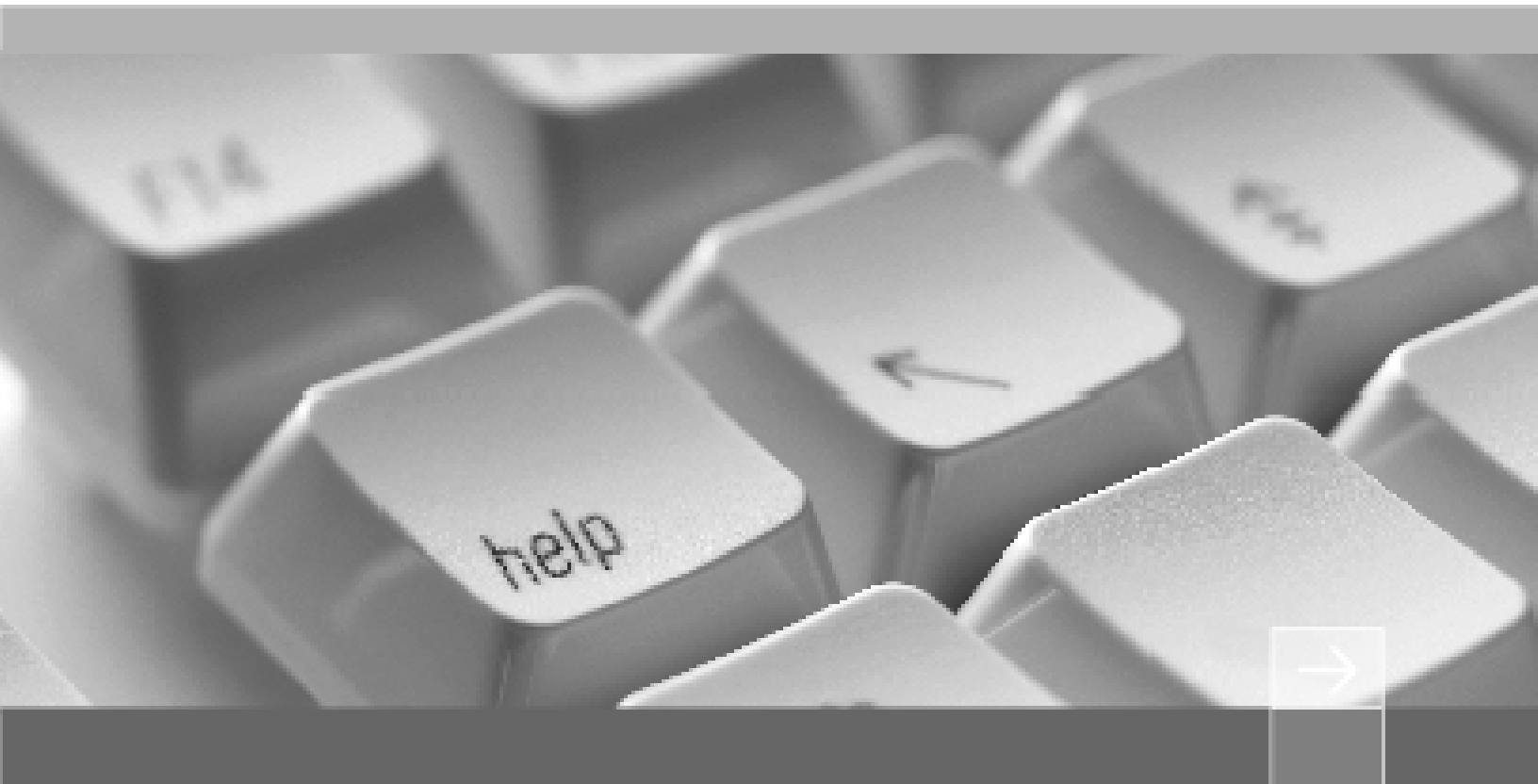


NetEye

IT SOLUTIONS & SERVICES



东软 NetEye VPN 网关快速向导

Neusoft[®]
Beyond Technology™

版权所有

本软件和相关文档的版权归沈阳东软系统集成工程有限公司所有，任何侵犯版权的行为都将被追究法律责任。未经版权所有者的书面许可，不得将本软件的任何部分或全部及其用户手册以任何形式、采用任何手段（电子的或机械的，包括照相复制或录制）、为任何目的，进行复制或传播。

版权所有 © 2016-2018 沈阳东软系统集成工程有限公司。所有权利保留，侵权必究。

沈阳东软系统集成工程有限公司不对因使用本软件及其用户手册所造成的任何损失承担任何责任。

东软 NetEye VPN 网关（以下简称“VPN 网关”）出厂时已经安装好系统，管理员只需将设备接入网络即可开始使用。本向导提供产品的快速部署过程，内容包括：

- 1. 产品概述
- 2. 选择部署模式
- 3. 登录 WebUI
- 4. 初始配置
- 5. 接入网络
- 6. 典型配置范例

1. 产品概述

VPN 网关支持 IPSec VPN 和 SSL VPN 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 网关支持用户通过浏览器或客户端方式访问 SSL VPN 资源：

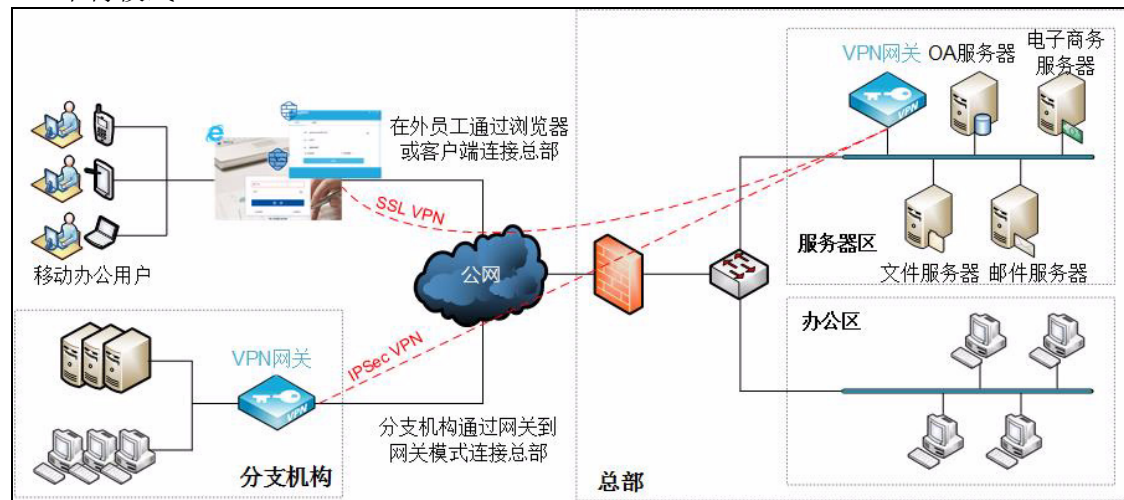
- Web 方式
通过浏览器访问 SSL VPN 资源。通过此种方式，用户无需安装任何插件即可在各主流系统上使用标准浏览器来访问资源。支持的浏览器包括 IE 7、Firefox 10、Google Chrome 9、Safari 5、Opera 12 及以上版本。
如果用户要访问的资源都是 Web 应用（如 HTTP 和 HTTPS），推荐使用 Web 模式 SSL VPN。
- 客户端方式
使用客户端访问 SSL VPN 资源。此种方式需要用户先下载、安装东软 NetEye SSL VPN 客户端，请在 SSL VPN Portal 登录页面下载相应操作系统的客户端软件，解压后安装使用。
如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。

2. 选择部署模式

VPN 网关支持单臂和网关两种部署模式，请根据实际需要选择相应的模式。

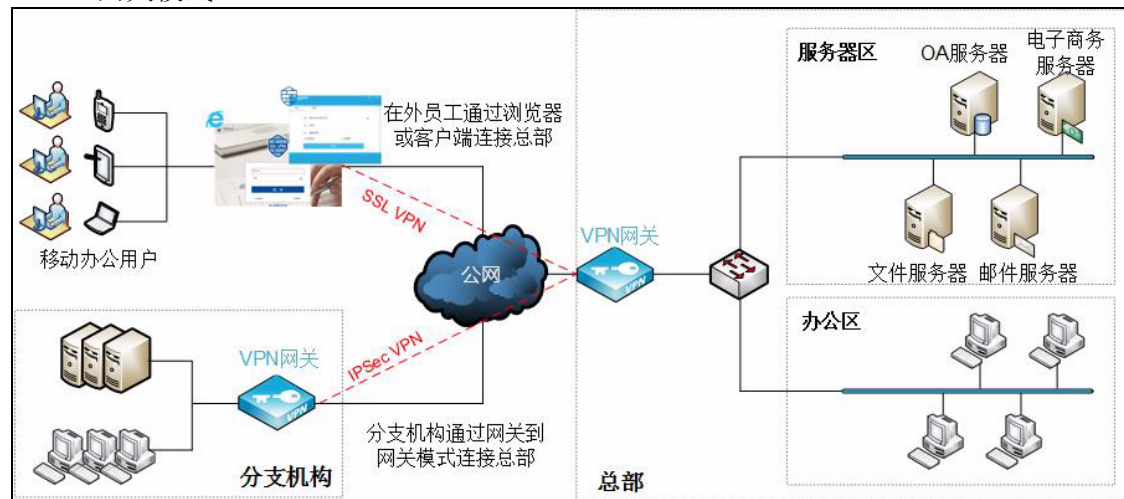
提示：推荐将 VPN 网关的以太网接口 eth0（缺省 IP 地址为 192.168.1.100）作为管理接口，完成配置后拔线。

■ 单臂模式



关于单臂模式 VPN 网关的具体配置信息，请参见 [5.1 单臂模式](#)。

■ 网关模式

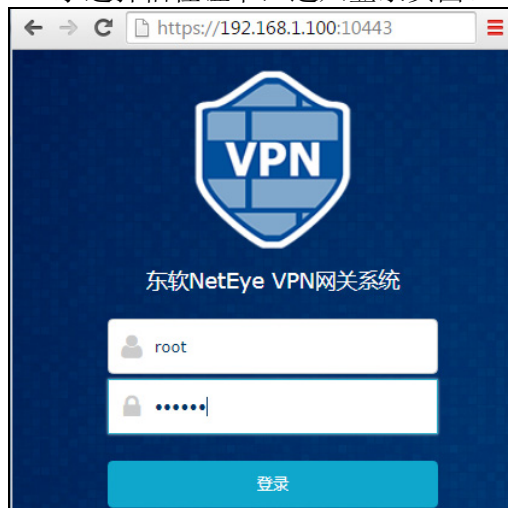


关于网关模式 VPN 网关的具体配置信息，请参见 [5.2 网关模式](#)。

3. 登录 WebUI

将管理 PC 的 IP 地址设置为 192.168.1.200，掩码设置为 255.255.255.0。打开 VPN 网关的电源开关，等待进入系统。

- 待系统启动后，在管理 PC 上打开浏览器，输入“https://192.168.1.100:10443”，根据提示选择信任证书，进入登录页面。



- 输入缺省用户名和密码（root/neteye）登录，可以看到如下管理界面：



- 点击 隐藏或展开界面左侧导航菜单。
- root 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**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**修改密码**，修改当前登录用户的密码。
 - 点击**退出**，退出系统。

4. 初始配置

1. 选择**系统管理 > 系统时间**，点击**当前时间**后面的编辑图标，手动更新系统时间。

日期时间

当前时间 2018-08-28 12:37:56 

自动同步 启用 

立即同步

2. 选择**系统管理 > 升级**，检查当前系统是否为最新版本。如果不是，上载升级包。

系统升级


当前系统版本 V3.0 BUILD8559

升级方式1

下载升级包，手动上载升级包，完成系统升级

下载升级包

低版本 VPN 网关可能没有此功能，可到东软 NetEye 官网 <http://neteye.neusoft.com> 的“技术支持 > 下载中心”获取升级包。


3. 在主页的**系统信息**区域点击**License 信息**后面的  或选择**系统管理 > License**，点击**导入**，输入 License 字符串。

导入License

输入License

取消 **确定**

提示： License 控制并发连接数和 VPN 用户数，请根据实际需要购买相应的 License。

4. 点击右上角的  root  图标，选择**修改密码**，修改 root 用户的 WebUI 缺省密码。

修改密码

当前密码 * (1-128)

新密码 * (1-128)

确认新密码 * (1-128)

