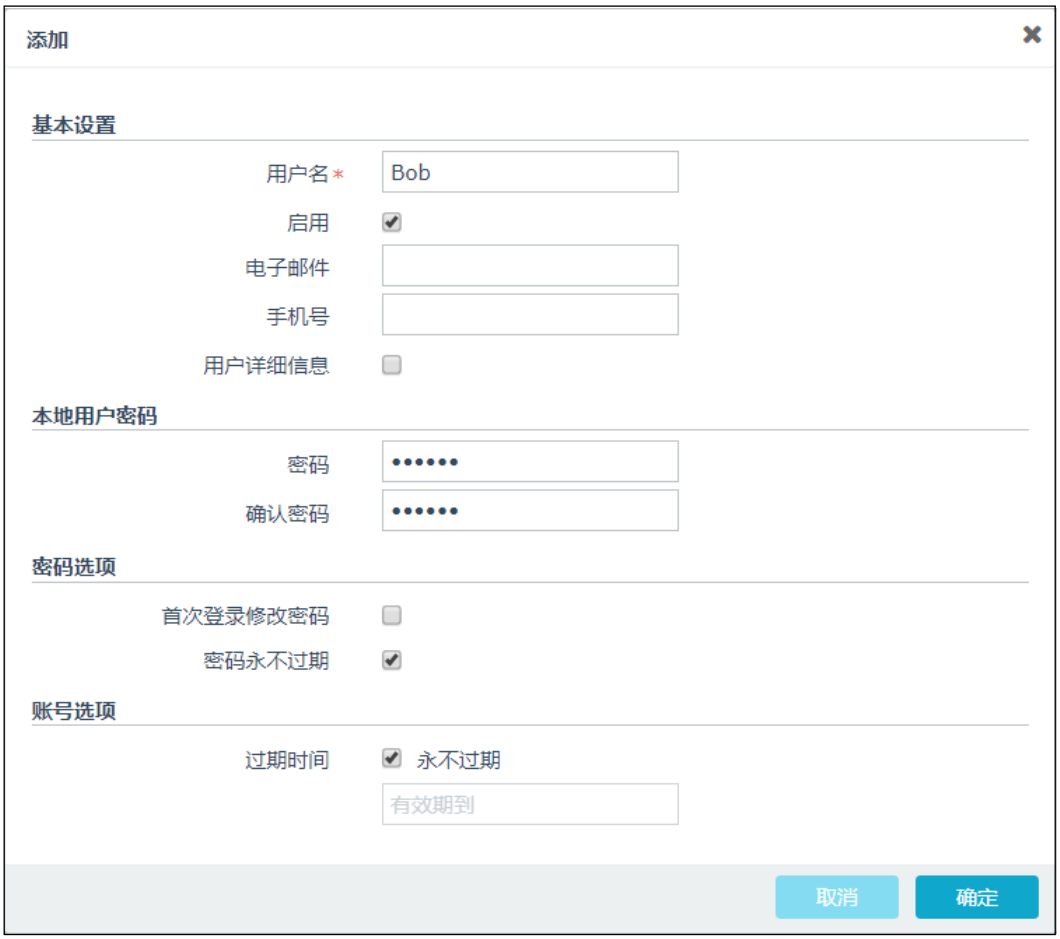
3. 点击**确定**。
4. 选择**基础功能>资源组**。
5. 点击**添加**，添加资源组，对资源组命名并选择要加入资源组的资源。



6. 点击**确定**。

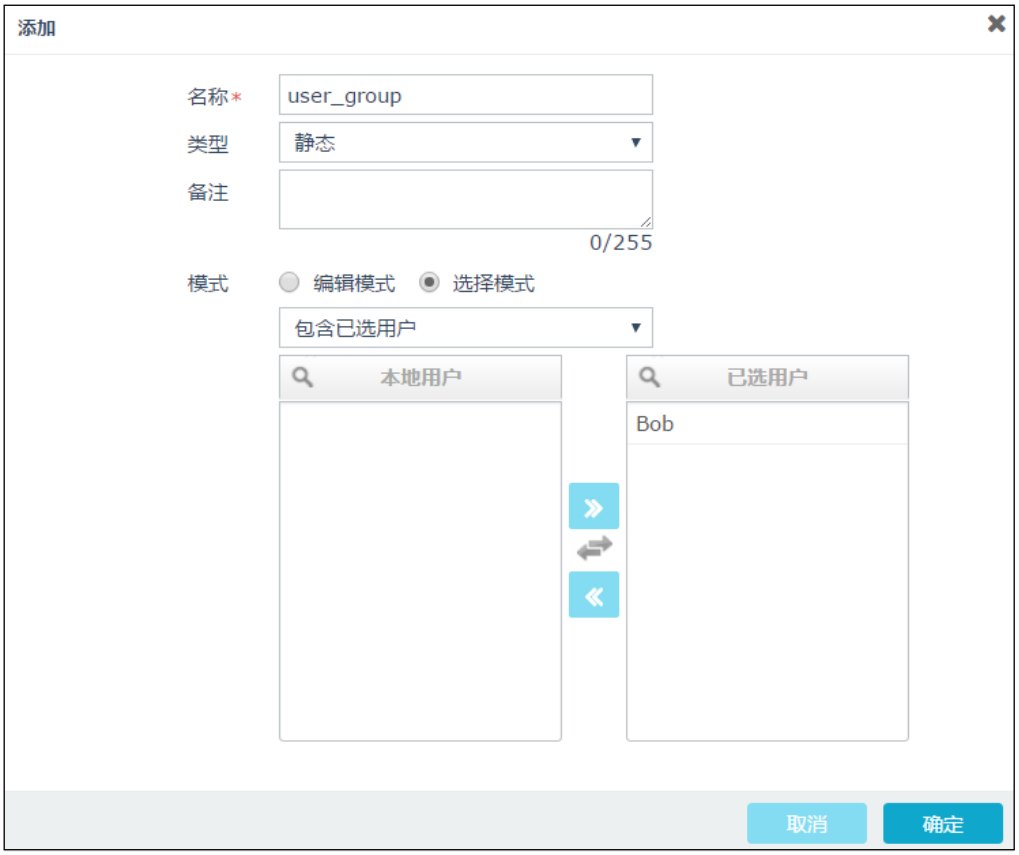
9.5.4. 配置用户和用户组

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**。

9.5.5. 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**。

9.5.6. 添加 CA 证书和本地证书

1. 选择**认证配置>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**。

9.5.7. 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**。

9.5.8. 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。

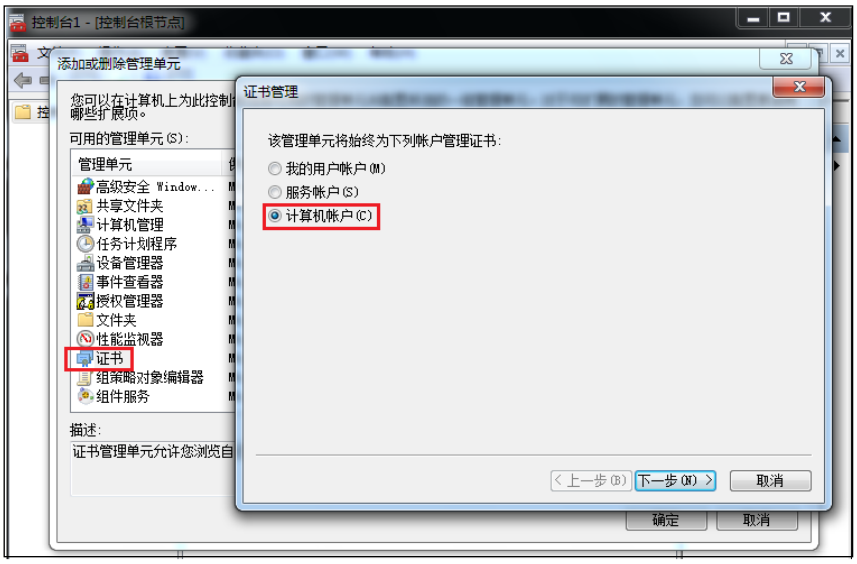
9.5.9. 配置 Windows 内置 IPSec VPN 客户端

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。

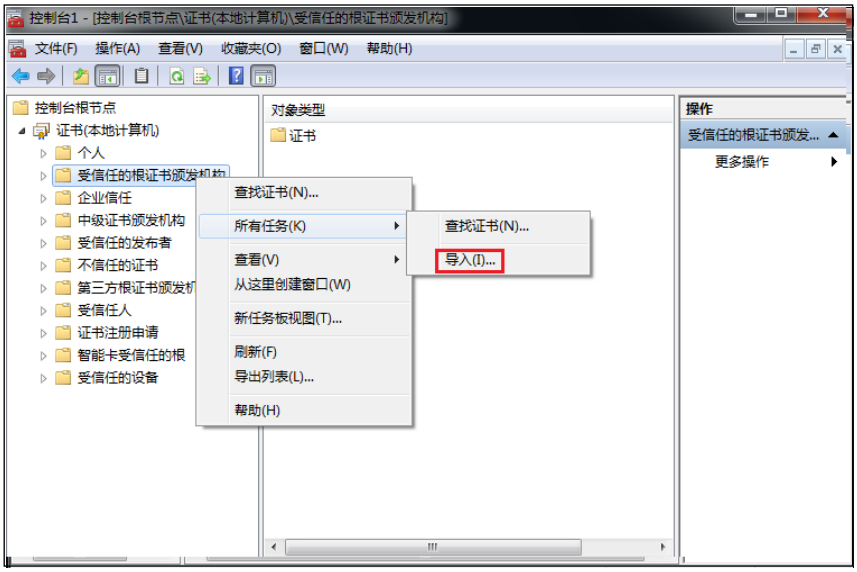
- 导入 CA 证书
- 创建 VPN 连接
- 修改 VPN 客户端配置

9.5.9.1.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**。

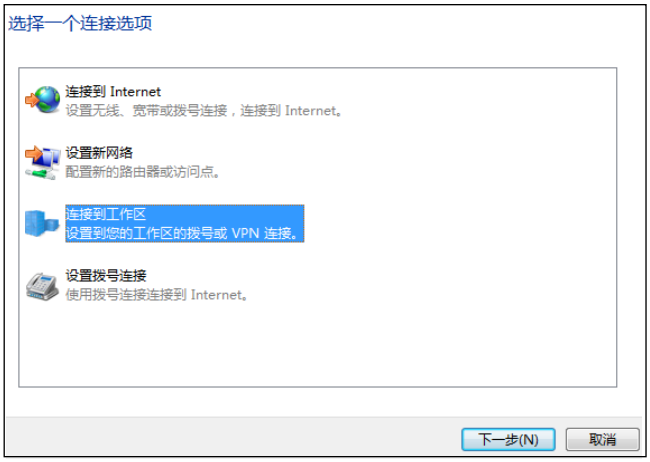


3. 点击**本地计算机**，点击**完成**，点击**确定**。
4. 在左侧控制台根节点，展开**证书**节点，选择**受信任的根证书颁发机构>所有任务>导入**，根据提示导入 CA 证书。

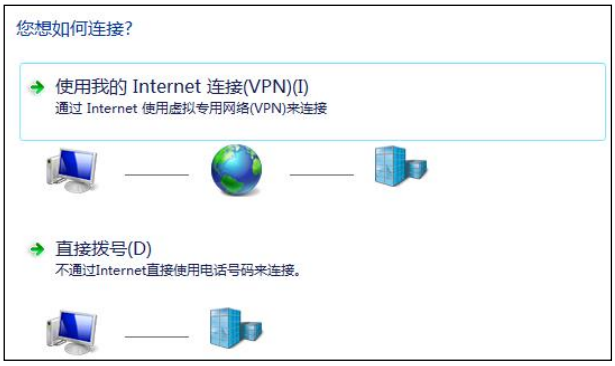


9.5.9.2.创建 VPN 连接

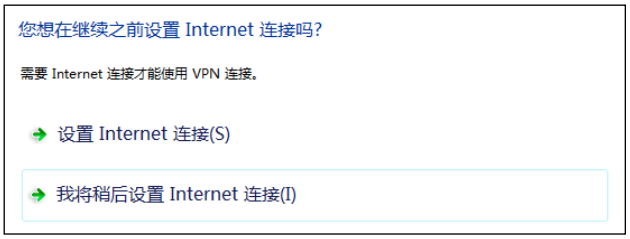
1. 打开**网络和共享中心**，点击**设置新的连接或网络**。
2. 点击**连接到工作区**，点击**下一步**。



