

IPsec VPN

V2.0 版本 操作指南

西安金箍棒信息技术服务有限公司

西安市碑林区雁塔北路 67 号红锋商务大厦 4 层

目 录

一、商品说明1
1、版本说明1
2、安全加固1
二、操作指南1
1、VPN 信息1
2、安全组开放相应的 UDP 端口 500 和 45001
3、登录操作系统修改 ipsec 配置文件2
4、重启 VPN 服务进程4
5、Windows 客户端配置4
6、Linux 客户端链接 6
7、IOS 手机客户端链接 9
8、安卓手机客户端链接13
9、链接使用13
10、用户管理14
11、环境说明
12、服务的启动以及关闭18
13、常规错误如何排查19
三、技术支持
1、售后服务
2、服务范围

一、商品说明

1、版本说明

此镜像为 IPsec VPN 镜像 V2.0 版本,系统: Aliyun (兼容 CentOS),更新 时间 2024 年 8 月。您可以一键快速搭建自己的 IPsec VPN 服务器。支持 IPsec/L2TP 协议。

2、安全加固

为进一步提升云服务的安全性,我公司对镜像产品实施了全面的安全加固, 共计完成 88 项基线加固措施。这些精细化的安全改进,不仅确保我们的镜像产 品严格符合等保 2.0 的安全标准,更在防御外部攻击、内部漏洞修复、数据加密 保护等多个安全维度上实现了显著增强,为您的数据的安全存储与业务的平稳运 行提供坚实保障。选择我们的镜像产品,意味着您将获得一个经过深度安全加固、 符合高标准安全要求的云端解决方案,让您的业务在安全的护航下稳健运行。

如您的业务环境有其他安全需求,请与客服联系,我们可为您提供一对一定 制服务。

二、操作指南

1、VPN 信息

包含四部分,公网 IP 地址、PSK、用户名、密码。

Server IP: VPN 服务端 IP 地址(阿里云公网 IP 地址)

IPsec PSK: BZyAmPwijTHyfU4DyBYN

Username: vpnuser

Password: Y23KKbnNyBd56HJq

2、安全组开放相应的 UDP 端口 500 和 4500

点击阿里云 ecs,点击安全组,入方向,手动添加



器 ECS Q	云服务器 ECS / 安全组 / sg-22e219e597oxOmbsy18d			
	← sg-2ze2t9e597ox0mbsy18	Ł		
	X TRIMIN X03/346 Herold In			
排查	基本信息 ^			⑤ 添加ClassicLink安全组规则
	安全组D sg-2ze2t9e597ox0mbsy18d ①	安全坦名称 金翅樺安全坦 <i>之</i>	同路 vpc-2ze9w60r0iyhakjbzpb88 [)	9
1	坦内连通策略	安全组类型	创建的问	
(RR I	组内互通 標改組內阿德進通策略	普通安全组	2023年6月29日 10:20:41	
	福述 金雞棒安全坦 之	资源组 rg-acfm3unj4nct4ua [提改	振器 未認定服器 企	
t	访问规则 上导入安全组织则 上导出 ② 健康检查			
	入方向 出方向			
ĸ	快速添加 手动添加 Q 输入端口或者授权对	b进行搜索 不合并展示	◇ 教我記靈規则	
	授权策略 优先级 ⑦ 协议类型	調口范围 ① 授权对象 ⑦	個述 创建时间	19412

允许 UDP、端口 500 和 4500、允许所有 IPv4,保存即可。

访问规则 上 入方向	导入安全组规则 出方向	」 号出 ◎健康检查					
快速添加	手动感加	Q、输入端口或者授权对象进	行搜索	不合并展示	~	教我配置规则	
授权策略	优先级 ①	协议类型	端口范围 ③		授权对象 ②	描述	点畫保存即可
允许 ∨	1	自定义 UDP	✓ * ■89: 500	/500 ×	* 源: 所有IPv4(0.0.0.0/ 0.0.0.0/時先許或后 何,设置时请务必遵	0) X	保存一预览 删除

