# VPN 管理系统使用手册 (Ver.1.1)

云顶云运维组

2017年7月13日

## 目录

-,	镜像说明
二、	登录说明
三、	功能介绍
四、	IPSec Site-to-Site VPN 使用指南4
五、	拨号 VPN
	1、应用场景
	2、Classic 网络场景
	3、VPC 网络场景
六、	SNAT 配置14
七、	TCP 隧道15

### 一、镜像说明

1、此镜像是基于 centos7.3 64 位的系统环境用 RPM 包安装完成,支持 IPSecVPN、拨号 VPN、SNAT、TCP 隧道等功能。

2、此安装包包含的软件及版本为 :

strongswan : 5.4.0

openvpn: 2.4.2

java : 1.8.0\_111

tomcat : 8.5.11

3、软件目录及配置列表

3.1、vpnManager

目录:/usr/local/tomcat/webapps/vpnManager

启动命令: systemctl start tomcat.service

数据库文件:/usr/local/tomcat/webapps/vpnManager/ vpnManager.db

数据库文件保存了我们所有的 VPN 配置, 建议定期备份.

3.2、Strongswan

目录:/etc/strongswan

日志文件:/var/log/strongswan.charon.log

启动命令: systemctl start strongswan.service

ipsec.conf 和 ipsec.secrets 配置文件, 由 vpnManager 程序自动生成, 请勿随便修改。

3.3、OpenVPN

目录:/etc/openvpn

日志文件:/etc/openvpn/openvpn.log

状态文件:/etc/openvpn/openvpn-status.log

启动命令:systemctl start openvpn@server.service

server.conf 配置文件,由 vpnManager 程序自动生成,请勿随便修改。

### 二、登录说明

使用 ECS 的系统账号密码即可登入系统,即所有可通过 SSH 登陆主机的用户都可以

#### 登入该系统。浏览器访问 http://公网 IP/

○ 示印云vPM著想系術 × ○ ○ 不安全		t⊒ - ∂ ¢
	<ul> <li>         云顶云VPN网关管理系统         ▲ %ABP®         ▲ %ABP®         ▲ %ABP          ▲ %ABP          ▲ %ABP         ▲ %ABP         ▲ %ABP</li></ul>	
	R by TandetunDinyten	

## 三、功能介绍

本程序提供了 VPN、SNAT 基础服务。主要提供以下几点功能:

1、IPSec Site-to-Site 功能。可快速的帮助你将两个不同的 VPC 私网以 IPSec Site-to-Site 的方式连接起来。支持可选的 IKEv2/ESP 加密算法、签名算法、DH 组。

2.、拨号 VPN 功能。可让你通过拨号方式, 接入 VPC 私网, 进行日常维护管理。

3. SNAT 功能。可方便的设置 Source NAT, 以让 VPC 私网内的 ECS 实例通过 Gateway ECS 访问外网。

4、TCP 隧道。可让你通过 Gateway ECS 的端口来访问 VPC 内部某台 ECS 的特定端口

#### 四、IPSec Site-to-Site VPN 使用指南

VPC1 私网为:10.0.1.0/24, VPC2 私网为:192.168.1.0/24。其中,两个 VPC 中各有一 合使用 VPN/SNAT 镜像安装的 GateWay ECS,并绑定了 EIP。现在想让两个 VPC 的私网 ECS 之间 能够相互访问,我们将需要在 VPC1 GateWay ECS 和 VPC2 GateWay ECS 之间建立一 条 IPSec Site-to-Site 隧道。在本例中:从 VPC1 的 10.0.1.10 访问 VPC2 的 192.168.1.10