否 **是**

提示： SSH 管理密码可以通过 SSH 连接使用 `passwd` 命令进行修改。

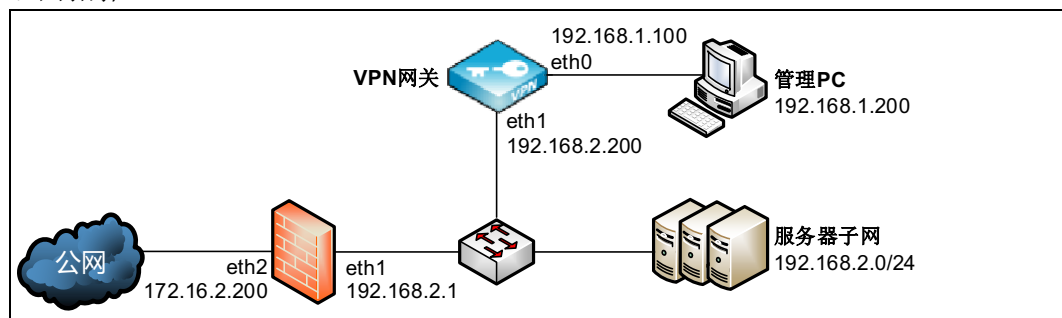
5. 接入网络

本节介绍如何将 VPN 网关以单臂 / 网关模式接入到网络。

- 5.1 单臂模式
- 5.2 网关模式
- 5.3 单臂模式（高可用性）
- 5.4 网关模式（高可用性）

5.1 单臂模式

组网拓扑：



配置步骤如下：

1. 选择网络 / 策略 > 接口 > 配置，设置接口 IP 地址。

接口	Active	属于	IP地址
eth0	●		192.168.1.100
eth1	●		192.168.2.200

2. 选择网络 / 策略 > 路由 > 静态路由，点击添加，添加一条缺省路由，出口接口设为 eth1，网关设为 192.168.2.1。

添加

目标地址 =
路由目标地址使用IP地址/掩码。例如：192.168.1.0/24

Metric = (0-255)

出口接口/网关

接口 =

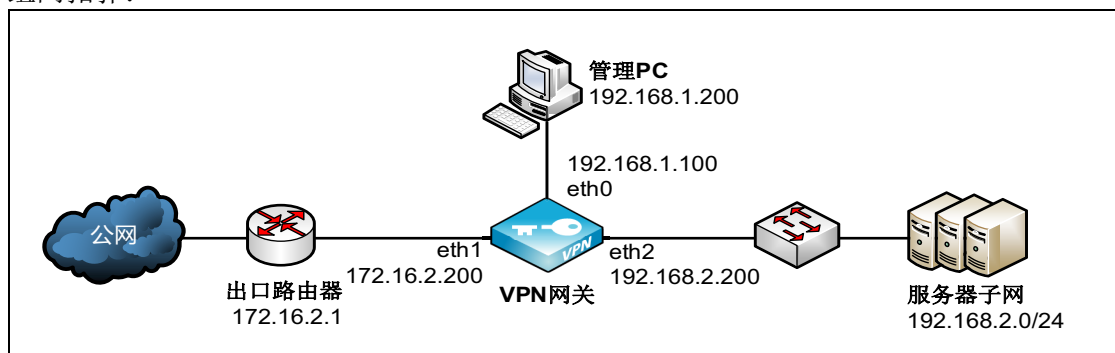
网关

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。

5.2 网关模式

组网拓扑：



配置步骤如下：

1. 选择网络 / 策略 > 接口 > 配置，设置接口 IP 地址。

重启网络服务				
接口	Active	属于	IP地址	
eth0	●		192.168.1.100	
eth1	●		172.16.2.200	
eth2	●		192.168.2.200	

2. 选择网络 / 策略 > 路由 > 静态路由，点击添加，添加一条缺省路由，出口接口设为 eth1，网关设为 172.16.2.1。

添加 ✕

目标地址 =

路由目标地址使用IP地址/掩码。例如：192.168.1.0/24

Metric = (0-255)

出口接口/网关

接口 =

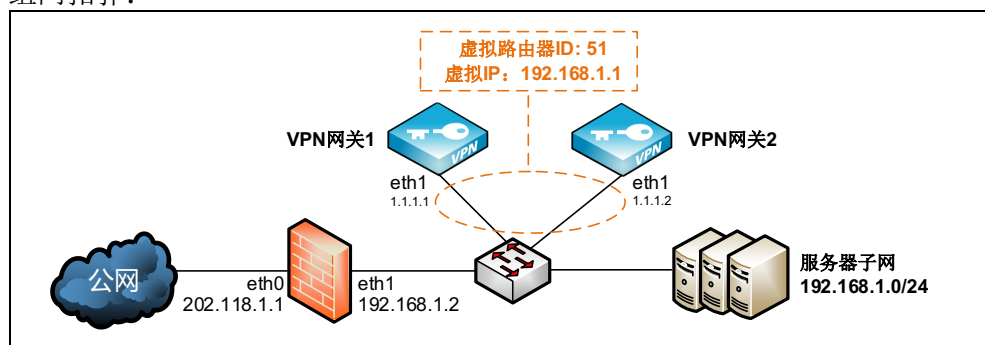
网关 =

3. 点击确定。

4. 根据需要添加其他静态路由。

5.3 单臂模式（高可用性）

组网拓扑：



配置步骤如下：

- 5.3.1 配置集群
- 5.3.2 设置配置同步

5.3.1 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。

启用	虚拟路由器ID	虚拟IP地址/掩码	接口	优先级		
<input type="radio"/>	51		eth0	100		
<input type="button" value="添加"/>						总数 1

3. 点击 对其进行修改。

启用	<input checked="" type="checkbox"/>	
虚拟路由器ID *	<input type="text" value="51"/>	主备设备的虚拟ID需一致，否则无法探测
虚拟IP地址/掩码 *	<input type="text" value="192.168.1.1"/>	
接口 *	<input type="text" value="eth1"/>	
优先级 *	<input type="text" value="100"/>	数值大的优先生效
密钥 *	<input type="password" value="....."/>	

4. 点击确定。点击提交。

5.3.2 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。

VPN 网关 1

启用	<input checked="" type="checkbox"/>
对端IP地址	<input type="text" value="1.1.1.2"/>
用户名	<input type="text" value="ha"/>
密码	<input type="password" value="....."/>
自动同步	<input checked="" type="checkbox"/>

VPN 网关 2

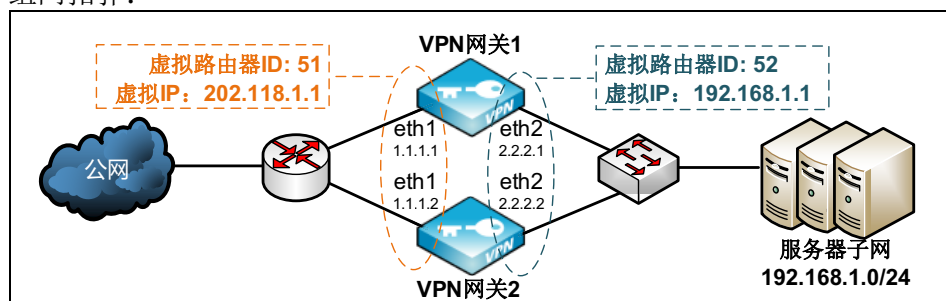
启用	<input checked="" type="checkbox"/>
对端IP地址	<input type="text" value="1.1.1.1"/>
用户名	<input type="text" value="ha"/>
密码	<input type="password" value="....."/>
自动同步	<input checked="" type="checkbox"/>

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。

5.4 网关模式（高可用性）

组网拓扑：



配置步骤如下：

- 5.4.1 配置集群
- 5.4.2 设置配置同步

5.4.1 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。

启用	虚拟路由器ID	虚拟IP地址/掩码	接口	优先级		
<input type="checkbox"/>	51		eth0	100		
<input type="button" value="添加"/>						总数 1

3. 点击 对其进行修改。

启用	<input checked="" type="checkbox"/>	
虚拟路由器ID *	<input type="text" value="51"/>	主备设备的虚拟ID需一致，否则无法探测
虚拟IP地址/掩码 *	<input type="text" value="202.118.1.1"/>	
接口 *	<input type="text" value="eth1"/>	
优先级 *	<input type="text" value="100"/>	数值大的优先生效
密钥 *	<input type="password" value="....."/>	

4. 点击确定。
5. 点击添加，添加虚拟路由器 ID 为 52 的条目。

启用	<input checked="" type="checkbox"/>	
虚拟路由器ID *	<input type="text" value="52"/>	主备设备的虚拟ID需一致，否则无法探测
虚拟IP地址/掩码 *	<input type="text" value="192.168.1.1"/>	
接口 *	<input type="text" value="eth2"/>	
优先级 *	<input type="text" value="100"/>	数值大的优先生效
密钥 *	<input type="password" value="....."/>	

6. 点击确定。
7. 点击提交。

5.4.2 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。

VPN 网关 1

启用	<input checked="" type="checkbox"/>
对端IP地址	<input type="text" value="1.1.1.2"/>
用户名	<input type="text" value="ha"/>
密码	<input type="password" value="•••••"/>
自动同步	<input checked="" type="checkbox"/>

VPN 网关 2

启用	<input checked="" type="checkbox"/>
对端IP地址	<input type="text" value="1.1.1.1"/>
用户名	<input type="text" value="ha"/>
密码	<input type="password" value="•••••"/>
自动同步	<input checked="" type="checkbox"/>

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。

6. 典型配置范例

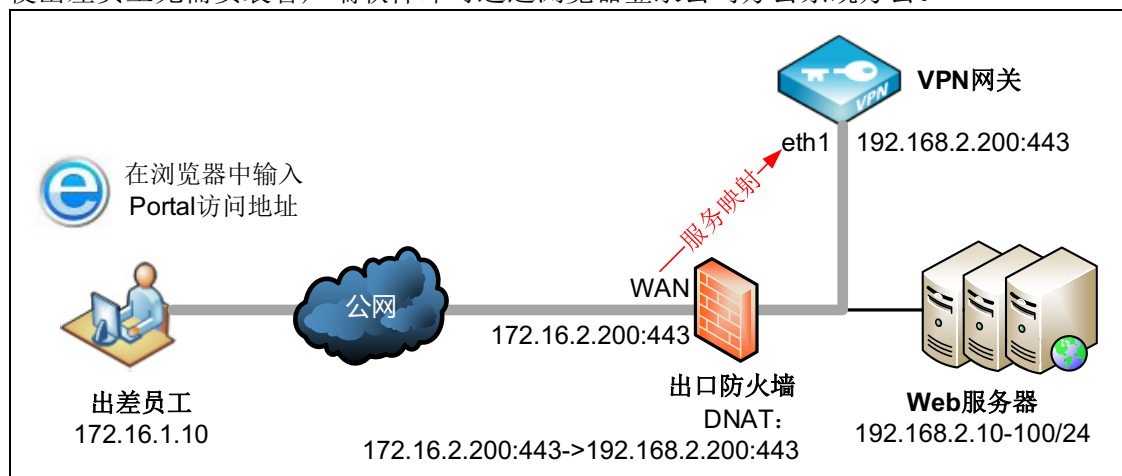
本节通过以下范例介绍如何配置 SSL VPN 和 IPSec VPN:

- 6.1 Web 模式 SSL VPN
- 6.2 隧道模式 SSL VPN
- 6.3 远程访问 IPSec VPN
- 6.4 网关到网关 IPSec VPN

6.1 Web 模式 SSL VPN

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。



配置步骤如下:

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

6.1.1 配置全局设置

1. 选择**基础功能 > 全局设置**。
2. 选择本地认证服务器，使用缺省的缓存 / 压缩设置，设置会话超时提醒。

认证配置

缺省认证服务器

辅助认证 [短信认证](#)
[OTP](#)
[硬件特征码认证](#)

缓存/压缩

Gzip压缩

HTML/JS/CSS 缓存

后缀
推荐使用：html,js,css ，用逗号分隔。

非HTML/JS/CSS 快速代理

非HTML/JS/CSS 缓存

后缀
建议配置二进制文件的扩展名，例如swf,jpg,png,gif,zip,pdf,doc等，用逗号分隔。

会话超时提醒

会话断开前 分钟提醒

3. 点击**提交**。

6.1.2 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。

添加

基础配置 缓存/压缩

名称 * webserver

显示名称 webserver 不填写此项在Web页面不显示

备注 0/255

类型 HTTP

使用源地址

地址 * 192.168.2.100 : 8080

首次访问路径

上传文件大小限制 2 MB

智能递推

自动登录

全局设置

取消 确定

提示：请务必填写**显示名称**，否则在客户端资源列表中不显示该资源。

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。

添加

名称* resource_group

备注

0/255

资源

备选资源

resource1

resource3

resource2

resource6

resource7

resource8

resource5

resource4

选定资源

webservers

app

developer

取消 确定

7. 点击**确定**。

6.1.3 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. 选择**基础功能 > 用户组**。
5. 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。

6. 点击**确定**。

6.1.4 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**，动作设置为**允许**。

The screenshot shows the 'Basic Configuration' tab of the VPN Policy configuration dialog. The fields are as follows:

- 名称*: vpn_policy
- 启用:
- 类型: Web模式SSL VPN 隧道模式SSL VPN IPsec VPN
- 动作: 允许
- 备注: (empty text area)
- 0/255 (character count)
- 时间表:

- b. 在**用户组**页签选择策略应用于的用户组。

The screenshot shows the 'Add' dialog box with the 'User Group' tab selected. It features two list boxes:

- 备选用户组 (Candidate User Groups): empty
- 已选用户组 (Selected User Groups): user_group

Navigation buttons include a right arrow (>) to move the selected group to the candidate list, and a double arrow (<=>) to toggle selection.

- c. 在**资源组**页签选择策略应用于的资源组。

The screenshot shows the 'Add' dialog box with the 'Resource Group' tab selected. It features two list boxes:

- 备选资源组 (Candidate Resource Groups): empty
- 已选资源组 (Selected Resource Groups): resource_group

Navigation buttons include a right arrow (>) to move the selected group to the candidate list, a double arrow (<=>) to toggle selection, and a left arrow (<) to move the selected group back to the candidate list.

