

# 天翼云・SSL VPN

## 管理员手册

天翼云科技有限公司



#### 目录

第1章	前言	3
第2章	系统管理	3
2.1	设备登录	3
2.2	管理员配置	4
2.2	2.1 修改管理员密码	4
2.2	2.2 创建二级管理员	4
2.3	系统基本信息配置	7
2.3	3.1 授权信息	7
2.3	3.2 系统时间	7
2.3	3.3 控制台配置	8
2.3	3.4 设备配置备份与恢复	8
第3章	SSL VPN 配置	9
3.1		
-	用户管理	9
3.1	用户管理 1.1  批量导入用户	9 9
3.1 3.1	用户管理 l.1 批量导入用户 l.2 手动创建用户	9 9 11
3.1 3.1 3.2	用户管理 l.1 批量导入用户 l.2 手动创建用户 资源管理	
3.1 3.1 3.2 3.2	用户管理 1.1 批量导入用户 1.2 手动创建用户 资源管理 2.1 手动创建资源	
3.1 3.1 3.2 3.2 3.3	用户管理 I.1 批量导入用户 I.2 手动创建用户 资源管理 2.1 手动创建资源 角色授权	
3.1 3.2 3.2 3.3 3.4	用户管理 I.1 批量导入用户 I.2 手动创建用户 资源管理 2.1 手动创建资源 角色授权 内网域名解析设置	
3.1 3.2 3.2 3.3 3.4 3.5	<ul> <li>用户管理</li> <li>1.1 批量导入用户</li> <li>1.2 手动创建用户</li> <li>资源管理</li> <li>资源管理</li> <li>2.1 手动创建资源</li> <li>角色授权</li> <li>内网域名解析设置</li> <li>其他设置</li> </ul>	
3.1 3.2 3.2 3.3 3.4 3.5 3.5	用户管理 1.1 批量导入用户 1.2 手动创建用户 资源管理 2.1 手动创建资源 角色授权 内网域名解析设置 其他设置	



本手册用于讲解 SSL VPN 常见功能操作方法,为管理员提供日常策略维护指导。

## 第2章 系统管理

## 2.1 设备登录

首先确保本机从网络可以访问到设备管理 IP 地址, 然后在浏览器中输入网关的 IP 及端口 https://192.x.x.x:4430。出现一个如下图的安全提示:

Attn://192168139.84/430/     O ▼ C      St お供知識、目前日間は     Y	
(mtps://152.106.159.0434430)	
<b>瓜网站的安全证书仔住问题。</b>	
此网站出具的安全证书不是由受信任的证书颁发机构颁发的。	
此网站出县的安全业书是为县他网站地址颁友的。	
安全证书问题可能显示试图欺骗你或截获你向服务器发送的数据。	
建议大闭此网贝 , 并且个安继续浏见该网站。	
🥝 单击此处关闭该网页。	
😵 继续浏览此网站(不推荐)。	
U PT-HUIDAN	

点击<继续浏览此网站(不推荐)>后出现以下的登录界面:

		<u> </u>	
售后服务:400-630-6430		SSL VPN	
新标准:	口大业经验值测验 记入业经验值测验		
有线无线 统一上网行为管理		密码	
	国内第二代防火墙		
	标准发布	登录	
	CONTRACT CONTRACT	版本信息	



在登陆框输入『用户名』和『密码』,点击<登录>按钮即可登录 SSL VPN 设备进行配置,默认情况下的用户名和密码均为 admin。

如果用户密码过于简单,则会被检测为弱密码,在控制台的处理为:登录后检测为弱密码则提示修 改密码,则会弹出如下提示:

告警信息						
⚠	<b>请修改登录密码</b> 当前帐号的密码为常见弱密码,为保障系统安全,请立即修 改。					
	立即修改					

#### 2.2 管理员配置

在『系统设置』-『管理员账号』页面,可修改 admin 管理员密码、删除管理员账号以及创建 二级管理员。

#### 2.2.1 修改管理员密码

管理员账号页面找到 admin 管理员,直接点击<编辑>,设置新密码即可修改 admin 账号的 密码信息。

#### 注: admin 账号只可修改密码,不可删除。

控制台	>> 新建/编辑管理员	
<ul> <li>运行状态</li> </ul>	: 基本属性	标记·的为必须填写项目
<ul> <li>              新建築査 予約構成置 )阿諾森置 )阿諾森電 )「「「「「」」」             "</li></ul>	管理気系統: ▲ ministrator 管理気楽証: ▲ ministrator 管理気楽証: ● 管理気 ● 订存 正明 ●●●●●●●●●●●●●● ● ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
	<ul> <li>该株书公许从任意中地址量录</li> <li>该株号位计从下面的地址量录</li> </ul>	
▶ SSL VPN设置	◎ 新建 ○ 粉線 @ 编辑	
▶ SC设置	□ 起始IF地址 结束IF地址	
▶ IPSec VPN次置		
▶ 防火墙设置		
▶ 系统维护		

