

华为云 vSSL 部署实施指导书



深信服科技股份有限公司



		修订历	使		
编号	修订内容简述	修订日期	修订前版本号	修订后版本号	修订人
1	华为云 vSSL 部署实施指导书	20191030	1.0	1.0	Qjj

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容,除另有特别注明,版权 均属深信服所有,受到有关产权及版权法保护。任何个人、机构未经深信服的书面授权许可,不得 以任何方式复制或引用本文的任何片断。





目录

第1章	需求背景	4
第2章	部署概述	4
2.1	华为云平台特性描述	4
2.2	镜像获取	4
2.3	部署方式	4
2.4	资源配置	4
2.5	授权方式	5
第3章	部署指导	5
3.1	云平台配置	5
	3.1.1 创建 CVM 虚拟机	5
	3.1.2 主机设置	8
	3.1.3 登录 vSSL	9
3.2	云组件授权配置	9
	3.2.1 在线授权	10
	3.2.2 申请试用	11
	3.2.3 vSSL 授权说明	.12
3.3	云组件配置	14
	3.3.1 SSL 功能配置	14
	3.3.2 IPSEC 功能配置	.19
第4章	常见问题	24



第1章 需求背景

目前大量用户为了减轻运维和数据不落地的需求采用了公有云托管业务,但是一直以来公有云 架构的安全防护方面一直处于劣势,需要借助第三方安全虚拟化组件来补齐短板。依托该需求 SSL 推出了基于华为云的安全远程接入解决方案,实现移动办公、混合云互联、分支与华为云互联、APP 安全接入等场景需求,解决客户痛点。

第2章 部署概述

2.1 华为云平台特性描述

- ◆ 底层架构为 KVM;
- ◆ 能够自定义安全规则;
- ◆ 支持绑定浮动 IP;
- ◆ 支持添加多块网卡;

2.2 镜像获取

vSSL 镜像已经上传华为云镜像市场,用户直接在华为云镜像市场搜索"深信服"就可以获取 相应镜像。

2.3 部署方式

vSSL 支持单臂模式部署,不支持集群部署,支持分布式集群部署。

2.4 资源配置

规格	配置参数	并发连接数	磁盘
vSSL-100	2 CPU,2G RAM	500	50G
vSSL-200	2 CPU,4G RAM	1000	50G
vSSL-400	4 CPU,4G RAM	2000	50G
vSSL-800	4 CPU,8G RAM	5000	50G
vSSL-1000	8 CPU,8G RAM	10000	50G

地址:深圳市南山区学苑大道1001号南山智园A1栋



2.5 授权方式

- 1、支持在线试用
- 2、支持在线授权

第3章 部署指导

3.1 云平台配置

深信服 vSSL VPN 是以系统镜像的方式提供的, 部署深信服 vSSL VPN 需要先提供一台独立的 ECS 主机来安装 vSSL VPN 镜像。

3.1.1 创建 ECS 虚拟机

登录华为云中国站,点击购买 ECS 云服务器。







出现以下选择页面。

计费方式根据实际的业务需求选择,暂不支持按需计费的方式。

深信服 vSSL 镜像仅上架到以下三个区域: 华南-广州、华东-上海二、华北-北京四。根据实际 情况选择区域。

需要选择业务虚拟机所在的 VPC。vCPU、内存参考【2.4 资源配置】,按照实际需求选择对 应的服务器,例如选择 2 核 CPU、2G 内存的云服务器。

注: 镜像市场的镜像不支持入门型主机实例。

费模式	包年/包月 按照	计费 竟价计费	0	用户	根据华为云特性根据实	际情况选择	
ŧ	华东-上海二	•		, 137		13/13/02234	
	不同区域的云服务产品之间内网互不相	1通;请就近选择靠近您业务的区域,	可减少网络时延,提高访问	速度。如何选择区域			
用区	随机分配 可用	区3 可用区2	可用区1	可用区4 ⑦			
格	最新系列 ▼	vCPUs 2vCPUs	▼ 内存 40	¥8 ▼	规格名称 Q	参考 vSSL 选型指导选型	
	规格名称	vCPUs 内·	≩ 1Ξ	CPU 1Ξ	基准/最大带宽 ⑦ ↓三	内网收发包 ⑦ ↓Ξ	规格参考价 ⑦
	C3ne.large.2	2vCPUs 4	GB	Intel SkyLake 6151 3.0GHz	1.3/4 Gbit/s	400,000	¥0.48//j\8₫
	C c6.large.2	2vCPUs 4	GB	Intel Cascade Lake 3.0GHz	1.2/4 Gbit/s	400,000	¥0.46//j\#j
	h3.large.2	2vCPUs 4	GB	Intel SkyLake 6146 3.2GHz	1/2 Gbit/s	300,000	¥0.55/小时
	hc2.large.2	2vCPUs 4	GB	Intel E5-2690V4 2.6GHz	0.5/1.5 Gbit/s	100,000	¥0.61/小时
	S2.large.2	2vCPUs 4	GB	Intel E5-2680V4 2.4GHz	0.2/0.8 Gbit/s	100,000	¥0.38//j\#j
	S3.large.2	2vCPUs 4	GB	Intel SkyLake 6161 2.2GHz	0.2/0.8 Gbit/s	100,000	¥0.36//j\8g
	s6.large.2	2vCPUs 4	GB	Intel Cascade Lake 2.6GHz	0.2/1.5 Gbit/s	150,000	¥0.36/小时

