NetEye

IT SOLUTIONS & SERVICES



东软 NetEye VPN 网关快速向导



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。

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。



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。



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。



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

www.streetexeeventexe	¥ﷺ 产品 Logo 和产品名称	快捷菜单 ≡ ▲ root ▼
希 主页	系統信息 ン	资源使用情况
□ ###3788 < ● 血腔 < □ 日志 < ■ 日志 < ○ 素乐能量 < 导航菜单	展現面目 C 型号 VPN 軟件板本 5.500-000-000-000-000-000-000-000-000-00	愛望使用描述 CPU 1% - 内存 18% 道金 25% 建合 25% 建築 4時間 使用 使用
	Jan 3 12:54:45 in obt.100.(10.9.224.106) execute system/namm.og/m Jan 3 12:54:45 in obt.root(10.9.224.106) execute synthylation.createInviteItems Jan 3 12:54:45 in obt.root(10.9.224.106) execute synthylation.setConf successi Jan 3 12:54:21 in obt.root(10.9.224.106) execute synthylation.setConf successi Jan 3 12:22:47 in obt.root(10.9.224.106) execute synthylation.setConf successi Jan 3 11:02:23 in obt.root(10.9.224.106) execute synthylation.setConf successi Jan 3 10:25:18 in obt.root(10.9.224.106) execute synthylation.setConf successi Jan 3 10:25:19 in obt.root(10.9.224.106) execute synthylation.setConf successi Jan 3 10:25:19 in obt.root(10.9.224.106) execute fw/Device.updateIfrdg successi Jan 3 10:03:19 in obt.root(10.9.224.106) execute fw/Rule.setRule successi Jan 3 10:02:14 in obt.root(10.9.224.106) execute fw/Device.setLayer3Ifrdg DEVICE=*br07) successi in obt.root(10.9.224.106) execute fw/Device.setLayer3Ifrdg	SBH#发用户 @ WebgstSSL VPN
		Neusoft

- 点击 □ 隐藏或展开界面左侧导航菜单。
- ■ 「Toot ▼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 自动同步	2018-0 启用	8-28 12:37:56	Ø		
	立即同步		***		化田子日	
2. 选择系统管	*埋>廾级,	检查当	<u></u> 前糸统是省	为最新版本。	如果个是,	上载廾级包。
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 上载升级包	载升级包,完成系统 低版本 Ⅴ 的"技术	升级 PN 网关可 支持 > 下	可能没有此功能 载中心"获取5	^{能,} 可到东软 Ne 升级包。	tEye 官网 http	://neteye.neusoft.com
2 左十五的名	法信息区域	ь L	。	≤ 盂 山 🌭 武 辺	以至法答理	I、I:

3. 在主页的系统信息区域点击 License 信息后面的 So 或选择系统管理 > License, 点击导入, 输入 License 字符串。

导入License	я
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	密码,修改 root 用户的 W	/ebUI 缺省密码。
= 🔺 root 👻	修改密码		×
。 测试用户	当前密码*	•••••	(1-128)
●修改密码	新密码*	•••••	(1-128)
健出	确认新密码*	•••••	(1-128)
·			音

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



配置步骤如下:

1. 选择网	Ⅰ. 选择 网络 / 策略 > 接口 > 配置 ,设置接口 IP 地址。						
重启网络服务	重启网络服务						
接口	Active	属于	IP地址				
eth0	•		192.168.1.100	1	4		
eth1	•		192.168.2.200	×			

 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:	0.0.0.0/0	
Metric∗ 地口接口/网关	路由目标地址使用IP地址/掩码。例如:192.168.1.0/24 0 (0-255)	
····································	eth1 v	
网关	192.168.2.1	
	取消 确定	

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



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	1
eth1	•		172.16.2.200	1
eth2	•		192.168.2.200	1

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		x
目标地址*	0.0.0.0/0 路由目标地址使用IP地址/掩码。例如:192.168.1.0/24	
Metric* 出口接口/网关	0 (0-255)	
接口*	eth1 ·	
网关	172.16.2.1	
	取消 确定	

- 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		
0	51		eth0	100	 â	
						-
添加					总数	ζ1

3. 点击 / 对其进行修改。

启用		
虚拟路由器ID*	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*	192.168.1.1	
接口*	eth1 *	
优先级*	100	数值大的优先生效
密钥*	•••••	۲

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	Ø
对端IP地址∗	1.1.1.2
用户名★	ha
密码	•••••
自动同步	

VPN	网	关2
-----	---	----

启用	
对端IP地址∗	1.1.1.1
用户名★	ha
密码	•••••
自动同步	•

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		
	51		eth0	100	 Ê	*
						-
添加					总数	女 1

3. 点击 / 对其进行修改。

启用	v		
虚拟路由器ID*	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*	202.118.1.1		
接口*	eth1	Ŧ	
优先级*	100		数值大的优先生效
密钥*	•••••		۲