#### 2.2.2 创建二级管理员

创建管理组

在管理员账户页面,可以创建二级管理员,设置不同的管理员可以管理不同的用户、资源以 及角色等内容。

点击新建后会出现[管理员]和[管理组]的选项,显示如下: ▶ 管理员帐号 ③新建 ● ●删除 ②编辑 ☑ 选择 管理员 管理组



选择[管理组]后,可新建	一个管理组并设置该管理组的权限。显示如下:
»» 新建/编辑管理组	
こ 基本属性	
管理组名称:	*
管理组描述:	
所属管理组: /	>>
☑ 启用该管理组	
an e de an la conte an de se	
1 配立官埋秋限和官埋内谷	
管理权限管理内容	
□ 运行状态	清輸入搜索的关键字 👂 🖻 📔
□ 系统设置	□ □ SSL VFN设置
SSL VPN设置	
☑ IPsec VPN设置	
☑ 防火墙设置	
■ 双机维护	□ □ 2 % ☆ 2 文王 東 哈 □ □ 2 内置规则库升级
□ 系统维护	
☑ 允许创建下级管理组	
☑ 允许创建角色	
☑ 允许创建资源	

『管理组名称』和『管理组描述』可自定义。

『所属管理组』:选择该管理组所属的组,若是在根组下建管理组,则保持默认即可。
『管理权限』里面可以设置该组成员能够管理设备的权限,只需在相应模块后打勾即可。
选择『管理内容』,即可对该组管理员管理的内容进行限制。包括用户,资源和角色的管理。
显示如下:

管理组名称:		¥
所属管理组:	1	»
	☑ 启用该管理组	
配置管理权	很和管理内容	
管理权限	管理内容	
用户		◎ 请输入搜索的关键字 ♀ 略   ■
资源		
角色		
		→ 日 □ 合 总部 田 □ P sangfor.com
		🗃 🖵 🚰 test 🗃 🗖 🖰 support
		- 🗆 🚔 shi chang

创建管理员



点击新建管理	里员,出现如下设置	页面:		
»» 新建/编辑管理员	t			
基本属性				
管理员名称:		*		
管理员描述:				
管理员类型:	<ul> <li>管理员</li> <li>访客</li> </ul>			
密码:		*		
确认密码:		*		
所属管理组:	/	*		
	☑ 启用该管理员			
□ ↔汝蓉录TPi	۵ <del>۲</del>			
<ul> <li>该帐号允</li> <li>这帐号允</li> </ul>	许从任意IP地址登录			
() 该帐号仪	九叶从下面的地址宣求			
③ 新	建 🤤 删除 📝 编辑			
	起始IP地址		结束IP地址	
保存	取消			

『管理员名称』即管理员登录 SSL 设备控制台时所使用的帐号。

『管理员描述』设置该管理员的相关说明信息,可任意填写。

『管理员类型』分为[管理员]和[访客],管理员对设备配置具有相应组的管理权限;访客只具备只读权限,只能看相应组权限下的设置信息。

『密码』和『确认密码』用于设定管理员登录的密码。管理员密码会自动进行复杂度检测, 不能设置简易密码。

『所属管理组』设置此管理员所属的管理组,选择后可匹配相应组的权限。

『允许登录 IP 限制』可以设置使用此管理员帐号登录 SSL 设备的 IP 地址。若设置了登陆 IP 限制,那么在 IP 列表外的地址将不能使用该账号登陆 SSL 设备。

注:管理员密码需要同时符合以下策略:

- (1) 长度至少为8位;
- (2) 密码中不能包括管理员用户名;
- (3) 必须包含数字、小写字母、大写字母和特殊字符中的任意两项;
- (4) 下级管理组的管理权限不会比上级管理组还多。即下级管理组的可管理的用户、资源、角色均由上级管理组授权,不会超出这个范围。



### 2.3 系统基本信息配置

#### 2.3.1 授权信息

在『系统设置』-『系统配置』-『序列号管理』页面,可以查看设备当前的授权信息。

控制台	授权信息 日期与时间 控制台配	置 设备证书	邮件服务器	数据中心	SNUP	运维配置			
▶ 运行状态	甘土合白							4	-
▼ 系统设置	- 坐牛 肩忍								
> 系統配置	授权类型: 在线授权(试用版	)							
> 网络配置	授权用户: SXF_TEST								
> 时间计划	授权ID: AOABE-C77D-9B09-F9	D-6CEB-FA87-CE54	I-0C19						
> 位置管理	初降成"在线帶机""授权目	·· 徐器授权"							
> 管理员帐号									
▲ SSL VPN选项	里 直   重直登求齐曲《	用尸使用协议◎免责	戸明// 选坝						
> 系统选项									
<ul> <li>&gt; 网络传输优化</li> <li>&gt; BZ000000</li> </ul>	VPN等权模块						图示: 🖌 已接	2 🙆 未授权	
) 土型官理 、 生型官理									
> 分布式部署	SSL VPM 用户忌数:	50		<b>«</b>					
22.0000000	IPSec移动用户数:	0		0		设 盂			
	线路数:	4		<b>v</b>					
	分支机构数:	2		<b>~</b>					1
	远程应用用户数:	50		<b>~</b>					
	跨运营商:	已授权		<b>v</b>					
→ SSL VPN设置	单点登录:	已授权		1					
▶ IPSec VPNigh	单边加速:	已授权		1					
▶ 防火擂破五	焦群:	已授权		1					
▶ 杀统维护		GIAIX		*					•