3. 点击**使用我的 Internet 连接（VPN）**。

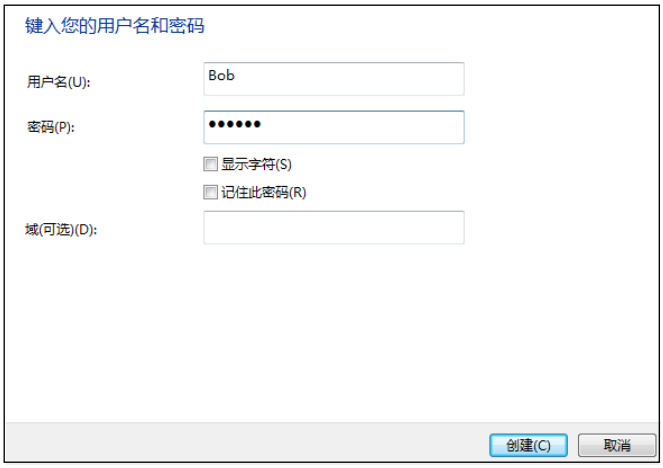


4. 点击**我将稍后设置 Internet 连接**。



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。

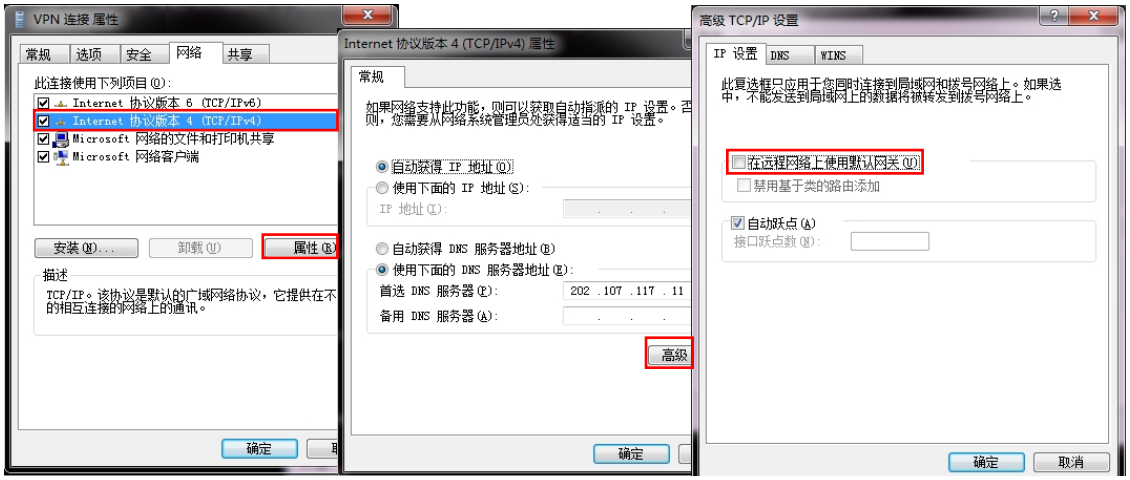
9. 点击**属性**，点击**安全**，配置安全选项。

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。

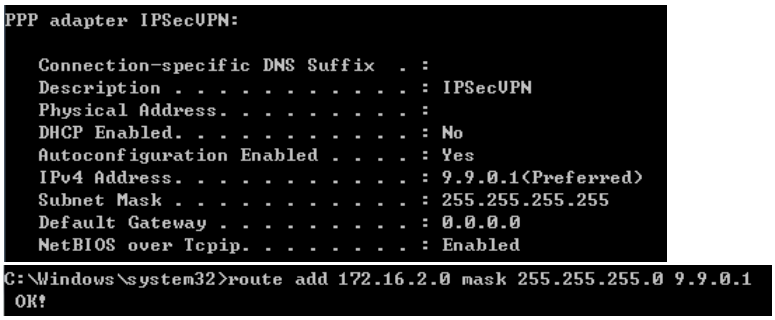
9.5.9.3.修改 VPN 客户端配置

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) >属性>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。



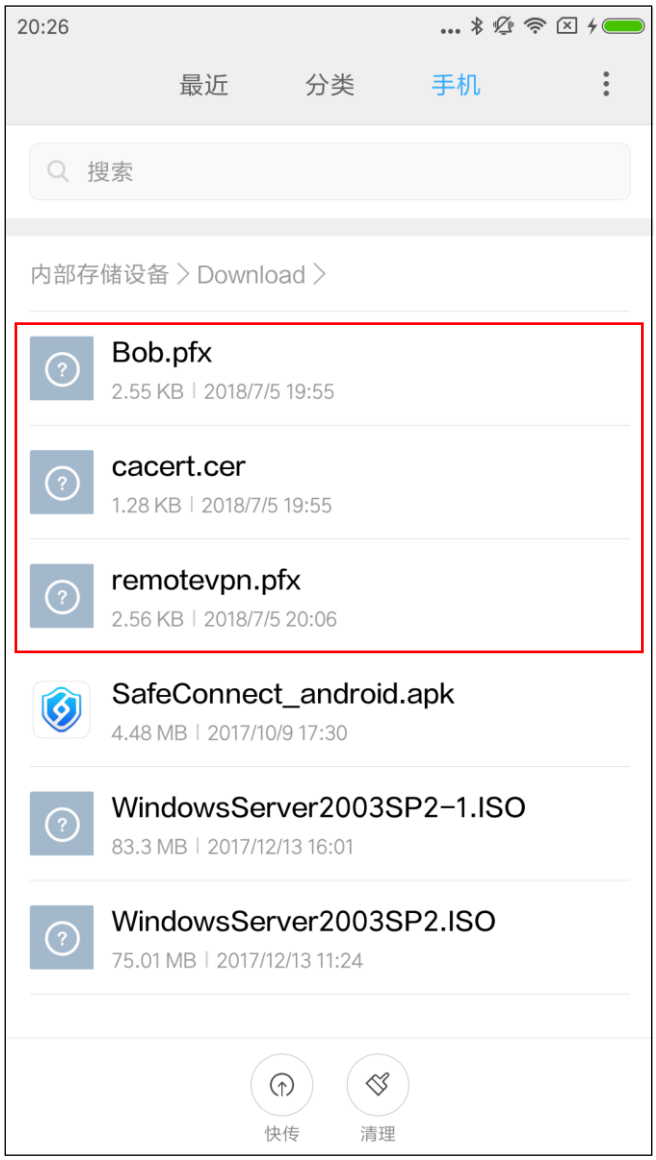
9.5.10. 配置 Android 内置 IPSec VPN 客户端

9.5.10.1.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。

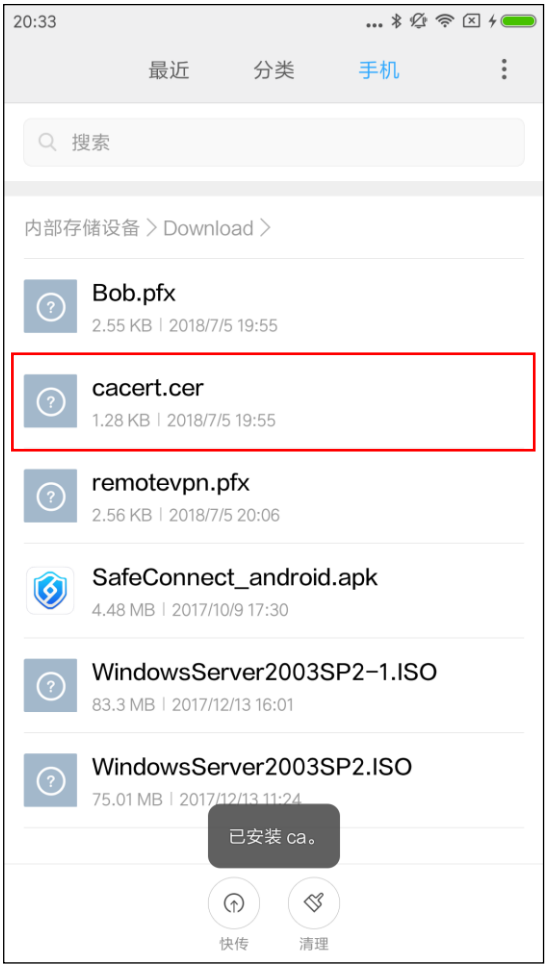
b. 将证书导入手机 Download 文件夹。



c. 点击证书文件进行安装。

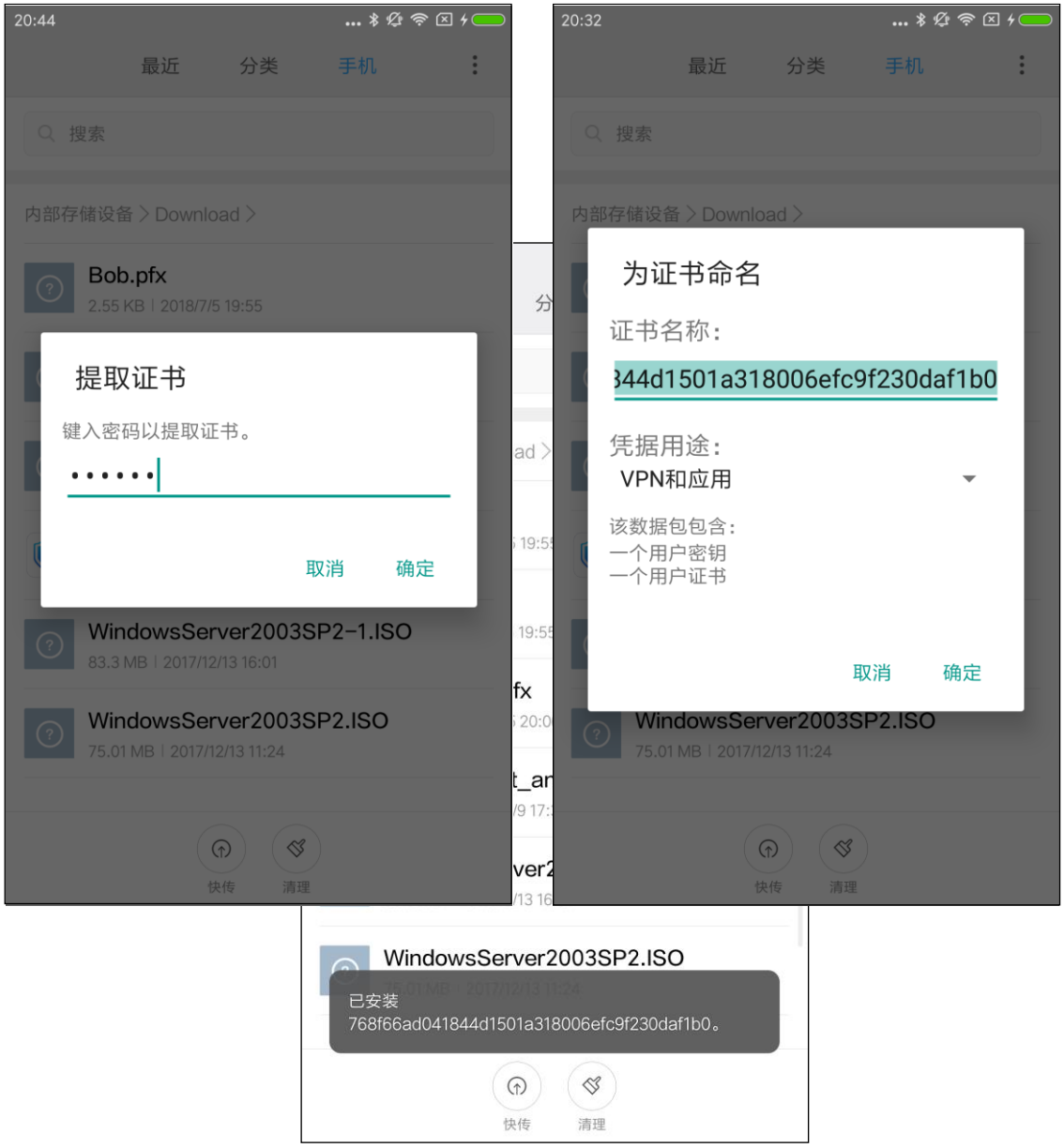
- 安装 CA 证书：


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

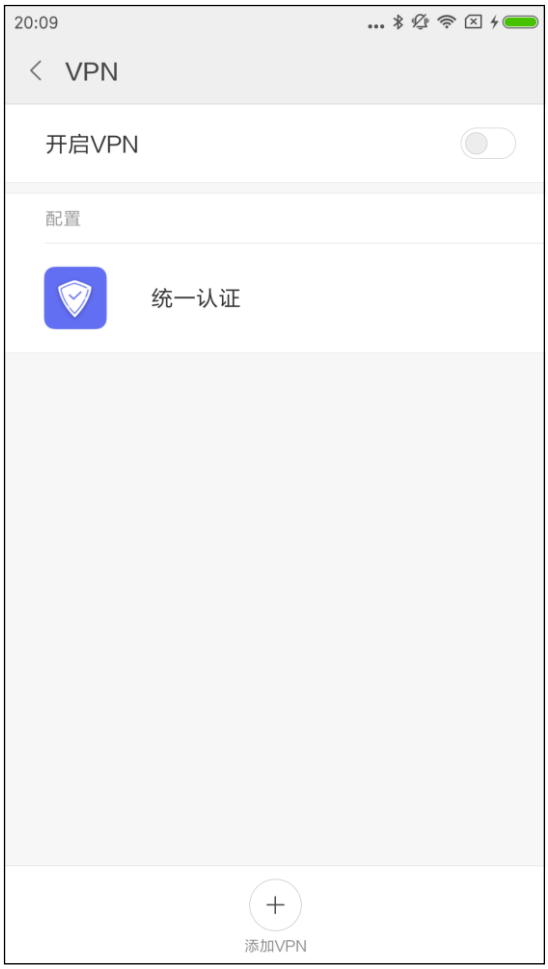
- 安装 IPSec 服务器证书：

- 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
WindowsServer2003SP2.ISO
已安装
768f66ad041844d1501a318006efc9f230daf1b0。