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			
虚拟路由器ID*	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*	192.168.1.1		
接口*	eth2	Ŧ	
优先级*	100		数值大的优先生效
密钥*	•••••		۲

- **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
```

VPN	网关 2
-----	------

启用	ø
对端IP地址∗	1.1.1.2
用户名★	ha
密码	•••••
自动同步	

启用	
寸端IP地址★	1.1.1.1
用户名★	ha
密码	•••••
自动同步	

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	Local 👻
辅助认证	短信认证 <u>OTP</u> 硬件特征码认证
缓存/压缩	
Gzip压缩	
HTML/JS/CSS 缓存	
后缀	html,js,css
	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	swf,jpg,png,gif,zip,pdf,doc
	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	5 分钟提醒
取消 提交	

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	1	基础配置缓存	科压缩
名称∗	webserver	全局设计	≝
显示名称	webserver 不填写此项在Web	页面不显示	
备注			
	0/255		
类型	HTTP T		
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			
	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。

名称*	resource_group			
备注				
		0/3	255	
资源	Q, 备选资源		Q、 选定资源	
	resource1		webserver	
	resource3		арр	
	resource2	>	developer	
	resource6	4		
	resource7	«		
	resource8			
	resource5			
	resource4			

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。

添加				×
其太设署				
1101	用户名★	test		
	启用			
	电子邮件	test@example.com		
	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				

- **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。

添加					×
名称*	user_group				
类型	静态		•		
备注					
		0/2	255		
模式	○ 编辑模式 ⑧ 选择模式				
	包含已选用户		•		
	Q、 本地用户		Q	已选用户	
	example]	test		
			user1		
		>	user2		
		4	user3		
		«			
				取消	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。

基础配置	用户组	LDAP安全组 资源组
	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	
		0/255
	时间表	

b. 在**用户组**页签选择策略应用于的用户组。

目 く 备选用户组 く 已选用户组	日 く 各洗用户組 く 已洗用户組
user_group	user_group

c. 在资源组页签选择策略应用于的资源组。

际加			
基础配置用	户组 LDAP安全组	资源组	
资源组	Q. 备选资源组	1	Q 已选资源组 resource_group
		×	

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:

导入本地证书					×
	文件*	C:\fakepath\WebSSLVPN.pfx		浏览	
	名称*	WebSSLVPN			
	密码	•••••			
			取消		导入

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。

启用	۲.		
访问日志			
IP地址*	192.168.2.200	*	
* □ #	443		
本机域名			
HTTP重定向到HTTPS			
本地证书*	WebSSLVPN	*	
页面模板	Default	*	配置模板
登录验证码			
邀请码	配置邀请码		
系统通知	配置系统通知		

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:

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。

← → G ▼	不安全 bttps://172.16.2	.200/login.html			
000	5	SL VPN	-		码 ≺ 退出
-	-			资源列表	
-	test		🖉 webserver		Ø
			apps.neusoft.co	m	Ø
	•••••		developer.neus	oft.com	Ø
	KS8b				
		登录			
ST BIT IST	忘记密码	注册用户			
13	z SSI	VPN客户端下载		 	

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。

ī	寄线								流量开关
	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
	user1	张三	NEU	NSD	172.16.1.10	2018-06-27 21:47:25	55	Mozilla/5.0 (Windows N	8724A04873F115D7F140BE7494DCF0A0

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	Local
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	html,js,css
	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	swf,jpg,png,gif,zip,pdf,doc
	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	5 分钟提醒
取消 提交	