#### 2.3.2 系统时间

『系统设置』-『系统配置』-『日期与时间』用于设定 SANGFOR 设备的系统时间。可以直接在界面上修改时间,也可以选择<自动与时间服务器>进行时间的同步。

注: 设备日志记录的时间与系统时间相关,请注意确保设备系统时间的准确性,手动获取本 地时间和系统时间会重启设备,请勿工作时间操作。

序列号管理	日期与时间 控制台配置 外置数据中心 设备证书 邮件服务器 Syslog SNMP
日期与	时间
日期:	2016-11-10
时间:	11:12:07 *
	获取本地时间
ा NTPBन हि	洞步
口自	动与时间服务器同步
时	间服务器: time.nist.gov ▼ 立即更新
最	近——次与time.nist.gov同步时间成功,在2012—01—01 00:00:01
1	<b>保存</b>



#### 2.3.3 控制台配置

『系统设置』-『系统配置』-『控制台配置』用于设定 SSL 设备的设备名称、WEBUI 管理页 面端口、超时时间以及远程维护支持选项。

序列号管	理 日期与6	时间 控	制台配置	外置数据中心	设备证书	邮件服务器	Syslog	SNMP			
: 控制	间台设置									标记*的为必须	填写项目
设	备名称:	Sangfor	SSL VPN								
ht	:tps端口:	4430		*							
	http沸口:	1000		*							
2 控制	自治超时时间										
超	朙时间: 10			★(5-1440分	钟)						
- 远移	呈维护支持										
С	〕启用	◉禁!	₹								
	保存	取消	í								
注	È: 为设	备安全	è考虑	,一般情	泥下建i	义禁用远	程维护	支持。	)		

#### 2.3.4 设备配置备份与恢复

『系统维护』-『配置备份/恢复』用于将设备已有的配置下载保存,或者是将已备份的配置文件恢复到设备中。

Joseph 75	
控制台	全向副法律份 SSL UMB法律份
<ul> <li>运行状态</li> </ul>	
▶ 系統设置	- 创建配置备份
▶ SSL VPN设置	创建配置备份: 下载当前配置
▶ SC设置	
▶ IPSec VPN设置	「「報告述原
▶ 防火墙设置	<b>洗择本地文件:</b>   清洗择_bef文件   湖路   *
▼ 系统维护	
<ul> <li>▲ 系統更新</li> <li>&gt; 系統升級</li> <li>&gt; 代理设置</li> <li>&gt; 日志宣看</li> </ul>	用这件成之前「1933年3月19日」 开始还原 : 备份提醒
▶ 配置备份/恢复	通过会时提醒,在话当的时候手动备份设备当前的所有配置信息,以备系统发生加速时或者配置损毁时进行修改。
> 重启/重启服务/关机	注意:该功能并不直接为您创建备份文件,您需要提到该提醒后,到该页面将备份下载到本地计算机并妥善保存。
	<ul> <li>✓ 连续一段时间内没有执行配置备份,则登录控制台时提醒时间间隔:10</li> <li>保存</li> <li>取消</li> </ul>

SSL 的配置包含全局配置和 SSL VPN 配置,都是点击 < 下载当前配置 > 进行下载,两者的区别 是:

全局配置:包含 SSL 设备系统配置、网络配置、SSL VPN 设置、IPSEC VPN 配置以及防火墙 设置等设备全部配置信息。导入全局配置时,设备需要重启。

SSL VPN 配置: 仅包含 SSL VPN 设置和 SSL VPN 选项的配置。导入 SSL VPN 配置时,设备 仅重启 SVPN 相关服务。



## 第3章 SSL VPN 配置

### 3.1 用户管理

### 3.1.1 批量导入用户

先在用户管理中创建模板用户,然后点击『其他操作』→『导出』,点击『选择导出内容』 选择模板用户,导出模板 csv 文件,编辑 csv 文件,按照模板用户格式中添加其他用户信息。