镜像在镜像市场中搜索"深信服"即可看到,选择"深信服虚拟 SSL/IPSec VPN 一体化镜像", 点击 确定 按钮。

【说明】国外华为云市场没有深信服 SSLVPN 镜像, 需要联系深信服工程师通过共享镜像的方式来提供。

存储选择按照需求选择高 IO、普通 IO、或是超高 IO,存储选择 40G 即可,不需要选择额外的数据盘。

镜像	公共镜像 深信服虚拟化SSL、IPS	私有镜像 SEC VPN镜像 ()	共享镜像	市场镜像 选择镜像	在市	场镜像选择深信服SSL
系统盘	高IO ④ 增加一块数据盘 您这	▼ 40 ▲ 40 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲ 50 ▲	9 + GB IOPS上開 F盘)	艮1,440, IOPS突发上	限5,000 ⑦	系统盘保持 40G 即可 不要扩大或缩小 无需添加数据盘



选择市场镜像

×

■ 所有镜像	深信服	×	Q
 • 基础软件 • 开发者工具 • 企业应用 • 专业服务 • 行业解决方案 • 网站建设 • 安全市场 	 規格:深信服虚拟化SSL、IPSEC VPN镜像 产品名称:深信服虚拟化SSL、IPSEC VPN镜像 描述:深信服虚拟化SSL VPN,安全、快速、稳定、易用、易管理, 9年市场第一,SSL、IPSEC 二合一VPN产品,市场占有率接近百分 版本:V3.0 操作系统:Linux 类型:网络安全 发布时间:2018/11/18 21:00:18 GMT+08:00 服务商:深信服科技股份有限公司 	¥0.00/ 月	
 ④ 物联网 ● API ● 域名服务 			
	備定取消		
择完成后,确认数量和费用	月, 点击 下一步 按钮进入下一步配置。		
実置 - 1 + 台 1个月 ◆ 2222.50 参考依約、具体和目着以次世界方法。	7%计查计指		F-#

3.1.2 网络设置

网络需要选择专有网络,安全组未配置默认进方向都是拦截,出方向都是放行的,若未定义则 会导致创建好云主机后无法访问的情况。所以需要在安全组中放通 TCP443 端口 (https 接入)、 TCP4430 端口 (控制台管理)、TCP51111 端口 (升级使用)、TCP22 端口 (后台维护),若有 http 接入需求也需放通 TCP80 端口。

网络 扩展网卡	vpc-907a(192.168.0.0/16) ▼ C subnet-407e(192.168.20.0/24) 幼園创建築的虚拟私有云、您可前往控制台创建。 ● 增加一块网卡 您还可以增加 0 块网卡	• c	自动分配PP地址 ▼ 自动分配PP地址 手动分配PP地址	^{可用私有IP設量250个} ⑦ 网络需选择专有网络VPC
安全组	SSL(入方向:- 出方向:-))	安全组可以理解为防火	墙规则



3.1.3 高级设置

为云主机命名,登录凭证设置一个密码密码即可,实际上后续无需使用此处密码,若有云备份 需求可以购买云备份服务,若没有可不购买。

云服务器名称	SSLVPN 允许重名
	购买多台云服务器时,名称自动按序增加4位数字后缀。例如:输入ecs,从ecs-0001开始命名;若已有ecs-0010,从ecs-0011开始命名。
登录凭证	密码 密钥对
用户名	^{root} 此处设置的密码实际上后续无需使用
密码	请牢记密码,如忘记密码可登录ECS控制台重置密码。
确认密码	
云备份	使用云备份服务,需购买备份存储库,存储库是存放服务器产生的备份副本的容器。 现在购买 使用已有 暂不购买 ⑦
高级选项	□ 现在配置
选择完成局	后,确认数量和费用,点击 下一步 按钮进入下一步配置。
购买量 - 1 + 台 1个月	
最后再一次	次确认配置信息,点击 立即购买 按钮创建 vSSL。