3. 点击**确定**。

6.1.5 导入 SSL VPN 服务器证书

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

提示： 推荐使用权威 CA 机构颁发的服务器证书。

3. 点击导入。

6.1.6 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。

6.1.7 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。

6.1.8 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。



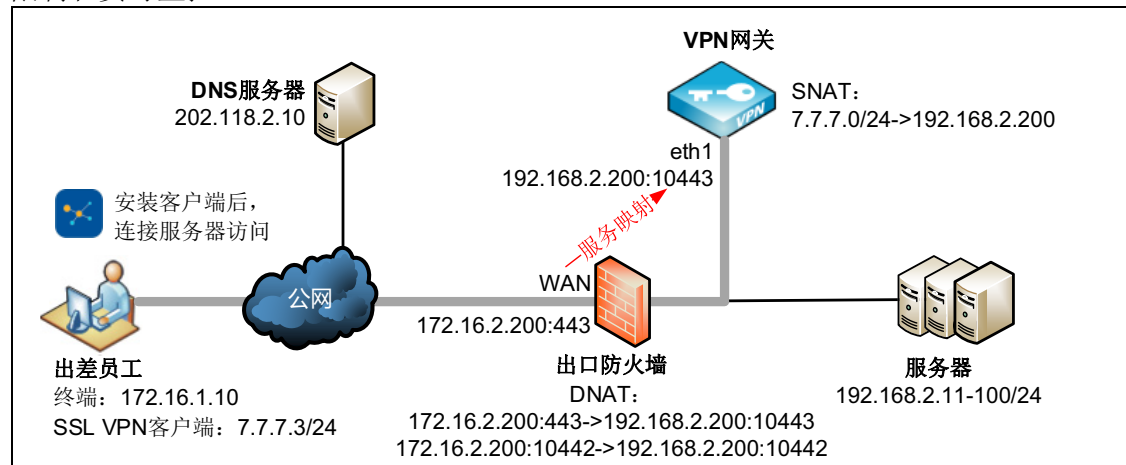
2. 当 SSL VPN 用户连接成功后，您可在 **监控 > 在线用户 > Web 模式在线用户** 页面查看到用户在线信息。

离线								流量	开	关
<input type="checkbox"/>	用户	姓名	公司	部门	客户端地址	登录时间	流量 (字节)	客户端信息	会话	
<input type="checkbox"/>	user1	张三	NEU	NSD	172.16.1.10	2018-06-27 21:47:25	55	Mozilla/5.0 (Windows N 8724A04873F115D7F140BE7494DCF0AC		

3. 如有需要，可以通过**离线**按钮强制用户下线。

6.2 隧道模式 SSL VPN

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。



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

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

配置步骤如下：

- [6.2.1 配置全局设置](#)
- [6.2.2 配置资源和资源组](#)
- [6.2.3 配置用户和用户组](#)
- [6.2.4 配置 VPN 策略](#)
- [6.2.5 添加 CA 证书和本地证书](#)
- [6.2.6 配置隧道模式 SSL VPN](#)
- [6.2.7 配置源地址转换](#)
- [6.2.8 配置出口防火墙 DNAT](#)
- [6.2.9 验证结果](#)

6.2.1 配置全局设置

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

认证配置

缺省认证服务器

辅助认证 [短信认证](#)
[OTP](#)
[硬件特征码认证](#)

缓存/压缩

Gzip压缩

HTML/JS/CSS 缓存

后缀
推荐使用：html,js,css ，用逗号分隔。

非HTML/JS/CSS 快速代理

非HTML/JS/CSS 缓存

后缀
建议配置二进制文件的扩展名，例如swf,jpg,png,gif,zip,pdf,doc等，用逗号分隔。

会话超时提醒

会话断开前 分钟提醒

3. 点击提交。

6.2.2 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。

添加

基础配置

名称* resources

备注

0/255

类型 子网

地址列表 192.168.2.0/24

示例：
192.168.2.0/32
192.168.1.1:443,80
192.168.3.1-192.168.3.50:20-21,8080

说明：
1) 使用回车分割每项配置
2) 每行只能配置单IP、网段、IP范围中的1个。
3) 端口可选，并支持端口范围，配置多个时使用逗号分割

取消 确定

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。

添加

名称* ResourcesGroup

备注

0/255

资源

Q 备选资源

resource1
resource2
resource3

Q 选定资源

resources

取消 确定

6. 点击确定。

6.2.3 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。

添加 ✕

基本设置

用户名 *

启用

电子邮件

手机号

用户详细信息

本地用户密码

密码 (1-128)

确认密码 (1-128)

密码选项

首次登录修改密码

密码永不过期

账号选项

过期时间 永不过期

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。

添加

名称* user_group

类型 静态

备注 0/255

模式 编辑模式 选择模式

包含已选用户

本地用户

已选用户

user1

user2

user3

取消 确定

7. 点击**确定**。

6.2.4 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**。

The screenshot shows the 'Basic Configuration' tab of the VPN Policy configuration dialog. The fields are as follows:

- 名称*: tunnel1
- 启用:
- 类型: Web模式SSL VPN 隧道模式SSL VPN IPSec VPN
- 动作: 允许
- 备注: (empty text box)
- 0/255 (character count)
- 时间表:

- a. 在**用户组**页签选择策略应用于的用户组。

The screenshot shows the 'User Group' tab of the VPN Policy configuration dialog. It features two search boxes: '备选用户组' (Candidate User Groups) and '已选用户组' (Selected User Groups). The '已选用户组' box contains the entry 'user_group'. A blue arrow button is located between the two boxes.

- a. 在**资源组**页签选择策略应用于的资源组。

The screenshot shows the 'Resource Group' tab of the VPN Policy configuration dialog. It features two search boxes: '备选资源组' (Candidate Resource Groups) and '已选资源组' (Selected Resource Groups). The '已选资源组' box contains the entry 'ResourcesGroup'. A blue arrow button is located between the two boxes.

3. 点击**确定**。

6.2.5 添加 CA 证书和本地证书

1. 选择系统管理 > 证书。
2. 点击添加，选择根 CA 证书，添加根 CA 证书。

添加 ✕

证书名称

有效期 天

哈希算法

密钥对选项

类型

密钥对长度

证书主题信息

高级

国家代码(C) (2字母)

省份(ST)

城市(L)

公司(O)

部门(OU)

公共名(CN)

电子邮件

3. 点击确定。

4. 点击**添加**，选择**本地证书**，添加服务器证书。

添加 ✕

CA证书	cacert	▼
证书名称*	TunnelSSLVPN	
有效期*	730	天
哈希算法	SHA256	▼
证书类别	服务器证书	▼

密钥对选项

类型	RSA	▼
密钥对长度	2048	▼

证书主题信息

高级	<input checked="" type="checkbox"/>	
国家代码(C)	CN	(2字母)
省份(ST)	LN	
城市(L)	SY	
公司(O)	NEU	
部门(OU)	NSD	
公共名(CN)*	172.16.2.200	
电子邮件		

取消 确定

5. 点击**确定**。

6.2.6 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，选择已添加的 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。

配置界面截图显示隧道模式 SSL VPN 的设置。主要配置项包括：

- 启用：已勾选
- 调试：开
- 访问日志：开
- CA证书：cacert
- 本地证书：TunnelSSLVPN
- DNS：202.118.2.10
- 高级：高级
- 双向认证：未勾选
- 推送网关：未勾选
- 数据压缩：已勾选
- 摘要算法：SHA1
- 加密算法：BF-CBC

服务列表：

服务	协议	子网	隧道接入
Any:10442	udp	7.7.7.0/24	
192.168.2.200:443	tcp	1.0.0.0/16	

添加对话框 1 配置：

- IP地址：任意
- 端口：10442
- 协议：UDP
- 子网：7.7.7.0/24

添加对话框 2 配置：

- IP地址：192.168.2.200
- 端口：443
- 协议：TCP
- 子网：1.0.0.0/16

为了兼容服务端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。

6.2.7 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。

序号	1
名称 *	for_tunnel
源地址	
IP地址 *	7.7.7.0 / 24
转换后地址	
<input checked="" type="checkbox"/> 使用此接口IP地址	eth1
IP地址 *	
动作	MASQUERADE
高级设置	
目的地址	任意
服务	任意

3. 点击确定。

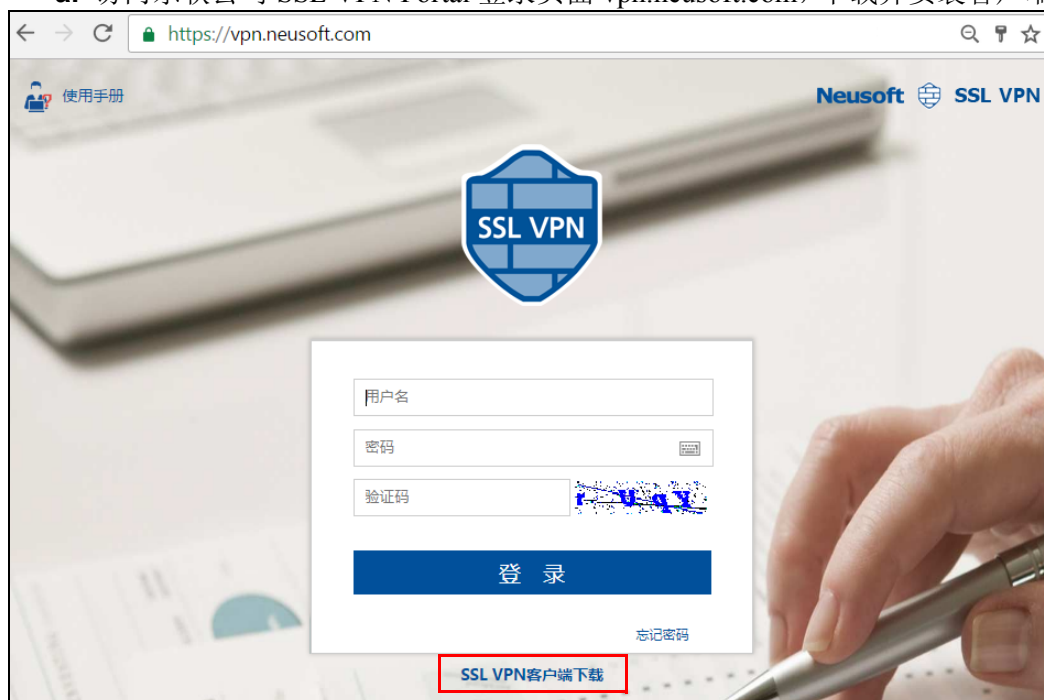
6.2.8 配置出口防火墙 DNAT

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。

6.2.9 验证结果

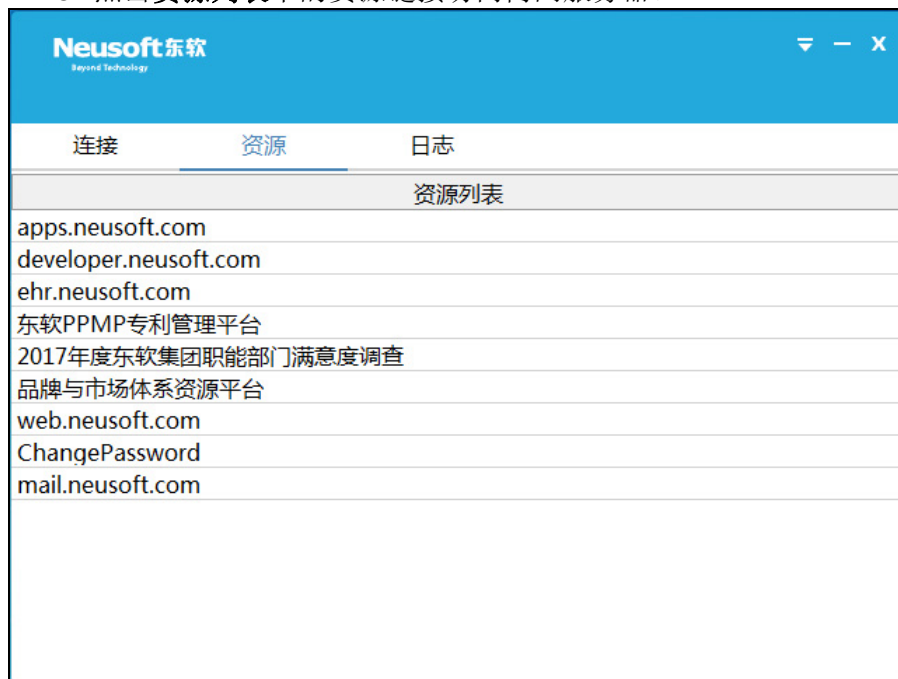
- 网络用户通过东软 SSL VPN 客户端连接之后，能够访问公司内部服务器。
 - 访问东软公司 SSL VPN Portal 登录页面 vpn.neusoft.com，下载并安装客户端软件。