控制台	⇒> 用户管理			
▶ 运行状态	📀 新建 ▾ 🤤 刪除 📝 编辑 📝 选择	▼│ 🧝 绑定信息管理 ▼ 🔜 导入 ▼ 👒 移动	◎其他操作 ▼ □> 发送短信	🥑 查看资源 📃 显示所
▶ 系统设置	请输入搜索的关键字 🔎 🗄 🗏 🗉	组名: /	导出	
▼ SSL VPN设置		组路径: Z	绑定角色	
> 用户管理 ▲		组信息: 直属子组数:3,总子组数:32,直	从帐号设置	1):13
> 资源管理	🔒 默认用户组		批重生成证书	
▶ 角色授权		□ 名称 ▲		
→ 认证设置			下载USB-KEV版动	
2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			下载USB-KEY导入控件	接口的用户
· 秋明坦 日注 。		🔲 📑 默认用户组	用广组 苏沅休再的用广组	~~能被删除

#### (1) 点击『SSLVPN 设置』→『用户管理』,点击『导入』→『从文件导入』;



(2) 选择"从文件中(\*.csv)导入用户", 点击"下一步";



»» 用户管理-从文件导入
**选择要导入的类型和数据
● 从文件中 (*. csv) 导入用户
<ul> <li>○ 从数字证书中导入用户</li> <li>○ 从文件中(*. xml)导入组织架构</li> </ul>
下一步 取消

(3) 在"选择文件"处,选择编辑好的用户信息表 csv 文件,同时勾选"用户所属组 不存在时,自动创建"选项后,点击"下一步"

→>> 用户管理-从文件导入
₩ 从文件中 (*. csv) 导入用户
所谓'CSV',是Comma Separated Value的英文缩写,通常都是纯文本文件,可以使用Excel进行编辑.技巧:首先使用Excel编辑
用户列表,然后使用菜单命令:文件->另存为,保存类型选择:CSV,保存即可.下载示例文件
241年文IT- C:\fakepath\userlist.csv 测觉
/ 默认用户组/ >>
对本地已存在用户:
● 继续导入,覆盖已存在的用户
○ 跳过, 不导入该用户
上一步

#### (4) 确认需要导入的用户信息没有问题后,点击"开始导入"。

镭确认导λf	言息是否正确,如果确认;	E误请占击' 完成	'按钮,否则诸占者	Ⴙ、F-−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−	7件.	
4000(037()					S11-	
沪名	所属组	手机号码	虚拟ip	用户描述	CA	证书绑定字段
ŧΞ	默认组	13800000000		研发部新同事		
四	/总部/研发部	1380000001				
五	/总部/销售部	1380000002		销售同事		
六	/总部/香港分	1380000003		香港分公司同	事	
						共 4 条用户信息



(5) 导入成	功后,在用户管理员	面回	似看到导入成功的用户组以	人及相关用户。	
>> 用户管理 ◎ 新建 ▼ 〇 删除 ◎ 濃緯 ■ 2 选择	▼ 扁妹征码管理 扁鳥〉 ▼ 隔移油 《	<b>美甘他</b> 揭作	: ▼ ③ 杏香浴酒   □ 見示所有(包括子組) ::		0. 真犯搜索
● 加速 ● Winh ● 用 ● 2 (2) 清約入授索的关键字 / E E ■ ● ○ D部 ● 研发部 - ● 消售部 - ● 消售部	组名: <b>研发部</b> 组路径: <u>/L記/研发部</u> / 组信息:直属子组数:0,总子组数:0,目 查看或编辑组图性	重属用户数	:1,总用户数(包含子组):1		T ST XEEL .
□ ● 香港方公司 ■ ● 野认用户组 ■ ● 野认组	<ul> <li>□ 名称 ▲</li> <li>□ ▲ 李四</li> </ul>	类型 用户	描述	其他信息私有用户	状态

### 3.1.2 手动创建用户

(1) 点击『SSLVPN 设置』→『用户管理』,点击『新建』→『用户』;

控制台	→>> 用户管理			
▶ 运行状态	◎新建 🔍 🤤 刪除 📝 编辑 📝 选择	🔹 🝓特征码管理 🔜 导入 🔹 潯移动 🧇其他	操作 ▼ 🥑 查看资源   🔄 显示所有(包括子组	按名称
> 系統设置		组名:研发部		
▼ SSL VPN设置	日 用戶組	組路径: /总部/研发部/		
▶ 用户管理		组信息: 直属子组数:0,总子组数:0,直属用戶	■数:1,总用户数(包含子组):1	
> 资源管理		<u>查看或编辑组属性</u>		
> 角色授权		□ 名称 ▲ 类型	「描述」	其他信息 状态
→ 认证设置	- 🚰 默认组	🗖 🚨 李四 🛛 用月		私有用户 🖌 🖌
> 策略组管理				
> 终端服务器管理				
▲ 企业移动管理				
> 移动设备策略		4		
> 移动设备管理				
<ul> <li>&gt; 应用商店</li> </ul>				
> 应用封装				
<ul> <li>▲ 端点安全</li> <li>&gt; 端点安全规则</li> </ul>				
▶ SC设置				
▶ IPSec VPN设置				
<ul> <li>防火墙设置</li> </ul>				
(2) 设置	置用户名、密码以	及用户所属组后点击	;"保存"即可。	