3	SANGFOR 深信服科技	会 深信服 SANGFOR S	智安全 SECURITY	ĩ	深信服,	让IT更简单,	更安全,	更有价值
1) #4121	i (2) Mårei							
配置	基礎配置	包举/包月 通用计算喷荡型 c6.large 2 2xCPUs 4GB	地域 链像	上海二 深稿服產與代SSL、IPSEC VPH積優 (深稿服產與代SSL、IPSEC VPN_	可用区系统盘	可用区4 液I0.40GB		
	國和私有云 高級配置 <u>2</u> 云燧务器名称	SSLVPN	<u>맞</u> 宝姐 登录凭证	Sys-default 문편	弹性公网IP	全动&BGP 计数方式 按带3	红行频 带宽: 5 Mbit/s	
购买时长		3 4 5 6 7 8 9	作月 1年 2年 3年					
购买数量	 ■ HAISSI () 1 + 又我已经阅读并同意 	您还可以创建200台云服务器。申请更多云服务器配额请单; 《华为 损保免责声明》	击申请扩 大配模 。					高い。
能置费用 ¥337	.50						Ŀ	·步 立即购买

3.1.4 登录 vSSL

部署完成后,在华为云的实例控制台可以看到创建好的 vSSL。

Ξ	云服务器控制台	ş	单性云服务器 ⑦					✓ 最新动态 □ ()	用指南 购买弹性云服务器
٢	总览		·····································						~
ස	弹性云服务器		D HIMMONTHINKING, MEMPINTHE, MEPP						^
707	安属主机		开机 关机 重量密码 更多 *				所有运行状态 * 名称 *	Q 标签报索 ※	C [] 🗐 😑
	裸金属服务器		名称/ID	可用区	状态	规格/镜像	IP地址	计费模式	操作
0	云硬盘		SSLVPN	可用区3	 运行中 	2vCPUs 2GB t6.large.1	139.9.213.232 (弹性公网) 1 Mbit/s	按需计费	远程登录 更多 ▼
•	专属分布式存储	•	fc0b40a7-ed0a-48f3-b3ff-e57cd422142d			copy_cn-north-1_M763_SP_DHCP	192.168.20.87 (私術)		
\odot	镜像服务								
4	弹性伸缩	e -							

通过分配的公网 IP, 例如 https://139.9.213.232:4430, 即可登录到控制台, 控制台帐号密码 默认为 admin/admin。

< > Ċ ☆ □ ☆ https://139.9.2	13.232:4430/cgi-bin/login.cgi?requestname=2&cmd=0	▼ 前往 > 🔤 ▼ 在此搜索	< @ ⊻ %• ⊃• & … ≡
	SANGFOR	③ 中文 English	
	#EEE茶 : 400-630-6430 如何告別 视频会议马赛克 正 正 上 四 行为管理 微信认证测试指导	SSL VPN 用户名 二 京码 日本名 成本信息	
c 200	4-2018 译在图448580/所有		Hereite

3.2 云组件授权配置

vSSL 授权分以下为三种,使用云主机只需关注"在线授权"和"申请试用"即可。



- ▶ 在线授权:需要先购买获得序列号,然后将序列号信息填写到对应的位置
- ▶ 本地授权服务器授权:需要在本地搭建一个授权服务器 (VLS),使用授权服务器对 vSSL 来授权。
- 申请试用:只要填写申请信息即可通过短信方式获得授权序列号,把序列号填入【在线授权】即可,使用此序列号可以免费试用 30 天。

【在线授权】与【申请试用】都需要 vSSL 能够连接互联网,与 vls.sangfor.com.cn 的 443 端 口保持通信。

	6.1 系統總非結果既犯。如何使用以下经 在就開放 本地級内閣防器開放 非	方式获得授权: 请试用	▲ 发始求助 ↓ ■ 在线路角 【社区疑问、	淡料撮索 Q 🏠 admin 🔻 査告茶
控制台	系统状态 在线用户 告聯日志 远端应用 加减反极			
▶ 运行状态	制新闻器 10秒 ▼ 参立即刷新 畅选择模块 ▼			系统时间:2019-10-14 15:04:9
▶ 系統设置 ▼ SSL WWW である	1、 请信达超级管理员差码 组织管理员使研究力相信完局、为保障系统安全。通力即将改变用力和位则上			
> 用户管理	Sidam	6902 H-X		×
> 淡源管理	Apprilia A	1492 TPithit	安洋	放 的
> 角色接投	100 CPU使用记录-当前:0%	35281 192.168.19.13	3.58bps	4.5Kbps 正常
> 认证设置	80			
, washinenia	40 / / / / / / / / / / / / / / / / / / /			
· MONETAL BALL	20			
/ 於靖康所苔言理	0 15:00:30 15:01:00 15:01:30 15:02:00 15:02:30 15:03:00 15:03:30 15:04:00 15:04:30 (0) 15:04:30			
* ENM 18/15/0-8-98/82	(1.00000.0)			
> 移动设备管理		Mall much state. where it		
, 应用高店	(*PerdetTat * 9,0), 526*1 0 X	开发用户题号 " 头时		e x
) 应用封装	13/p.s 280	1	授权数:0,历史最高:0 (2016-04-05 02:18)	
▲ 議点安全	200			
> 端贞安全规则				
> 端贞安全策略	50			
> 内置规则库升级	0	0 15:00:00 15:00:30 15:01:00 1	5:01:30 15:02:00 15:02:30 15:03:00	15:03:30 15:04:00 15:04:30
	— 下行:0.5 128ps — 上行:0.4 138ps	—— 在线人数:0		
	#发会话题 - 实时 0 ×	流爆存状态 - 英时, 20间总流速对比		0 ×
	600	KBps 0.05	加速服务未授权	
	500	0.04		
	300	0.03		
	200	0.02		
		0 15:00:00 15:00:30 15:01:00	15:01:30 15:02:00 15:02:30 15	03:00 15:03:30 15:04:00 15:04:30
	— 会選款 509		8:0.0 13px	
→ SC设置				
▶ IPSee VTR设置				
▶ 防火墙设置				
 系統維护 				
-	R			