IZZZE.	59uwj59zx:	siouszingz ·	● ÆIJŦ						ALCOLOGICA -	-		
实例详情	监控 安全组	快存储 (云盘)	快照一致性组	快照	弹性网卡	定时与自动化任务	5 操作记录	健康诊断	事件			
内网入方向会	全部规则内网	出方向全部规则 安	全组列表									
优先级	授权策略	协议类型	目的端口范围			授权对象	所屬安全组		描述			
100	⊘ 允许	UDP	4500/4500			0.0.0/0	sg-2zegeu1b9hjz2v	37btkl	System	created ru	ile.	
100	◎ 允许	UDP	500/500			0.0.0.0/0	sg-2zegeu1b9hjz2v	37btkl	System	created ru	ile.	
100	② 允许	TCP	RDP(3389)			0.0.0/0	sg-2zegeu1b9hjz2v	37btki	System	created ru	le.	
100	② 允许	ICMP	全部(-1/-1)			0.0.0.0/0	sg-2zegeu1b9hjz2v	37btkl	System	created ru	ile.	
	0.015	200				0.0.0.0		271.44			12	

3、登录操作系统修改 ipsec 配置文件

使用(Crt、putty、xshell等远程工具进行链接)

选择 ssh 协议、输入公网地址以及账户名密码,进行远程链接。





🔚 10.0.04 - SecureCRT	
File Edit View Options Transfer Script Tools Window Help	
🏗 💱 🕼 🔏 Enter host <alt+r> 🛛 🗅 🖹 👫 🖓 🔂 🚰 💥 📍 🕻</alt+r>	
Session ivianager	
🗐 🔂 🕺 💁 🛝 🗡 🚰 🏦 🎽 📕 Failed	
TASK [8.7]	
A 10.0.5 Pass	
	ew Session Wizard
-3 158.1.1.156 TASK [8, 8]	This wizard will help you create a new session for connecting to a
A 158.1.1.158 [检查邮件传输代理是	remote server.
	What type of connection do you want to establish?
	P <u>r</u> otocol: SSH2 ~
172.29.68.15 Pass	
172.29.68.4	
- 過 192.168.16.161 [检查SETroubleshoon	
192.168.253.1	
192.106.253.2 3 192.168.254.17 DLAV DECAR	
- 3 192.168.254.19 Total Policies	
- 3 192.168.254.21 Total Policies P.	Do not use this wizard when creating sessions
Total Policies E	
A 47.92.23.162	下一页(N) > 完成 取消 01
fws-crm [root@docker benchmark	
- 過 fws-毎超 [root@docker benchmark	
× 10004 ×	
Falleu	
TASK [8.7]	
[检查密码字段是否不为空]	
Pass New Session Wizard	X
TASK [8 8]	
「检查邮件传输代理長	What is the name or IP address of the remote host?
Pass	The user name can be left blank. 公网IP地址
	Hostname
IASK [8.9] 「松本CPC kovr 目不可	
L检查GPG KEys是否面	Port: 22
	<u>F</u> irewall: None ~
TASK [8.10]	
L检查SETroubTeshoo	Username: 田户名root
Falleu	
PLAY RECAP	
Total Policies	
Total Policies P.	
Total Policies F	下一步
Result file: : /	
[root@docker benchma	
[root@docker benchmark]#	
[root@docker benchmark]#	
[root@docker_benchmark]#	

双击链接即可

修改 VPN 配置文件 IP 地址为 vpn 服务端 ECS 公网 IP 地址

vi /etc/ipsec.conf





4、重启 VPN 服务进程

service ipsec restart

```
[[root@vpn ~]#
Redirecting to /bin/systemctl restart ipsec.service
[root@vpn ~]# AC
```

5、Windows 客户端配置

点击开始按钮进行搜索 VPN, 到达 VPN 配置按钮(不同的系统或许有差异,

以win11为类)。

Q vpn 设置			
← 全部 应用 文档 网页	设置	文件夹 照片 ▶	
目注示되 此にここれ			
VPN 设置 系统设置			
应用		VPN 设置	
Fix_ VPN _Error_809_Windows_Vi sta_7_8_10_Reboot_Required(1).	>	<u> </u>	
Fix_ VPN _Error_809_Windows_Vi sta_7_8_10_Reboot_Required(2).	>	17 打开 从网站获取快速帮助	
≸ 启动EasyConnect	>	正在设置 VPN	
设置			