- 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。



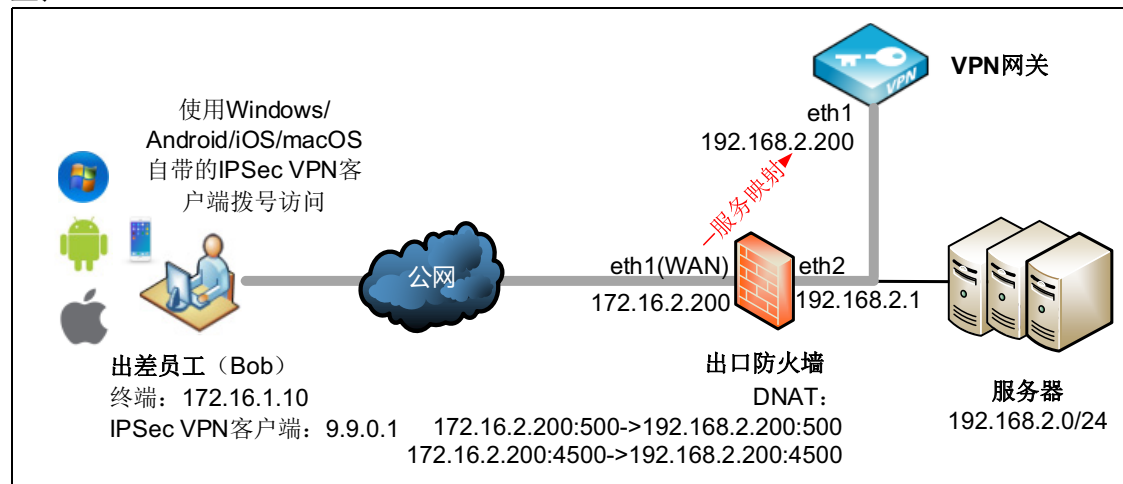
2. 管理员登录VPN网关，选择**监控 > 在线用户 > 隧道模式在线用户**，能够查看到VPN用户的在线信息。

离线									
<input type="checkbox"/>	用户	姓名	公司	部门	服务	IP地址	连接时间	发送(字节)	接收(字节)
<input type="checkbox"/>	user1	张三	NEU	NSD	Any:10442 udp	172.16.1.10:1590	2018-02-10 22:57:12	4101	2519

提示：如有需要，可以通过**离线**按钮强制用户下线。

6.3 远程访问 IPsec VPN

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。



配置步骤如下：

- [6.3.1 单臂模式部署设备](#)
- [6.3.2 配置全局设置](#)
- [6.3.3 配置资源和资源组](#)
- [6.3.4 配置用户和用户组](#)
- [6.3.5 配置 VPN 策略](#)
- [6.3.6 添加 CA 证书和本地证书](#)
- [6.3.7 配置远程访问 IPsec VPN](#)
- [6.3.8 配置出口防火墙 DNAT](#)
- [6.3.9 配置 Windows 内置 IPsec VPN 客户端](#)
- [6.3.10 配置 Android 内置 IPsec VPN 客户端](#)
- [6.3.11 配置 iOS 内置 IPsec VPN 客户端](#)
- [6.3.12 配置 iMAC 内置 IPsec VPN 客户端](#)
- [6.3.13 验证结果](#)

6.3.1 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。

6.3.2 配置全局设置

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

认证配置

缺省认证服务器

辅助认证 [短信认证](#)
[OTP](#)
[硬件特征码认证](#)

缓存/压缩

Gzip压缩

HTML/JS/CSS 缓存

后缀
推荐使用：html,js,css ，用逗号分隔。

非HTML/JS/CSS 快速代理

非HTML/JS/CSS 缓存

后缀
建议配置二进制文件的扩展名，例如swf,jpg,png,gif,zip,pdf,doc等，用逗号分隔。

会话超时提醒

会话断开前 分钟提醒

3. 点击提交。

6.3.3 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。

添加

基础配置

名称* resources

备注

0/255

类型 子网

地址列表 192.168.2.0/24

示例：
192.168.2.0/32
192.168.1.1:443,80
192.168.3.1-192.168.3.50:20-21,8080

说明：
1) 使用回车分割每项配置
2) 每行只能配置单IP、网段、IP范围中的1个
3) 端口可选，并支持端口范围，配置多个时使用逗号分割

取消 确定

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。

添加

名称* ResourcesGroup

备注

0/255

资源

备选资源

resource1
resource2
resource3

选定资源

resources

取消 确定

6. 点击**确定**。

6.3.4 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。

添加

基本设置

用户名 * Bob

启用

电子邮件

手机号

用户详细信息

本地用户密码

密码 (1-128)

确认密码 (1-128)

密码选项

首次登录修改密码

密码永不过期

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。

添加

名称 * user_group

类型 静态

备注

0/255

模式 编辑模式 选择模式

包含已选用户

本地用户

已选用户

Bob

取消 确定

6. 点击**确定**。

6.3.5 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。

The screenshot shows the 'Basic Configuration' tab of the VPN Policy configuration page. The 'Name' field is set to 'tunnel1'. The 'Enable' checkbox is checked. The 'Type' section has three options: 'Web Mode SSL VPN' (unchecked), 'Tunnel Mode SSL VPN' (unchecked), and 'IPSec VPN' (checked). The 'Action' dropdown is set to 'Allow'. The 'Remarks' field is empty with a character count of 0/255. The 'Schedule' checkbox is unchecked.

4. 在用户组页签选择策略应用于的用户组。

The screenshot shows the 'User Group' tab of the VPN Policy configuration page. It features two search boxes: 'Candidate User Groups' (empty) and 'Selected User Groups' (containing 'user_group'). A blue arrow button is positioned between the two boxes to move items from the candidate list to the selected list.

5. 在资源组页签选择策略应用于的资源组。

The screenshot shows the 'Resource Group' tab of the VPN Policy configuration page. It features two search boxes: 'Candidate Resource Groups' (empty) and 'Selected Resource Groups' (containing 'ResourcesGroup'). A blue arrow button is positioned between the two boxes to move items from the candidate list to the selected list.

6. 点击确定。

6.3.6 添加 CA 证书和本地证书

1. 选择系统管理 > 证书。
2. 点击添加，选择根 CA 证书，添加根 CA 证书。

添加

证书名称 = cacert

有效期 = 3650 天

哈希算法 = SHA256

密钥对选项

类型 = RSA

密钥对长度 = 2048

证书主题信息

高级

国家代码(C) = CN (2字母)

省份(ST) = LN

城市(L) = SY

公司(O) = NEU

部门(OU) = NSD

公共名(CN) = neu.com

电子邮件

取消 确定

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。

添加

CA证书 = cacert

证书名称 = remotevpn

有效期 = 730 天

哈希算法 = SHA256

证书类别 = 服务器证书

密钥对选项

类型 = RSA

密钥对长度 = 2048

证书主题信息

高级

国家代码(C) = CN (2字母)

省份(ST) = LN

城市(L) = SY

公司(O) = NEU

部门(OU) = NSD

公共名(CN) = 172.16.2.200 CN 必须为提供 VPN 服务的 IP

电子邮件

CA证书 = cacert

证书名称 = Bob

有效期 = 730 天

哈希算法 = SHA256

证书类别 = 个人证书 IKEv1 必配, IKEv2 不配 (Android 使用 IKEv1, iOS 使用 IKEv2/v1)

密钥对选项

类型 = RSA

密钥对长度 = 2048

证书主题信息

高级

国家代码(C) = CN (2字母)

省份(ST) = LiaoNing

城市(L) = ShenYang

公司(O) = Neusoft

部门(OU) = NetEye

公共名(CN) = Bob

电子邮件 = bob@neusoft.com

5. 点击确定。

6.3.7 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）。

		添加	删除	重启服务	启用	禁用			
<input type="checkbox"/>	名称	类别	启用	对端	出口	认证模式	状态		
<input type="checkbox"/>	RemoteAccess	Remote Access	<input type="radio"/>	任意	任意	预共享密钥	客户端		

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，配置认证方式。

基础配置	本地配置	对端配置
名称 *	RemoteAccess	
类别	Remote Access	
启用	<input checked="" type="checkbox"/>	
日志	<input checked="" type="checkbox"/>	
备注	<input type="text"/>	
	0/255	
认证方式	证书	
本地证书 *	remotevpn	

- b. 点击**本地配置**页签，配置本端 IP 地址。

基础配置	本地配置	对端配置
本地地址	192.168.2.200	
类型		

- 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。

基础配置	本地配置	对端配置
客户端虚拟地址池	9.9.0.0/16	

- d. 点击**确定**。

6.3.8 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。

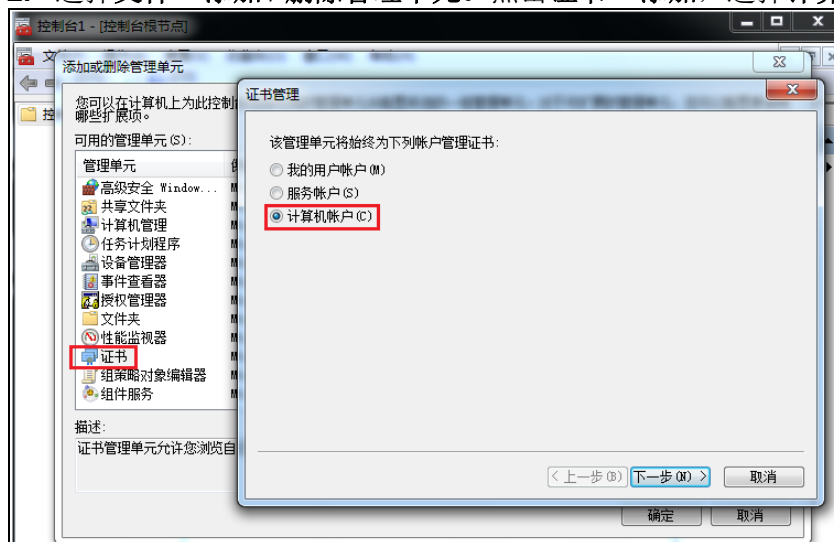
6.3.9 配置 Windows 内置 IPsec VPN 客户端

IPsec VPN 远程访问用户可以使用 Windows 7 系统内置的 VPN 客户端连接到 VPN 网关。请预先从 VPN 网关上下载 CA 证书并将证书导入到远程用户的 PC 上。

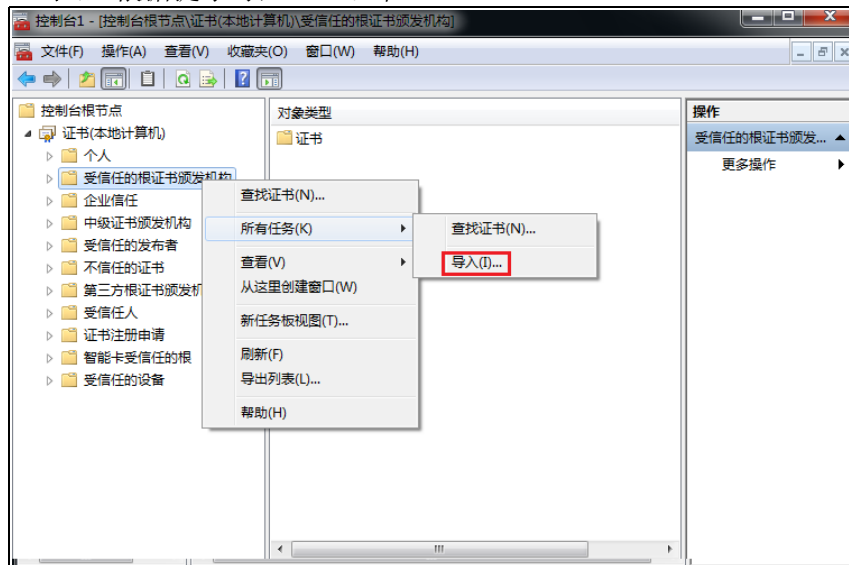
- 6.3.9.1 导入 CA 证书
- 6.3.9.2 创建 VPN 连接
- 6.3.9.3 修改 VPN 客户端配置

6.3.9.1 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。

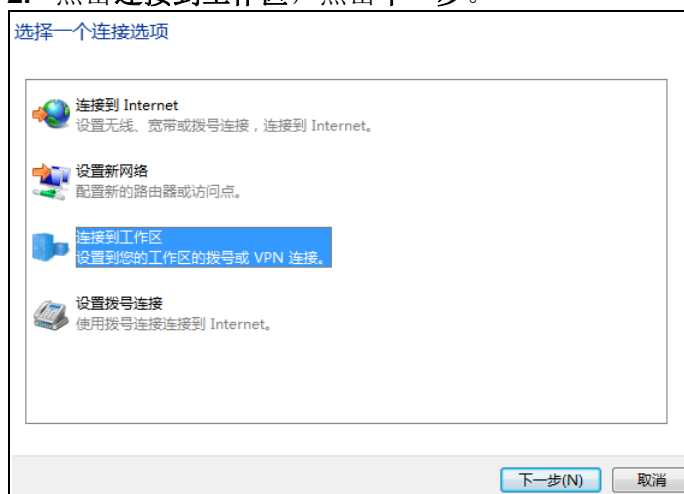


3. 点击本地计算机，点击完成，点击确定。
4. 在左侧控制台根节点，展开证书节点，选择受信任的根证书颁发机构 > 所有任务 > 导入，根据提示导入 CA 证书。