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。

ba			>
基础配置			
	名称*	resources	
	备注		
		0/255	
	类型	구ळ] •	
Ħ	地列表	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。

名称*	ResourcesGroup		
备注			
		0/255	
资源	Q. 备选资源	Q. 选定资源	
	resource1	resources	
	resource2		
	resource3		

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*	user1]	
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		
	有效期到		
		取消	确定

- **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	T	
备注			
		0/255	
模式	◎ 编辑模式 💿 选择模式		
	包含已选用户	T	
	Q、 本地用户	Q 已选用户	
		user1	
		user2	
		» user3	
		<i>4</i>	
		«	
		取消	腚

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。

基础配置	用户组	LDAP安全组 资源组
	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	
		0/255
	时间表	

b. 在用户组页签选择策略应用于的用户组。

动口						
基础配置	用户组	LDAP安全组	资源组			
用户组	٩	备选用户组		٩	已选用户组	
				user	_group	
			>			

c. 在资源组页签选择策略应用于的资源组。

基础配置	用户组	LDAP安全组	资源组		
资源组	٩	备选资源组		٩	已选资源组
				Resour	cesGroup
			>>		

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*	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(0)	NEU		
部门(OU)	NSD		
公共名(CN)*	neu.com		
电子邮件			
		取消	确定

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				
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

4. 点击**添加**,选择**本地证书**,添加服务器证书。

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。

百田					
调试	一 开 关		添加		×
访问日志	开 关		IP地址*	任意 •	
	cacert		端□*	10442	
CANT D .			协议*	UDP •	
本地证书*	TunnelSSLVPN	1	子网*	7.7.7.0/24	此网段包含256个IP地址
DNS	202.118.2.10		512(\ \\	例如:7.7.0.0/16	
	高级 🗸		隧 旦 接入 家白端百许		
双向认证	□ 建议不启用 , 只有EKey版署	\$户端支持》	 III 10000000000000000000000000000000000		
推送网关	🔲 启用后 , 客户端使用推送网	关,所有济	专享用户		输入多个用户,用逗号分割。
数据压缩	 Image: A start of the start of				
摘要算法*	SHA1			/	
加密算法*	BF-CBC				取消 确定
服务列表	服务	协议	子网	隧道接入	
	Any:10442	udp	7.7.7.0/24		🖍 前 🔺
	192.168.2.200 :443	tcp	1.0.0/16		✓ 前
			添加		×
			IP地址*	192.168.2.200 -	
			端口*	443	
	添加		协议*	ТСР 🔻	
			子网*	1.0.0.0/16	此网段包含65536个IP地址
			[26] 第十五 》	例如:7.7.0.0/16	
			客户端互连		
			隧道专享		
			专享用户		输入多个用户,用逗号分割。
				~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
					取消 确定

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。

#### 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	
☑ 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。
 a.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。



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。

Neusoft东 Beyond Technology	软			<b>₹</b> - X	
连接	资源	日志			
		资源列表			
apps.neusoft.com	m				
developer.neuso	oft.com				
ehr.neusoft.com					
东软PPMP专利管	理平台				
2017年度东软集团	团职能部门满意度	调查			
品牌与市场体系资	资源平台				
web.neusoft.com	n				
ChangePasswor	d				
mail.neusoft.com	n				
2. 管理员登录	表VPN 网关,	选择 <b>监控&gt;在线</b>	用户>隧道模式	<b>在线用户</b> ,俞	能够查看到 VPN
户的在线信	言息。				

离线								
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)
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	Local 💌
辅助认证	<u>短信认证</u> <u>OTP</u> 硬件特征码认证
缓存/压缩	
Gzip压缩	✓
HTML/JS/CSS 缓存	
后缀	html,js,css
	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	swf,jpg,png,gif,zip,pdf,doc
会话超时提醒	
会话断开前	5 分钟提醒
取消 提交	

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。

出配置					