(VPN 登录信息在公告页面上面)

添加 vpn 链接

西安金箍棒信息技术服务有限公司



← 投置		
Administrator 本地能户	网络和 Internet > VPN	
直接設置 Q	VPN 连接	添加VPN
🧾 系统	所有 VPN 连接的扁极设置	
3 蓝牙和其他设备	会许通过共活用计规约网络进行 VPN 连接	
💎 网络和 Internet	2091 @2232/massi puttyr954213 **** 2218	
🥖 个性化	☆许温游时进行 VPN 连接	=
1 成用		
<mark>鲁</mark> 帐户		
🔊 मंगिकांस्तेत्र		
3. 新式		

公网信息, PSK 信息输入, 然后输入账户名密码

网络和	Inter	添加 VPN 连接		
		VPN 提供商		
VPN 连接		Windows (内置)		
		连接名称		
所有 VPN 迫	接的高级设计	test		
允许通过	按流量计费的	服务器名称或地址		
		ecs公	网IP地址	
允许漫游	时进行 VPN į	VPN 类型		
		使用预共享密钥的 L2TP/IPsec	- ×	
				L.
		预共享密钥		
		<u> </u>		
		登录信息的类型		
		用户名和密码		PSK信息
		用户名(可选)		
		原友	即沿	



VPN 连接		添加VF	PN
① test _{未连接}		连接	
	高级选项	删除	

Windows 需要修改注册表信息,并且需要重启客户端操作系统。

vpn 注册表链接如下,

http://note.youdao.com/noteshare?id=ed25c9b654464a0f4020ef5933cca

ba4&sub=37D5005876B141F8A94CF9914EB291AA

\leftrightarrow \rightarrow \mathcal{C} \mathfrak{S} note.youdao.com/ynoteshare/index.h	tml?id=ed25c9b654464a0f4020ef5933ccaba4&ttype=note&_time=1722927582107
✓ 有道云笔记 vpn注册表	保存文件到第记
Pix_VPN_Error d.reg ↓	

点击进行下载,然后双击运行,运行完成之后,进行重启 window 操作。

然后进行客户端链接

 网络和 Interne	t > VPN > test	ð		
连接属性			编辑	
连接名称 服务器名称或地址 登录信息的关型 用户名(可选) 密码(可选)	test 用户名和密码 vpnuser			¢.
网络配置文件类型				4

6、Linux 客户端链接

CentOS 需要安装图形界面,然后在进行如下操作。

使用(Crt、putty、xshell等远程工具进行链接)

选择 ssh 协议、输入公网地址以及账户名密码,进行远程链接





5 10.0.0.4 - SecureCRT	
File Edit View Options Transfer Script Tools Window Help	
🐂 🕅 🎣 🛣 Enter host <alt+r></alt+r>	
	· Eu
Session manager 4 × v 10.0.0.4 ×	
- 💭 🔂 🕺 🐴 🛝 🗙 😁 🏦 🎽 👘 🛛 Failed	
E-C Sessions	
- 10004	
L检查密码子校是否个7	5至1
Ne	w Session Wizard X
118.190.207.157	
TASK [8, 8]	This wizard will help you create a new session for connecting to a
	remote server.
	what type of connection do you want to establish?
	Protocol: SSH2 ~
- 🔊 172.29.68.4	
- 4 192 168 16 161 [检查SETroub]eshoo	
- 102 168 253 1 Failed	
A 102 169 252 2	
102 160 254 17	
PLAY RECAP	
Total Policies	
192.168.254.21	□ bo not use this <u>wizard</u> when creating sessions
Total Policies F	
39.105.200.55	
47.92.23.162	
- fws-crm [root@docker benchmark	
- 過 fws-毎超 [root@docker benchmark]#
Eroot@docker_benchmark	#
× 10004 ×	
► 10.0.0.4 ×	
" Failed	
TACK FO 71	
L 检查密码子段是否不为空」	
Pass New Session Wizard	×
New Session Wizard	~
TASK [8,8]	Whet's the same or ID address of the same to here?
「捡本邮件供給份理具	What is the name or IP address of the remote host?
Pass	The user name can be left blank.
TASK [8.9]	Hostname:
「检查GPG kevs 是否面」	
Pass	Port: 22
	rt u Name
	Firewall: None
TASK [8.10]	
■ [检査SETroubleshoo]	
Failed	用户名root
PLAY RECAP	
Total Policies	
Total Policies P	
Total Policies Fi	
Total Policies E	卜一步
Result file: //	
[root@docker_benchma	
[root@docker benchmark]#	
[root@docker benchmark]#	