名称: testuser	★ * 数字证书/USB-KEY:无
描述:	生成证书 导入证书 创建USB-KEY
密码: ●●●●●●	虚拟IP: <i>● 自动获取  <li>● 手动设置 0.0.0.0</li></i>
确认密码: ●●●●●●●	过期时间: ● 永不过期 ○ 手动设置 2021-11-02 四
手机号码:	账户状态: ● 启用 ● 禁用
所属组: /总部/销售部	>> 离线访问:接入策略未启用离线访问
<ul> <li>☑ 驱承所属组队促迟项</li> <li>认证选项</li> </ul>	
<ul> <li>▼ 建序所属组队配送项</li> <li>● 认证选项</li> <li>● 除户类型: ○ 公有用户 ● 私有月</li> </ul>	用户
<ul> <li>▼ 建承纳离组 (N ш 200)</li> <li>* 认证 送顶</li> <li>账户类型: ○ 公有用户 ● 私有)</li> <li>主要认证</li> <li>▼ 用户名/密码</li> </ul>	用户 
<ul> <li>▼ 建华所属组 () 健 2000</li> <li>● 认证 选项</li> <li>● 账户类型: 公有用户 ● 私有</li> <li>● 主要认证</li> <li>● 用户名/密码</li> <li>● 数字证书/Dkey认证</li> </ul>	用户 辅助认证 硬件特征码 短信认证
<ul> <li>▼ 建本所属组 () 健 2000</li> <li>★ W D 20</li></ul>	用户 <b>辅助认证</b> 硬件特征码 短信认证 动态令牌
<ul> <li>▼ 建华所属组 以 ш 边坝</li> <li>▼ 认证 送项</li> <li>● 秋戸类型: 公有用户 ● 私有</li> <li>● 主要认证</li> <li>● 用户名/密码</li> <li>● 数字证书/Dkey认证</li> <li>● 外部认证</li> <li>● 多认证方式: ● 同时使用 ●</li> </ul>	用户
<ul> <li>★ 本外的属组 以 能 必须</li> <li>★ 认证 选项</li> <li>● 然有用户 ● 私有的</li> <li>● 主要认证</li> <li>● 如户名/密码</li> <li>● 数字证书/Dikey认证</li> <li>● 外部认证</li> <li>● 外部认证</li> <li>● 多认证方式: ● 同时使用 ●</li> <li>★ 入 策略相</li> </ul>	用户
● 独本所属组以键达级       认证 选项       账户类型:     公有用户       主要认证       ● 用户名/密码       數字证书/Dkey认证       ● 外部认证       多认证方式:     ● 同时使用 <b>益入策略组</b>	用户 <b>辅助认证</b> 通件特征码 短信认证 →

所属组信息在点击新建用户时,可提前选择指定组,则新建的用户会自动选择该组。

▶ 用尸昏理					
◎新建 - 🗢 刪除 📝编辑 🗹 选择	•   👼特征码管理 🔜 导入 • 潯移动 🐇	■其他操作 ▼ ③查看资源	]显示所有(包括子组)	按名称 ▼ 请输入搜索关键字 👂	🛯 🔍 高级搜索
请输入 读的关键字 P 图 ■ ■ 2 2 部 - 2 初次部 - 2 消售部	组名: <b>销售部</b> 组路径: <u>(总部)销售部</u> / 组信息:直属子组数:0,总子组数:0,副 查看或编辑组属性	属用户数:2, 总用户数(包含子	组) -2		
□ 香港分公司 □ 日本	□ 名称 -	类型 描述		其他信息	状态
👍 默认组	🔲 🚨 testuser	用户		私有用户	<b>v</b>
	🔲 💩 王五	用户 销售同事		私有用户	<b>v</b>
注:					

(1) 用户或用户组导入成功后,缺省会继承上级组的组属性,如果需要调整用户组的认证 方式和账户类型,可单独编辑用户或用户组进行修改,如下图:



>> 修改用户组	
- 基本属性	
名称: 总部 描述: 所属组: / 最大并发用户数: 0 (0表示不限制) 账户状态: ④ 启用 ① 禁用 ① 继承上级用户组关联角色、认证方式和策略级 ② 继承上级用户组关联角色、认证方式和策略级	* >>
<ul> <li>□ 认证选项</li> <li>账户类型: ○公有用户组 ● 私有用户组</li> <li>主要认证</li> <li>☑ 用户名/密码</li> <li>□ 数字证书/Dkey认证</li> <li>○ 外部认证</li> <li>● 外部认证</li> <li>● 多认证方式: ● 同时使用 ○ 任意一种</li> </ul>	<ul> <li>辅助认证</li> <li>□ 硬件特征码</li> <li>□ 短信认证</li> <li>□ 动态令牌</li> </ul>