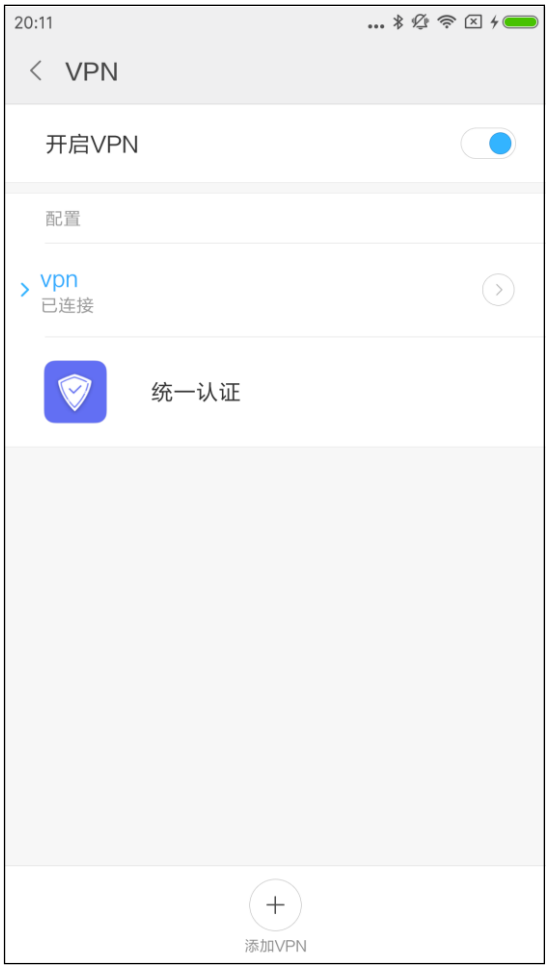
9.5.10.2.添加和建立 VPN 连接

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。

9.5.11. 配置 iOS 内置 IPSec VPN 客户端

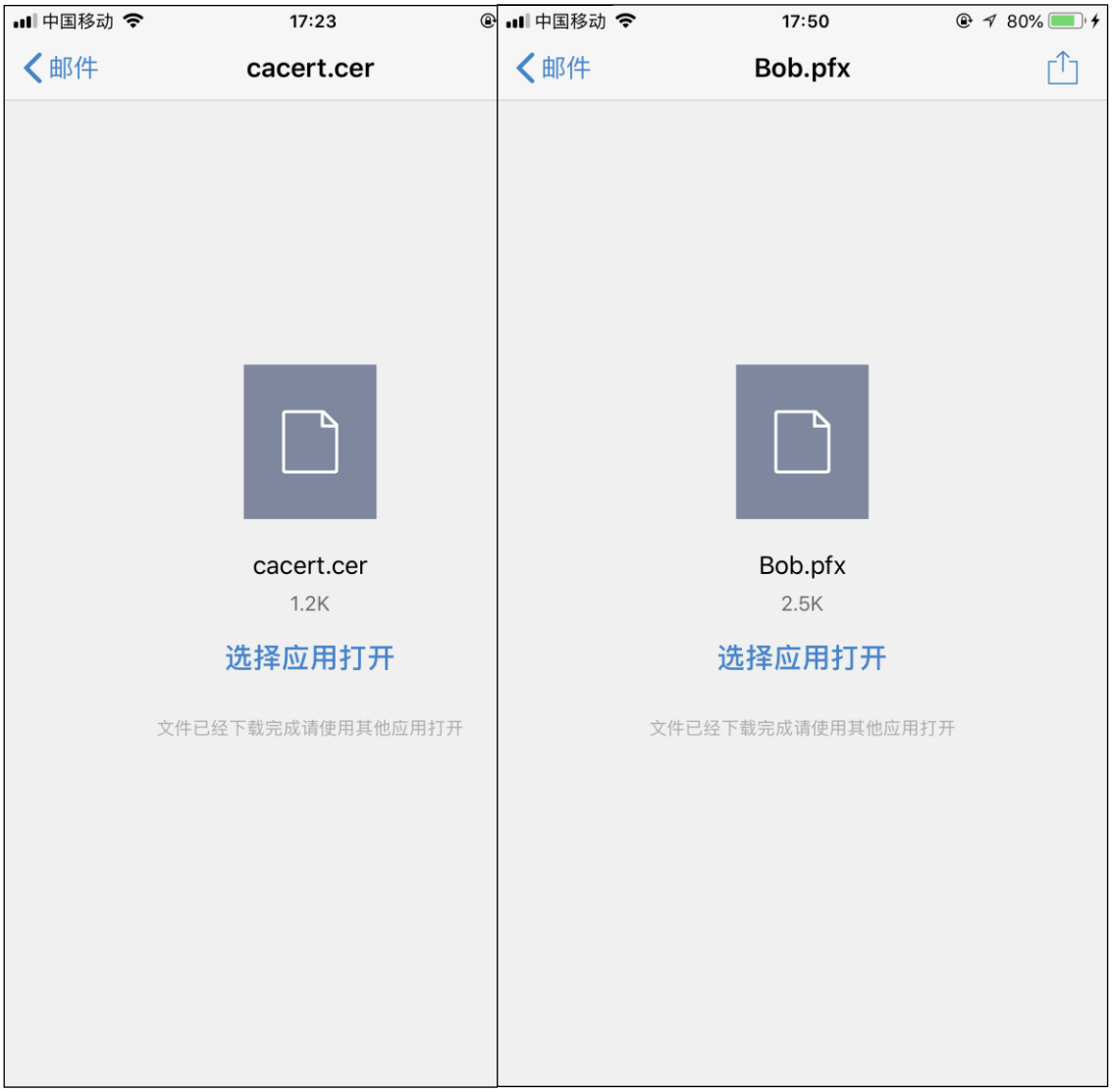
9.5.11.1.导入和安装证书

- 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。

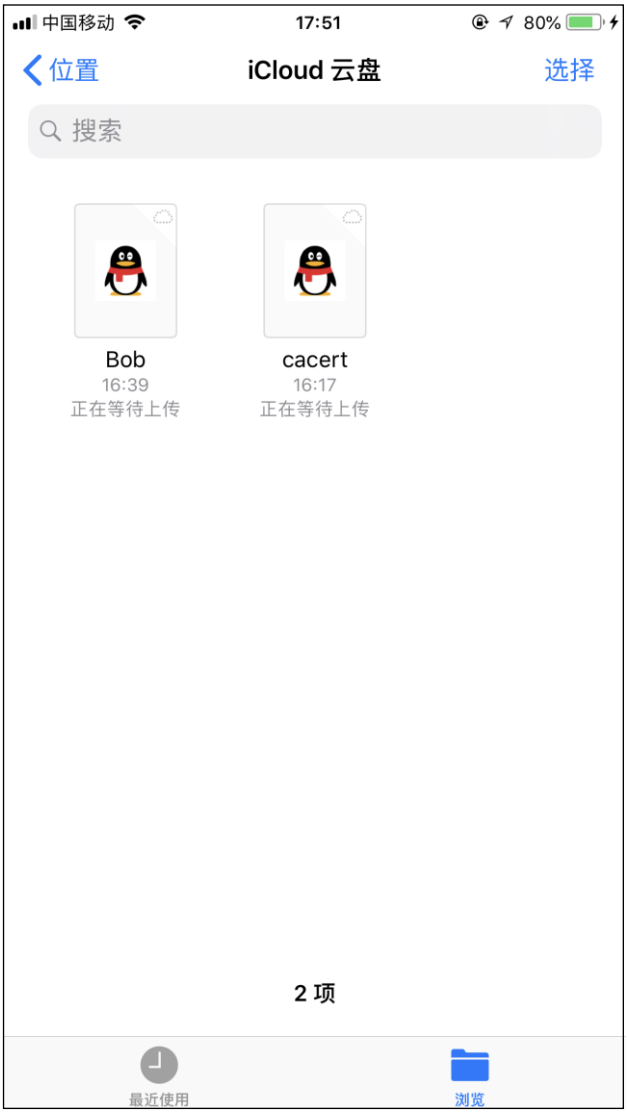
1. 从 VPN 网关上下载证书到本地，并通过邮件发送给远程用户。
2. 远程用户通过 iPhone 手机接收邮件，将证书存储到 iCloud 云盘。

a. 点击证书附件。


中国移动
17:23
邮件
cacert.cer
cacert.cer
1.2K
选择应用打开
文件已经下载完成请使用其他应用打开
中国移动
17:50
80%
邮件
Bob.pfx
Bob.pfx
2.5K
选择应用打开
文件已经下载完成请使用其他应用打开

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
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
1
2
-
/
#+=
.
ABC

9.5.11.2.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。

- 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。

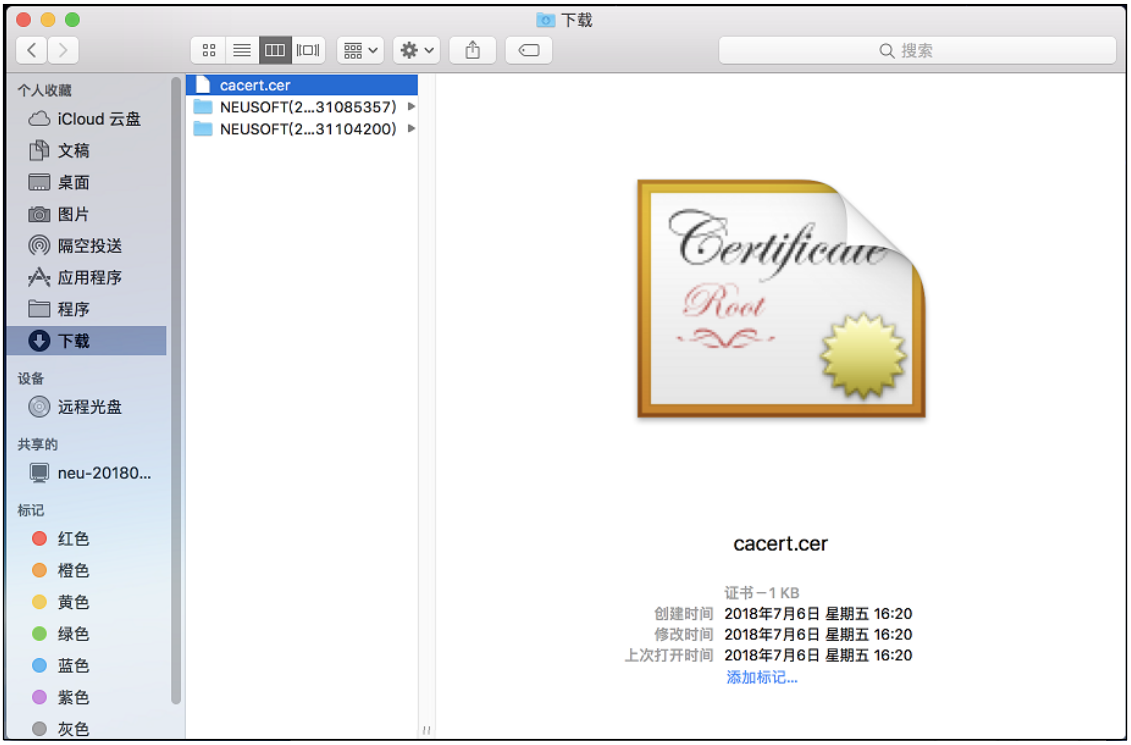
4. 回到 VPN 连接界面，选择新建的 VPN 连接，滑动状态按钮，建立 VPN 连接。