双击链接即可执行如下命令

yum install epel-release

yum --enablerepo=epel install NetworkManager-libreswan-gnome

[root@vpn ~]# yum install -y NetworkMa AnolisOS-8 - AppStream AnolisOS-8 - BaseOS AnolisOS-8 - Extras AnolisOS-8 - PowerFools 上次元教程过期检查: 0:00:01 前,执行于 依赖关系解决。	5.1 MB/s 11 MB 3.3 MB/s 6.3 MB 397 B/s 2.3 kB 2.3 MB/s 1.5 MB	00:02 00:01 00:05 00:00		
	架构	版本		大小
安装: NetworkManager-libreswan-gnome	x86_64	1.2.10-5.0.1.an8	AppStream	41 k
gnutls qnutls-dane	x86_64 x86_64	3.6.16-8.0.2.an8 3.6.16-8.0.2.an8	BaseOS AppStream	1.0 M 52 k

西安金箍棒信息技术服务有限公司

地址: 西安市雁塔路 67 号红锋商务大厦 4 层



打开主机,然后点击设置

e	活动 🗘 设置	7月30日 22:44	
-	次里 三	网络	× ////////////////////////////////////
ġ	网络	以太网 (enp0s3) +	
*	蓝牙	已连接 - 1000 Mb/秒	
	背景		root@vpn:~
	通知	以太网 (enp0s8) +) 搜索(S) 终端(T) 帮助(H)
٩	搜索	已连接 - 1000 Mb/秒	27:97:8c:b2 txqueuelen 100 002724 bytes 1474168011 (1 dropped 0 overruns 0 fra
O	多任务	VPN +	09974 bytes 6747707 (6.4 M dropped 0 overruns 0 carr
88	应用程序 >	test VPN	P,BROADCAST,RUNNING,MULTICA 4 netmask 255.255.255.0 b a00:27ff:fe14:f2e1 prefixl
4	隐私 >	—————————————————————————————————————	27:14:f2:e1 txqueuelen 100 32 bytes 75986 (74.2 KiB) VDD dropped 0 overrups 0 fra
0	在线帐号	网络代理 关 🍳	174 bytes 307723 (300.5 Ki dropped 0 overruns 0 carr
<	共享		BACK,RUNNING> mtu 65536 .1 netmask 255.0.0.0
4(1)	声音		elen 1000 (Local Loopback) bytes 240 (240.0 B)
G	电源		dropped 0 overruns 0 fra bytes 240 (240.0 B) dropped 0 overruns 0 carr
	C - 20		

配置链接信息

i.

Q. 设置	■ 网络	× ///
♀ 网络	以太网 (enp0s3) +	
* 蓝牙		
□ 背景	取消(C) test VPN 应用(A)	
▲ 通知	+ 详细信息 身份 IPv4 IPv6) 搜索
Q 搜索	名称(N) [test	00272 drop
◎ 多任务	常规 +	09974 drop
BB 应用程序	^{网关GI} ← ecs公网IP地址 ● ●	P, BR0 4 ne a00:2
● 隐私	认证 类型 [KFv1(XAUTH) ▼	27:14 32 b drop
@ 在线帐号	用户名 vpnuser 关 🖉	174 drop
< 共享	用户密码(U) 4	BACK,
● 声音		
Ce 电源	● 星示密码	drop byt drop
O 8-0	远程 ID(R)	WIRamu
	PSK % Advanced	