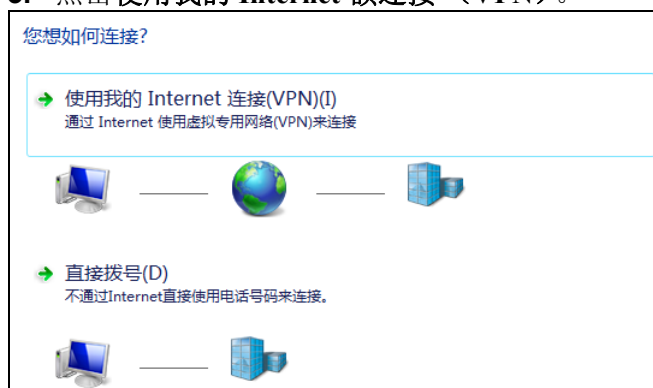


6.3.9.2 创建 VPN 连接

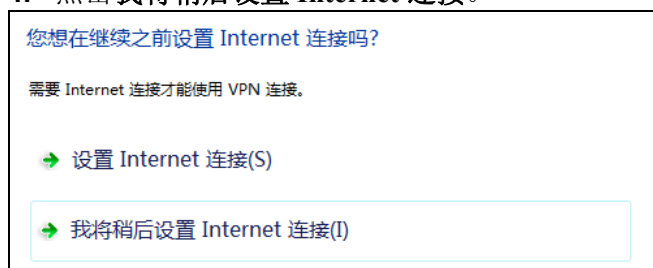
1. 打开网络和共享中心，点击**设置新的连接或网络**。
2. 点击**连接到工作区**，点击**下一步**。



3. 点击**使用我的 Internet 额连接 (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**。

键入要连接的 Internet 地址

网络管理员可提供此地址。

Internet 地址(I): 172.16.2.200

目标名称(E): Remote VPN 连接

使用智能卡(S)

允许其他人使用此连接(A)
这个选项允许可以访问这台计算机的人使用此连接。

现在不连接；仅进行设置以便稍后连接(D)

下一步(N) 取消

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

键入您的用户名和密码

用户名(U): Bob

密码(P): 123456

显示字符(S)

记住此密码(R)

域(可选)(D):

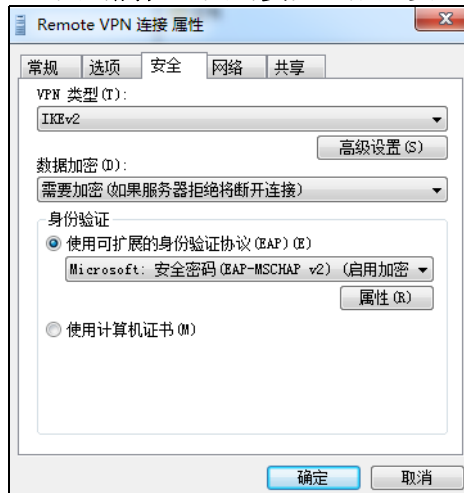
创建(C) 取消

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。



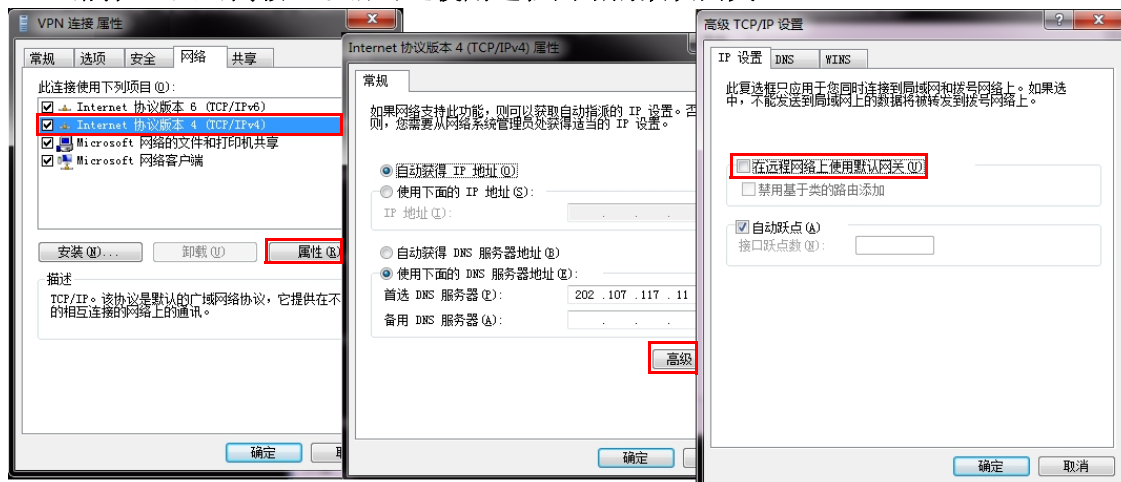
10. 点击**确定**。

11. 点击**连接**。待成功连接后，用户即可访问内网资源。

6.3.9.3 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)**，点击**属性**，点击**高级**，取消勾选**使用远程网络的默认网关**。