1、启动 IPSec VPN 服务

进入 IPSec 的 VPN 服务管理页面,确保 VPC 两端的 GateWay VM1、GateWay VM2 均 启动了 IPSec VPN 服务。

	📤 云顶云VPN网				
IPSec VPN         V           原語外容         自然外PN 服务           常知認知         自然外PN 服务           常知認知         自然外PN 服务           修理》         自然外PN 服务           常知認知         自然外PN 服务           小 WN服务管理         自然小PN 服务           ()         KPS VPN           ()         KPS           ()         KPS           ()         KPS	功能菜单 🔳	IDCar VDM MHERE I			
	IPSec VPN	IFSEC VERVISEPEARTS I			
新田田田田         和区が外 範囲, 不会地会自己自己行 がいやり 範囲,         単立いやり 範囲, 不会地会自己自己行 いいり 範囲, 部の母上之后,所件 日は当時的は道路的中部,         下知時的いりN 範囲, 再合主之気, 第件 区位者区VPN 範囲と言用出行使用,           ③ 茨芬 VPN →         面の         契約         予知意応           ④ 茨芬 VPN →         面の         契約         予知意応           ④ SNAT →	▶ 隧道列表	启动VPN 服务	停止VPN 服务	配置下发&重载	
· VPAESIRE         印动         900         192/星色           ③ SNAT         >         -         -           ③ TCP描述         >         -         -	> 新增超距温	启动VPN 服务。不会影响到已经运行 的VPN 服务。	停止VPN 服务。服务停止之后,所有 已经连接的隧道都将中断。	下发新的VPN 配置,并使之生效。建 议在修改VPN 配置之后再进行使用。	
該提示 VPN 方         部論         Xiii         下知里思           ③ SNAT 方	▶ VPN服务管理				
SNAT     SNAT     TCPREN		启动	<b>新</b>	下发重载	
C терябан	a snat 🦻				
	TCP隧道 >				

- 启动 VPN 服务:仅启动本机的 IPSec VPN。启动时,启动类型为自动连接的隧道将自动尝试连接对端 VPN。
- ▶ 停止 VPN 服务:停止本机的 IPSec VPN。已经连接上的隧道将全部断开。
- 配置下发&重载:一般情况下,该动作在新增、修改或删除隧道时会自动进行。但某些 情况下,如果你想重新生成 VPN 配置,可手动执行该操作。
  - 2、新增隧道

VPC1 GateWay ECS:

0	IPSec VPN			
	融資列表	*SEXBID	vpn_test	
1.	RF 1054-00	IKE版本	IKEV1 *	
	VPN服务管理	启动类型	于工造地	
	總号 VPN	协商模式	主动模式	
	SNAT	DPDH2m	None *	
	TOTAL	IKEv2 加密算法	3DES *	
0	ICP MAD	IKEv2 验证算法	MD5 *	
		IKEv2 DH 细	Group 1 modp768	
		ESP 加索算法	3DES *	
		ESP 验证算法	MD5 *	
		ESP DH 组	无	
		*本编ID	119.23.219.43	
		*本靖子网	10.0.1.0/24	
		"#JikiD	112.74.83.189	
		*对该公网IP	112.74.83.189	
		*对端子网	192.168.1.0/24	
		*预共享秘钥	*C	

VPC2 GateWay ECS:

0	IPSec VPN	×			
	配加利用		*题道ID	vpn_test	
1.1	RF-MILLIM		IKE版本	IKEV1	*
	VPN服务管理		启动类型	于工造接	•
	拨号 VPN		协商模式	主动模式	•
	SNAT		DPD检测	None	•
	TODEL		IKEv2 加密算法	3DES .	•
U	ICP <u>IEID</u>		IKEv2 验证算法	MD5	•
			IKEv2 DH 组	Group 1 modp768	•
			ESP 加索算法	3DES .	•
			ESP 验证算法	MD5	•
			ESP DH 细	无	•
			*本编ID	112.74.83.189	
			*本油子网	192.168.1.0/24	
			*93481D	119.23.219.43	
			"对输公网IP	119.23.219.43	
			1000		
			*\$346.710	10.0.1.0/24	
			"预共享他们		
				84	

- ▶ 两边的隧道 ID、加密算法、验证算法、DH 组、预共享密钥必须一致才能建立连接。
- ▶ 本端子网、对端子网:即前面例子中的 10.0.1.0/24, 192.168.1.0/24。
- ▶ 对端公网 IP: 对端 GateWay 所绑定的 EIP。
  - 3、查看隧道列表或删除

在 VPC1 和 VPC2 的 GateWay ECS上将隧道添加完毕之后,进入隧道列表页面。对 我们刚刚配置好的隧道,点击连接,即可看到如下图,也可以点击删除,删除我们建立 的隧道:

			/PN网 <del>)</del>	、管理系统	充							ژ ا	±销
		功能菜单		隧道ID	启动类型	本端子网	对编EIP	对端子网	状态	操	en: m	HRR	
				vpn_test	手工连接	10.0.1.0/24	112.74.83.189	192.168.	.1.0/24 offlin	e 连	接册	HPR .	
		IPSec VPN	×										
		▶ 隧道列表											
		▶ 新增隧道											
		▶ VPN服务管理											
		● #E VPN											
		SNAT											
		TCP隧道											
$\triangleright$	连接.	连接隧道	左	両台	Gate	Wav	FCS任音		遗损化	とし	Пп	T	
	在1941	正接隧道。	71	къл	uaic	may	LOOLT	27	圳床	μN	р н <u>.</u>	10	
	Mar	Nr		<i>1</i> .	~		Dec La F	*	an te n	6 DI	н—	Ŧ	

- ▶ 断开:断开隧道。在两台GateWay ECS任意一端操作即可。
- ▶ 删除:点击删除,将该隧道删除,同时会自动断开该隧道,立即生效。

4、修改隧道

点击对应的隧道ID 进入修改页面,修改后,点击保存,配置将立即生效,但不会 影响已经连接上的隧道。需要手工断开、再连接隧道。

Ć	占 云顶云	<u></u> ₹VPI	N网关管理系统		① 注销
功俞	「菜单	=	*隧道ID	vpn_test	
0	IPSec VPN	>	启动类型	手工连接	
÷	隧道列表		IKEv2 加密算法	3DES .	
×	新增隧道		IKEv2 验证算法	MD5	
÷	VPN服务管理		IKEv2 DH 组	Group 1 modp768	
<b></b>	拨号 VPN	>	ESP 加密算法	3DES .	
	SNAT	>	ESP 验证算法	MD5	
0	TCP隧道	>	ESP DH 组	无	
			*本端子网	192.168.1.0/24	]
			*对端公网IP	119.23.219.43	
			*对端子网	10.0.1.0/24	
			*预共享秘钥	3fwe12frgefq	
				保存	

## 五、拨号 VPN

#### 1、应用场景

▶ Classic 网络场景。跨账号、跨地域的云服务器之间内网互通。

▶ VPC 网络场景。管理员接入 VPC 进行私网访问、管理。

#### 2、Classic 网络场景

用户在杭州、北京、青岛区域用不同的账号各买了1台 ECS,现在想让这3台 ECS 实 例之间进行内网通信,我们需要把这3台 ECS 拨入到同一个 VPN 网络中,用 VPN 分配的 地址进行通信。在本例中:杭州的 ECS 选为 VPN GateWay,北京和青岛的 VM 拨入到杭州 的 VPN 中。使用 VPN 分配的地址 10.8.8.7、10.8.8.9 进行相互通信。

2.1、启动 IPSec VPN 服务

进入拨号 VPN 的 VPN 服务管理页面,确保 GateWay ECS 启动了拨号 VPN 服务。

IPSec VPN	TPCar VDN 配合将下下等 I		0
· 新·昭叔:道	A OUL VERY MERTANY JALE NE 1		
・ VPN服务管理	启动VPN 服务 启动VPN 服务。不会影响到已经运行 的VPN 服务。	停止VPN 服务 停止VPN 服务。服务停止之后,所有 已经连接的隧道都将中断。	配置下发及重载 下波新的VPN 配置,并使之生效。讓 议在移改VPN 配置之后再进行使用。
SNAT     TCP6516	500 States	žiā	下发重线
im >	Ea	,¥iû	下发重载

▶ 启动 VPN 服务:仅启动本机的拨号 VPN。

▶ 停止 VPN 服务:停止本机的拨号 VPN。已经连接上的隧道将全部断开。

配置下发&重载:进行拨号 VPN 设置时,该动作会自动进行。但某些情况下,如果你想 重新生成 VPN 服务端配置,可手动执行该操作。

2.2、设置

进入拨号 VPN 的设置页面进行如下设置

功能	菜单		康抑IP 地址や・カVPN Server イ	Narkas户端的唐凯10 他带袖,子网网段,为客户端连续	之后可以访问的子网网段 可以错写条个子
0	IPSec VPN	>	网,用英文「,」分割。 注:保存修改后,会重载VPN B	255 , 所有客户端将会自动断开重连。	
<b></b>	拨号 VPN	v			
Þ	账号列表		通信协议	ТСР	
ŀ	新增账号		*虚拟IP 地址池	10.8.8.0/24	
•	设置		允许client 问通信	杏 · ·	
÷	VPN服务管理		允许单个账号同时在线	否 •	
ŀ	客户端下载		*子网网段	10.171.112.120/32	]
	SNAT	>		保存	0
0	TCP隧道	>			