(2) 公有用户和私有用户的区别:

公共用户: 该类型账户允许多人同时登陆, 用户登录后不可修改自己的密码等属性, 公有用 户不可选择证书认证和短信认证。

私有用户:私有用户同一时间仅允许同一用户在线,本地密码认证的私有用户可在登录后修 改自己的密码、手机号码、描述等信息。

#### 3.2 资源管理

#### 3.2.1 手动创建资源

(1) 在『资源管理』页面,点击新建按钮,VPN 设备提供三种四种类型资源可选,为支持 移动终端 VPN 直连业务系统,本次资源全部选择 L3VPN 类型,如下图:





(2)	选择-	一种应用类型,	如[L3VPN],	弹出	『编辑 L	3VPN 资源』	对话框	, 设置界面如下:
>>> 编辑L3VPN资源 								标记*的为必须填写项目
名称: 描述: 选型: 地址: 应用程序路径: 所属组: 图标:	知识管理系 HTTP http://192 程序路径可U 办公系统	统 ▼ 协议: ICP 2. 200. 200. 162/cm±/80:80 以使用给对路径也可以使用环: >>	* ② ③ ③ 添加 〕 微 微 微 微 微 微 微 微 微 微 微 微 微					
(3)		<sup>源,</sup> <sup>河观</sup> 资源名称,设备 以及地址,保存	新定义了一 <u>4</u> 存立即生效即可	些资源	类型,如	<b>!</b> 果没有可选	择 Othe	er 即可,选择协议
注:				_				
(1) (2)	非必要 HTTP 带 HT	史场景(无插作 <sup>9</sup> 类型的系统, 「TP 前缀的完整	F),不建议使 如果访问地 隆路径,如下	門 we 业有带 图:	b 应用漆 文件路径	\$加资源。 2,在创建资	源时,均	地址列表应该填写
添加/编辑资源	她址				×			
单个添加								
域名资源,请林	☆査是否醒	配置好域名解析 内网	域名解析					
	◉单-	-IP地址或域名	IP地址段					
IP/掝名	: http:/	/192.200.200.162/c	=s  X *					
端口范围	: 80  ] 启用	到 80 ]资源地址伪装	*					
(2)	次运动	长期以分四。	确定	: ][	取消			

(3) 资源类型说明:

WEB 应用: 支持无任何插件的 WEB 资源, 建议仅对移动终端开放。

TCP 应用: 支持 TCP 协议的业务, 如果没有移动终端接入需求, 大部分 TCP 协议的应用建议 使用该类型的资源, 如 HTTP、FTP 等。

L3VPN:使用隧道支持全 IP 协议,支持 TCP、UDP、ICMP 等应用,支持 Android4.0, IOS9.0 以上版本的移动终端的 VPN 接入,如需考虑移动终端接入,建议使用该类型资源。

远程应用:需借助 Windows server 搭建终端服务器,可发布服务器上的应用程序访问内网 系统。



## 3.3 角色授权

『角色授权』是"用户/用户组"和"资源"的中介,通过『角色授权』把SSL VPN 登录用户 /用户组和 SSL VPN 内网资源"关联"起来的。通过角色可以把多个"用户/用户组"、多个资源 进行关联,更加有效管理资源和用户组的权限。

例如,研发部仅允许访问公司门户和知识管理系统,销售部可以访问公司门户和 CRM 系统等禁止外发上网策略配置,具体配置如下:

控制台	▶ 角色管理			
▶ 运行状态	💿 新建 - 😄 删余 📝 编辑 │ 🖌 选择	▼ 🛃 生成权限报告		按名称 - 请输入搜索关键字 🔎
▶ 系统设置	新建角色	描述	授权给	状态
▼SSL VPN设置	🖊 以所选角色为模板新建		hu. li	×
→ 用户管理 ^	🔲 🍐 怕亚通所有用户		eascs	
· 读 ··································	🔲 🍐 sangfor测试		sangfor	×
/ 贝森自主				
▶ 用巴提权				
> 认证设置				
> 策略组管理				
> 终端服务器管理				
▲ 企业移动管理	4			
> 移动设备策略				
> 移动设备管理				
<ul> <li>&gt; 应用商店</li> </ul>				
› 应用封装				
▲ 端点安全				
> 端点安全规则				

(1) 在『SSL VPN 设置』→『角色授权』,点击新建角色。

(2) 在新建角色页面,『关联用户』处选择授权用户,例如关联研发部,『授权资源列表』 处编辑资源授权列表,关联公司门户和知识管理系统两个资源。

>> 新建角色			
- 基本属性			
<ul> <li>角色名称:研发部角色</li> <li>描述:</li> <li>关联用户:研发部</li> <li>角色准入策略:</li> <li>✔ 启用该角色</li> </ul>		* 选择授权用户 选择角色准入策略	
🛃 编辑授权资源列表			
名称	类型		描述
🧔 公司门户	HTTP		
🕗 知识管理系统	HTTP		