5. 待连接成功后，用户即可访问内网资源。

9.5.12. 配置 macOS 内置 IPSec VPN 客户端

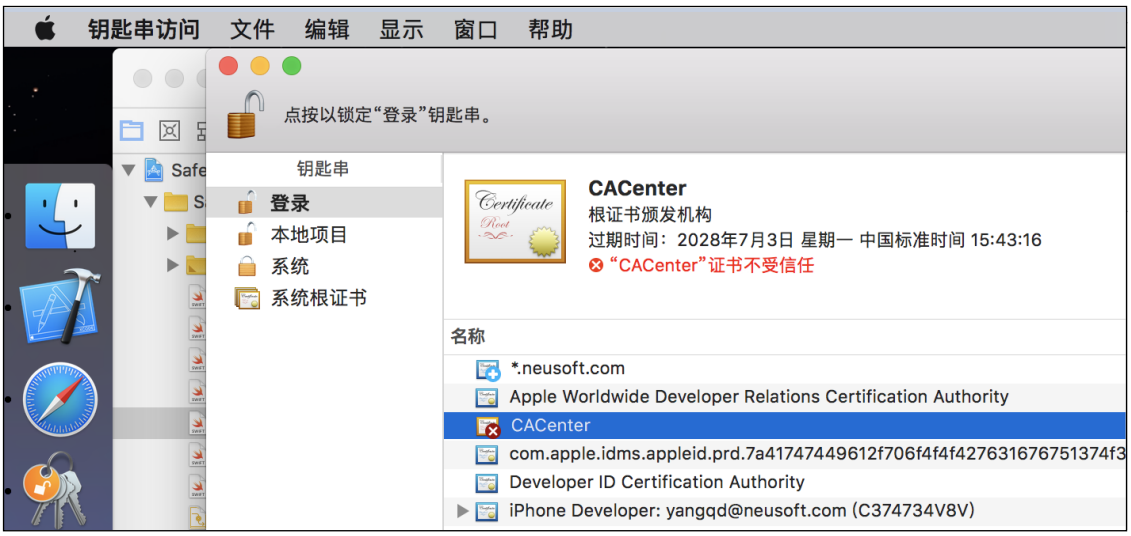
9.5.12.1.导入证书

1. 将 CA 证书导入苹果电脑。

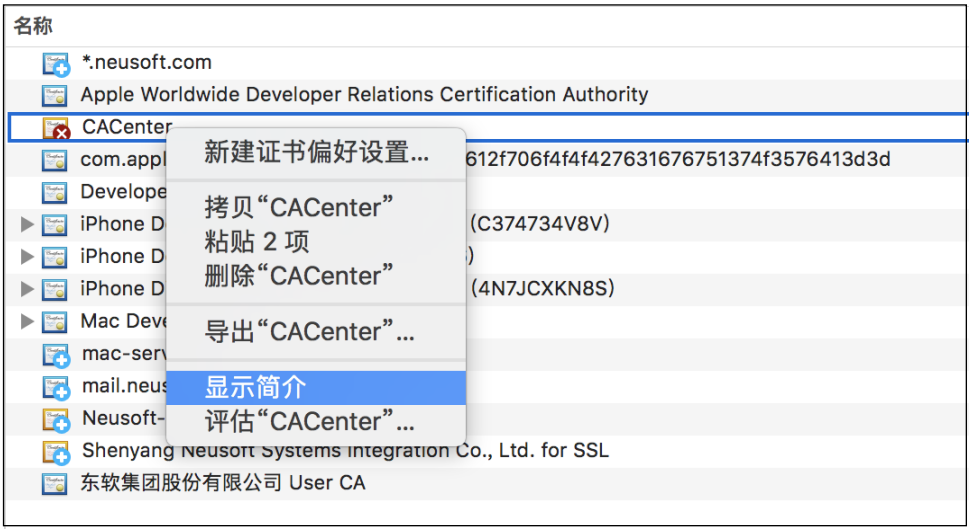


2. 双击证书文件，将证书添加进钥匙串。

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**。



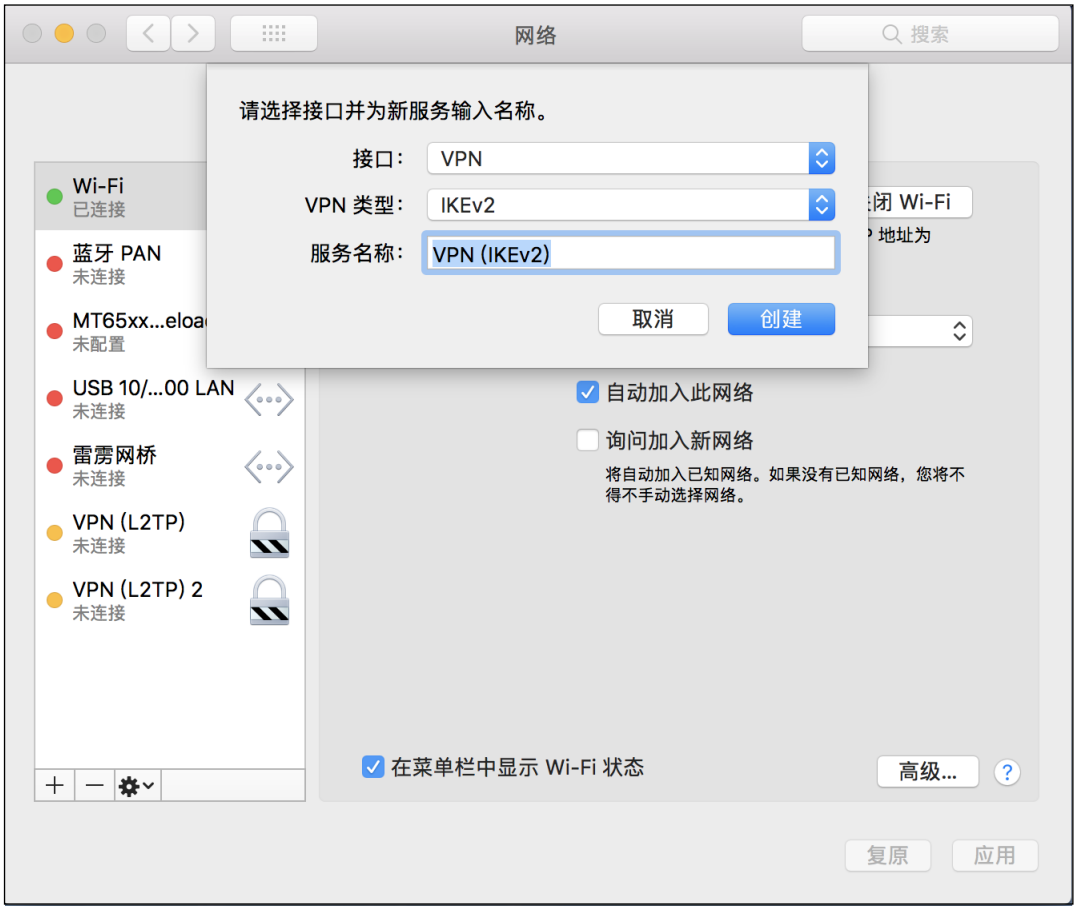
5. 在**信任**区域的下拉框中选择**始终信任**。

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。

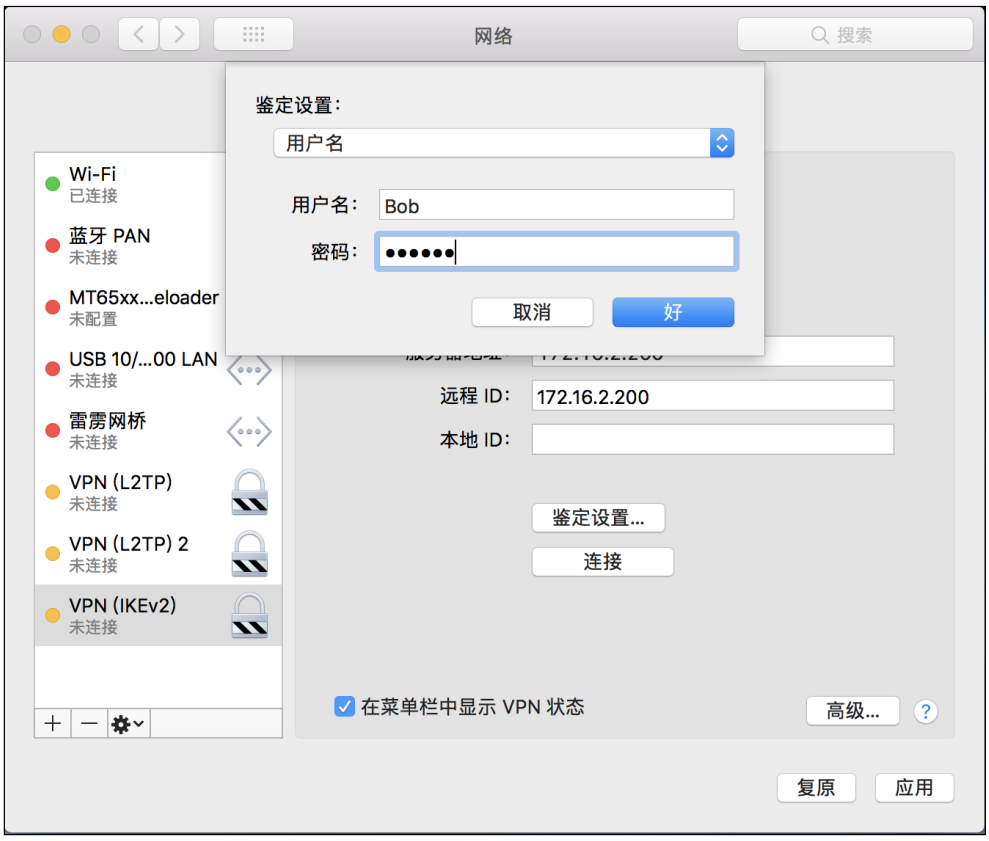
9.5.12.2.建立 VPN 连接

1. 选择**系统偏好设置>网络**，点击连接列表下方加号+，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。

9.5.13. 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。

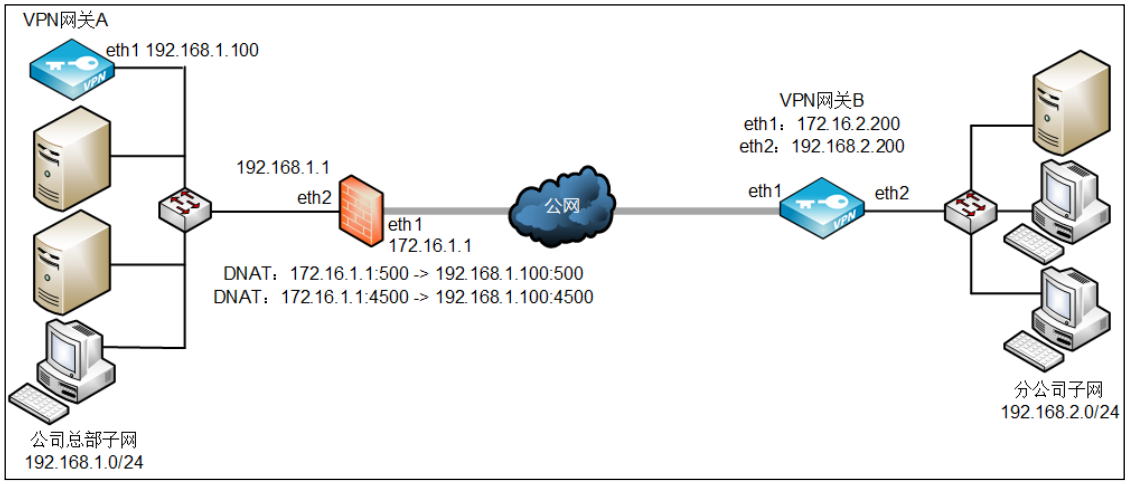
   需要事先在远程访问 IPSec VPN 中开启日志记录功能（选择**基础功能> IPSec VPN**，点击 RemoteAccess 对应的编辑图标）。

9.6.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

9.6.1. 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

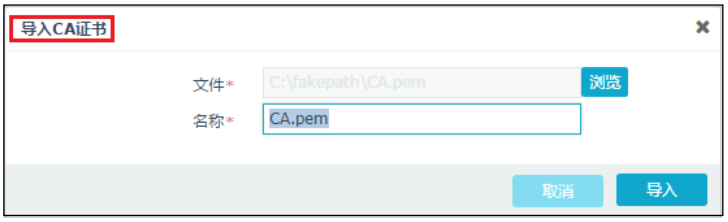
由于各个厂家设置方法有所不同，以上配置此处不截图说明。

9.6.2. 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：

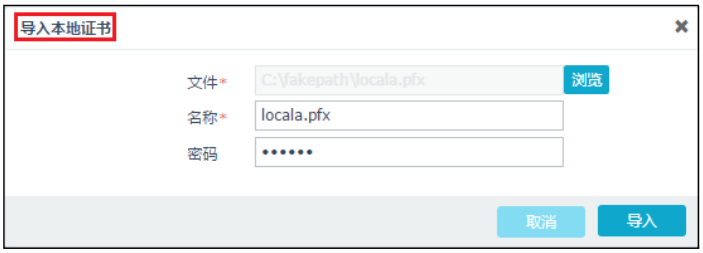
   a. 选择**系统管理>证书**。

   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。

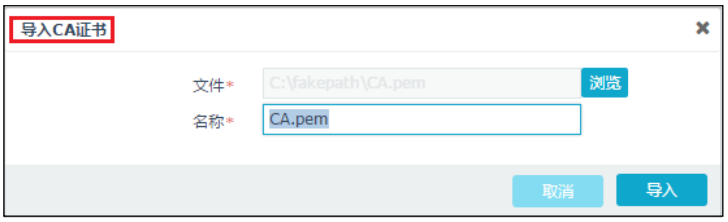
d. 点击**对端配置**，设置对端地址、认证类型和对端子网。

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。

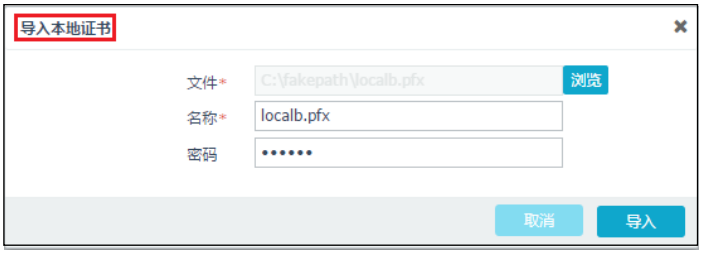
9.6.3. 配置分部 VPN 网关 B

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。

9.6.4. 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。

9.7.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

...