- ▶ 通信协议:可选"UDP"、"TCP"。注:每次修改保存后,请重新下载客户端配置文件。
- ▶ 虚拟 IP 地址池:即 VPN Server 分配给客户端的虚拟 IP 地址池。本例为: 10.8.8.0/24
- ▶ 允许 client 间通信:本例子中,这里请选"是"。
- ▶ 允许单个账号同时在线:可选"是"或"否"。

▶ 子网网段:即允许拨号 client 访问的子网。本例不需要 client 访问子网,填写 VPN GateWay VM 私网 IP 即可: 10.171.112.120/32。

2.3、添加 VPN 账号

点击新增账号按钮,即可新增账号:

📤 云顶云VPN	网关管理系统	① 注朝
功能菜单 🏾 🔳	注意:「账号名」只可包含如下字符:数字、字母、下划线。	
IPSec VPN		
	*账号名 test	
> 账号列表	*歲得	
• 新潮所会	保存	
• 说面		
▶ VPN服务管理		
· 查户浏下载		
SNAT >		
C TCP隧道 >		

- ▶ 账号名:只可包含如下字符:数字、字母、下划线。
- ▶ 密码:只可包含如下字符:数字、字母、下划线。
  - 2.4、配置客户端

点击客户端下载按钮,可以下载 VPN 客户端和相应的配置文件。

INSECTORY         Idlife         Idli
Installer (25-bit), Windows XP and Liter operspri-install-2.3.4-003-1466.exe windows-operspro-client.zip         windows-operspro-client.zip           Installer (64-bit), Windows XP and Liter operspri-install-2.3.4-003-1466.exe windows-operspro-client.zip         windows-operspro-client.zip           Installer (64-bit), Windows XIsta and Liter operspri-install-2.3.4-003-1466.exe windows-operspro-client.zip         windows-operspro-client.zip           Installer (64-bit), Windows XIsta and Liter operspri-install-2.3.4-1603-1466.exe windows-operspro-client.zip         windows-operspro-client.zip
installer (32-bit), Windows Vista and later openypn-install-2.3.4-1003-b86.exe windows-openypn-client.zp installer (64-bit), Windows Vista and later openypn-install-2.3.4-1003-b86.exe windows-openypn-client.zip
、 设置 Centos sudo yum instali openypn linux-openypn-client.tar.gz Debian/Ubuntu sudo apt-get instali openypn linux-openypn-client.tar.gz
VVRANDER  VVRANDER  SNAT  TCREE  TCREE

➢ Windows 平台:安装完客户端后,将配置文件 client.ovpn 和 ca.crt 文件放到安装目录 下的 config 文件夹中。然后启动 openvpn-gui.exe,根据提示进行连接。

➢ Linux 平台:在配置文件 client.conf 和 ca.crt 的目录下执行命令 :openvpn client.conf, 根据提示进行连接。若要以 daemon 形式在后台执行,请执行 : openvpn client.conf & 来 建立连接。

▶ 注:在 Linux 平台下载客户端时,需要关闭证书验证。wget 请加上参数--no-checkcertificate, curl 请加上参数--insecure。

2.5、查看账号列表

点击账号列表按钮,可以查看已经添加的账号列表。如果该账号已经拨入 VPN,将看到 更明细的信息:

功能学年         ■           ・ IPSec VPN コン         ●           ・ IPSec VPN コン         ●           ・ RG2#         ●           ・ RG2# <td< th=""><th>金 云顶云V</th><th></th><th>① 注销</th></td<>	金 云顶云V		① 注销
功能算単         ■           ・ PSec VPN 、         ・           ・ 取写形         ・           ・ 取写所         ・           ・ 取写描         ・           ・ 、 取目         ・           ・ 、 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・			
<ul> <li>PSec VPN &gt;</li> <li>読む VPN v</li> <li>取りたい v</li></ul>	功能菜单 🔚	于VPN 的keepalive 机制,会有1分钟左右的超时。	
取り VP         V         取りた         取りた </td <td>IPSec VPN</td> <td></td> <td></td>	IPSec VPN		
R 67)液     R 67)流     R 67)     R 67)     R 67)     R 67)    R 67)     R	参 援号 VPN	P 虚拟IP 状态 Bytes Received Bytes Sent 连接时间 账号创建时间 offline 2017-07-13 10:58:32	操作
<ul> <li>新期時号</li> <li>協業</li> <li>VPN振号期間</li> <li>動P加下期</li> <li>SNAT 2</li> <li>TCP協会 2</li> </ul>	▶ 账号列表	STITUE COTTO TO	
<ul> <li>協業</li> <li>VPN服务策策</li> <li>衛P斯下戦</li> <li>SNAT 2</li> <li>TCP協者 2</li> </ul>	> 新增账号		
・ VPN服用物理器         ・ 廠PMFF報         ・ 廠PMFF報         ・ 家         ・ 家         ・ 家	→ i記面		
<ul> <li>         · 愈户函下现         · ③         · SNAT         · ○         · CP 函         · ·         · ·         · CP 函         · ·         · ·         · ·</li></ul>	→ VPN服务管理		
<ul> <li>SNAT</li> <li>TCP服用</li> </ul>	▶ 春户端下载		
C тср廠通 >	SNAT		
	て ア 隧道		

状态:由于 VPN 的 keepalive 机制,会有1分钟左右的延时
 2.6、使用 vpn 进行通信
 现在,即可使用 VPN 分配的地址 10.8.8.7、10.8.8.9 进行相互通信了。

#### 3、VPC 网络场景

管理员想接入 VPC2 的私网内,以便管理维护 VM1 和 VM2。其中, VPC2 中有一台使用 VPN/SNAT 镜像安装的 GateWay VM,并绑定了 EIP。在本例中:管理员从公网通过 VPN 隧道访问 VPC2 的 192.168.0.3 。

3.1、启动 IPSec VPN 服务

进入拨号 VPN 的 VPN 服务管理页面,确保 GateWay ECS 启动了拨号 VPN 服务。

功能菜单				
IPSec VPN		VPN BOSE ALIGNO 1		×
	v	OpenVPN 服务运行正常!		
> 账号列表		户动/DN 服务	at iFVDN RR4c	石寧下的な面影
> 新增账号		启动/VPN 服务 启动/VPN 服务。不会影响到已经运行	停止VPN 服务 停止VPN 服务。服务停止之后,所有 已运动的限制新闻中新	配置下及る里彩 下没新的VPN 配置,并使之生效。建 均本線的VPN 配置,并使之生效。建
・ wa ・ VPN服务管理		837F11 (802)	Coldense and an and a second s	ACCEPTIANT A REPEATING TO DO
) 客户端下载		18% ith	<b>BUR</b>	下发重载
SNAT				
🚺 ТСР隧道				

▶ 启动 VPN 服务:仅启动本机的拨号 VPN。

▶ 停止 VPN 服务:停止本机的拨号 VPN。已经连接上的隧道将全部断开。

配置下发&重载:进行拨号 VPN 设置时,该动作会自动进行。但某些情况下,如果你想 重新生成 VPN 服务端配置,可手动执行该操作。

3.2、设置

进入拨号 VPN 的设置页面进行如下设置

功俞	「菜单	=	虚拟IP 地址池: 为VPN Server	分配给客户端的虚拟IP 地址地。子网网段:为客户端连接之后可以访问的子网网段。可以填写多个子	
9	IPSec VPN	>	网 , 用英文「,」分割。 注:保存修改后 , 会重载VPN	服务,所有客户端符会自动断开重连。	
9	拨号 VPN	v			
F	账号列表		通信协议	ТСР	
÷	新增账号		*虚拟IP 地址池	10.8.8.0/24	
•	设置		允许client 间通信	Ξ. Y	
×	VPN服务管理		允许单个账号同时在线		
÷	客户端下载		*子网网段	192.168.0.0/24	
	SNAT	>		保存	
	TCP隧道	>		_	

- ▶ 通信协议:可选"UDP"、"TCP"。注:每次修改保存后,请重新下载客户端配置文件。
- ▶ 虚拟 IP 地址池:即 VPN Server 分配给客户端的虚拟 IP 地址池。
- ▶ 允许 client 间通信:可"是"或"否"。

▶ 允许单个账号同时在线:可选"是"或"否"。

▶ 子网网段:即我们 VPC2 的子网 192.168.0.0/24。

2.3、配置 SNAT

进行拨号 VPN 设置之后,为了让管理员能够访问 VPC2 的私网,需要手工调整相应的 SNAT 设置!