名称*	resources				
备注					
	0/255				
类型	子网	•			
地址列表	192.168.2.0/24				
	示例: 192.168.2.0/32 192.168.1.1:443,80 192.168.3.1-192.168.3.50:20-2 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	1,8080 中的1个	~		
	3)端凵刂远,开支持端凵沱围,配置	多个时便用;	逗号分割		
点击 <b>确定</b> 。 选择 <b>基础功</b> 食	<b>≿&gt;资源组</b> 。		取消	确定	
点击 <b>确定。</b> 选择 <b>基础功能</b> 点击 <b>添加,</b> 涵	<b>2 &gt; 资源组</b> 。 ^家 加资源组,对资源组合	命名并加	^{取消} 先择要加	^{确定} 入资源	组的 ×
点击 <b>确定。</b> 选择 <b>基础功</b> 角 点击 <b>添加</b> ,溺	ٷ <b>&gt;资源组</b> 。 ≋加资源组,对资源组6 ResourcesGroup	命名并过	^{取消} 先择要加	入资源	组的 ×
点击 <b>确定</b> 。 选择 <b>基础功</b> 角 点击 <b>添加</b> , 涵 ^{名称*} ^{备注}	<b>٤ &gt; 资源组</b> 。 ≤加资源组,对资源组a ResourcesGroup	命名并知	选择要加	入资源	组的 ×
点击 <b>确定。</b> 选择 <b>基础功</b> 角 点击 <b>添加,</b> 刻 ^{名称*} ^{音注}	€ > 资源组。 ≲加资源组,对资源组6 ResourcesGroup	冷名并让 □	取消 先择要加	入资源	组的 ×
点击 <b>确定</b> 。 选择 <b>基础功</b> 創 点击 <b>添加</b> , 剂 ^{名称*} ^{备注} 资源	E > 资源组。 ≤加资源组,对资源组。 ResourcesGroup Q 备选资源	⑦名并↓	取消 先择要加 选定资源	入资源	<u>组的</u> ×
点击 <b>确定。</b> 选择 <b>基础功f</b> 点击 <b>添加,</b> 刻 ^{名称。} ^{名称。} ^{音注} 资源	E > 资源组。 ≤加资源组,对资源组备       ResourcesGroup       Q       G       G       Fesource1       resource2	命名并述 )/255 Q resource	取消 先择要加 选定资源 Ces	入资源	<u>组的</u> ×
点击 <b>确定。</b> 选择 <b>基础功</b> 角 点击 <b>添加</b> , 初 ^{名称*} ^{备注} 资源	E > 资源组。 ≤加资源组,对资源组合 ResourcesGroup	命名并赴 )/255 Q resource	取消 先择要加 选定资源 ces	入资源	组的 ×

# 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					
			0/2	255		
	模式	○ 编辑模式 ● 选择模式				
		包含已选用户		•		
		Q、 本地用户		Q	已选用户	
			1	Bob		
			>			
			÷			
			«			
					取消	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。

基础配置	用户组	LDAP安全组 资源组
	名称*	tunnel1
	启用	
	类型	□ Web模式SSL VPN □ 隧道模式SSL VPN
	动作	允许   ▼
	备注	
		0/255
	时间表	

#### 4. 在用户组页签选择策略应用于的用户组。

基础配置	用户组	LDAP安全组 资	源组		
用户组	Q	备选用户组		٩	已选用户组
				user_	group

#### 5. 在资源组页签选择策略应用于的资源组。

н					
基础配置	用户组	LDAP安全组	资源组		
资源组	Q	备选资源组		٩	已选资源组
				Reso	urcesGroup
			>		

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 <b>*</b>	
	密钥对长度	2048 •	
证书主题信息			
	高级	•	
E	国家代码(C)	CN	(2字母)
	省份(ST)	LN	
	城市(L)	SY	
	公司(0)	NEU	
	部门(OU)	NSD	
3	公共名(CN)*	neu.com	
	电子邮件		
			取消 确定
1. 1			

- **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 .	
CA证书	cacert •		证书名称*	Bob	
证书名称	<ul> <li>remotevpn</li> </ul>		有效期*	730	] 天
有效期	* 730	] 天	哈希算法	SHA256	
哈希算法	SHA256		证书类别	个人证书	
证书类别	服务器证书  ▼	]	密钥对选项 IKEv1	必配,IKEv2 不酉	5
密钥对选项			(Android 使用IK	Evi, 105 使用 [	(Ev2/v1)
类型	RSA 🔻	]	密钥对长度	2048 •	
密钥对长度	2048 •		证书主题信息		1
证书主题信息			高级		
高级	<b>2</b>	7	国家代码(C)	CN	(2字母)
国家代码(C)	CN	(2字母)	省份(ST)	LiaoNing	
省份(ST)	LN			ChenVang	]
城市(L)	SY	]	- 泉(口)	Shenrang	]
公司(0)	NEU		公司(0)	Neusoft	]
部门(OU)	NSD		部门(OU)	NetEye	
公共名(CN)	* 172.16.2.200 CN	必须为	公共名(CN)*	Bob	
电子邮件	提供 VPN 月	最务的 IP	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			
	2	称	类别	启用	对端	出口	认证模式	状态	
	Remote	Access	Remote Access		任意	任意	预共享密钥	客户端 🔚	

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。

<b>a.</b> 11	- 坐加肌	且火	金, 但用	败退,	ΠЩ	
基础配置	本地配置	对端面	置			
		名称*	RemoteAcce	ess		
		类别	Remote Acc	ess		
		启用	•			
		日志	<b></b>			
		备注				
					0/255	
	认证	方式	证书		•	
	本地	证书*	remotevpn		*	
<b>b.</b> 点	〔击 <b>本地</b>	配置	页签,配	置本端	∄ IP ₺	也址
基础配	置 本地	配置	对端配置			
	本地地址	۱Ŀ	192.168.2.	200		•
	类型	型				•