打开链接信息



😗 活	动 🗘 设置		7月30日 2	22:46	é ÷ 0
۹	设置	Ξ	网络	×	
₽ 网 ★ 英	络		以太网 (enp0s3)	+	
ा =0			已连接 - 1000 Mb/秒		
	京		以太网 (enp0s8)	+	root@vpn:~
▲ 通	知) 捜索(S) 终端(T) 帮助(H) 27:97:8c:b2 txqueuelen 1000 (Ethernet)
Q 扱	索		已连接 - 1000 Mb/秒		002724 bytes 1474168011 (1.3 GiB) dropped 0 overruns 0 frame 0
0 3	任务		VPN	+	dropped 0 overruns 0 carrier 0 collisions 0
部应	用程序	>	test VPN		P,BROADCAST,RUNNING,MULTICAST> mtu 1500 4 netmask 255.255.255.0 broadcast 10.0.0.255 a00:27ff:fel4:f2el prefixlen 64 scopeid 0x20 <lir 777-34-677-1 txnueulen 1000 (Ethernet)</lir
≝ 隠	私	>			dropped 0 overruns 0 frame 0
@ 在	线帐号		网络代理	× Ŷ	174 bytes 307723 (300.5 KiB) dropped 0 overruns 0 carrier 0 collisions 0
< #	享				BACK,RUNNING> mtu 65536 .1 netmask 255.0.0.0
● 声	音				refixlen 128 scopeid 0x10 <host> elen 1000 (Local Loopback) bytes 240 (240.0 B) dropped 0 overruns 0 frame 0</host>
[r et	测试 oot@vpn h0: fla ii e R R T T	连 ["] "#4 gset 6 net 6 tx x per 7	1 ifconfig 163 <up.broadcast,running,mult netmask 255.2 fe80</up.broadcast,running,mult 	ICAST> mtu 150 55.240.0 broad efixlen 64 sco n 1000 (Etherr .1 MiB) frame 0 .2 MiB) carrier 0 col	00 dcast 1 opeid 0x20 <link/> net) llisions 0



7、IOS 手机客户端链接

点击设置、下一步通用、通用里面的 VPN 与设备管理。

.

〈 设置	通用	
iPhone 储存空间		>
后台 App 刷新		>
日期与时间		>
键盘		>
字体		>
语言与地区		>
词典		>
		_
VPN与设备管理		>
法律与监管		>
传输或还原 iPho	ne	>
关机		

点击添加 VPN 链接

11:36	.ıı 5G [15]
✔ VPN与设备管理	/PN
VPN状态	未连接
设备VPN	
✓ teat 未知	í
添加VPN配置	
VPN 可设置用于控制某些 <mark>与隐私…</mark>	网络流量的路由。关 <mark>于VPN</mark>

类型选择 L2TP, 输入 IP 地址、账户、用户名、密码, 密钥完成链接即可

IKEv2	
IPsec	
L2TP 🗸	

西安金箍棒信息技术服务有限公司

地址: 西安市雁塔路 67 号红锋商务大厦 4 层



取消		添加配置		完成	
类型				L2TP >	,
描述	必填				
服务器	必填				
账户	必填	服务器	:公网	ЯIР	
RSA Securl	D	账户:	用户名		
密码	每次出	密码: 密码:	密码 共享图	密钥对	
密钥	必填	点击完	成, 银	连接即可	•
发送所有流	里)
代理					
关闭		手动		自动	



8、安卓手机客户端链接

由于 VPN 使用较老的 L2TP 协议,各个安卓厂家处于安全考虑已经对此协议 不支持,或者已经屏蔽,无法使用。

9、链接使用

使用 ping 协议,以及 ssh 链接 VPN 局域网 IP 地址

查看服务端 VPN 局域网私有 IP 地址

ifconfig(Linux 客户端直接可以访问阿里的内网地址, windows 客户端需要

查看 VPN 分配 192.168.42.0 网段的局域网地址,使用 ssh 192.168.42.2 进行

访问)

ping 172.28.141.212

也可进行 ssh 远程链接 VPN 服务器,远程完成之后可进行业务使用。

ssh 172.28.141.212



10、用户管理

查看 VPN 用户

more /etc/ppp/chap-secrets

"vpnuser" 12tpd "Y23KKbnNyBd56HJq" *

Done:

[root@vpn ~]# more /etc/ppp/chap-secrets "vpnuser" 12tpd "Y23KKbnNyBd56HJq" * [root@vpn ~]# ■

查看共享 PSK

more /etc/ipsec.secrets

[root@vpn ~]# more /etc/ipsec.secrets

%any %any : PSK "BZyAmPwijTHyfU4DyBYN"