沈松菜単     正要: [何時紙回的P] 为本可从从用P,非本可得在的公開性能加度IP 地能。     正要: [何時紙回的P] 为本可从从用P,非本可得在的公開性能加度IP 地能。     「     「    IPSec VPN      「     「    SNAT      」     「     SNAT      マ     · 新社作用の     「     SNAT      マ     · SNAT      四
iPSec VPN       *         後 按 VPN       *         第 放行 P(編集)       10.8.0.0/24         1 SNAT       *         * SNAT P(素)       *         ·       SNAT P(素)         ·       SNAT P(素)
SNAT v     ''GRAGABIP     192.168.1.0     SNAT FVER     SNAT FVER     SNAT FVER
▶ SNAT 新增
С тсряза

在上面的例子中,虚拟地址池为 10.8.0.0/24,子网网段为 192.168.0.0/24,则需要配置 SNAT: 10.8.0.0/24 → 192.168.0.1

2.4、添加 VPN 账号

点击新增账号按钮,即可新增账号:

	网关管理系统	(1) 注销		
功能菜单 🔳	注意:「账号名」只可包含如下字符:数字、字母、下划线。			
IPSec VPN				
	*账号名 test			
> 账号列表	"歲得			
• 新電影響	9277			
・ 设置				
→ VPN服务管理				
奋户如下载				
SNAT >				
💭 ТСР隧道 >				

- ▶ 账号名:只可包含如下字符:数字、字母、下划线。
- 密码:只可包含如下字符:数字、字母、下划线。

2.5、配置客户端

功食	喋单	=	注意:「配置」文件下数后,请将配置文件中的「	remote IP] 字段修改为本机新模击的IP 地址	
0	IPSec VPN				
6	拨号 VPN	~	说明	客户端	配置文件
-			Installer (32-bit), Windows XP and later	openvpn-install-2.3.4-1003-1686.exe	windows-openvpn-client.zip
÷	账号列表		Installer (64-bit), Windows XP and later	openvpn-install-2.3.4-1003-x86_64.exe	windows-openvpn-client.zip
	ex MADI/ 77		Installer (32-bit), Windows Vista and later	openvpn-install-2.3.4-1603-i686.exe	windows-openvpn-client.zip
	机械带写		Installer (64-bit), Windows Vista and later	openvpn-install-2.3.4-1603-x86_64.exe	windows-openvpn-client.zip
	设置		Centos	sudo yum install openvpn	linux-openvpn-client.tar.gz
			Debian/Ubuntu	sudo apt-get install openvpn	linux-openvpn-client.tar.gz
,	VPN服务管理	Ł			
•	有户纳下载				
6	SNAT				
0	TCP隧道				
J	ICP脏道				

点击客户端下载按钮,可以下载 VPN 客户端和相应的配置文件。

- Windows 平台:安装完客户端后,将配置文件 client.ovpn 和 ca.crt 文件放到安装目录 下的 config 文件夹中。然后启动 openvpn-gui.exe,根据提示进行连接。
- Linux 平台:在配置文件 client.conf 和 ca.crt 的目录下执行命令:openvpn client.conf, 根据提示进行连接。若要以 daemon 形式在后台执行,请执行:openvpn client.conf & 来建立连接。
- ▶ 注:在 Linux 平台下载客户端时,需要关闭证书验证。wget 请加上参数--no-checkcertificate, curl 请加上参数--insecure。

2.6、查看账号列表

点击账号列表按钮,可以查看已经添加的账号列表。如果该账号已经拨入 VPN,将看到 更明细的信息:

6	云顶	云VP	PN
功能	溁单	=	
0	IPSec VPN		
<b></b>	拨号 VPN	×	
	账号列表		
÷	新增账号		
•	说服		
•	VPN服务管理		
•	春户端下载		
(	SNAT		
0	TCP隧道		