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

```

PPP adapter IPsecUPN:

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

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

6.3.10 配置 Android 内置 IPsec VPN 客户端

6.3.10.1 导入和安装证书

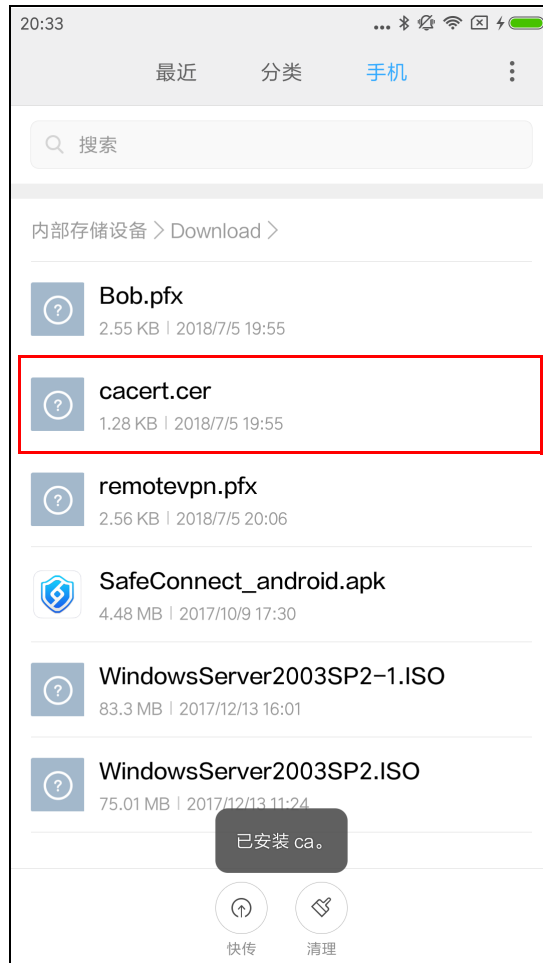
1. 管理员将 CA 证书和远程用户个人证书发送给远程用户。
2. 远程用户将证书导入 Android 手机并安装。
 - a. 连接手机和电脑，设置 USB 用途为**传输文件（MTP）**。



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。**

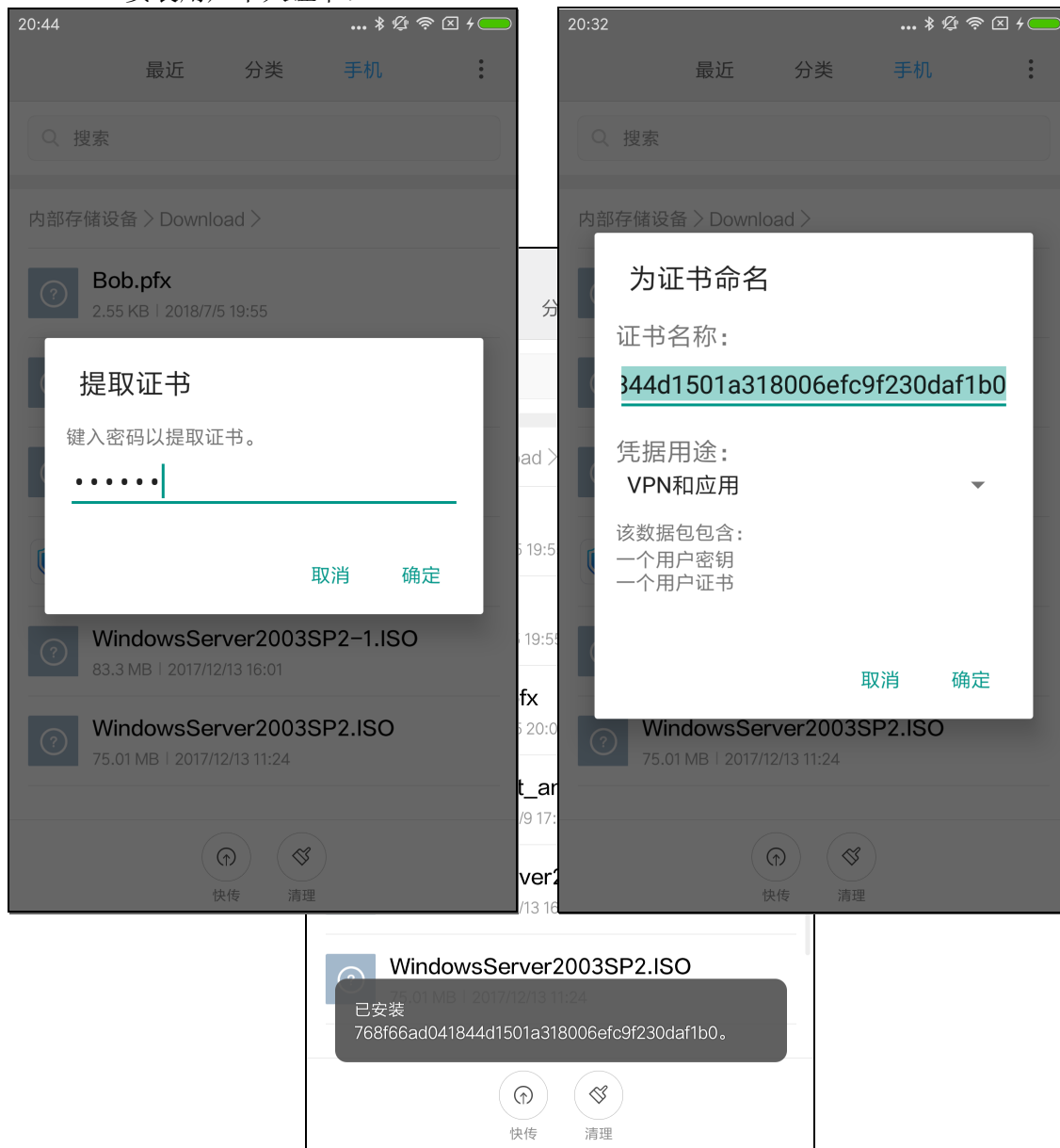
■ 安装 CA 证书:



■ 安装 IPSec 服务器证书:

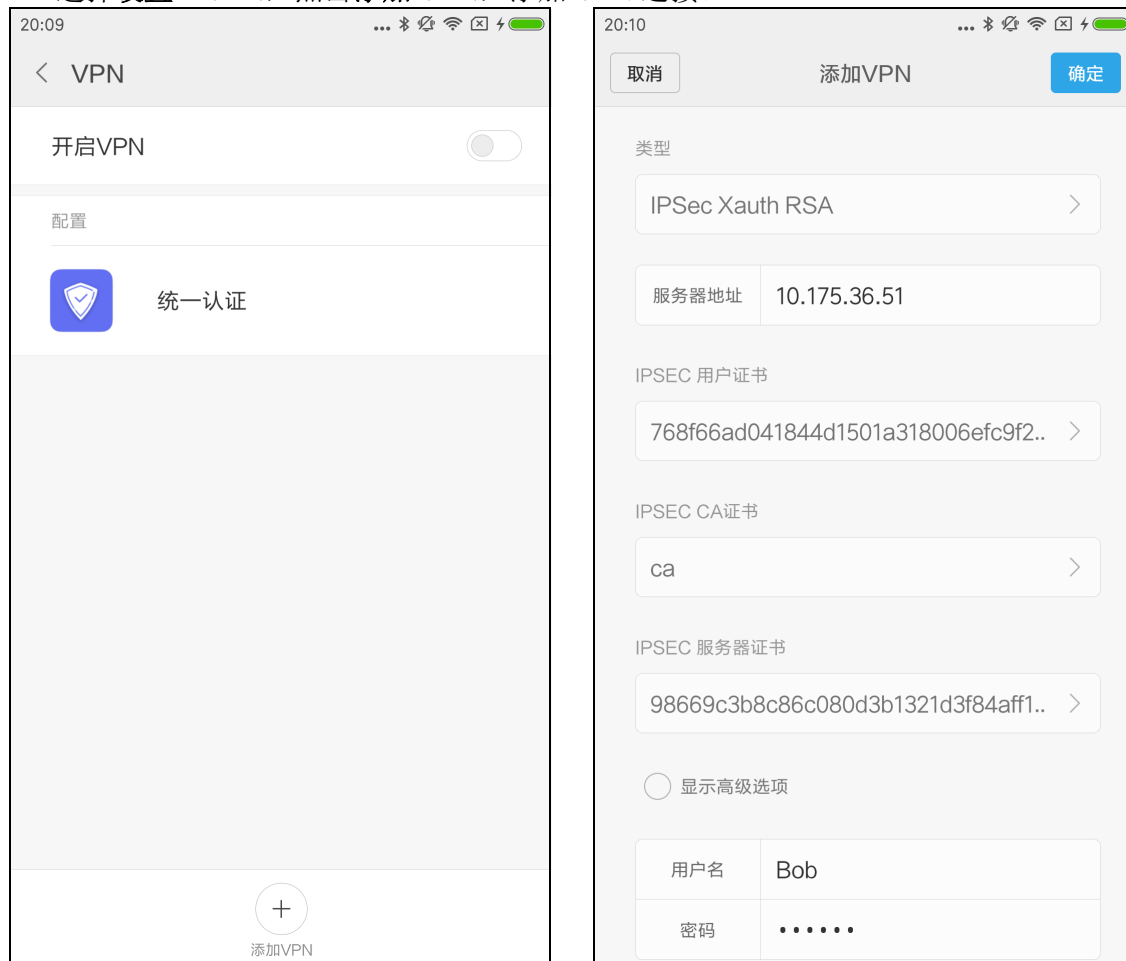


■ 安装用户个人证书:



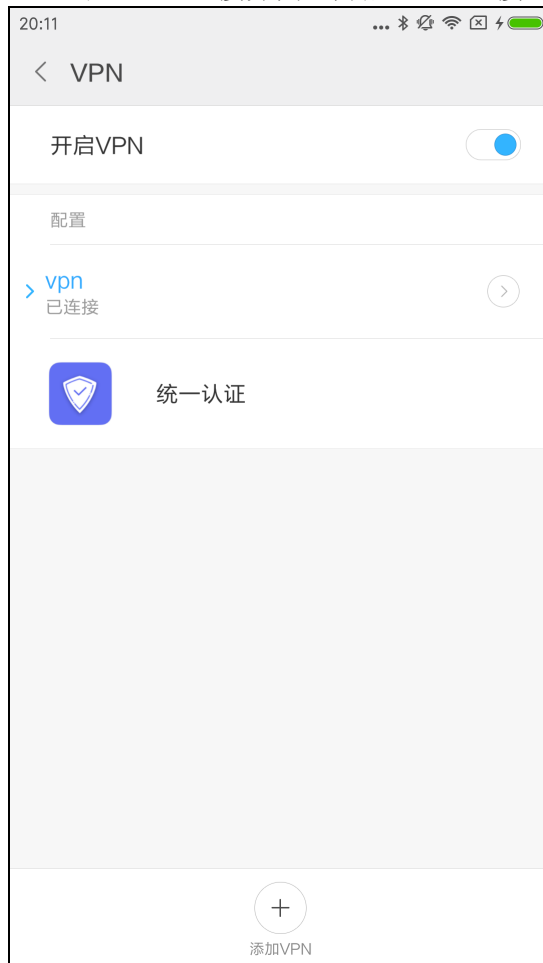
6.3.10.2 添加和建立 VPN 连接

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。

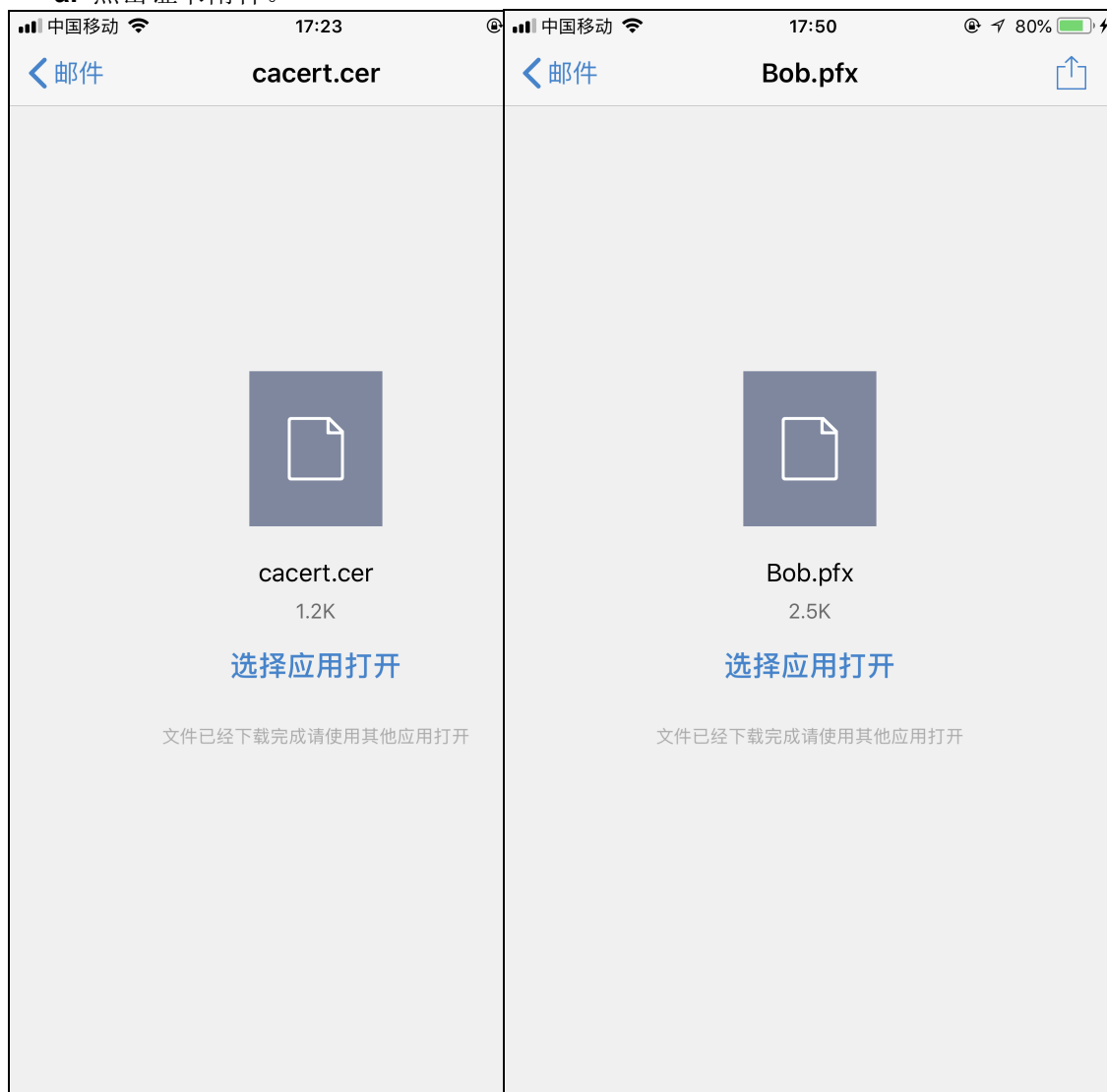
6.3.11 配置 iOS 内置 IPsec VPN 客户端

6.3.11.1 导入和安装证书

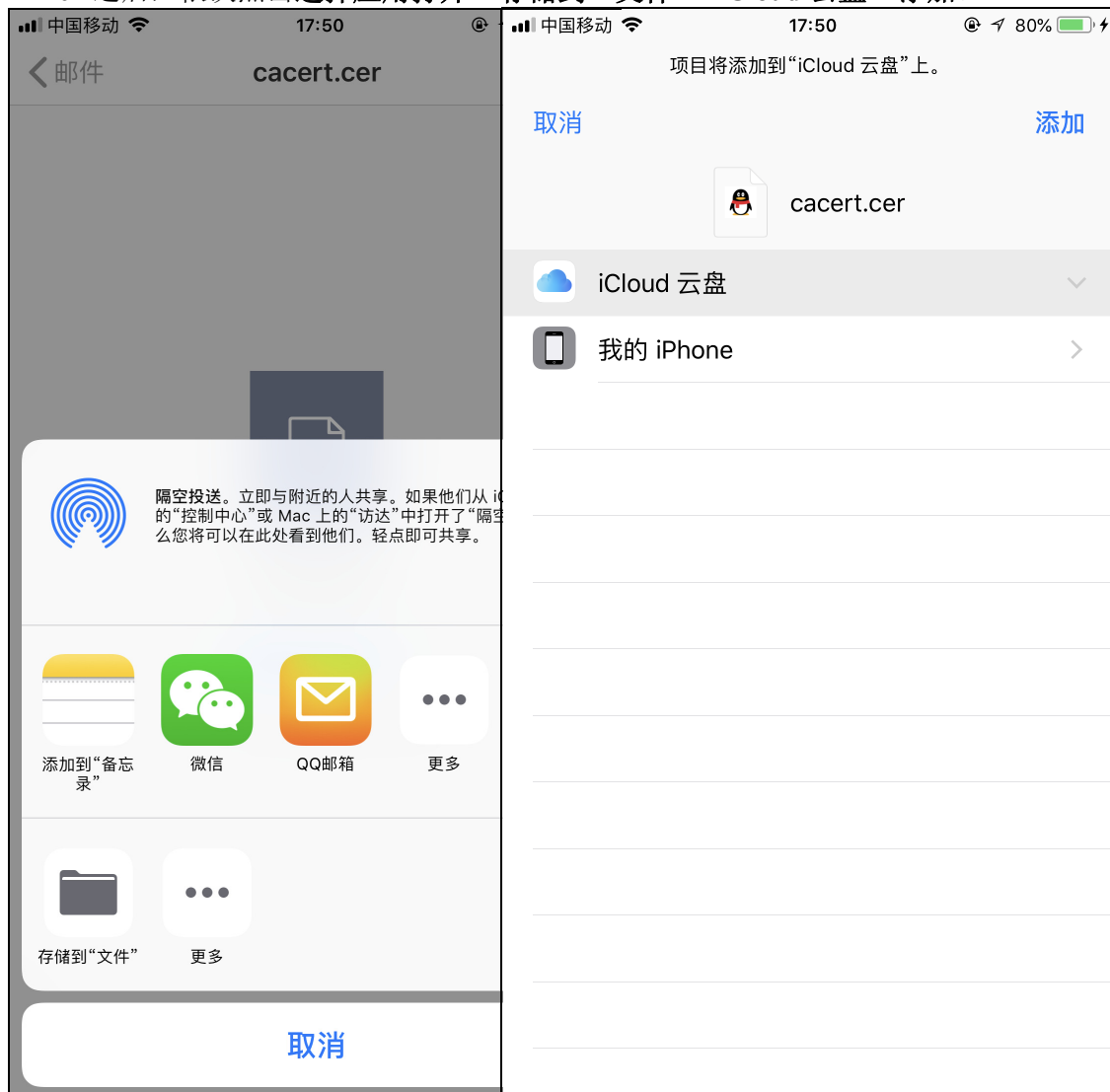
- 如果远程用户使用 IKEv2 类型接入，只需要导入和安装 CA 证书。
- 如果远程用户使用 IPsec（IKEv1）类型接入，则 CA 证书和个人证书都需要安装。

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。

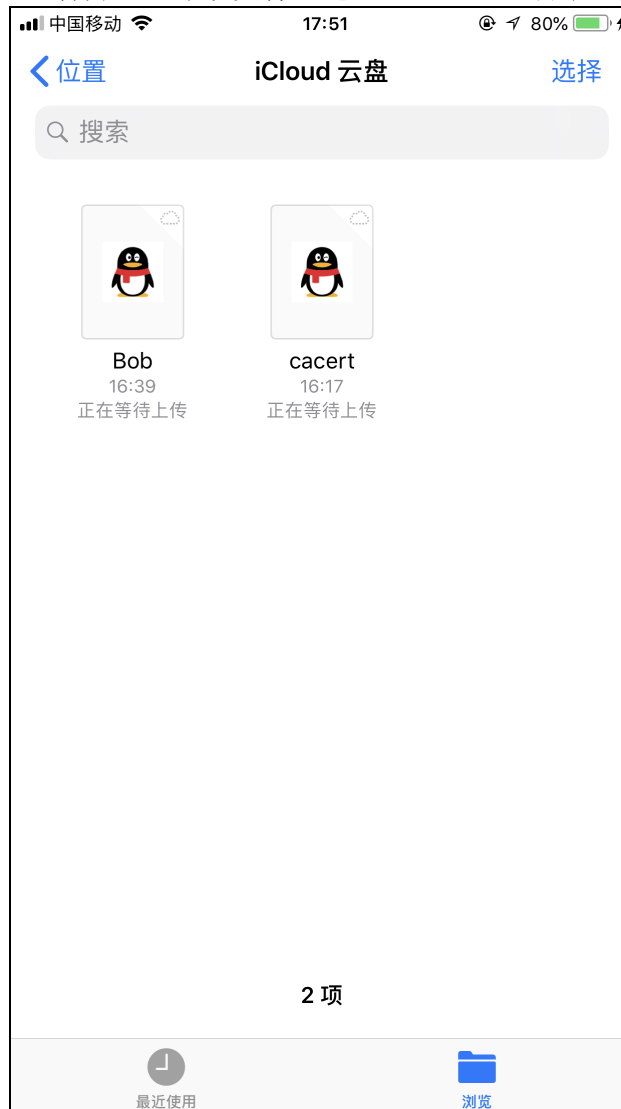
1. 从 VPN 网关上下载证书到本地，并通过邮件发送给远程用户。
2. 远程用户通过 iPhone 手机接收邮件，将证书存储到 iCloud 云盘。
 - a. 点击证书附件。



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:



■ 安装个人证书：



6.3.11.2 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，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）：



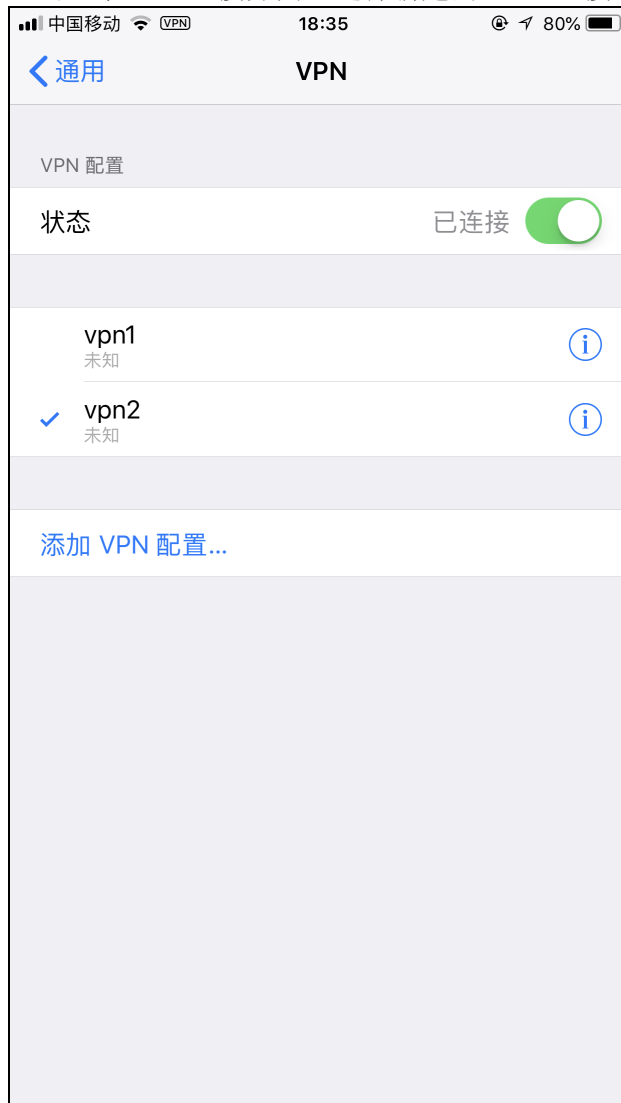
■ 如果使用 IPsec（即 IKEv1），请填写如下信息：

The screenshot shows a mobile application interface for adding a VPN configuration. At the top, there are three buttons: '取消' (Cancel), '添加配置' (Add Configuration), and '完成' (Done). Below the buttons is the Cisco logo. The configuration details are as follows:

类型	IPsec >
描述	vpn2
服务器	172.16.2.200
帐户	Bob
密码	••••••
使用证书	<input checked="" type="checkbox"/>
证书	Bob >
代理	<input checked="" type="radio"/> 关闭 <input type="radio"/> 手动 <input type="radio"/> 自动

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。

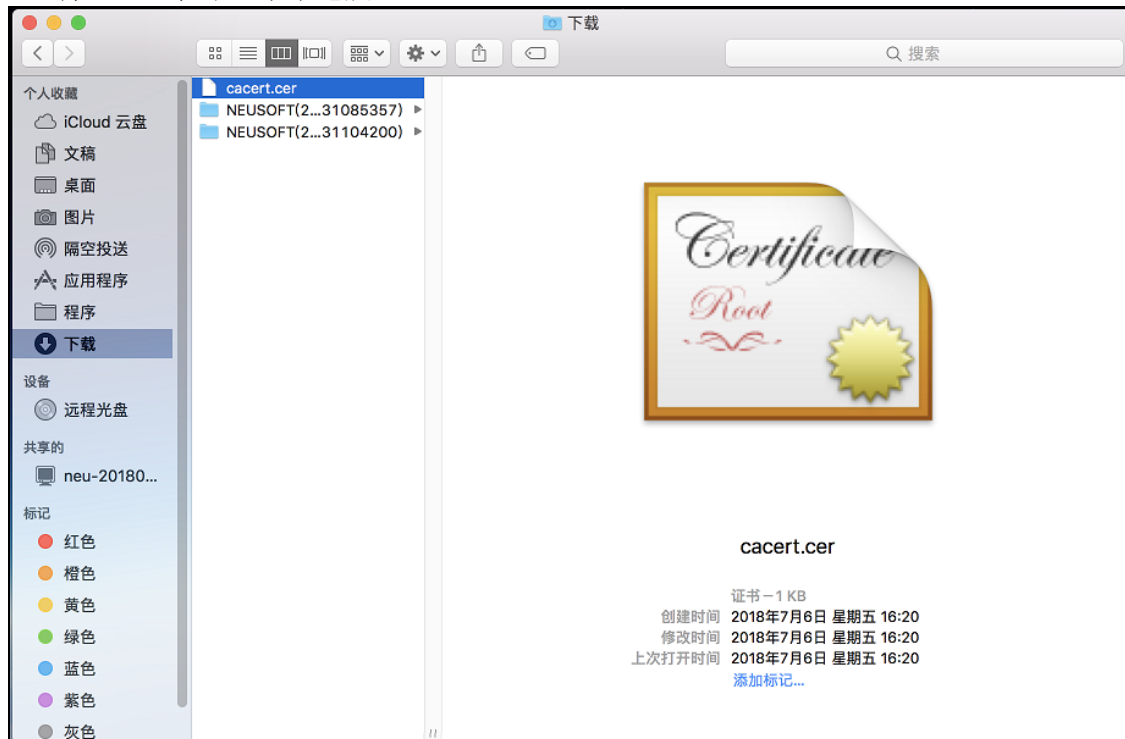


5. 待连接成功后，用户即可访问内网资源。

6.3.12 配置 macOS 内置 IPsec VPN 客户端

6.3.12.1 导入证书

1. 将 CA 证书导入苹果电脑。

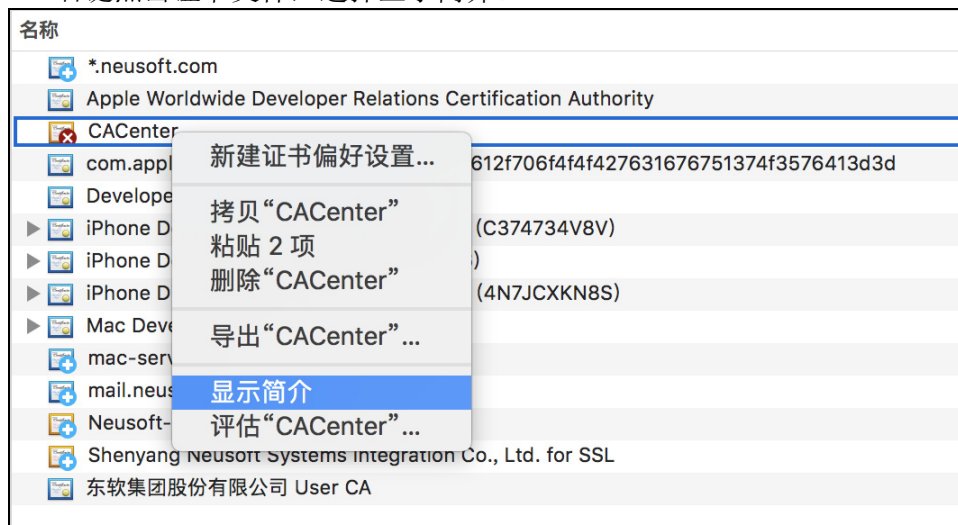


2. 双击证书文件，将证书添加进钥匙串。

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。



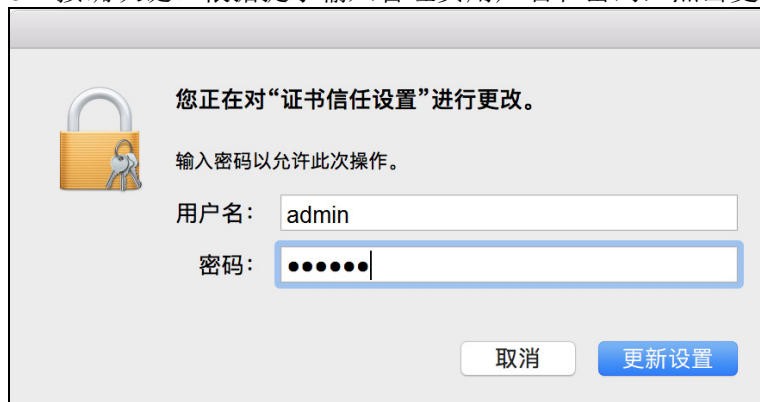
