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

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

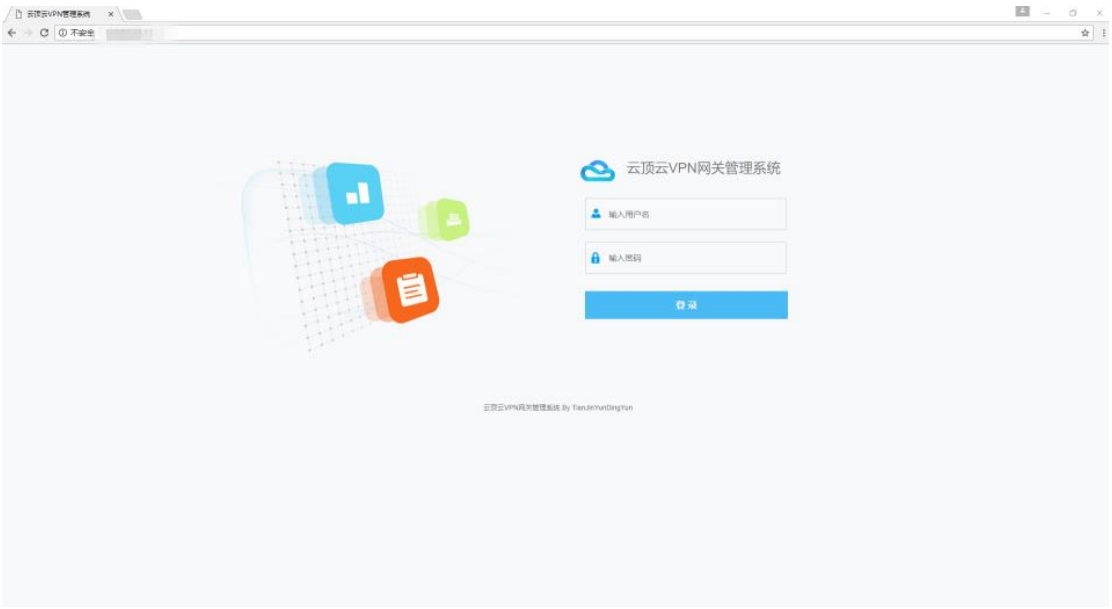
启动命令：systemctl start openvpn@server.service

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/



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 中各有一台使用 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