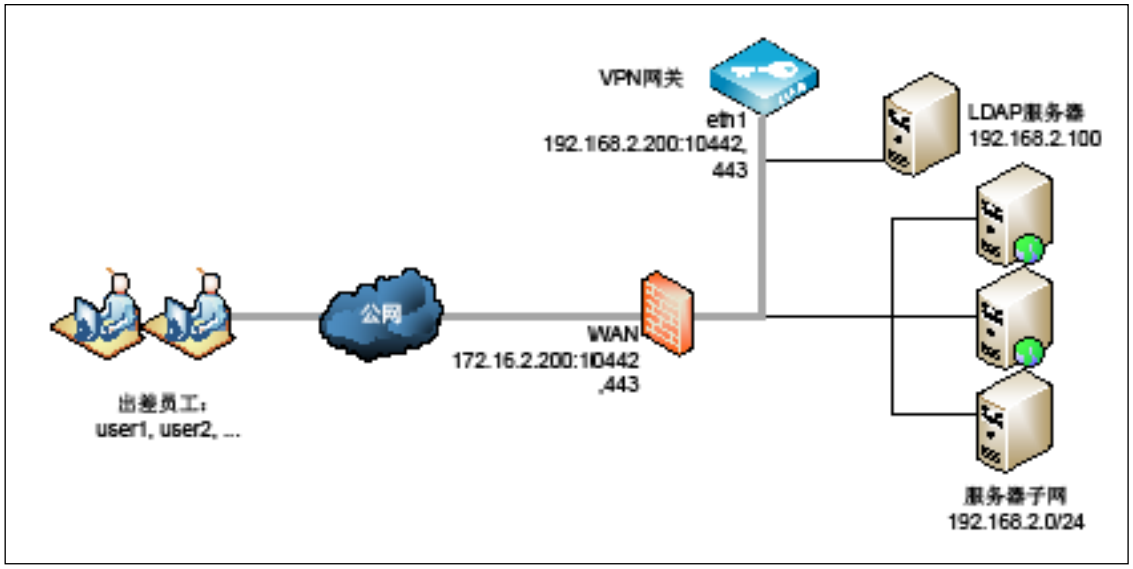
ou=groups

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

9.7.1. 配置 LDAP 外部认证服务器

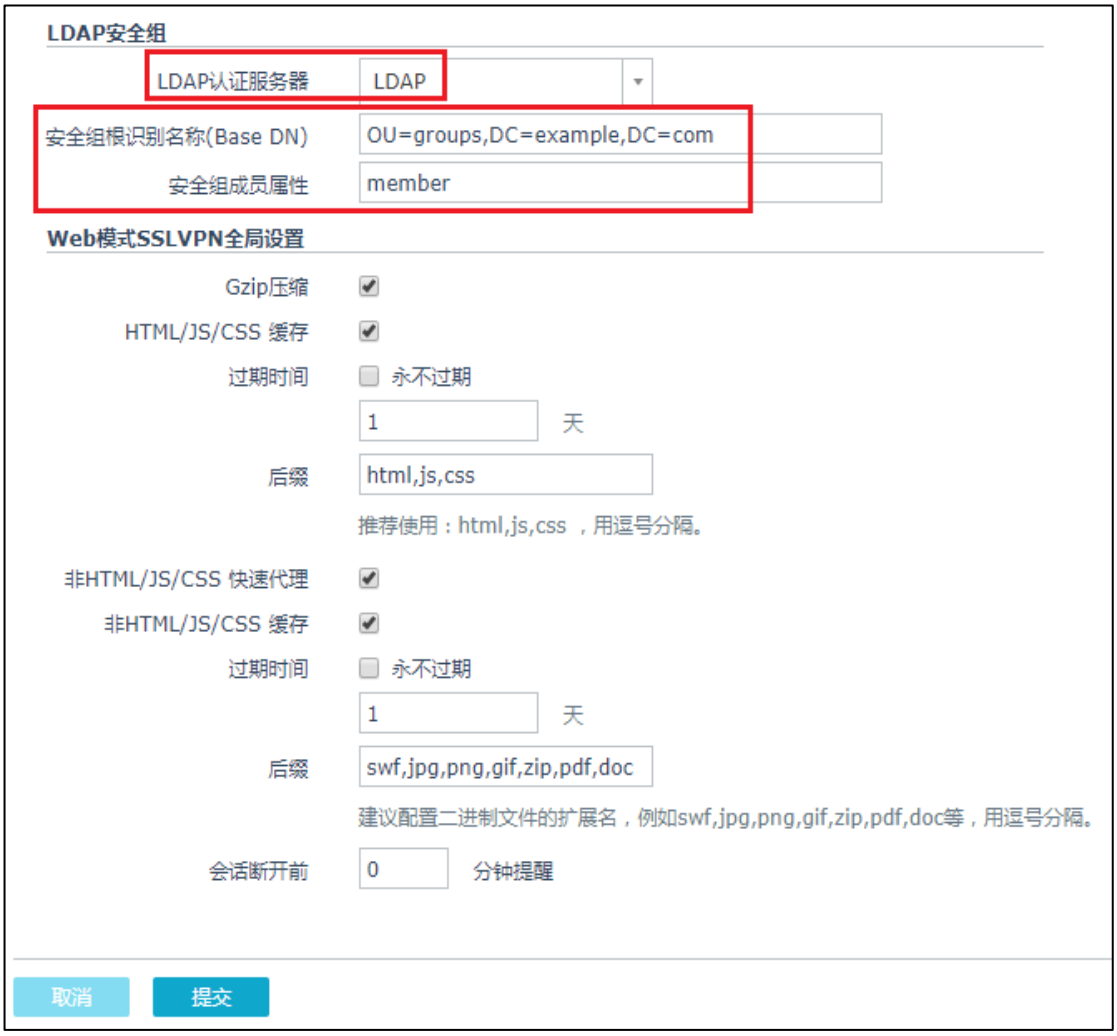
1. 选择**认证配置>外部认证服务器**。
2. 点击**新建**，在下拉菜单中选择 **LDAP**，添加 LDAP 认证服务器。

3. 点击**确定**。

9.7.2. 配置 VPN 全局设置

1. 选择**认证配置>缺省认证服务器**，选择 Local。

2. 选择**基础功能>全局设置**，选择 **LDAP** 认证服务器，并可配置 LDAP 安全组信息。



3. 点击**提交**

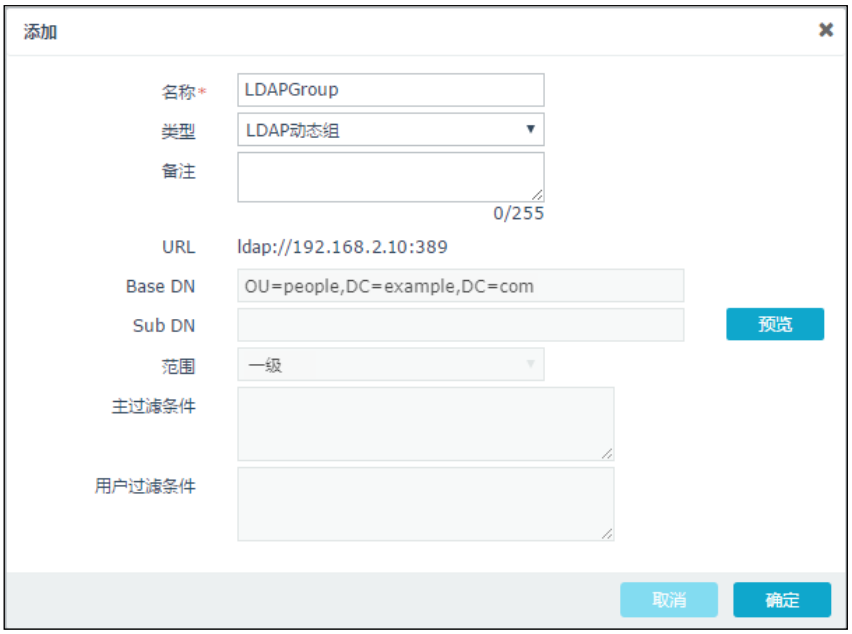
9.7.3. 配置用户组

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**。

9.7.4. 配置资源和资源组

添加内网资源以及资源组 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。

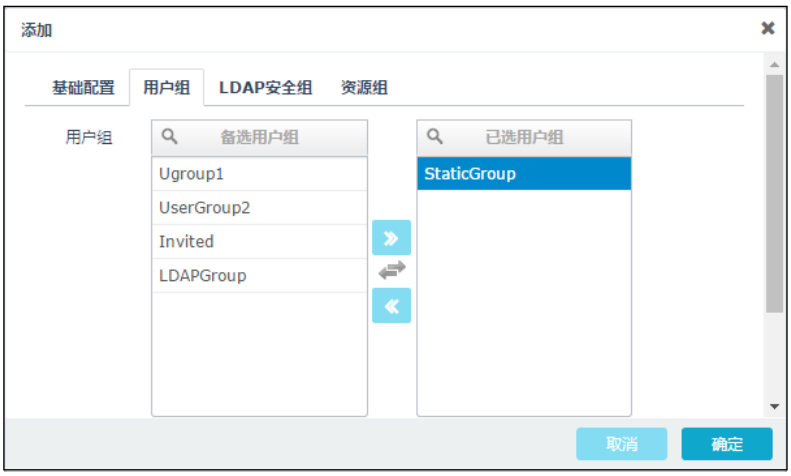
9.7.5. 配置 VPN 策略

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。

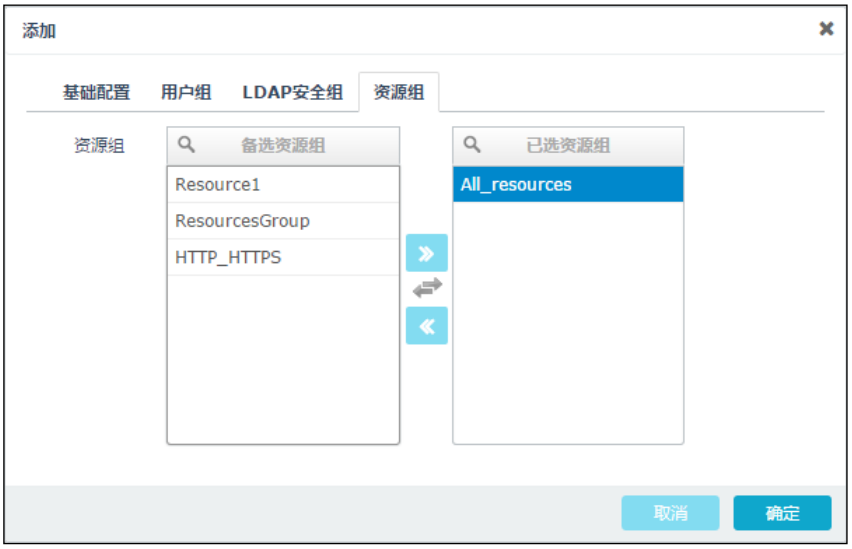
a. 在**基础配置**页签进行相关配置。

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。

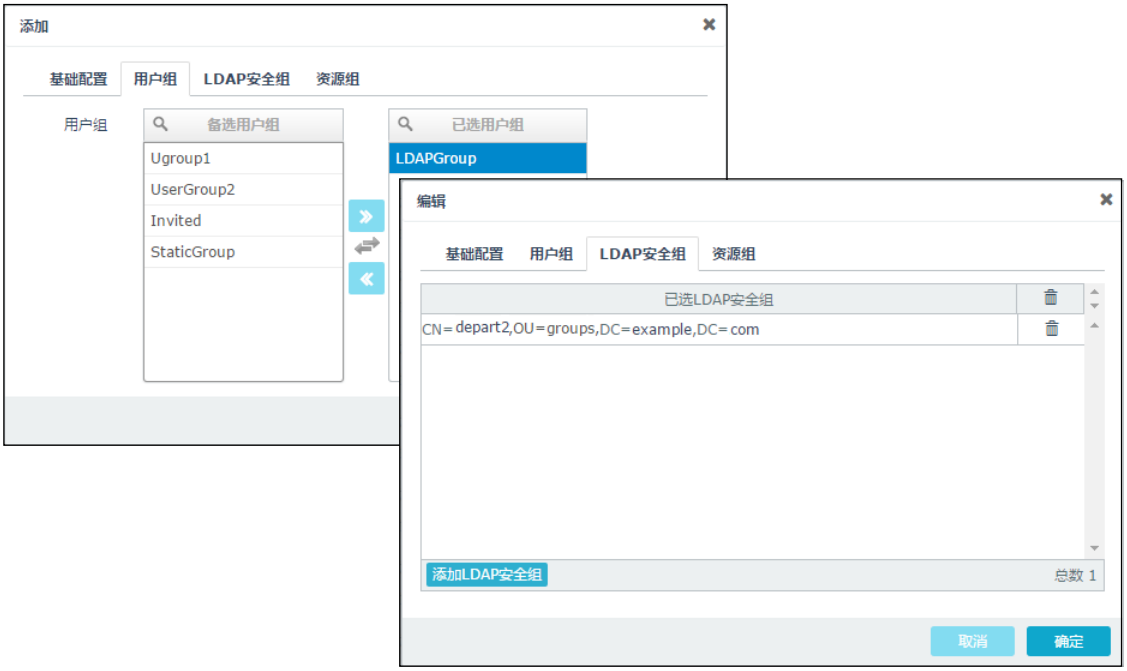


d. 点击**确定**。

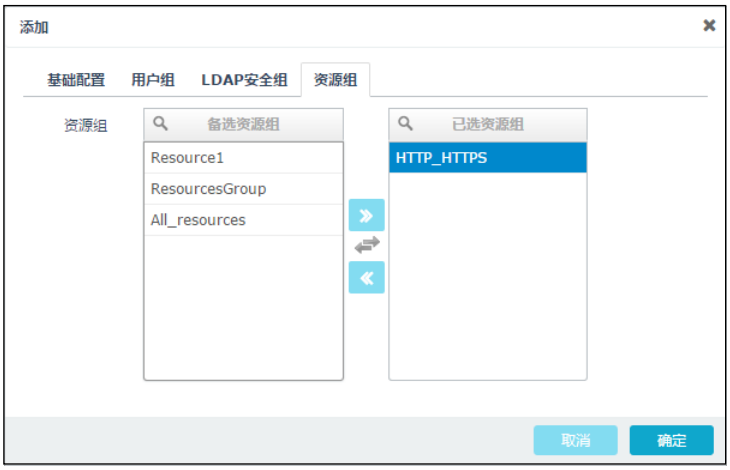
3. 点击**添加**，添加一条 Web SSL VPN 策略，允许其他用户访问 HTTP 和 HTTPS 资源。

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**。

9.7.6. 配置 SSL VPN 服务

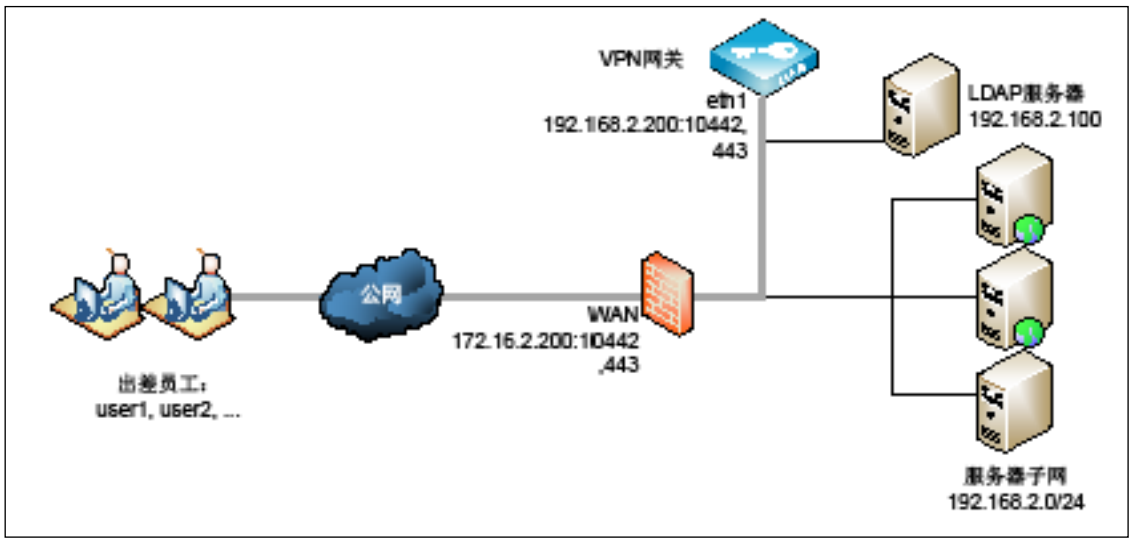
参考 3.8 Web 模式 SSL VPN 和 3.9 隧道模式 SSL VPN 配置 SSL VPN 服务。

9.8.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

9.8.1. 配置本地 RADIUS 认证服务

1. 选择**认证配置>外部认证服务器**，点击页面右上角的**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**。

9.8.2. 添加外部认证服务器

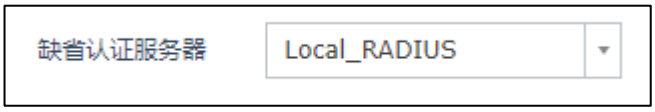
1. 选择**认证配置>外部认证服务器**。
2. 点击新建，在下拉菜单中选择 RADIUS，添加外部 RADIUS 服务器，IP 地址指向本地 RADIUS 服务器。