4. 右键点击证书文件，选择显示简介。



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。

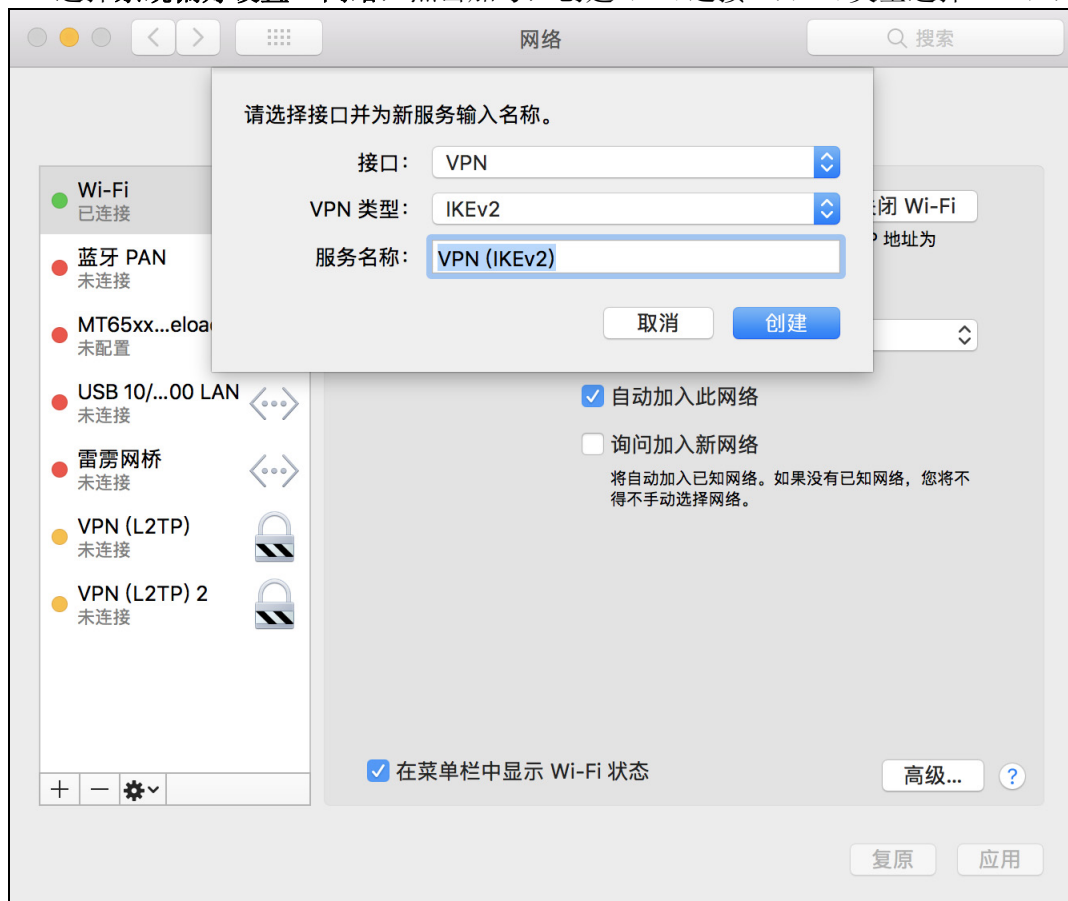


7. 查看证书状态，可发现证书变为受信任状态。



6.3.12.2 建立 VPN 连接

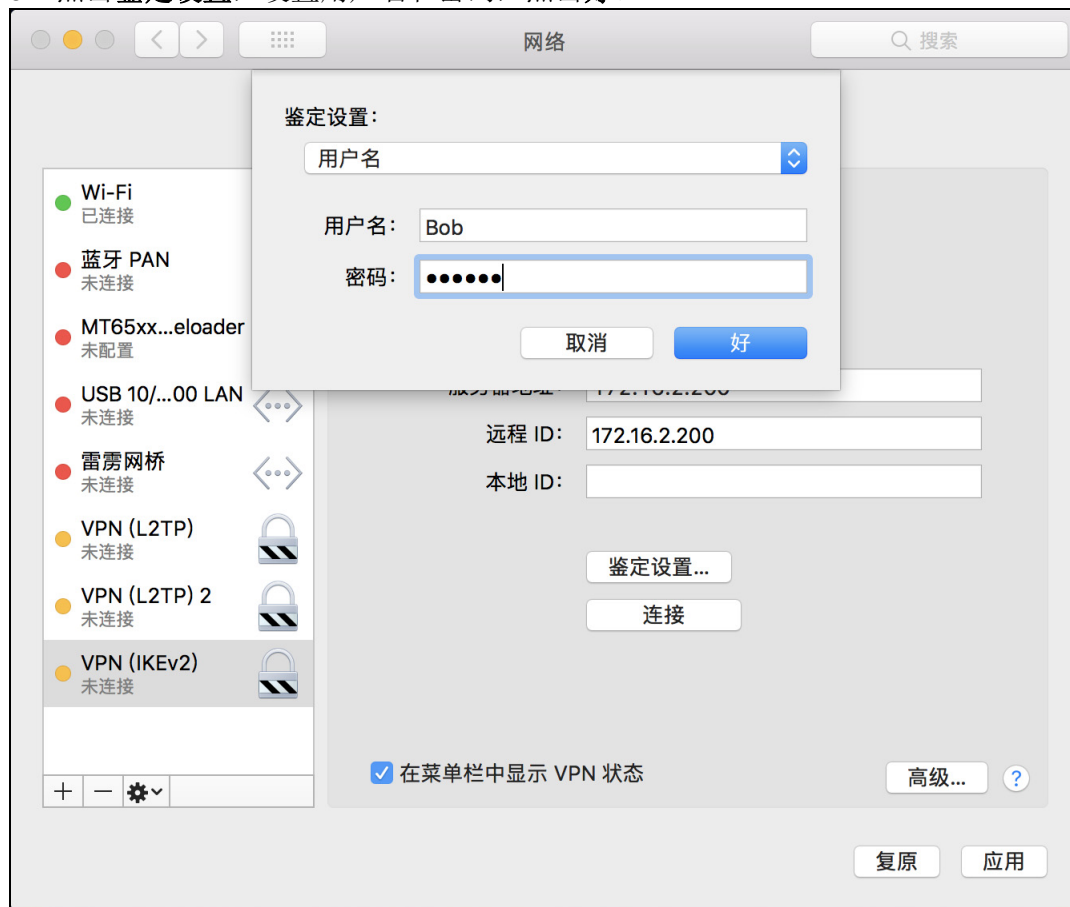
1. 选择系统偏好设置 > 网络，点击加号，创建 VPN 连接（VPN 类型选择 IKEv2）。



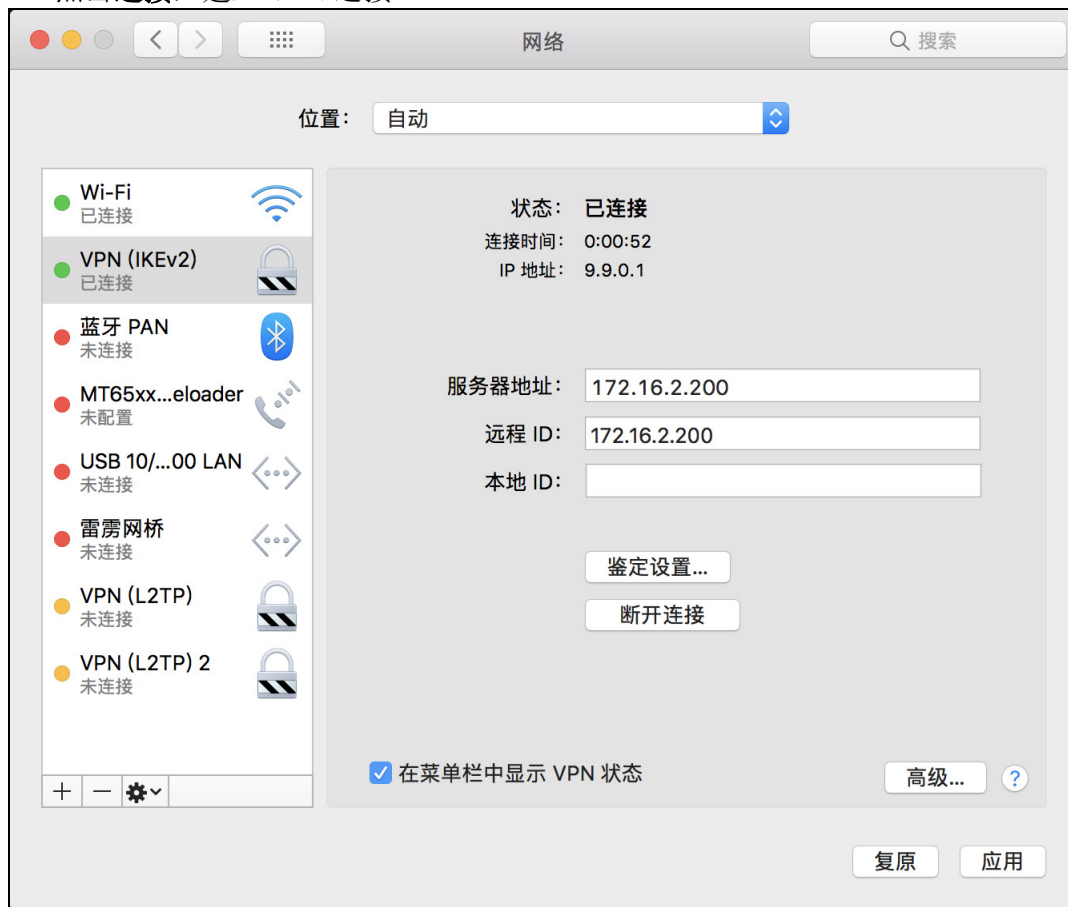
2. 设置 IPSec VPN 服务器地址和远程 ID。



3. 点击**鉴定设置**，设置用户名和密码，点击**好**。



4. 点击**连接**，建立 VPN 连接。



6.3.13 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。

离线								流量	开	关
用户	姓名	公司	部门	IKE版本	源地址	在线时间	发送	接收		
test					9.9.0.1					

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。

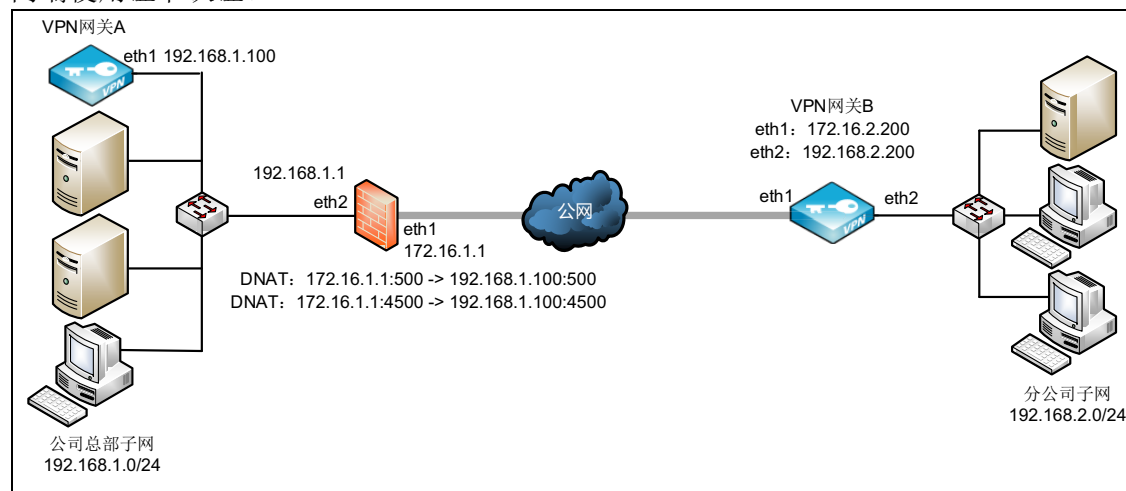
3. 可选择**网络/策略 > 访问策略**，点击**配置 IPSec VPN 访问策略**，查看是否自动生成远程访问 IPSec VPN 访问策略。
4. 如果监控不到在线用户，也查看不到自动生成的访问策略，则选择**日志 > 调试 > IPSec VPN 协商日志**，查看远程访问 IPSec VPN 协商过程，分析连接失败原因。

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）。

6.4 网关到网关 IPSec VPN

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。



配置步骤如下：

- [6.4.1 配置总部防火墙 DNAT](#)
- [6.4.2 配置总部 VPN 网关 A](#)
- [6.4.3 配置分部 VPN 网关 B](#)
- [6.4.4 验证结果](#)

6.4.1 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

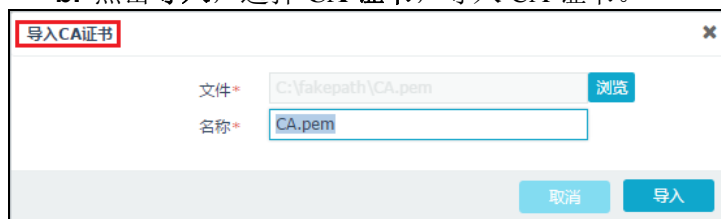
由于各个厂家设置方法有所不同，以上配置此处不截图说明。

6.4.2 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：

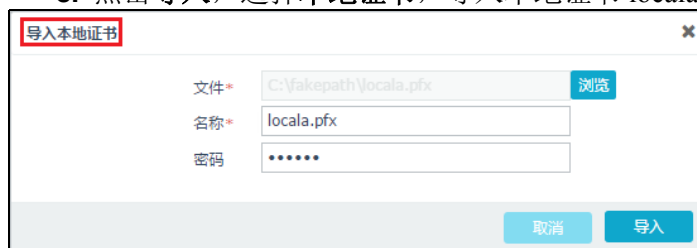
a. 选择系统管理 > 证书。

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 6.3.6 添加 CA 证书和本地证书。

2. 单臂模式部署设备。

- 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。

The screenshot shows the 'Basic Configuration' tab for an IPsec VPN tunnel. The configuration is as follows:

Field	Value
名称 *	IPSec1
类别	Site-to-Site
启用	<input checked="" type="checkbox"/>
日志	<input checked="" type="checkbox"/>
主动协商	<input type="checkbox"/> IPSEC VPN两端只能有一处启用
备注	<input type="text"/> 0/255
IKE版本	ikev2
认证模式	证书
本地证书 *	locala
加速卡	<input type="checkbox"/> 未发现加速卡

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。

The screenshot shows the 'Local Configuration' tab for the IPsec VPN tunnel. The configuration is as follows:

Field	Value
本地地址	192.168.1.100
类型	证书主题
ID	C=CN,ST=LiaoNing,O=Neusoft,OU=neteye,CN=a,emailAdd
本地子网	192.168.1.0/24

每个子网使用回车分隔，示例如下：
 192.168.1.0/24
 192.168.2.1/32

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。