- 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	2
	客户端虚拟地切	止池	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。 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。 _ 0 23 , 添加或删除管理单元 X 证书管理 您可以在计算机上为此控制; 哪些扩展项。 🗋 控 可用的管理单元(S): 该管理单元将始终为下列帐户管理证书 管理单元 ◎ 我的用户帐户 (#) 💣高级安全 Window... ◎ 服务帐户(S) 🛍 共享文件夹 ◉ 计算机帐户(C) 🌆 计算机管理 一任务计划程序 🛁 设备管理器 💽 事件杳看器 20 授权管理器 文件夹 ○ 性能监视器 ■证书 组策略对象编辑器 通4年間約1 描述 证书管理单元允许您浏览自 < 上一步 (B) 下一步 (R) > 取消 确定 取消 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。 🚘 控制台1 - [控制台根节点\证书(本地计算机)\受信任的根证书颁发机 _ 0 🚘 文件(F) 操作(A) 查看(V) 收藏夹(O) 窗口(W) 帮助(H) - 5 > 🗢 🄿 🙍 🗊 📋 🧟 🗟 🚺 🧰 控制台根节点 对象类型 操作 🔺 🗊 证书(本地计算机) 🎬 证书 受信任的根证书颁发... 🔺 ▷ 📔 个人 更多操作 Þ ▷ 🧮 受信任的根证书颁发和物 查找证书(N)... ▷ 📔 企业信任 ▷ 📔 中级证书颁发机构 查找证书(N)... 所有仟条(K) ▷ 🚞 受信任的发布者 导入(I)... 音看(V) ▷ 📔 不信任的证书 ▷ 🧰 第三方根证书颁发机 从这里创建窗口(W) ▷ 📔 受信任人 新仟务板视图(T)... ▷ 🚞 证书注册申请 刷新(F) ▷ 🚞 智能卡受信任的根 导出列表(L)... ▷ 📔 受信任的设备 帮助(H)

#### 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。

选择一个连接选项	
<b>连接到 Internet</b> 设置无线、宽带或拨号连接,连接到 Internet。	
<b>公司新网络</b> 《二》配置新的路由器或访问点。	
连接到工作区 设置到您的工作区的拨号或 VPN 连接。	
<b>设置拨号连接</b> 使用拨号连接连接到 Internet。	
L	
	下一步(N) 取消

#### 3. 点击使用我的 Internet 额连接(VPN)。



#### 4. 点击我将稍后设置 Internet 连接。



键入要连接的 Interne	ət 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 这个选项允许可以访	接(A) 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	马	
用户名(U):	Bob	
密码(P):	•••••	]
	🔲 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。

🐓 连接 Remo	te VPN 连接	x
用户名(の):	Bob	
密码(P):	•••••	
掝(M):		
☑ 为下面用/	□保存用户名和密码(S):	
◎ 只是我	(N)	
	用此计算机的人(A)	
	取消 属性 (0) 帮助 어	0
。 点击属	<b>属性</b> ,点击 <b>安全</b> ,配置:	安全选项。
Remote VPN	N 连接 属性	x
堂坝 诜顶	安全网络土草	
VPN 类型(T):	I I'M I VIII	
IKEv2		•
新堀加変のい	高级设置(	5)
需要加密 如	果服务器拒绝将断开连接)	•
身份验证一		
<ul> <li>使用可扩</li> </ul>	展的身份验证协议(BAP)(B)	
Microso	ft:安全密码(BAP-MSCHAP v2)(启用加密	-
◎ 使用计算	(属性 (B) 机证书 (M)	
	NHAL A	

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。

**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。

PPI	adapter	IPSe	cVPN	1:										
	Connectio	on-sp	ecif	ic	Dŀ	IS	Sı	ıff	i	ĸ		=		
	Descripti	ion .										:	IPSecVPN	
	Physical	Addr	ess.									:		
	DHCP Enal	bled.										:	No	
	Autoconfi	igura	tior	ı Er	nal	<b>)</b> ]e	ed					:	Yes	
	IPv4 Addı	ress.										:	9.9.0.1(Preferred)	
	Subnet Ma	ask .										:	255.255.255.255	
	Default (	Gatew	ay.									:	0.0.0.0	
	NetBIOS o	over	Tcpi	ip.								=	Enabled	
C:\ 0}	Windows \s !!	syste	m32)	rou	ute	; a	ıdd	1 1	72	2.1	.6.	.2	.0 mask 255.255.255.0	9.9.0.1



# 6.3.10 配置 Android 内置 IPSec VPN 客户端



提示:也可以通过邮件导入证书。

20:26		We Downie	*ይ令	· 🛛 4 🛑
	最近	分类	手机	• • •
Qŧ	叟索			
内部存	储设备>Down	load >		
?	<b>Bob.pfx</b> 2.55 KB   2018/7	//5 19:55		
?	<b>cacert.cer</b> 1.28 KB   2018/7	/5 19:55		
?	<b>remotevpn.</b> 2.56 KB   2018/7	<b>pfx</b> 7/5 20:06		
Ø	<b>SafeConne</b> 4.48 MB   2017/1	ct_android	l.apk	
?	WindowsSe 83.3 MB   2017/1	erver2003 12/13 16:01	SP2-1.ISO	
?	WindowsSe 75.01 MB   2017,	erver2003 /12/13 11:24	SP2.ISO	
	(	(テ)         (ジ)           快传         清理	2	

**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	让书 <b>:</b>							
20:33			* 🖞 🐔	▶ 🛛  💭	20:33			\$ Q 4	À 🗙 ک
	最近	分类		:		最近	分类	手机	0 0 0