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**。

9.8.3. 设置缺省认证服务器

1. 选择**认证配置>缺省认证服务器**。
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**。

9.8.4. 配置 SSL VPN 或远程访问 IPSec VPN

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

9.9.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

9.9.1. 测试用户账号和密码

1. 以 root 或管理员账号登录。
2. 点击界面右上角工具右侧的向下箭头，选择菜单中测试用户。

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）。

9.9.2. 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：

9.10.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 Web 模式 SSL VPN。

9.10.1. 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**。

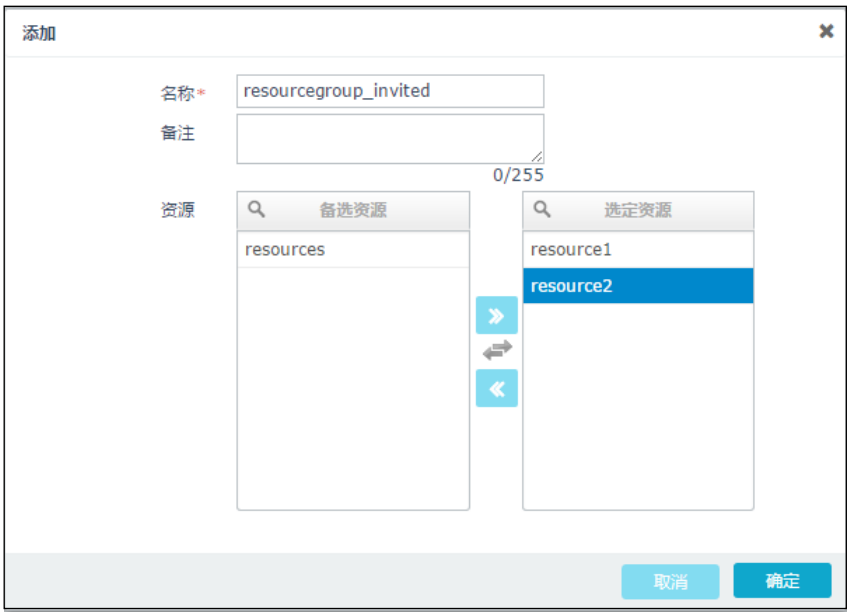
提示：创建被邀请人用户组时，包含用户应该为空。

3. 点击**确定**。

9.10.2. 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**。

9.10.3. 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**。

9.10.4. 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。

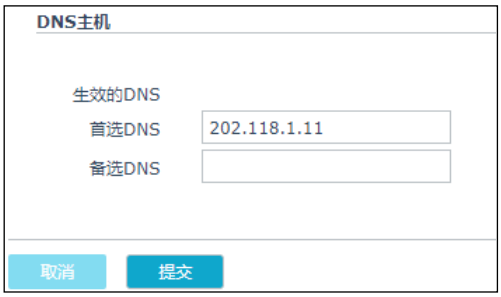
1. 选择**系统管理>邮件服务器**。
2. 配置邮件服务器和发件人信息。

3. 点击**提交**。

9.10.5. 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**。

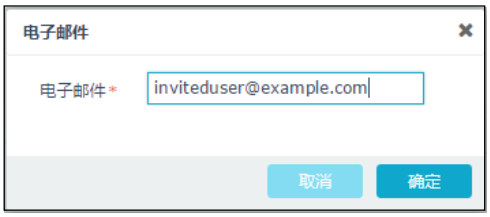
9.10.6. 配置邀请注册功能

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。

9.10.7. 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**。



9.10.8. SSL VPN 用户发送邀请码

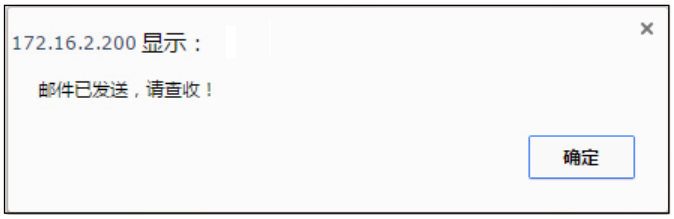
1. SSL VPN 用户可在浏览器中输入 https://portal-IP/domain_name:port（如 https://172.16.2.200:443），登录 SSL VPN Portal。
2. 点击**邀请注册**按钮，输入被邀请人邮件地址，邀请他人注册。

9.10.9. 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。

9.11.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**错误!未找到引用源。**。以下步骤默认已建立 Web 模式 SSL VPN 隧道。

9.11.1. 配置邮件服务器

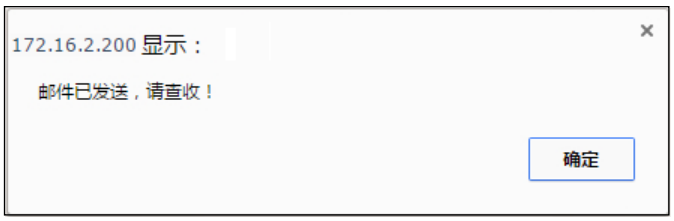
1. 选择**系统管理>邮件服务器**。
2. 设置邮件服务器和发件人信息。

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。

9.11.2. 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。

9.12.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。

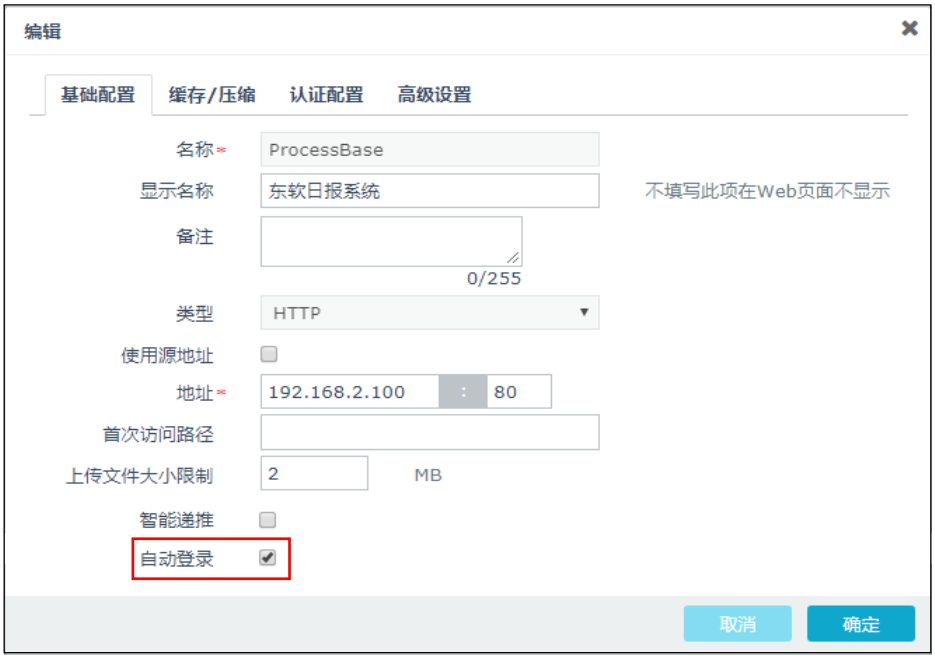
配置要点

- 为资源开启单点登录
- 允许例外资源使用独立账号
- 用户单点登录

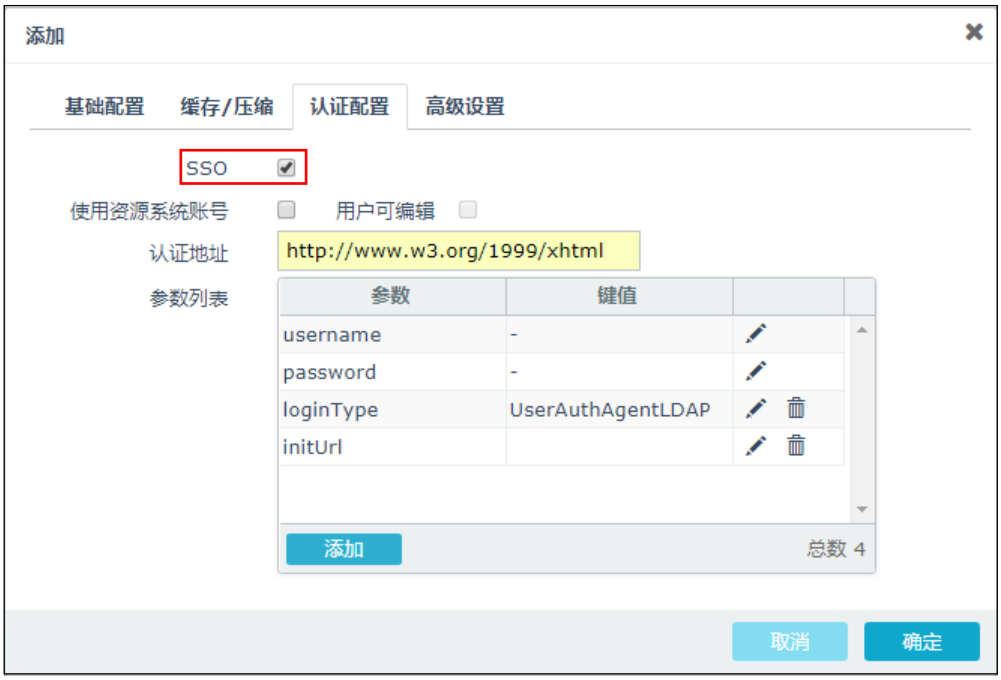
配置步骤

9.12.1. 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。



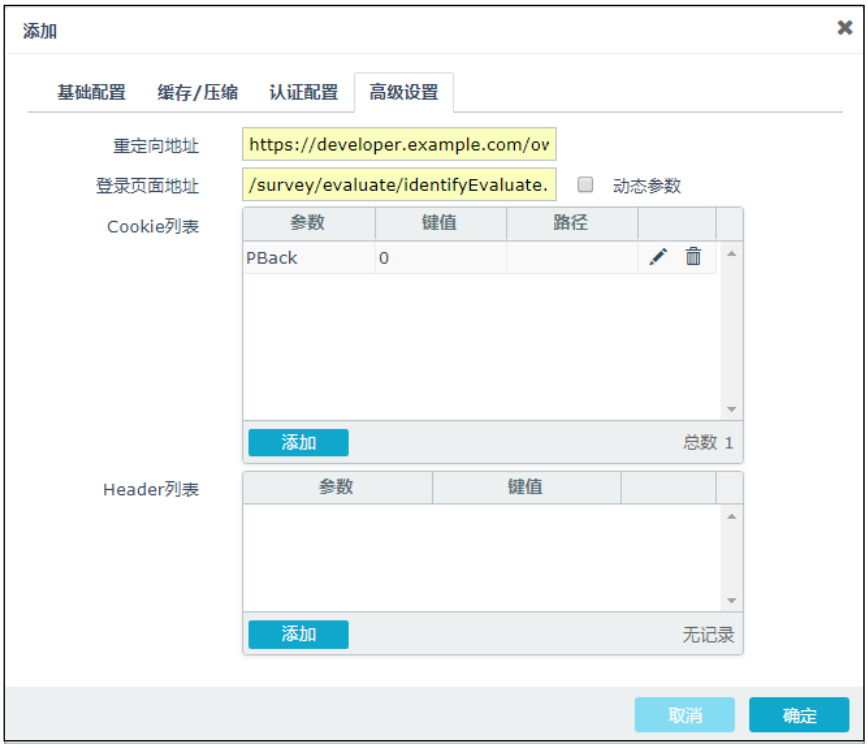
a. 认证地址是用户提交用户名、密码时，携带用户名及密码等认证信息的 URL 地址。必须填写正确的 URL 地址，才能认证通过。

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。

9.12.2. 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**。点击**提交**。

9.12.3. 用户单点登录

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。

9.13.智能递推

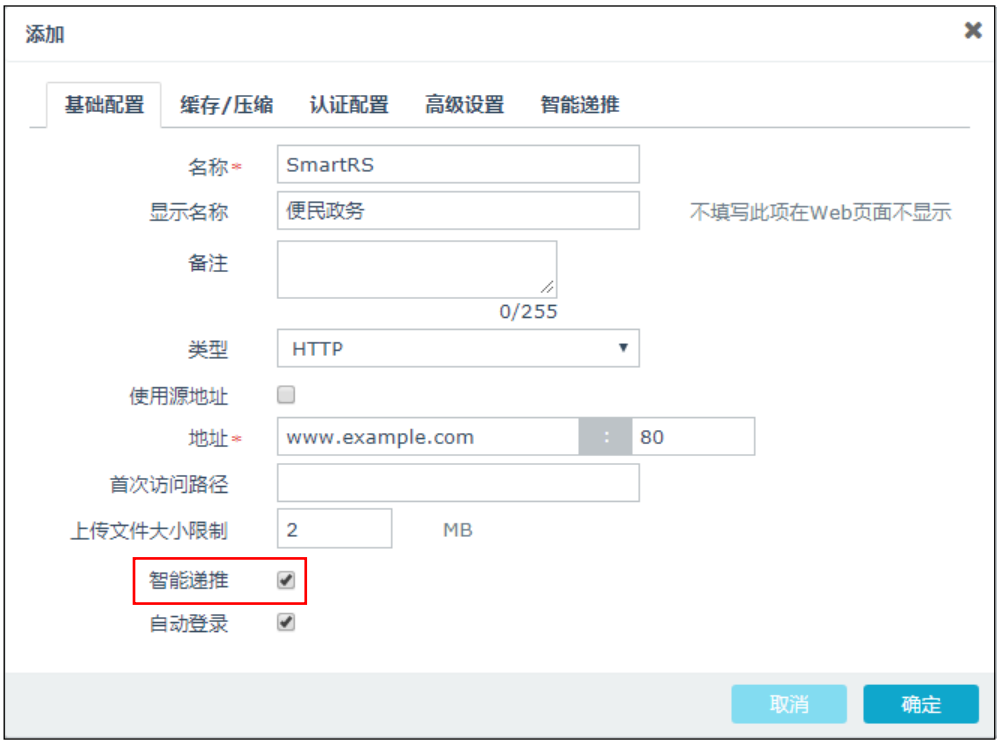
某政务网站包含大量下级机关或合作机构的网站链接。对于此类嵌套链接，逐一添加 VPN 资源不但工作量大，而且很容易漏填。此时可以开启 VPN 网关的智能递推服务，只需要添加网站主页资源和递推的 URL 范围即可，而无需逐一添加嵌套的链接资源。