基础配置	本地配置	对端配置	IKE	ESP
IP地址/域名	172.16.2.200			
类型	证书主题 ▼			
ID	C=CN,ST=LiaoNing,O=Neusoft,OU=neteye,CN=b,emailAdd			
对端子网	192.168.2.0/24			
	每个子网使用回车分割，示例如下： 192.168.1.0/24 192.168.2.1/32			

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。

6.4.3 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。

导入CA证书 ✕

文件* 浏览

名称*

取消 导入

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。

导入本地证书 ✕

文件* 浏览

名称*

密码

取消 导入

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 [6.3.6 添加 CA 证书和本地证书](#)。

2. 网关模式部署设备。

- 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**。

The screenshot shows the configuration page for an IPsec VPN tunnel. The 'Basic Configuration' tab is active. The 'Active Negotiation' checkbox is checked and highlighted with a red box. Other settings include Name: IPsec2, Category: Site-to-Site, Enabled: checked, Log: checked, IKE Version: ikev2, Authentication Mode: Certificate, Local Certificate: localb, and Acceleration Card: Not found.

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。

The screenshot shows the 'Local Configuration' tab. The 'Local Address' is set to 172.16.2.200, 'Type' is Certificate Subject, 'ID' is C=CN,ST=LiaoNing,O=Neusoft,OU=neteye,CN=b,emailAdd, and 'Local Subnet' is 192.168.2.0/24. Below the subnet field, there is a note: '每个子网使用回车分割, 示例如下: 192.168.1.0/24 192.168.2.1/32'.

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。

6.4.4 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:

添加	删除	重启服务	启用	禁用					
<input type="checkbox"/>	名称	类别	启用	对端	出口	认证模式	状态		
<input type="checkbox"/>	RemoteAccess	Remote Access	<input type="radio"/>	任意	任意	预共享密钥	客户端		
<input checked="" type="checkbox"/>	IPSec1	Site-to-Site	<input checked="" type="radio"/>	172.16.2.200	192.168.1.100	证书	已连接		

■ 分部 VPN 网关 B:

添加	删除	重启服务	启用	禁用					
<input type="checkbox"/>	名称	类别	启用	对端	出口	认证模式	状态		
<input type="checkbox"/>	RemoteAccess	Remote Access	<input type="radio"/>	任意	任意	预共享密钥	客户端		
<input checked="" type="checkbox"/>	IPSec2	Site-to-Site	<input checked="" type="radio"/>	172.16.1.1	172.16.2.200	证书	已连接		

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。

沈阳浑南新区新秀街 2 号
客服热线：400 655 6789
<http://neteye.neusoft.com>