3.2.1 在线授权

在线授权需要填写授权 ID 和序列号,请联系当地销售或致电 400-806-6868 进行咨询购买。 点击控制台的在线授权,将购买的授权序列号填写到对应位置,提交后等待设备进程重启后即可变 为授权状态。

SANGFOR SSL NT.	.6.1	系統過未获得授权,忽可使用以下任息 在线授权 本地授权服务器授权 申	方式获得授权: 请试用	▲ 发船来	助 📗 在线咨询 🤇 社区疑问、		、admin▼ (查答和助)	
控制台	系统状态 在线用户 告輩曰志 远程应用 1990授权							
> 运行状态	\$1\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$					系統	前月:2019-10-14 16:19:26	
▶ 系统设置	1、请修改超级管理员密码							
▼ SSL VPW设置	超级管理员的密码为初始密码,为保障系统安全,请立即修改密码为时位以上							
> 用户管理	系统信息	×	线路状态				×	
> 資源管理	CPU使用记录_当前:7%		1538	IP地址	发送	接收	状态	
> 角色授权	100 000 0000 0000 0000	在刻用户数:0 (遊 覧)	组路1	192.168.19.13	1.23bps	4.2Kbps	正常	
> 认证设置	60	方线后的女具	~	1				
> 解释组管理	40	125035CTO HI	^					
> 终端服务器管理		 授权ID和序列号请联系当她销售或致电400-006-6868进行 	谘询购买。					
4 EM	16:16:00 16:16:30 16:16:00 16:16:30 16:17:00 16:17:30 16:10:00	• 试用产品,请先申请免费试用以获得授权10和序列号						
> 移动设备编唱								
> 移动设备管理	网络吞吐量 - 突时,结路#1	费权ID: T565F-1					e x e	
) 成用刻装	13p 5 140	序列号: AC46-C10 100 0015 170 2-0780 授权数:0,历史最高 0 (20			,历史最高:0 (2016-04-05 02:18)	016-04-05 02:18)		
▲ 潮点安全	120							
> 識点安全規则	80 60	1、在线接权需在系统造网的情况下才能进行。						
> 議由安全策略	40	2、通过在线授权的系统需要系统保持连网状态,否则一段时	间后系统功能将会受					
> 内置规则库升级	0 16:14:30 16:15:00 16:15:30 16:16:00 16:16:30 16:17:00	- R.		00 16:15:30 16:16:00 16	16:30 16:17:00 16:17:30	16:18:00 16:18:30	16:19:00	
	- 下行 0.5 18ps - 上行 0.1 18ps	3、授权II和I序列号只能在一个系统中使用,如您的授权II和 使用。連絡面系结由的原机TI和IE和IF#N除之后再使用。	席列号已经在其它地方					
		POOL INTO CONTRACTOR OF STREET, STREET						
	开发会说到一头的	報定	取消	民黨運行民	4/08/09/19 + 18240		0 X	
	400				JULE MAY THERE			
	300		0.04					
	200		0.03					
	100		0.01					
	16:14:30 16:15:00 16:15:30 16:16:00 16:16:30 16:17:00	16:17:30 16:18:00 16:18:30 16:19:00	0	16:14:30 16:15:00 16:15:30	16:16:00 16:16:30 16:1	7:00 16:17:30 1	6.18:00 16:18:30	
	— 並結款 303		- Alleni:0.0 KBps	— 加速后 0.0 33ps				



授权成功后在授权信息页面会有【更改授权】、【删除授权】和【授权服务器授权】三个选项。 【删除授权】和【授权服务器授权】都是删除掉当前的授权信息,使设备变为初始化状态;【更改 授权】则是将新的序列号覆盖掉当前的,授权 ID 不会更改。

授权信息	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	
- 基本	信息							
授权 授权	2类型: 在线授 2用户: 分支	权(商业版)						
授权授权	(ID: S1234-56 (序列号: 2F9B	78-90AB-CDEF-1 -910D-7573-7FF	234-5678-90AB-C) 5-13E4-29FC-2D9)	D55 F-2ADF				
软件	÷使用有效期至: 2.授权 删除授权	2017-11-03 切换成"授权用	服务器授权"					