一般不建议修改 PSK, 建议保留。



更新 PSK

如果要更换一个新的 PSK,可以编辑此文件。不要在值中使用这些字符: \ ",

vi /etc/ipsec.secrets

```
LLOOL@Abu ~]#
 [root@vpn ~]#
  root@vpn ~]#
                         vi /etc/insec
           %any : PSK "BZyAmPwi
⊠an∨
     完成后必须重启服务:
     service ipsec restart
     service x12tpd restart
     添加新 VPN 链接用户并且设置密码 test 为用户名, 密码为 test123
     addvpnuser.sh 'test' 'test123'
[root@vpn ~]# addvpnuser.sh 'test' 'test123
welcome! Use this script to add or update a VPN user account for both IPsec/L2TP and IPsec/XAuth ("Cisco IPsec") modes.
If the username you specify already exists, it will be updated with the new password. Otherwise, a new VPN user will be added.
VPN user to add or update:
Username: test
Password: test123
Write these down. You'll need them to connect!
VPN client setup: https://vpnsetup.net/clients
Do you want to continue? [Y/n] y
Adding or updating VPN user...
Done!
Note: All VPN users will share the same IPsec PSK.
If you forgot the PSK, check /etc/ipsec.secrets.
```



账	号	测	试	链	接	,	链	接	成	功
	09:0	5			U			ul S	5G [27]	
<	VPN				teat				编辑	ŧ
	类型							L	2TP	
	服务	器					39.10	5.200).55	
	账户								test	
	地址						192.1	68.4	2.10	
	连接	时间						(0:12	
				删	除 VP	N				



✓ VPN与设备管理	/PN			
VPN状态	已连接			
设备 VPN				
✓ teat _{未知}	í			
添加 VPN 配置				
VPN 可设置用于控制某些网 与隐私	网络流量的路由。关于 VPN			
更改 VPN 用户密码,test1234 为	新密码			
addvpnuser.sh 'test' 'test1	234'			
[root@vpn ~]# [root@vpn ~]# addvpnuser.sh 'test'	'test1234'			
Welcome! Use this script to add or IPsec/L2TP and IPsec/XAuth ("Cisco	update a VPN user account for both IPsec") modes.			
If the username you specify alread with the new password. Otherwise,	ly exists, it will be updated a new VPN user will be added.			
VPN user to add or update:				
Username: test Password: test1234				
Write these down. You'll need them to connect!				

VPN client setup: https://vpnsetup.net/clients

Do you want to continue? [Y/n] Y

Adding or updating VPN user...

Done!

Note: All VPN users will share the same IPsec PSK. If you forgot the PSK, check /etc/ipsec.secrets.

删除指定 VPN 用户

delvpnuser.sh 'test'

[root@vpn ~]# delvpnuser.sh 'test'

Welcome! Use this script to delete a VPN user account for both IPsec/L2TP and IPsec/XAuth ("Cisco IPsec") modes.

VPN user to delete:

Username: test

金箍棒

Do you want to continue? [Y/n] Y

Deleting VPN user...

Done!

11、环境说明

服务配置文件/etc/ipsec.conf

如何查看服务是否启动: ps - ef | grep ip

prosevani ~] ps -ef | grep ip root %pr ~] ps -ef | grep ip root 7月30 ? 00:00:00 [ipv6_addrconf] root 00:00:00 /usr/sbin/dnsmasg -conf-file=/var/lib/libvirt/dnsmasg/default.conf --leasefile-ro --dhcp-script=/usr/libkee c/libvirt_leaseshelper root 4308 4250 0 09:28 pts/0 00:00:00 /usr/sbin/dnsmasg -conf-file=/var/lib/libvirt/dnsmasg/default.conf --leasefile-ro --dhcp-script=/usr/libkee root 6302 1 0 7月30 ? 00:00:00 /usr/sbin/dnsmasg -conf-file=/var/lib/libvirt/dnsmasg/default.conf --leasefile-ro --dhcp-script=/usr/libkee root 6302 1 0 7月30 ? 00:00:00 /usr/local/libkec/ipsec/pluto --leak-detective --config /etc/ipsec.conf --nofork