▶ 状态:由于 VPN 的 keepalive 机制,会有1分钟左右的延时

## 六、SNAT 配置

当你想让 VPC 内的私网 ECS 能够访问公网时,需要在 VPC 中的 GateWay ECS 进行 SNAT 配置

1、添加 SNAT 条目 进入 SNAT 的 SNAT 新增页面:

		云VPN网	於管理系统		() 注销	
	ひが記葉単         ・ 1 PSec VPN         ・ 1 PSec VPN         ・ 1 PSec VPN         ・ 1 SNAT PU         ・ SNAT PU         ・ SNAT PU         ・ SNAT PU         ・ SNAT PU	2 (PINA ) ) ) )	972 E14E56437 128 : [HIAKKOP] 3/4474 *@HERMONIP (10782) *HERMONP	MARIP , 42-471/06/2015/1749/04/06/17 Hole. 10.0.1.20 10.0.1.1 0277		
~		1 ~ 7 \				

需转换的源 IP(或网段):为 VPC 中需要访问公网的私网网段或 IP。本例中为: 10.0.1.20

▶ 转换后的 IP:为 VPC 中 GateWay ECS 的私网 IP,而非 EIP。本例中为:10.0.1.1
 2、查看 SNAT 列表

新增 SNAT 条目之后,可以去 SNAT 列表页面中查看:

			网大自连系统		
the field of the field					
IDSEC VPN         <	功能鼓前	_	需转换的源IP(或网段)	转换后的IP	操作
<ul> <li>IPSec VPN →</li> <li>炭号 VPN →</li> <li>SNAT v</li> <li>SNAT pra</li> <li>SNAT ##</li> <li>SNAT ##</li> </ul>	-908634-44	-	10.0.1.20	10.0.1.1	删除
<ul> <li></li></ul>	IPSec V	VPN >			
<ul> <li>SNAT yx</li> <li>SNAT P3R</li> <li>SNAT #38</li> <li>TCP医器 &gt;</li> </ul>		PN >			
SNAT 時間     SNAT 時間     TCPRE語 >	SNAT	v			
・ SNAT 新田 <b>、 TCP版語</b> >	• SNAT	列表			
С тсрва	► SNAT	新增			
	🗔 тср膨	ă >			
	源 IP(武	网段	):为VPC 中需要	要访问公网的私网	网段。本伯

- ▶ 转换后的 IP:为 VPC 中 GateWay ECS 的私网 IP,而非 EIP。本例中为:10.0.1.1
- ▶ 删除:点击删除按钮,即可删除该 SNAT 条目,且立即生效。

## 七、TCP 隧道

当您想要访问 VPC 内部某台 ECS 的特定端口,可以通过本功能将该端口映射到 vpnManager 机器,然后通过 vpnManager 的 EIP 访问。

 1、	添加	TCP	隧道
T /	7/Jiv /J H	101	

ć	<b>》</b> 云顶	云VP	N网关管理系统		(1) 进
功能	藻单	-	*本地端口	3306	
0	IPSec VPN		*日标IP	10.0.1.10	
(2)	拨号 VPN		*目标端口	3306	
	SNAT			<del>977</del>	
0	TCP隧道	v			
•	TCP 隧道列表	ŧ			
	TCP 隧道新增				

- ▶ 本地端口:为 vpnManager 为转发打开的端口。本例中为:3306
- ▶ 目标 IP:为 VPC 中需要访问公网的私网 IP。本例中为:10.0.1.10
- ▶ 目标端口:为目标机器的端口。本例中为:3306
- 2、查看 TCP 隧道列表

新增 TCP 隧道条目之后,我们可以在 TCP 隧道列表页面中查看如下:

ළ	去顶云VPN网关管	管理系统				
功能	標单 ■	本地端口	目标IP	目标端口 3306	操作	
0	IPSec VPN					
۵	拨号 VPN >					
۷	SNAT >					
0	TCP醛道 v					
	TCP 隧道列表					
÷	TCP 隧道新增					

- ▶ 本地端口:为 vpnManager 为转发打开的端口
- ▶ 目标 IP:为 VPC 中需要访问公网的私网 IP。本例中为:10.0.0.1
- ▶ 目标端口:为目标机器的端口。本例中为:3306
- ▶ 关闭:点击关闭按钮,即可关闭该 TCP 隧道,且立即生效。