3.2.2 申请试用

点击 申请试用, 填写对应信息。

姓名:	*
手机号码:	* 获取验证码
短信验证码:	*
公司名称:	*
产品用途:	* 200字以内,如公司用于监管上网行为 🗙
	我们会优先处理填写有真实产品用途的试用申请 产品用途不能为空
推荐人:	
推荐人电话:	
	我们会优先处理填写有推荐人信息的试用申请
	提交申请

【姓名】、【手机号码】、【短信验证码】、【公司名称】和【产品用途】是必填项,提交申 请后,会有审核人审批,审批完成后,会收到授权 ID 和授权序列号,把授权 ID 和授权序列号填入 【在线授权】,填写成功后控制台会有提示:您还可以免费试用 30 天,您可以使用【在线授权】 或【本地授权服务器授权】。



重新登录 vSSL 控制台,系统就会显示可以免费试用 30 天。

	.6.1	念近可以免费试用×天・参可以使用 在纵振仪 素 本地探び部外装置仪 金 法定部 社区経河・美料批素 Q ▲ admin ▼ 室谷志助
控制台	部署模式 多线路 路由设置 Hosts DEEP 本地子网	
 >> 运行状态 ▼ 系统设置 	- 内网接口	
 · 지역2품 · 이성振振 · 日间计划 · 位置管理 · 位置管理 · 首届現泉休号 · 조利285页 · 不利285页 · 丙利646%前代 	LAR WC: 17時間: 102:100:10:13: 子科規範: 105:00:00 0 発い現象: 100:100:2:18 合規範: 100:100:18 合規範: 100:100:18 合題[100:100:100:18] 合規範: 100:100:18 合題[100:100:100:18] 合題[100:100:18] 合題[100:100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合題[100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18] 合][100:18]	
 ● 聖茶和助 > 貫作的著 > 分布式部署 > 否約卡管理 		

3.2.3 vSSL 授权说明

授权成功后, vSSL 控制台有授权客户和授权有效期的提示。

	5 授权用户:深信服测试专用;有效时间至:2	018-04-01 社区疑问、资料搜索 Q
控制台)运行状态)系统设置 ~ SSL VPR设置	系统状态 在线用户 告警日志 远程应用 EMM授权 刷新间隔 10秒 全立即刷新 《选择模块 + 请修改超级管理员密码 超级管理员的密码为初始密码,为保障系统安全,请立即修改	
 「ハノーミュ 茨源管理 角色授权 认证设置 策略组管理 终端服务器管理 2000 42000 	未续信息 × 100 CPU使用记录-当前:20% 40 60 40 60 40 60 40 60 40 60 40 60 40 60 40 60 40 60 40 60 40 60 55 CPU服务: 运行中 64 64:56	
 移动设备管理 应用商店 应用封装 端点安全 端点安全规则 端点安全策略 内置规则库升级 	阿銘吞吐里 - 実时, 线路#1 ④ X KBps 400 300 200 ● (本) 100 ● (本) 0 ● (本)	并发用户组织 - 实时 1 授权数:50,历史最高:0 (2018) 0 01.15



查看【系统设置】-【系统配置】-【授权信息】页面,即可显示授权信息

授权信息	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	
二 基本	信息							
授权	Q类型: 授权服	务器授权						
授权	2月户: 许文锋							
软件	‡使用有效期至:	2018-04-20						
切掛	美成 "在线授权	"						
: VPNS	受权模块							
SSL	VPN 用户总数:		10		4			
IPS	ec VPN 移动用户	•数:	0		0			设置
线路	各数:		4		1			
分支	5机构数:		4		~			
远移	星应用用户数 :		20		1			
跨速	运营商:		已授权		1			
单点	ē登录:		已授权		4			
短信	言认证:		已授权		4			
流缓	爰存:		已授权		1			
单边	b加速:		已授权		1			
集郡	¥:		已授权		4			
EMM	夏权模块							
版	本: EMM高级)	版						
授	权数: 10							
功	能: 📀 SSL	VPN安全接入		📀 EasyApp	-SDK接入		0	自动封装SSLVPN接入
	🥑 落地	文件加密		📀 应用统-	-入口		0	双域安全隔离
	😒 单点	登录		📀 安全数	剧察除		0	设备行为管控

若因为某种原因(网络不可达等),连续7天未收到授权服务器的心跳信息,此时 vSSL 从授权切换到非法状态,非法状态时控制台不可配置业务,但原有的业务还可以继续使用。非法状态的设备登录后在首页头部有非法状态的提示。