VPN 日志会记录到系统日志中/var/log/messages

tail -f /var/log/messages



12、服务的启动以及关闭

重启服务命令

service ipsec restart

启动服务命令

service ipsec start



关闭服务命令

service ipsec stop

查看服务状态

service ipsec status

13、常规错误如何排查

首先,重启 VPN 服务器上的相关服务:

service ipsec restart

service x12tpd restart

然后重启你的 VPN 客户端设备,并重试连接。如果仍然无法连接,可以尝试删除并重新创建 VPN 连接。请确保输入了正确的 VPN 服务器地址和 VPN 登录凭证。

确认服务器 EC2/GCE 是否打开 安全组 UDP 端口 500 和 4500

检查 IPsec VPN 服务器状态:

ipsec status

[root@vpn log]# ipsec status 000 using kernel interface: xfrm 000 000 interface lo uop [::1]:4500 000 interface lo uop 127.0.0.1:4500 000 interface to uop 127.2.0.10.53:4500 000 interface etho uop 172.2.0.10.53:500 000 interface virbr0 uop 192.168.122.1:4500 000 interface virbr0 uop 192.168.122.1:500 000 fips mode=disabled; 000 setlinux=disabled 000 config setup options: 000 config setup options: 000 config setup options: 000 setcomp=unsupported 000 sist=/etc/ipsec.d, dumpdir=/run/pluto, statsbin=unset 000 sist=/etc/ipsec.d, dumpdir=/usr/local/libexec/ipsec 000 pluto_version=4.14, pluto_vendorid=rusr/local/libexec/ipsec 000 pluto_version=6.14, pluto_vendorid=rusr/local/libexec/ipsec 000 pluto=version=6.14, pluto_vendorid=rusr/local/libexec/ipsec 000 otsp=rrugue=veys, crl=strict=no, logappend=ves, logip=ves, shuntlifetime=900s, xfrmlifetime=30s 000 ddos-cookies=threshold=25000, ddos=max=halfopen=50000, ddos=made=auto, ikev1=policy=accept 000 otsp=trust=name=cunset> 000 ocsp=cache=size=1000, ocsp=cache=min=age=3600, ocsp=cache=max=age=86400, ocsp=method=get 000 global-redirect=no, global-redirect=to=cunset> 000 ocsp=cache=size=1000, ocsp=cache=min=age=3600, ocsp=cache=max=age=86400, ocsp=method=get 000 global-redirect=no, global-redirect=to=cunset> 000 ocsp=cache=size=1000, ocsp=cache=min=age=3600, ocsp=cache=max=age=86400, ocsp=method=get 000 secctx=attr=type=32001 000 debug: 000 nat=traversal=yes, keep=alive=20, nat=keport=4500 000 virtual=private(%priv): 00 = atlowed subnets: 10.0.0/8, 192.168.0.0/16, 172.16.0.0/12 000 = excluded subnets: 192.168.42.0/24, 192.168.43.0/24

查看当前已建立的 VPN 连接:

ipsec trafficstatus



|[root@wpn log]#" [root@wpn log]# jpsec trafficstatus 006 #40: "|2tp-psk"[32] 113.201.132.177, type=ESP, add_time=1723430916, inBytes=1900, outBytes=2356, maxBytes=2^63B, id='10.179.19.136' [Γεοτβ⁴μση Ιοη!#"

查看链接日志

VPN 日志会记录到系统日志中/var/log/messages

tail -f /var/log/messages



三、技术支持

1、售后服务

- (1)您可以第一时间在阿里云市场联系售后获取服务。
- (2) 服务时间: 09:00-18:00 (紧急情况请打电话)
- (3) 服务热线: 18091296777、4009030002 转 15953
- (4) 服务邮箱: 22958288@qq.com

2、服务范围

远程支持:如果您在使用过程中遇到技术操作问题,请及时联系客服,我们的 工程师可远程协助您完成操作。

定制服务:本公司支持一对一定制服务,如您的业务环境有特殊需求,请与客服联系。

付费服务:本公司可提供镜像部署、故障处理、安全运维代维等一站式托管服务,全面涵盖服务器环境配置,网站程序调试,数据库配置更改,数据库权限、账户,系统安全加固,故障排查,系统调优,数据库优化等范围。如您有相关需求,请咨询客服。

20