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

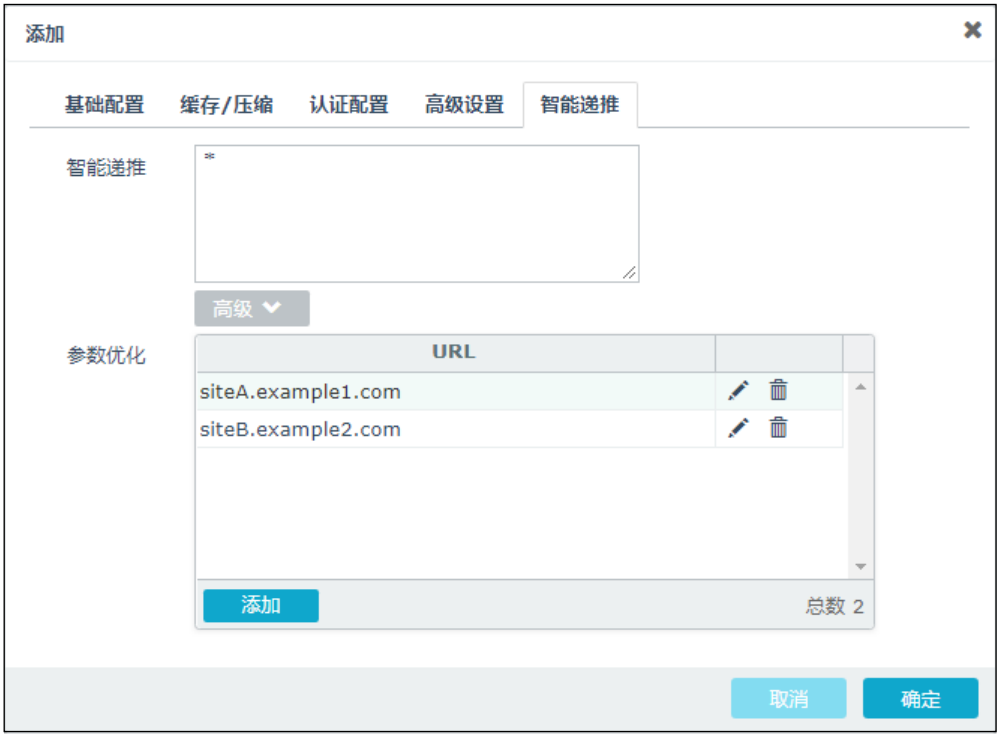
配置步骤

1. 选择**基础功能>资源**，添加网站主页资源，开启智能递推。



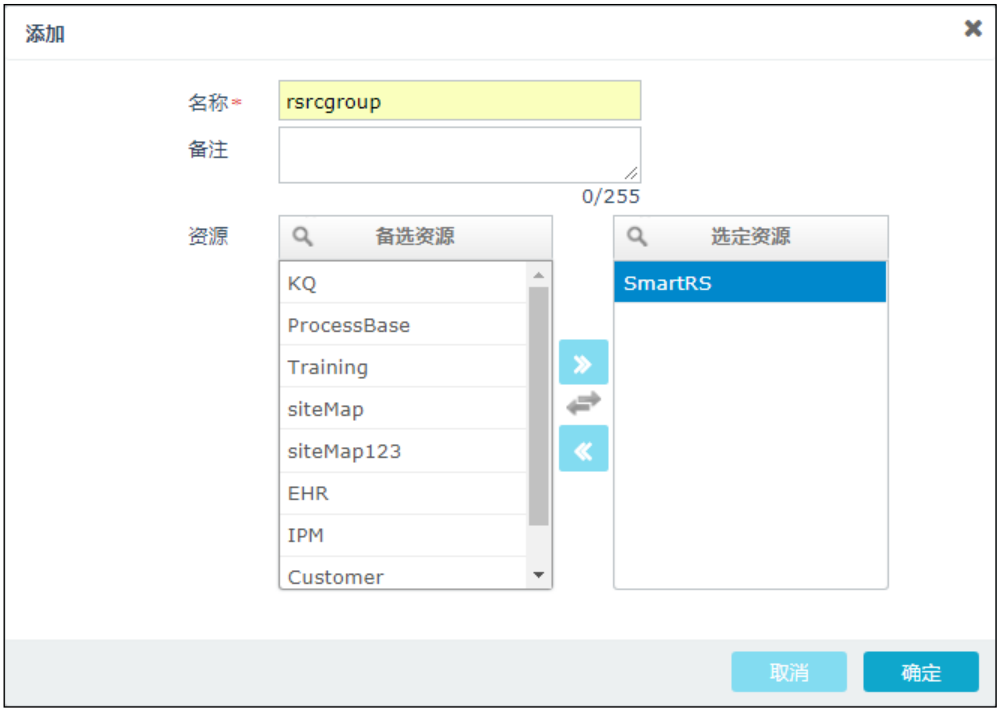
2. 在**认证配置**页面勾选 **SSO**，允许用户多点登录。

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。



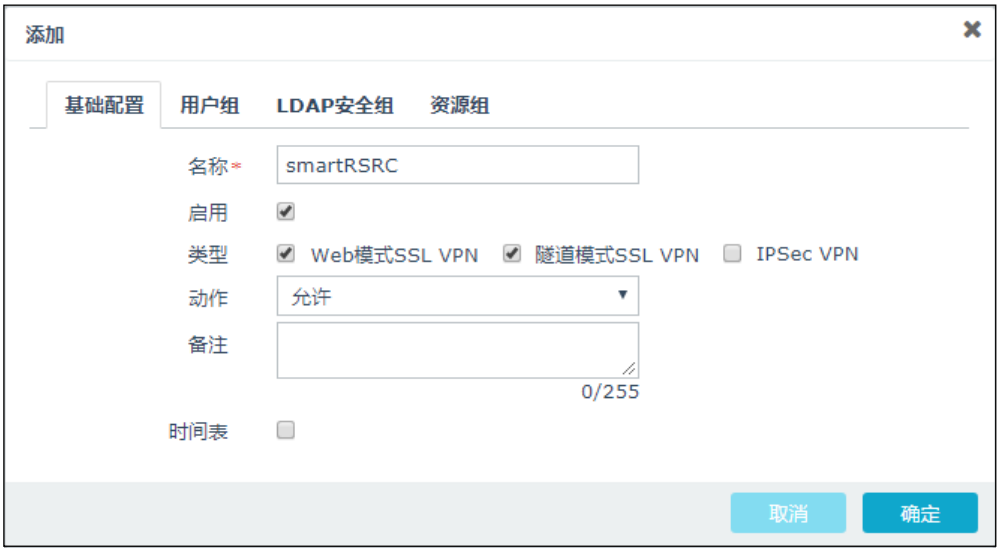
点击**添加**，可添加更多需要优化的网页 URL 及优化策略。

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。

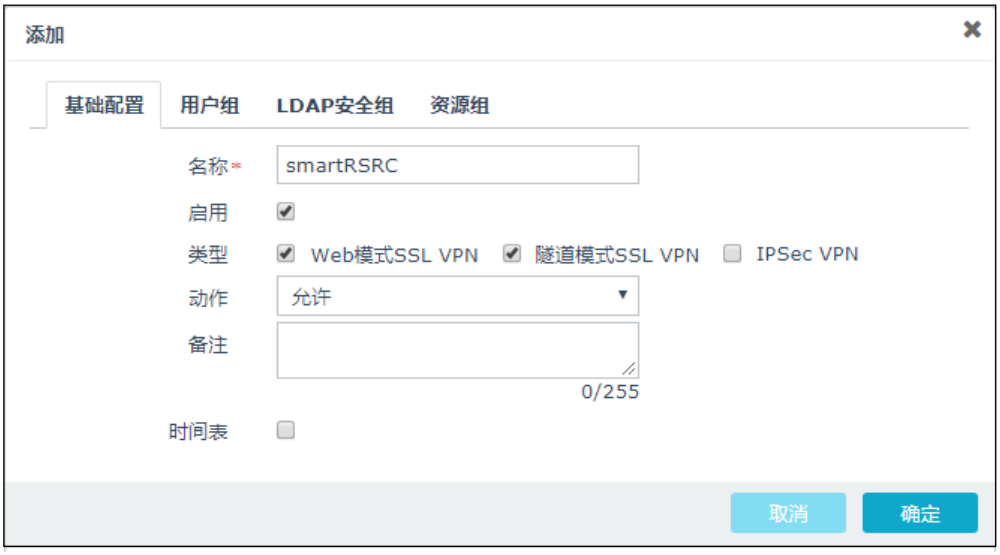


6. 选择**基础功能> VPN 策略**，添加 VPN 访问策略，授权指定用户访问已添加资源。

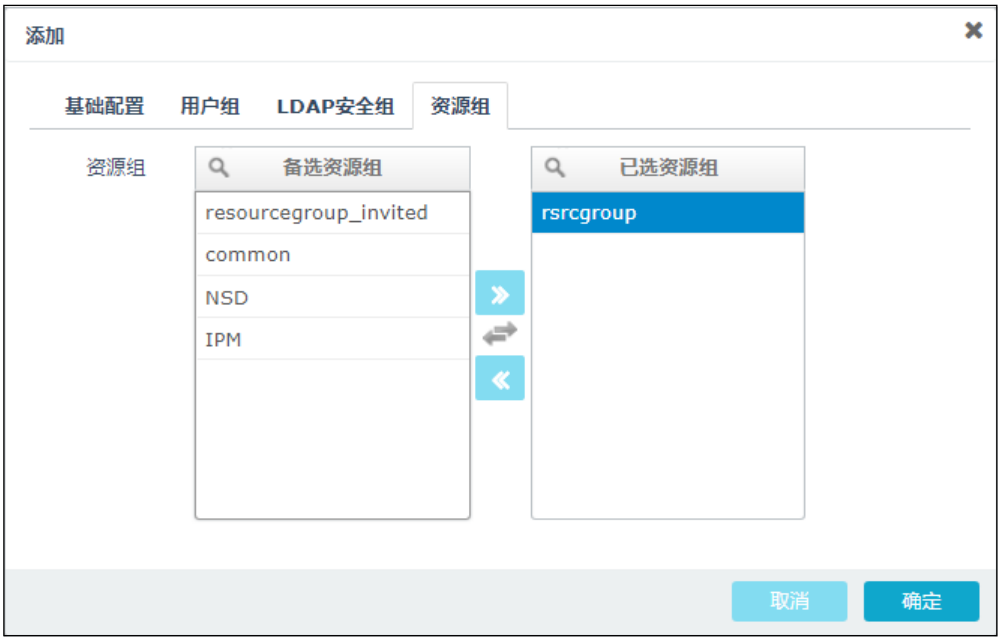
a. 添加策略，指定 VPN 服务类型。



b. 指定授权用户。



c. 指定允许访问的资源组。



d. 点击**确定**。

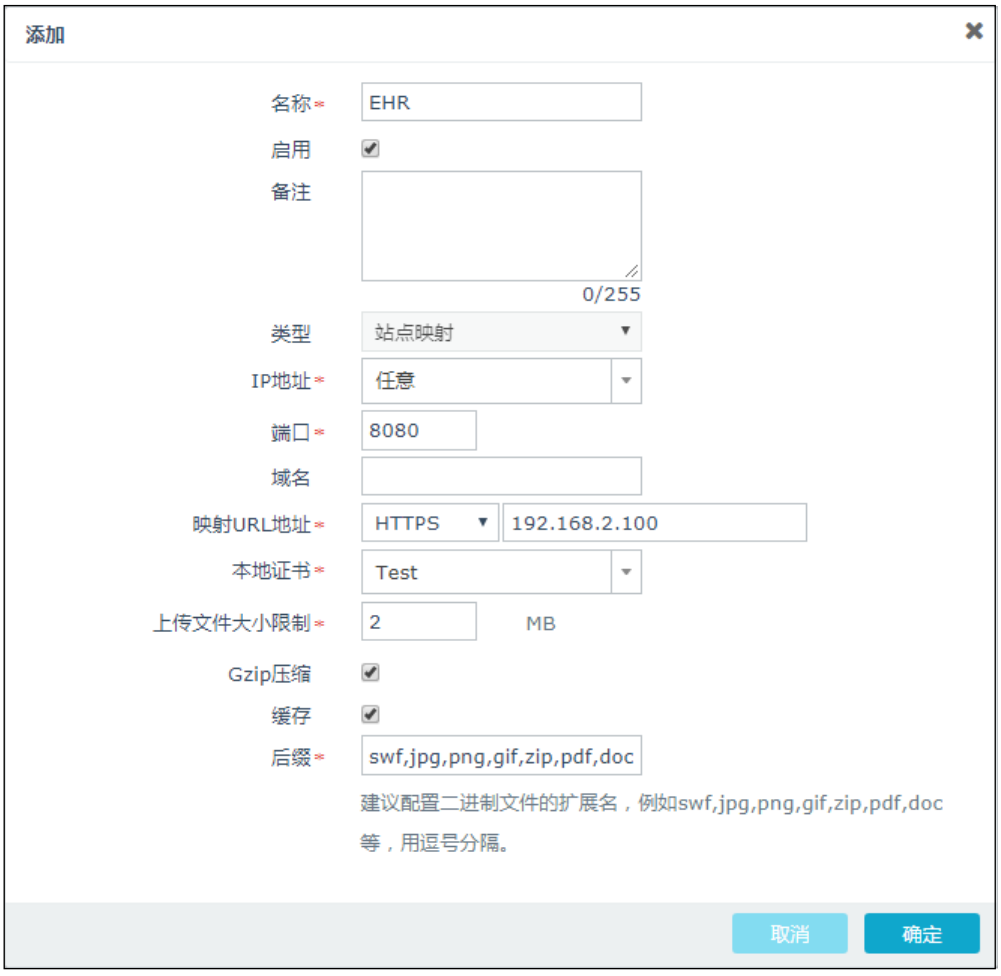
7. SSL VPN 用户可通过 Portal 方式或 SSL VPN 客户端访问该网站主页及嵌套的链接。