					Q 搜索	TEKC			
内部存储设	设备 > Downloa	ad >			内部存储	设备〉Downl	oad >		
为	证书命名				⑦ E	3 <b>ob.pfx</b> 55 KB   2018/7/	/5 19:55		
证书 ca	这名称:				⑦ 1	<b>acert.cer</b> .28 KB   2018/7/	5 19:55		
( 凭 援 VPI	引用途: N和应用			-	⑦ ^r	emotevpn.j 56 KB   2018/7,	<b>ofx</b> /5 20:06		
( 该数 1个C	据包包含: A证书					SafeConnec 48 MB   2017/1	ct_android 0/9 17:30	l.apk	
ł.		取	消 确定	<del>ت</del>	⑦ N 8	<b>VindowsSe</b> 3.3 MB   2017/1	rver2003\$ 2/13 16:01	SP2-1.ISO	
⑦ W 75	/indowsServ .01 MB   2017/12	ver2003SF 2/13 11:24	2.ISO		⑦ N	VindowsSe 5.01 MB   2017/	<b>rver2003</b> \$ ^{12/13 11:24} 已安装 ca。	SP2.ISO	
	快	6 清理					(中)         (************************************		

#### th th





	点击将加 VPN,称加	」 V F IN 庄 按。		
20:09	🖇 💯 🛜 🗵 4 🛑	20:10	•••	\$∅≈⊻≁━
< VPN		取消	添加VPN	确定
开启VPN		类型		
配置		IPSec Xa	auth RSA	>
统一认证		服务器地址	10.175.36.51	
		IPSEC 用户证	正书	
		768f66ad	d041844d1501a318006e	fc9f2 >
		IPSEC CA证	书	
		са		>
		IPSEC 服务署	暑证书	
		98669c3	b8c86c080d3b1321d3f8	4aff1 >
		○ 显示高约	及选项	
		用户名	Bob	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	+ VPN	密码	•••••	

6.3.10.2 添加和建立 VPN 连接

17:1 た拉

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 V	PN 连接界面,	廾启 VPN 连接。
20:11		\$ \$ \$? X 4
< VPN		
开启VPN	I	
配置		
> vpn 已连接		(>)
	统一认证	
	+	
	添加VPN	

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。
- 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	🕑 💵 中国移动 🗢	17:50	
✔邮件	cacert.cer	✔邮件	Bob.pfx	
	cacert.cer		Bob.pfx	
	1.2K		2.5K	
	选择应用打开		选择应用打开	
	文件已经下载完成请使用其他应用打开		文件已经下载完成请使用其他应用打开	F

	1110 111		199921	11 12 12 12	Tereau		4 H -
•••• 中国移动 🗢		17:50	•	💵 中国移动 🗢	17:	50	🕑 🕈 80% 💷 🗲
く邮件	C	acert.cer			项目将添加到"iC	loud 云盘"上	0
				取消			添加
					🐣 Ca	acert.cer	
				iClouc	云盘		~
		_		① 我的 i	Phone		>
	嗝空投送 。立即 的"控制中心"፤	叩与附近的人共享。 或 Mac 上的"访达"	,如果他们从 id "中打开了"隔空				
	口心付可以任日	し处有到他们。在外	点即可关子。				
	? ~		•••				
添加到"备忘	微信	QQ邮箱	更多				
录" 							
	•••						
存储到"文件"	更多						
		取消					
		-1/11					

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 ┉ 奈	17:51			
取消	安装描述文件	安装		
automatica and a second	【文件 ↓11 マ	17:51		
CACente	er 取消	警告	安装	
签名者 CACenter 尚未验证	未受管理的根证=	书		
包含证书	若安装证书"C	ACenter",此证书将	被添加到 iPhone	
更多详细信息	上被信任的证 [。] 启用,网站才:	书列表中。只有在"讧 会信任此证书。	E书信任设置"中	
	+ 20 > 7 66 44 > 2 + 2	4		
	木痘证的描述又作			
	个能验证"CAC	Center"的真实性。		
		< 文件 →□ マ	17:51 그며박地ᅷ <i>소</i> 쓰	@ √ 80% , ≁
			已女装抽还又件	元成
		CAC	Center	
		签名者 CAC 已验	Center 证 ✓	
		包含证书	i	
		更多详细信息	3	>



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。

비 中国移动 🗢	17:56	🕑 🕈 80% 💷 🖌
く通用	VPN	
添加 VPN 配置		

■ 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):

📲 中国移动 🗢	17:58	@ √ 81% 💷 +
取消	添加配置	完成
类型		IKEv2 >
描述	vpn1	
服务器	172.16.2.200	
远程 ID	172.16.2.200	
本地 ID		
鉴定		
用户鉴定		用户名 >
用户名	Bob	
密码	•••••	
q w e	ertyu	i o p
a s	d f g h j	k I
순 Z	x c v b n	m 🗵
123	space	return

■ 如果使	E用 IPsec (即 IKEv1),请填写如下信息
💵 中国移动 🗢 🗵	PN 18:34	# 4 80%
取消	添加配置	完成
	cisco	
类型		IPsec >
描述	vpn2	
服务器	172.16.2.200	
帐户	Bob	
密码	•••••	
使用证书		
证书		Bob >
代理		
关闭	手动	自动

3. 点击完成,完成 VPN 连接的添加。

	18:35		
✔通用	VPN		
VPN 配置			
状态		已连接	
ure m1			
vpm 未知		(i)	
✓ vpn2 未知		i	
添加 VPN 配置			

아슈 부조 후디 가락 무언 マント ,建立 VPN 连接。

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。