### 3.4 内网域名解析设置

SSL VPN 支持需要通过内部域名才能访问的资源应用。内网存在此类应用时,一般有一台或



多台内网 DNS 服务器,给内网电脑提供内网域名解析服务。通过 SSL VPN 需要访问此类应用时,可以通过『内网域名解析』配置来实现

(1) 在『系统设置』→『SSL VPN 选项』→『系统选项』,选择『内网域名解析』选项 卡,在首选和备选 DNS 处设置客户的内网 DNS 服务器地址,如下图内网 DNS 为 172.29.12.11 和 172.29.10.11。

控制台	按入选项 客户端选项 虚拟IP池 内网域名解析 单点登录设置 资源服务选项				
▶ 运行状态	「 山岡経女/2015				
▼ 系统设置					
▶ 系统配置	如果资源中使用的地址是内部域名,则需要在此处输入正确的内网DNS地址(内网地址),并且把内部域名添加到内网域名列表中,使得这部分域名				
▶ 网络配置	的解析请求优先由内网DMS服务器解析.				
» 时间计划	此功能仅对LP,L3PP型用的更都有效,如来定#LD型用页源,对而安体证以會能軒列成功以內中或石(在內站电量平电量LLMS或nUS1S)				
》管理员帐号	首选DNS:       172. 29. 12. 11       ×         备选DNS:       172. 29. 10. 11         □       按入计算机使用此DNS服务器作为首选的DNS服务器				
▲ SSL VPN选项					
> 系统选项					
» 网络传输优化	启用该选项后,会自动启用L3VPN服务,使得接入计算机上所有的域名解析请求都优先到此处配置的DNS服务器来解析.断开VPN后会自动恢复接》				
> 登录策略	• 计算机的DNS设置. 启用此功能后, 无需再配置页面下方的域名解析规则. 同时, 用户无操作自动注销功能将失效.				
> 集群部署	- 内网NS规则设置				
> 分布式部者					
	③新建 ⊜ 删除 》编辑 》选择 ·				
	□ 規则 描述				
▶ SSL VPN设置	zdcm. eascs. com				
▶ SC设置	Zdcml.eascs.com				
▶ TPSec VPN设置	Zdcm2. eascs. com				
▶ 防火墙设置	www.380fs.com				
<ul> <li>▶ 系统维护</li> </ul>	admin. 365hele.com				

# (2) 在此页面『内网 DNS 规则设置』处,将定义资源的域名全部在此处添加,如 oa.sangfor.com.cn。

接入选项 著	客户端选项 虚拟IP池	内网域名解析	单点登录设置	资源服务选项			
内网域名	- 内网域名解析						
如果 <sup>3</sup> 域名的 此功能	资源中使用的地址是内音 的解析请求优先由内网D 能仅对TCP, L3VPN应用的	PM或名,则需要在此处 MS服务器解析. 资源有效,如果是WEB	输入正确的内网D 应用资源,则需要	NS地址(内网地址),并且把内部域名添加到 保证设备能解析成功该内部域名(在网络酉	则内网域名列表中,使得这部分 就置中配置DMS或HOSTS)		
首选DNS	S: 172.29.12.11						
备选DNS	S: 172.29.10.11		新建域名	解析规则	×		
	🗌 接入计算机使用	此DNS服务器作为首说	的DD 域名:	oa. sangfor. com. cn			
启用该选项后、会自动启用L3VPN服务,使得接入计算机 接入计算机的DNS设置,启用此功能后,无需再配置页面 <b>内闷DNS规则设置</b>		算机 页面 — 规则艺 — 如:*.· — b?s.d 如:bb	0 <b>4系统</b> 詩*和?匹配符号,*表示任意字符串,?表 com 规则表示所有以,com结尾的域名 nsever.com表示第二个字符为任意字符, a. dnsever.com	★自动恢复 示任意字符:			
③ 新	建 乏删除 📝编辑	☑ 选择 ▼		确定	取消		
± ±	规则		L	描述			
注:							

(1) 此处添加的规则最多支持 100 条;不支持中文域名解析



(2) 添加内网 DNS 规则后,对应域名的解析请求,会优先走内网 DNS 解析,未通过 VPN 发 布的域名,请不要在此添加任何规则!