9.14.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。

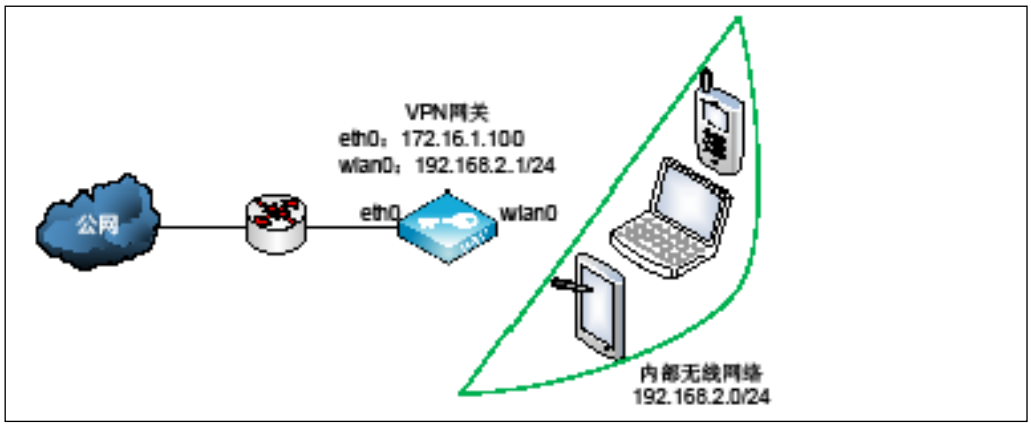


3. 点击**确定**。
4. 内网 SSL VPN 用户在浏览器中输入 https://VPN 网关地址（IP/域名）:8080，即可直接访问内网 EHR 系统。

9.15.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

9.15.1. 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**。

9.15.2. 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**。

9.15.3. 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**。

9.15.4. 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**。

9.15.5. 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**。

9.15.6. 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。

9.15.7. 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。

附录 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

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

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

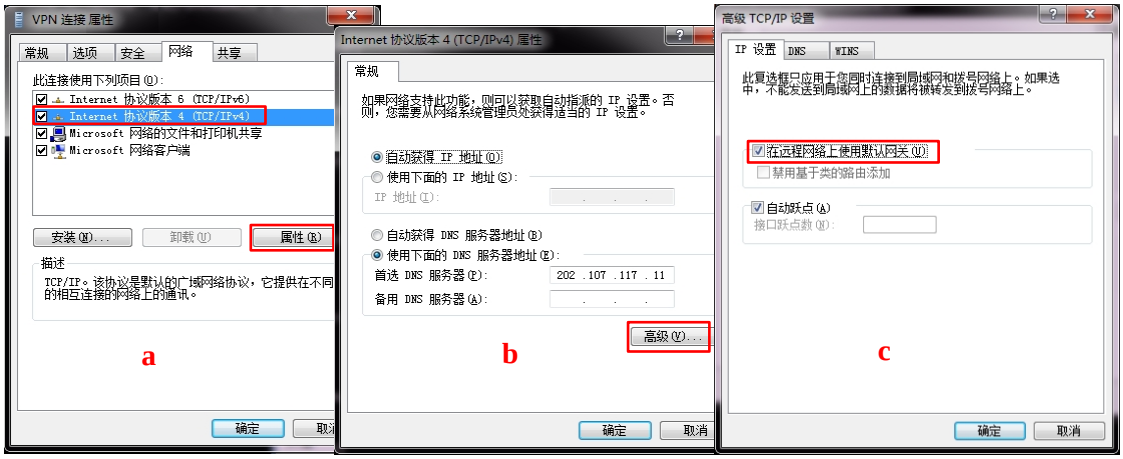
通过 IPSec VPN 连接的目的是保证通讯过程的安全。默认情况下，一旦 IPSec VPN 连接建立，所有客户端流量都走隧道，已有的互联网和局域网连接将断开。

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：

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

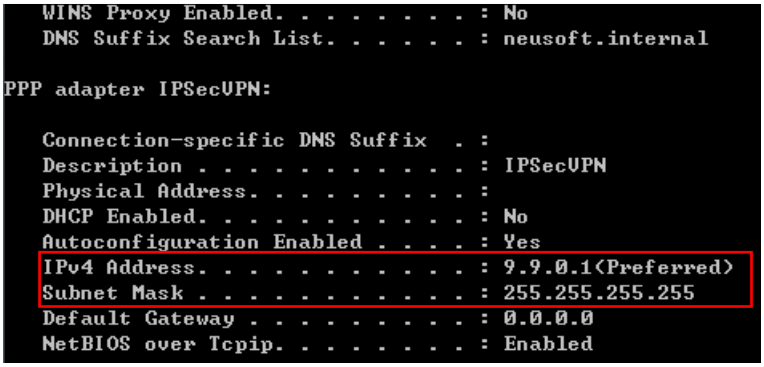
详细步骤如下：

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



4. 在运行中输入 **cmd**，打开 Windows 命令行。

5. 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：



6. 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

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

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

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

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

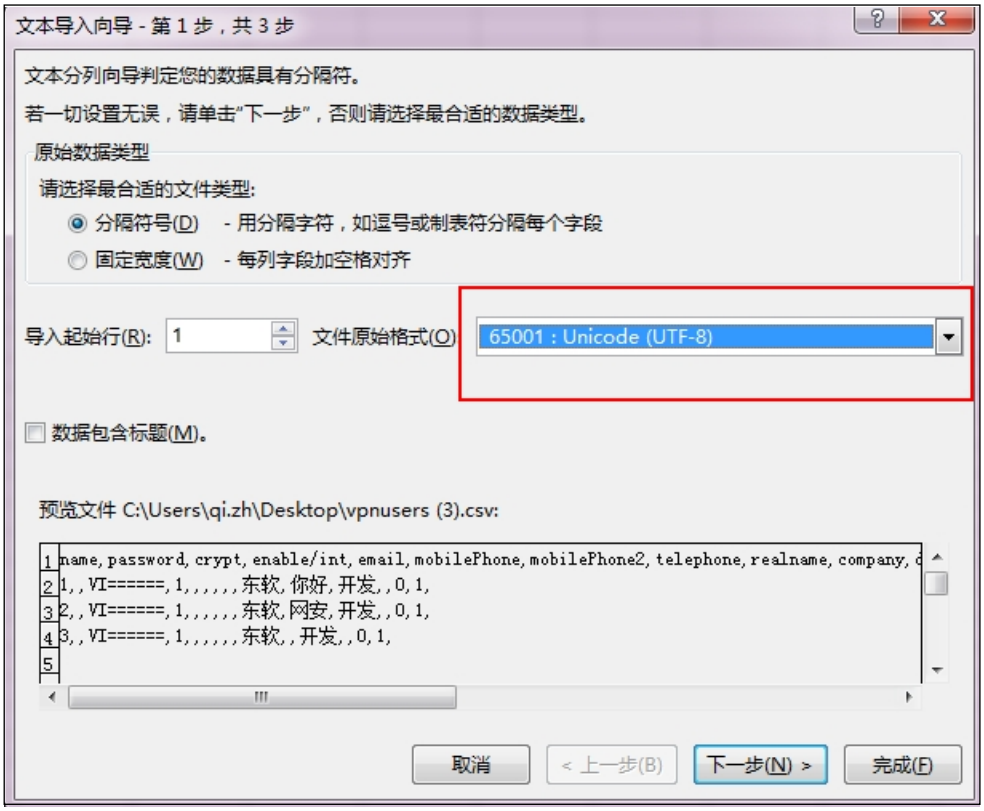
导出数据显示乱码。

解决办法

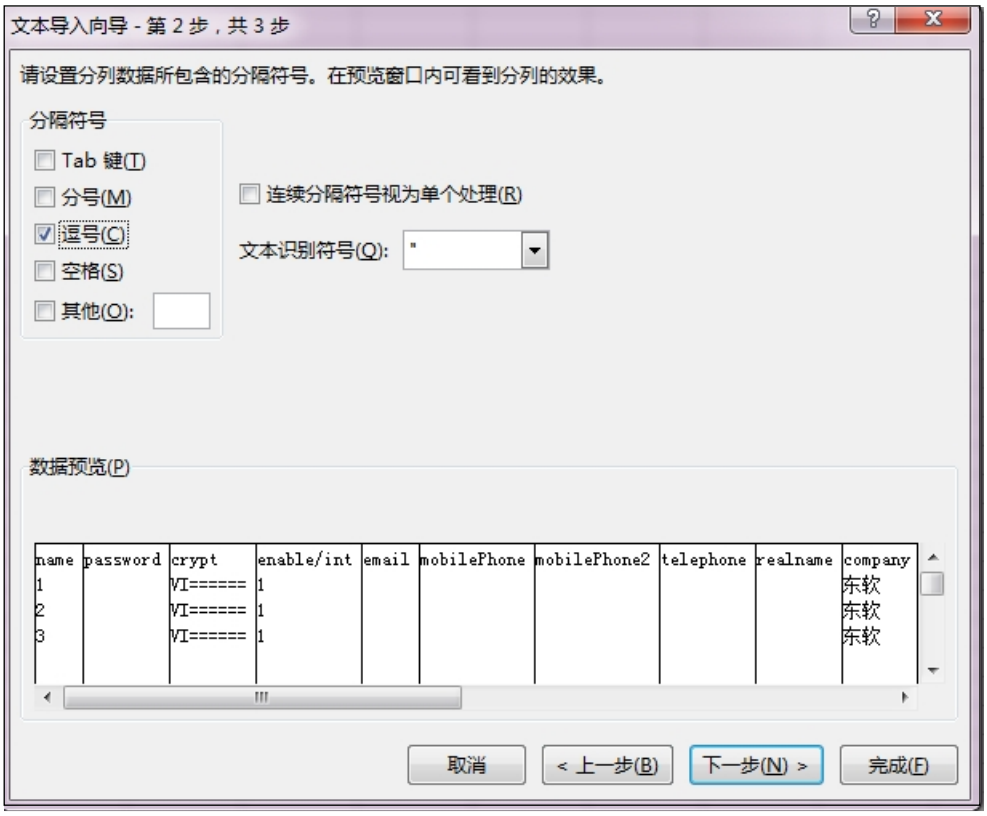
如果想批量编辑用户或策略信息，可将当前用户或策略信息导出，编辑后再导入。

1. 点击**导出**按钮，导出当前用户或策略信息为 csv 文件。
2. 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：



3. 编辑用户或策略信息，另存为 csv 格式（逗号分隔）。
4. 备份 VPN 网关的系统信息，导入编辑后的 csv 文件。

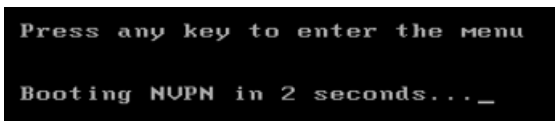
常见问题

修改初始密码后，忘记密码。

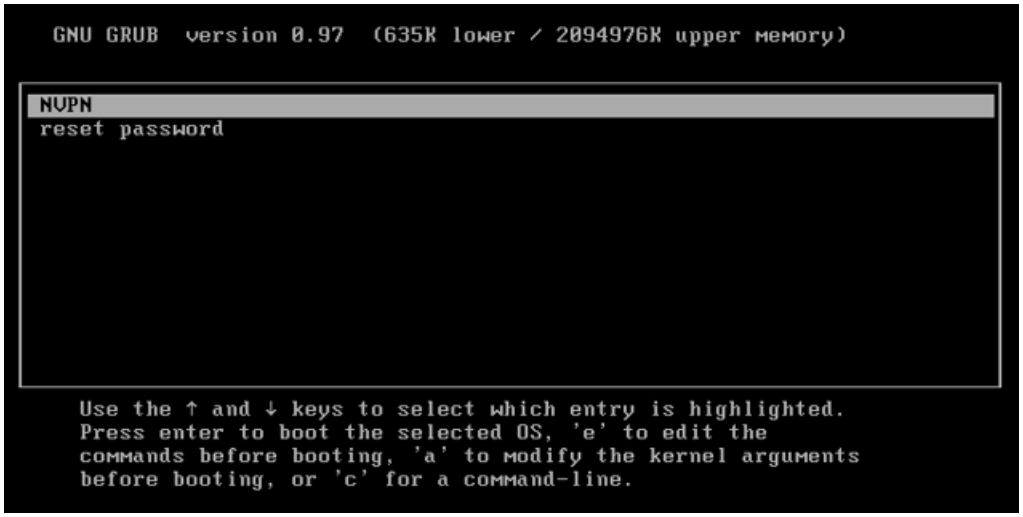
解决办法

通过 Console 重置密码：

1. 将管理主机连接到设备串口。
2. 重启设备。系统启动过程中，出现如下打印时按回车键：



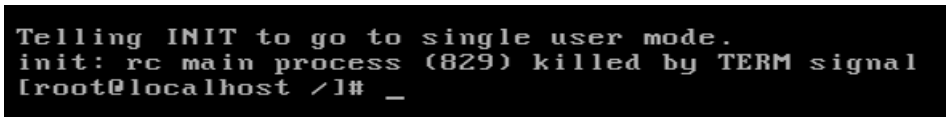
3. 之后出现如下界面：



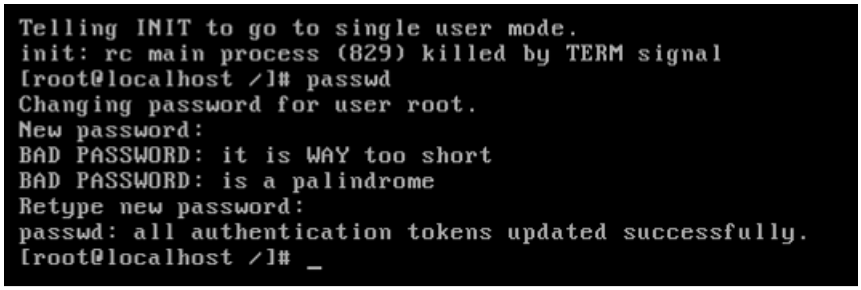
4. 选择 reset password 后回车（虚拟机需要在 reset password 上按 E，然后在 kernel 行上再按 e，然后进去把 console=ttyS0 去掉后，回车，然后按 b）。

5. 输入密码 neteye 后回车。

6. 看到如下页面后，在#后输入 passwd。



7. 输入新密码，回车。如果有些密码过短之类的提示，可忽略。



8. 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