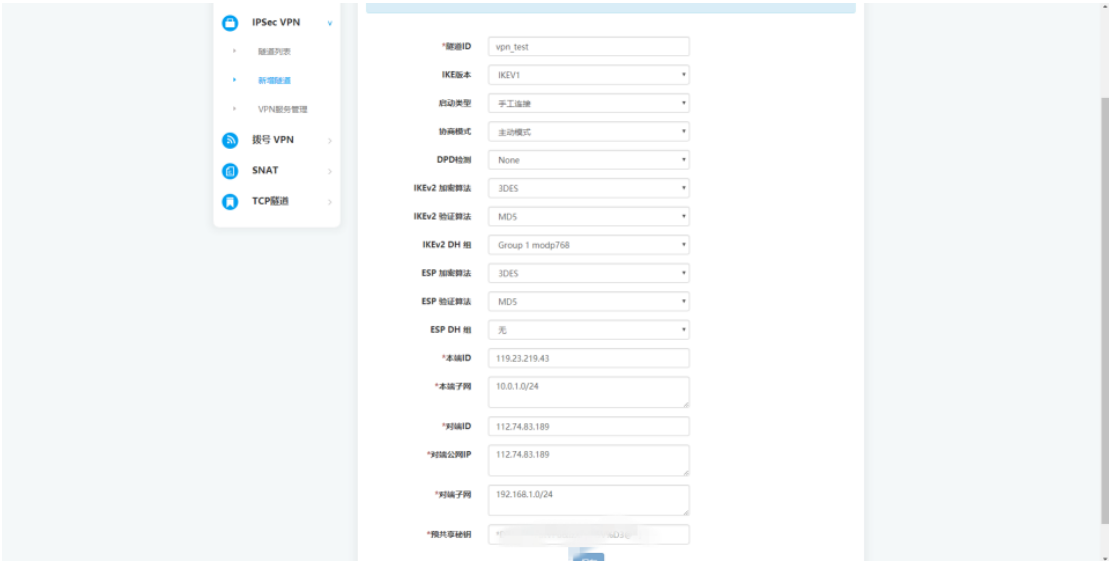
1、启动 IPSec VPN 服务

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。

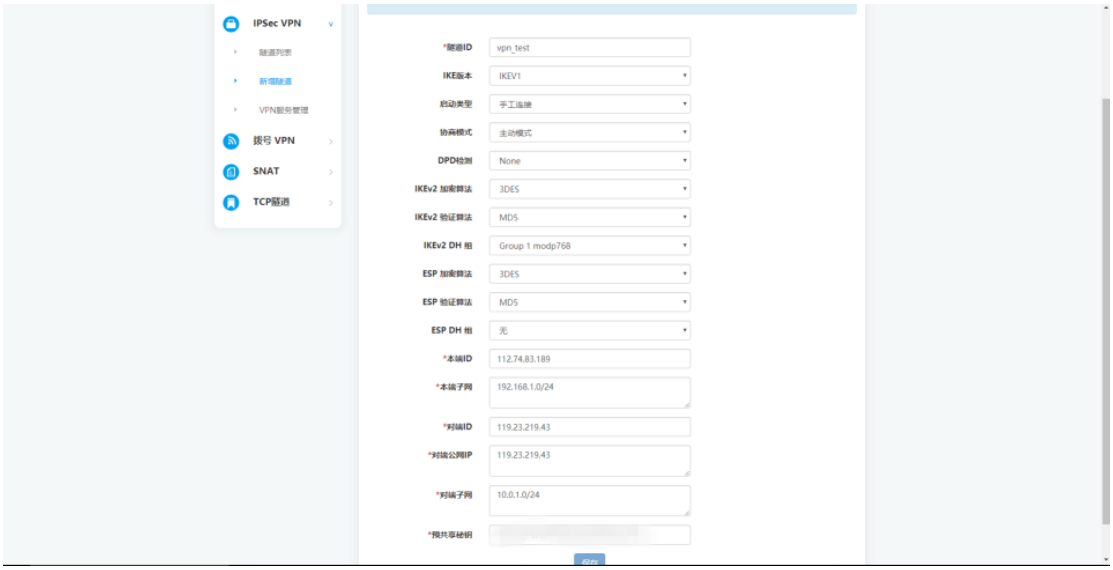
- 启动 VPN 服务：仅启动本机的 IPSec VPN。启动时，启动类型为自动连接的隧道将自动尝试连接对端 VPN。
- 停止 VPN 服务：停止本机的 IPSec VPN。已经连接上的隧道将全部断开。
- 配置下发&重载：一般情况下，该动作在新增、修改或删除隧道时会自动进行。但某些情况下，如果你想重新生成 VPN 配置，可手动执行该操作。

2、新增隧道

VPC1 GateWay ECS:



VPC2 GateWay ECS:



- 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。

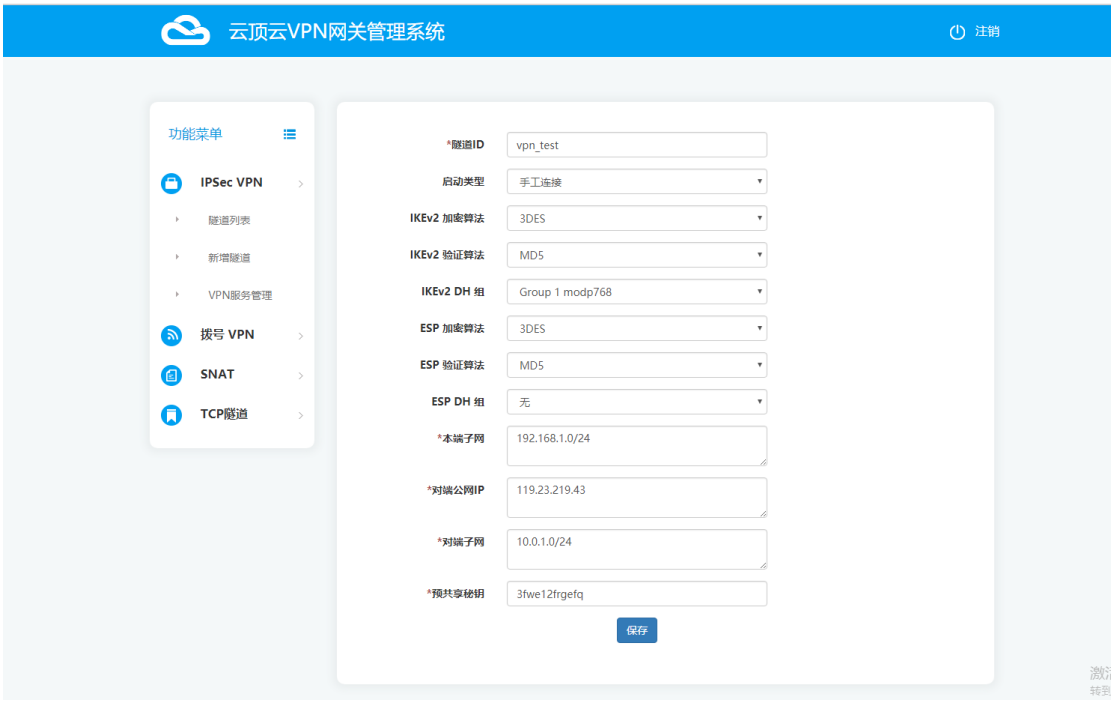
3、查看隧道列表或删除

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：

- 连接：连接隧道。在两台GateWay ECS任意一端操作即可。
- 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。