#### 3.5 其他设置

#### 3.5.1 密码安全策略

密码安全策略可以要求用户必须修改初始密码,并且满足密码复杂度要求。

(1) 在『认证设置』→『主要认证』→『本地密码认证』设置页面

控制台	
▶ 运行状态	: 主要认证
▶ 系统设置	
▼ SSL VPH设置 > 用户管理	25 <b>本地宏码以证</b> 设置 本地宏码安全解解设置,限制态码格式与态码创建时间 需主意。该设置仅对本地用户数据原的运网生效
> 资源管理	
> 角色授权	- LDAP认证 设法
> 认证设置	外部认证LDAS服务器管理,通过外部认证用户数据库的映射或与入到本地的形式未托管用户密码认证操作.
<ul> <li>末昭组管理</li> <li><k端昭名哭管理< p=""></k端昭名哭管理<></li> </ul>	■ - Redius认证 设置
▲ 企业移动管理	₩₩ 外部认证Redius服务署管理。通过外部认证用户数据库的项射或导入到本地的形式来托管用户密码认证操作。
<ul> <li>移动设备策略</li> </ul>	🗻 - 证书与usp-turi认证 设置
<ul> <li>移动设备管理</li> <li>&gt; 応用商店</li> </ul>	黄家证书与CA中心, 创建证书及证书申请等。2万载在尝识SF2页写显动 2万载在送现SF2页写入持性     书字。
<ul> <li>&gt; 应用封装</li> </ul>	
▲ 端点安全 () ) () () () () () () () () () () () ()	以实现境用户在客户端的自动登录,1.217/1917的40域认证和根安装控件功能
<ul> <li>満点安全策略</li> <li>、由果和同時升級</li> </ul>	· ARMAN TST
「自血和吸引率开報	and the second
(2) 左	〕选"启用密码安全策略",并开启响应复杂度要求。
»» 本地密码 <u>认证</u> i	
- 家祖安全領	
☑ 启用密	的安全策略《王思:密码束略只对本地密码认证的私有用尸有效!)
- 密码	不能包含用户名
≤ 新空	
🕑 限党	密码最小长度为 6 位
- 毎期	R 0 天用户必须修改密码,密码过期前 0 天开始提醒用户修改密码
☑ 用户	P必须修改初始密码(新建用户第一次登录必须修改密码)
☑ 密辞	必须包括 ✔ 数字 🛛 字母 🛑 特殊字符 (shift+数字)
- 田白石谷雪	
■ 用尸名束嘴	
🗌 用户名	不区分大小写
保存	



## 3.5.2 开启防暴力破解选项

防暴力破解可以避免恶意用户暴力破解 SSL 账号,入侵内网系统。

(1) 在『讥	认证设置』→『认证选项设置』→『密码认证选项』设置页面
控制台	>> 认证设置
▶ 运行状态	数字证书与C4中心。创建证书及证书申请等。》下载安装USB-XETY版計 》下载安装USB-XETY最入 や体
▶ 系统设置	
▼ SSL VPN设置	- 城单点登录认证 设置
> 用户管理	以实现域用户在客户端的自动登录,L2TP/PPTP的AD域认证和域安装控件功能.
> 资源管理	
> 角色授权	:" 辅助认证
→ 认证设置	
> 策略组管理	- 短信物証料 没置
> 终端服务器管理	在用户登录时结合短信验证码进行认证准入的相关设置,包括短信发送接口,验证码信息格式等内容.
▲ 企业移动管理	- 硬件特征码 设置
> 移动设备策略	会確性特征码认证的相关设置。句紙硬件特征码的炒售方式。特征码审批程度等
> 移动设备管理	
》 应用 树 选	· 元 本态令牌认证 设置
	动态令牌认证是Radius服务器的一种扩展使用.
> 端点安全规则	
> 端点安全策略	" 认证选项设置
> 内置规则库升级	
	- LDAP与Radius服务器认证优先级设置 设置
	当配置了多个LDAF与Radius认证服务器时,将依据该配置项中所设置的顺序优先级进行用户认证
	- 察到认证法师
	121. Z. YAB TI BARKA OGANA MARKA MARKA YAH MUNAKTIN MARKA MARKA MARKA MARKA MARIANA MARKA MARKA MARKA MARKA MA
▶ SC设置	🔮 - 匿名登录设置 设置
▶ IPSec VPN设置	■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
(2) 勾选	历暴力破解选项下的三个选项。
»» 密码认证选项设置	
用户登录时校验选项	
启用软键盘 《防止术	<b>に</b> 马记录雑盘输入信息)
- 字母键随机	变化 数字键随机变化
₿ 防止暴力破解选项	
☑ 佐徳惑悪機足。	
✔ 同名用户登录连续出	出错 5 (1-32)次后锁定用户 600 (30-1800)秒后恢复正常状态(仅针对本地用户有效)
✓ 同IP用户登录连续器	出错 64  (64-2048)次后拒绝同IP登录,并在 45   (30-1800)秒后恢复正常状态
1. 登录连续出错是指	两次登录错误间隔在45秒之内:
2. 同名用户登录连续	出错次数设置范围为1至32次:
3. 同IP用户登录连续	出错次数设置范围为64至2048次:
4.恢复正常状态时间	值设置范围为30至1800秒,0表示永久锁定,需管理员手动释放.
保存	取消