	FOR S	深信服智安全 SANGFOR SECURITY			深信	服,让ITj	更简单,	更安全,夏	更有伯
	17.5-vSSL	日子元 所有止	法连接网络,系统未能持续获得 务将在30天后中断,重试	裴授权,部分功能 习	石川, 在线咨询 (社区	疑问、资料搜索 Q	adı	nin ▼ 查看帮助	
制台	系统状态 在线用户 告警日志	远程应用							
运行状态	刷新间隔 10秒	▼ 🛸立即刷新 🍕选择模块 ▼					系统时间:20	16-11-05 12:59:02	
> SSL VFB运行状态	请修改超级管理员密码 超级管理员的密码为初始密码,为	罪障系续安全,请立即修改							
	系统信息		×	线路状态				×	
	CPU使用记录	_当前:27%		线路	IP地址	发送	接收	状态	
	100	- = 119.2170	在线用户数:0 [查看]	线路1	11.11.137.92	192bps	137.8Kbps	正常	
	80		(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	线路2				禁用	
	60		待审批特征码:0 [管理]	线路3	terre.	1		禁用	
	20 0 12:54 1	2:58 12:58	SSL VPN服务:运行中 停止服务	SADE .				787.03	
	网络吞吐里 - 实时,线路#1		@ ×	并发用户趋势	- 实时			(a) (X)	
	1355 60 40 0 12:54 12 54 12 747.16.8 Ибря	55 12.56 12.57 一上行.0.0 路ps	12:58 12:5	1 0 一 在线人赖	授权数:50,历5 12:54 12:55 (0	22.56	14:29)	58 12:5:	
7/2-10 m	并发会话数 - 实时		@ X	流缓存状态 -	实时, 双向总流速对比			۵×	

导致非法状态的原因有序列号过期、授权资源与实际资源不匹配、序列号被禁用、序列号失效 等,在控制台头部都会有对应的提示信息。

如果非法状态的设备经过 **30** 天还是没有收到正确的授权则都会变为初始化状态。由于设备是 由已经授权过的设备转变为初始化状态,因此将不会再有免费试用的选项。



3.3 云组件配置

3.3.1 SSL 功能配置

3.3.1.1 用户环境与需求

A 公司在华为云上部署了若干业务服务器,公司内部的业务人员需要访问其中的销售系统,公司内部的运维人员需要访问数据库服务器。



3.3.1.2 设备配置步骤

配置步骤如下:

第一步:进入『SSL VPN 设置』→『用户管理』,点击<u>新建</u>,新建两个 SSL 接入用户,配置 完以后点保存,本案例配置界面如下:

控制台	→ 新建用户							
▶ 运行状态	基本属性					标记*的	为必须填写项目	
 ▶ 系统设置 ▶ 系统设置 ▼ SSL YP+设置 > 用户管理 > 资源管理 > 角色质权 > 认证设置 > 就職相管理 > 终端服务器管理 > 端点安全规则 > 端点安全规则 	基本萬性 名称: 描述: 密码: 确认密码: 手机号码: 所属组: OTF密钥:	张三 业务人员 ●●●●●●● / / / 继承所属组认证选项和翰 ☑ 继承所属组接入策略约	* 	数字证	E书/USB-KEY: 无 生成证书 虚拟IF: ● 自动获取 过期时间: ● 永不过期 账户状态: ● 启用 离线访问: 接入策略未成	 标记·493 导入证书 手动设置 手动设置 手动设置 算用 明离线访问 	め必須慎与项目 ②提USB-KEY 0.0.0 2020-11-20	
> Intel ¥ = 2444	: 认证选项 账户类型: 主要认证 ✓ 用户4	 建築所属組认证选项 公有用户 私有用户 私有用户 私有用户 		辅助认证 硬件特征码 短信认证				
▶ IPSec VPN设置		AUE	~	动态令牌	TOIP			

第二步:进入『SSL VPN 设置』→『资源管理』,新建一个 TCP 应用。点击新建,选择 TCP 应用,设置资源名称,选择资源类型,配置界面如下:

SANGFOR 深信服科技	会 深信服智安全 SANGFOR SECURITY	深住	言服,让IT更简单,	更安全,更有价值
控制台	»»编辑TCP应用资源			
▶ 运行状态	基本属性			
▶ 系统设置				
▼ SSL VPN设置	名称:	销售系统	*	
> 用户管理	描述:			
> 资源管理	类型:	HTTP]	
> 角色授权	+++++++-			
▶ 认证设置	NOVE -			
> 策略组管理			2	
> 终端服务器管理				
 ▲ 端点安全 > 端点安全规则 	。 应用程序路径:			
> 端点安全策略		程序路径可以使用绝对路径也可以使用环境变量。例	刘女D%windir%	
> 内置规则库升级	所属组:	默认资源组 >>		
	图标:	示何 <u>■</u> この日 支 (2)		
		✓ 允许用户可见		

配置资源地址,点击后面的<mark>添加</mark>按钮,配置完后点击确定,配置界面如下:

添加/编辑资源地址	×
单个添加 批里添加	
域名资源,请检查是否配置好域名解析 内网域名解析	
● 单一IP地址或域名 ○ IP地址段	
IP/城名: 10.87.23.123 *	
端口范围: 80 到 80 *	
🗌 启用资源地址伪装	
确定	取消

第三步:角色关联,即将资源和用户关联,进入『SSL VPN 设置』→『角色授权』,点击新建,选择新建角色,配置角色名称,选择关联用户,界面如下:

SANGFOR 深信服科技	② 深信服智安全 SANGFOR SECURITY		深信服,让	T更简单,	更安全,	更有价值
控制台	>> 新建角色					
 > 运行状态 > 系统设置 	= 基本属性					
 SSL VPN设置) 用户管理 > 资源管理 , 角色授权 > 认证设置 > 试证设置 > 策略组管理 > 终端服务器管理 > 端点安全 > 端点安全规则 	角色名称: 业务 描述: 可以 关联用户: 角色准入策略: ✓)	:人员 【访问销售系统 自用该角色	* 	受权用户 已進入策略		
 > 端点安全策略 > 内置规则库升级 	 → 编辑授权资源列表 名称 	类型			描述	

关联用户,点击后面的选择授权用户按钮,配置完后点击确定,配置界面如下:

适用用户		×
请输入搜索的关键字 👂 🗟 🛙 🗉		睛输入搜索的关键字 🔎
	名称 🔺	类型
🔤 🗆 🚰 默认用户组	🔲 🤷 默认用户组	用户组
	🗹 🚨 张三	用户
	🔲 🚨 李四	用户
	▶ 🛛 🗍 🗍 🗍 🖓 萬	页显示 25 条记录
		定取消

进入『编辑授权资源』页面,选择关联资源,界面如下:

SANGFOR 深信服科技	服智安全 For security	深信服,让IT更简单,更安全,更有价化
编辑授权资源列表		×
请输入搜索的关键字 👂 📴 🗉		请输入搜索的关键字 🔎
🕒 🔲 📥 全部资源	□ 资源名称 ▲	描述
🔲 🖳 🔛 默认资源组	🔲 쿋 L3VFN全网资源(或服务)	可以访问LAN口、DMZ口以及
	☑ 📰 销售系统	
	🔲 🎫 数据库	
	4	
	▶ 4 第 1页,共1页 ▶	▶ 25 条记录
		确定取消

配置完以后点保存.

第四步:配置完成后点击【立即生效】,使配置生效。

控制台	🔔 配置已更改,但还未生效,点击"立即	吐效"按钮以应	如果我的配置。		立即生效
▶ 运行状态	>> 角色管理				
▶ 系统设置	🔾 新建 🕶 🤤 删除 📝 编辑 🛛 🐼 选	择 • 🗸 生成	权限报告	按名称 → 请输入搜索 >	长健字 👂
▼ SSL VPN设置	□ 角色名称	描述	授权给		状态
> 用户管理	🔲 🍐 运维人员	允许访	李四		1
> 资源管理	🔲 🍐 业务人员	可以访	张三		*
> 角色授权					
→ 认证设置					
> 策略组管理					
> 终端服务器管理					
⊿ 端点安全	4				
> 端点安全规则					
> 端点安全策略					
> 内盂规则库升级					

第五步:用户在浏览器上输入 SSL 的登录地址,登录界面如下:





登录SSL VPN

用户名:		
密 码:		
	登录	

其它登录方式: **证书登录 USB-Key登录** 下载USB-Key驱动 <u>手动安装组件</u> 下载svpntool工具

第六步:输入用户名密码登录 SSL,便可以看到资源列表,界面如下:

这时,用户就可以访问被关联的资源了。

3.3.2 IPSEC 功能配置

3.3.2.1 用户环境与需求

A 公司在华为云 VPC 专有网络里部署了一个灾备中心,希望通过公司总部内网部署的深信服 VPN 设备与华为云上的深信服 VPN 设备建立一个 IPSec VPN 隧道,将公司内部机房的数据同步到 灾备中心。

3.3.2.2 设备配置



公司总部防火墙上的配置

由于公司总部的深信服 VPN 设备接在内网, 且该设备做 VPN 连接时是以总部部署, 所以需要 在前置防火墙上将公网 IP 的 TCP/UDP 的 4009 (默认端口) 端口映射给 VPN 设备。

公司总部三层交换机上的配置

添加到华为云 VPC 专有网络网段的路由,下一跳指向深信服 VPN 设备,将数据交由深信服 VPN 设备进行封装处理。

总部 VPN 设备上的配置

第一步:配置 WEBAGENT,进入『IPSEC VPN 设置』→『基本设置』,设置好主 webagent 信息,MTU 和最小压缩值默认即可,监听端口采用默认值,其中,主 webagent 配置成"防火墙映射的公网 IP 地址:4009"。