	💿 下载	
$\langle \rangle$		Q 搜索
个人收藏	cacert.cer	
iCloud 云盘	■ NEUSOFT(231085357) ► NEUSOFT(231104200) ►	
🗅 文稿		
□□ 桌面		
回 图片		
@ 隔空投送		Certificare
🕂 应用程序		Derigical
🛅 程序		Root m
● 下载		·20- 5 3
设备		2 mart
◎ 远程光盘		~~~
共享的		
💻 neu-20180		
标记		
● 红色		cacert.cer
● 橙色		
● 黄色		
● 绿色		修改时间 2018年7月6日 星期五 16:20
● 蓝色		上次打开时间 2018年7月6日 星期五 16:20 添加标记
● 紫色		
● 灰色	н	
2. 双击证书文	文件,将证书添加进钥匙串。	
3. 点击钥匙目	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。

Ś	钥匙串访问	文件	编辑	显示	窗口	帮助	
			● 点按以锁定	2"登录"钉	月匙串。		
	💌 🔻 📐 Safe		钥匙串			_	CACenter
•	I 🛛 🔽 🔚 S	🚽 👔 👔	<u></u> 全录		Cen	lificate	根证书颁发机构
		🧃 🖞	5地项目		Root	· 5003	过期时间: 2028年7月3日 星期一 中国标准时间 15:43:16
		<u></u>	系统			"me	❷ "CACenter"证书不受信任
		[]] 著	系统根证书				
Z					名称		
ALL THE REAL PROPERTY OF	New Y				1	*.neusof	t.com
•						Apple W	orldwide Developer Relations Certification Authority
Contraction of the second						CACente	r
-0	3					com.app	le.idms.appleid.prd.7a41747449612f706f4f4f427631676751374f3
. 🕝						Develop	er ID Certification Authority
					▶ 📷	iPhone [eveloper: yangqd@neusoft.com (C374734V8V)

4. 右键点击证书文件,选择显示简介。

名称								
	💽 *.neusoft.com							
Bastan Go	Apple Wo	rldwide Developer Relations C	Certification Authority					
	CACente							
	com.appl	新建证书偏好设置	612f706f4f4f427631676751374f3576413d3d					
Bagfan Go	Develope	按□"CAContor"						
▶ 📷	iPhone D	拷贝 CACENTER 粘贴 2 项	(C374734V8V)					
•	iPhone D							
▶ 📷	iPhone D	删际 CACenter	(4N7JCXKN8S)					
•	Mac Deve	导出"CACenter"…						
	mac-serv	ОЩ олоонног ш						
	mail.neus	显示简介						
	Neusoft- 评估"CACenter"							
Shenyang Neusort Systems integration Co., Ltd. for SSL								
Chaptan Chaptan	东软集团周	股份有限公司 User CA						

5. 在信任区域的下拉框中选择始终信任。

	CACenter					
Certificate Rui 书颁发机构 1 2028年7月3日 星期一 中国标准时间 15:43:16 ② "CACenter"证书不受信任 ▼ 信任						
使用此证书时:	始终信任 🗘 ?					
加密套接字协议层 (SSL)	始终信任 ♀					
安全邮件 (S/MIME)	始终信任					
可扩展认证协议 (EAP)	始终信任					
IP 安全 (IPsec)	始终信任					
代码签名	始终信任					
时间戳	始终信任					
X.509 基本策略	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。

\bigcirc	您正在对"	'证书信任设置"进行更改。				
R	输入密码以允许此次操作。					
	用户名:	admin				
	密码:	•••••				
		取消 更新设置				

7. 查看证书状态,可发现证书变为受信任状态。

Certificate Root	CACenter 根证书颁发机构 过期时间:2028年7月3日 星期一 中国标准时间 15:43:16 <Ⅰ 此证书已标记为受此帐户信任
名称	
📷 *.neusof	t.com
📷 Apple W	orldwide Developer Relations Certification Authority
CACente	er

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)。

$\bigcirc \bigcirc \bigcirc \bigcirc \checkmark >$		网络	Q 搜索	
	请选择接口并为新朋	设务输入名称。		
● Wi-Fi 已连接	按口: VPN 类型:	IKEv2	び ☆ ぶ 湖 Wi-Fi	
● 蓝牙 PAN 未连接	服务名称:	VPN (IKEv2)	,地址为	
● MT65xxeloa 未配置		取消	创建	
● USB 10/00 LAN 未连接	↓	🔽 自动加入此	网络	
● 雷雳网桥 _{未连接}	$\langle \cdots \rangle$	□ 询问加入新 将自动加入已经 得不手动进程	网络 印网络。如果没有已知网络,您将不 网络	
●		4±6770772-11.42L	°° ⊐2 °	
<mark>● VPN (L2TP) 2</mark> 未连接				
	2 左き	ㅎ 여산 머 모 국 WiL Ci 방초	室 //	
+ - *~			高级 ?	
			复原应用	

	网络	Q. 搜索
位置:	自动	0
● Wi-Fi 已连接	状态: 未连接	
● 蓝牙 PAN → 赤连接		
● MT65xxeloader v ³ 未配置		
● USB 10/00 LAN ↔ → 去连接	服务器地址: 172.16.2.200	
雷雷网桥 人	远程 ID: 172.16.2.200	
◆未连接	本地 ID:	
● VPN (L2TP) 未连接	华 定设置	
● VPN (L2TP) 2 ① 未连接	连接	
● VPN (IKEv2) 入 未连接		
+ - *	✓ 往米早忙屮並示 VPN 状态	高级 ?
		复原 应用

2. 设置 IPSec VPN 服务器地址和远程 ID。