4 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			Ű1
È WEBAGENT:	200.11.22.33:4009	修改密码	
备份WEBAGENT:		修改密码	
MTV 值(224-2000):	1500	共享密钥	
最小压缩值(99-5000):	100		
VPN监听端口(默认为4009):	4009		
☑ 修改MSS (仅在UDP传输时有多	女)		
 直连 C 非直连 			

第二步:为分支建一个 VPN 账号,进入『IPSEC VPN 设置』→『用户管理』,新增一个 VPN 账号,选择类型为分支,配置界面如下:

用户名:	test		认证方式:	本地认证			
密码:	•••••		算法:	AES		•	
确认密码:	•••••		类型:	分支		•	
描述:			用户组:	非组用户		•	
				🔲 使用约	且属性		
□ 启用硬件	捆绑鉴权	硬件证书:					
	r	DKRY ·					
		DELT.					
■ 启用虚拟	,IP	虚拟IP:	0.0.0.0				
(效时间:	全天 👤						
🗌 启用过期	时间	过期时间:	0-00-00		0 : 0	: 0	
自用用户		Г	启用网上邻居		☑ 启用压约	ì	
接入总部所	后禁止该用户上网	a 🗆	启用多用户登	录	□ 禁止在約	能修改密码	

第三步:新增本地子网,宣告总部需要进行 VPN 互连的网段,进入『系统设置』→『网路配置』→『本地子网』,新增总部需要进行 VPN 互连的网段,配置界面如下:



×
*
Travil

部署模式 多线路 路由设置 HOSTS DHCP 本地子网	
◎新増 - 🤤 刪除 📓 编辑	如何配置本地子网
□ 子网网段	网络掩码
172.16.1.0	255. 255. 255. 0
172.16.2.0	255. 255. 255. 0
172. 16. 3. 0	255. 255. 255. 0

以上步骤结束,总部配置完成。

华为云深信服 VPN 设备的配置:

建立 VPN 连接,进入『IPSEC VPN 设置』→『连接管理』,新建一个连接,填写总部设置的 WEBAGNET,总部建的 VPN 账号,界面如下:

ľ		33 Q 12			
	总部名称:	VPN			
	描述:				
	\pm Webagent:	200.11.22.33:4009			
	备份Webagent:		测试		
	数据加密密钥:			<i>e</i>	
	确认密钥:				
	传输类型:	VDP 💌			
	用户名:	test			
	密码:	•••••			
	确认密码:	•••••			
	🗌 跨运营商	低丢包率 💽 丢包率:	10 %		
	☑ 启用				

以上配置结束后, 华为云 VPN 设备与公司总部的 VPN 设备就能够建立 IPSec VPN 隧道, 但是此时两边的服务器通信还是无法实现的, 还需要进行下一步的配置——在华为云 VPC 虚拟路由器上 配置路由。

在华为云 VPC 虚拟路由器上配置路由

在华为云 VPC 虚拟路由器上添加目的网段是公司总部内网网段的路由,下一跳指向深信服 VPN,目的在于把 VPC 网络指定目的 ip 组的流量引流到深信服 VPN 上,将数据交由深信服 VPN 进行封装处理。

\bigcirc	虚拟私有云,vpc-907a			C
网络控制台 ^{总宽} 虚拟私有云	名称 vpc=907a ✔ 10 c03199aa-a704-43bd-a021-8ccd2a0573f2 子所介数 3 个	× # 添加路由信息 2.168.0.016 ダ 目的地址 172 - 16 - 2 - 0 / 24 ⑦		
访问控制	子网 路由表 拓扑图 标签	下一跳地址 192 . 168 . 20 . 87 ⑦		
弹性公网IP和带宽 ~	自定义路由表			
NAT网关	添加路由信息	确定 取消		C
弹性负载均衡 ~	目的地址	下一跳地址	操作	
对等连接	172.16.1.0/24	192.168.20.87	修改删除	
VPC 终端节点 ~	对等连接路由表			
虚拟专用网络 ~	目的地址	下一跳地址	操作	
云专线				
云连接 ~				20

至此,公司总部内网的服务器就可以与华为云上的服务器进行通信,实现数据的同步。



1. vSSL 授权不成功怎么办

答: 先查看提示信息。检查项主要包括: 网络是否可达, 授权的序列号信息与设备资源是否匹 配、序列号是否已经导入授权服务器数据库表等。

2. 为什么 vSSL 使用一段时间后授权失败了

答: 可检查下网络是否可达, 授权是否被删除, 或授权有效时间是否已过期等。

3. vSSL 开机非常慢怎么办

答: 通常情况下是主机的内存和 CPU 不足导致。

4. 授权成功、删除授权、切换授权后登录控制台,头部显示不全、提示断网怎么办

答: 授权的状态在切换的时候后台会有很多进程进行重启, 控制台登录后有些进程可能还没有重启完成导致, 可以在设备切换状态后等待一段时间再登录, 如果头部显示不全可以刷新几次。

5. 是否包含 EMM 功能

答: 包含

6. 是否能够升级

答: 可以