<u>.</u>	点山 壶足以且 ;	以且/11/	口作山門,	示山 为 。	
C				网络	Q.搜索
		鉴定设置: 用户名			
	● Wi-Fi 已连接 ● 蓝牙 PAN	用户名	Bob		
	● MT65xxeloader 未配置			取消	
	● USB 10/00 LAN 未连接	<>	· · · · · · · · · · · · · · · · · · ·	程 ID: 172.16.2.200	
	● 雷雳网桥 _{未连接}	$\langle \cdots \rangle$	本地	也 ID:	
	● VPN (L2TP) 未连接			鉴定设置	
	● VPN (L2TP) 2 未连接			连接	
	● VPN (IKEv2) 未连接				
	+ - *~		2 在菜单栏中5	显示 VPN 状态	高级 ?
					复原 应用

3. 点击鉴定设置,设置用户名和密码,点击好。

	网络	Q 搜索
位置	自动	0
● Wi-Fi 已连接	状态: 已连接 连接时间: 0:00:52	
● 広方 PAN	IP 地址: 9.9.0.1	
★注接 MT65xxeloader ★配置	服务器地址: 172.16.2.200 远程 ID: 172.16.2.200	
● USB 10/00 LAN	本地 ID:	
● 雷雳网桥 未连接	鉴定设置	
VPN (L2TP) 未连接	断开连接	
● VPN (L21P) 2 未连接		
+ - *	✓ 在菜单栏中显示 VPN 状态	高级 ?
		复原 应用

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 廾 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

- 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** $d = \frac{1}{2} \lambda$, $d = \frac{1}{2} \lambda$,

导入CA证书		×
文件*		浏覧
名称*	CA.pem	
		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 locala.pfx。

导入本地证书			×
	文件*		浏览
	名称*	locala.pfx	
	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. 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。

基础配置 本地配置 对端配	置 IKE ESP
名称*	IPSec1
类别	Site-to-Site
启用	 Image: A start of the start of
日志	
主动协商	IPSEC VPN两端只能有一处启用
备注	
	0/255
IKE版本	ikev2 •
认证模式	证书 ▼
本地证书*	locala 👻
加速卡	■ 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。

基础配置本地配置	对端配置 IKE ESP
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	172.16.2.2	200		
	类型	证书主题		▼	
	ID	C=CN,ST=	LiaoNin	g,O=Neusoft,OU	=neteye,CN=b,emailAdd
X	端子网	192.168.2	.0/24		
					//
		每个子网使用	洄车分割	削,示例如下:	
		192.168.1.0	0/24		
		192.168.2.3	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

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 导人 ,道	『择 CA 证书,导入	CA 证书。
导入CA证书		×
文件* 名称*	C:\fakepath\CA.pem	浏览
		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 lo	calb.pf
导入本地证书				×
	文件*		浏览	
	名称*	localb.pfx		

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。

基础配置本地	配置 对端配	配置 IKE ESP
	名称*	IPSec2
	类别	Site-to-Site
	启用	
	日志	
	主动协商	☑ IPSEC VPN两端只能有一处启用
	备注	
		0/255
	IKE版本	ikev2 🔻
	认证模式	证书 🔻
	本地证书*	localb 👻
	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。

基础配置	本地配置	对端配置	IKE	ESP	
4	5地地址	172.16.2.2	200	•	
	类型	证书主题		•	
	ID	C=CN,ST=	LiaoNing	g,O=Neu	soft,OU=neteye,CN=b,emailAdd
4	地子网	192.168.2.	0/24		
					1
		每个子网使用	回车分割	」, 示例如「	،
		192.168.1.0)/24		
		192.168.2.1	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	172.16.1.1
类型	征书主题 ▼
ID	${\sf C}{=}{\sf CN}, {\sf ST}{=}{\sf LiaoNing}, {\sf O}{=}{\sf Neusoft}, {\sf OU}{=}{\sf neteye}, {\sf CN}{=}{\sf a}{,}{\sf emailAdd}$
对端子网	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

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:

i	添加制除	重启服务 启用	禁用]				
	名称	类别	启用	对端	出口	认证模式	状态	
	RemoteAccess	Remote Access		任意	任意	预共享密钥	客户端 🔝	1
	IPSec1	Site-to-Site	•	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 启邦	割	用				
名称	类别	启用	对端	出口	认证模式	状态	
RemoteAccess	Remote Access		任意	任意	预共享密钥	客户端 🔚	1
IPSec2 🔁	Site-to-Site	٠	172.16.1.1	172.16.2.200	证书	已连接	1 📩

- 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