五、拨号 VPN

1、应用场景

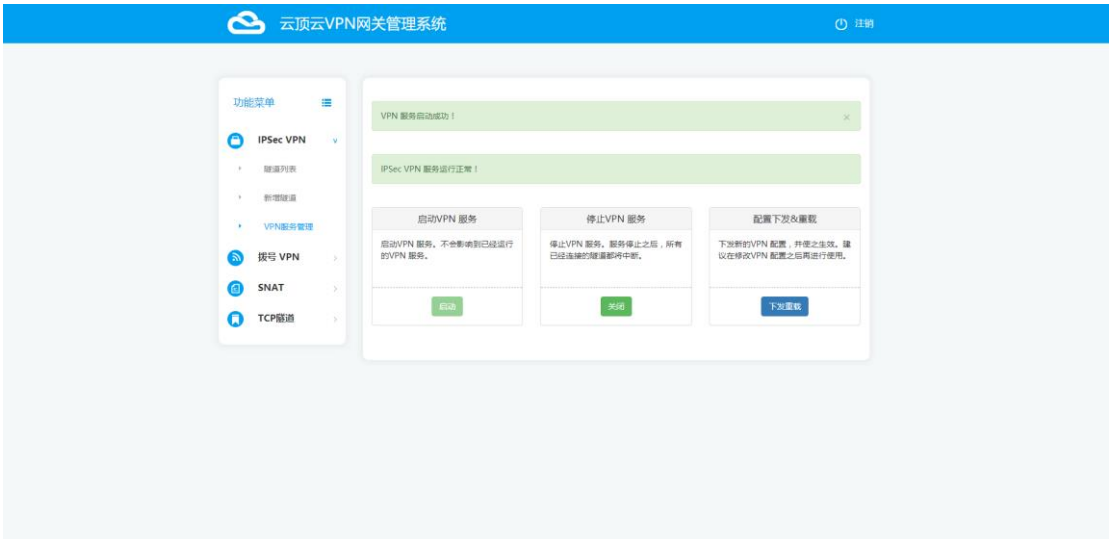
- Classic 网络场景。跨账号、跨地域的云服务器之间内网互通。
- VPC 网络场景。管理员接入 VPC 进行私网访问、管理。

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

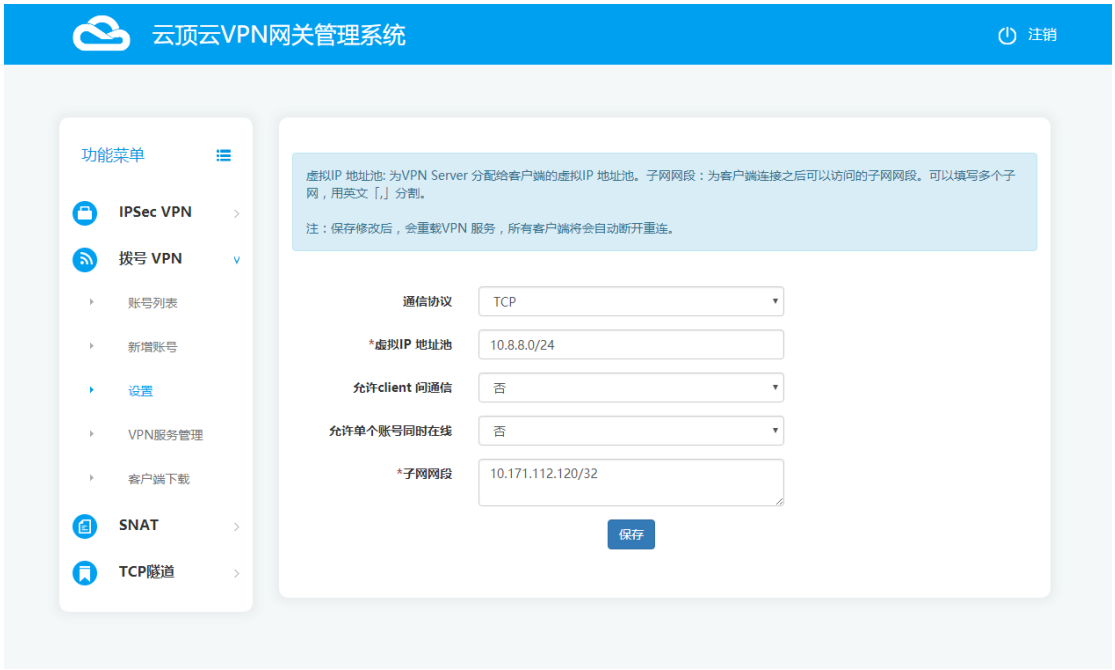
进入拨号 VPN 的 VPN 服务管理页面，确保 GateWay ECS 启动了拨号 VPN 服务。



- 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

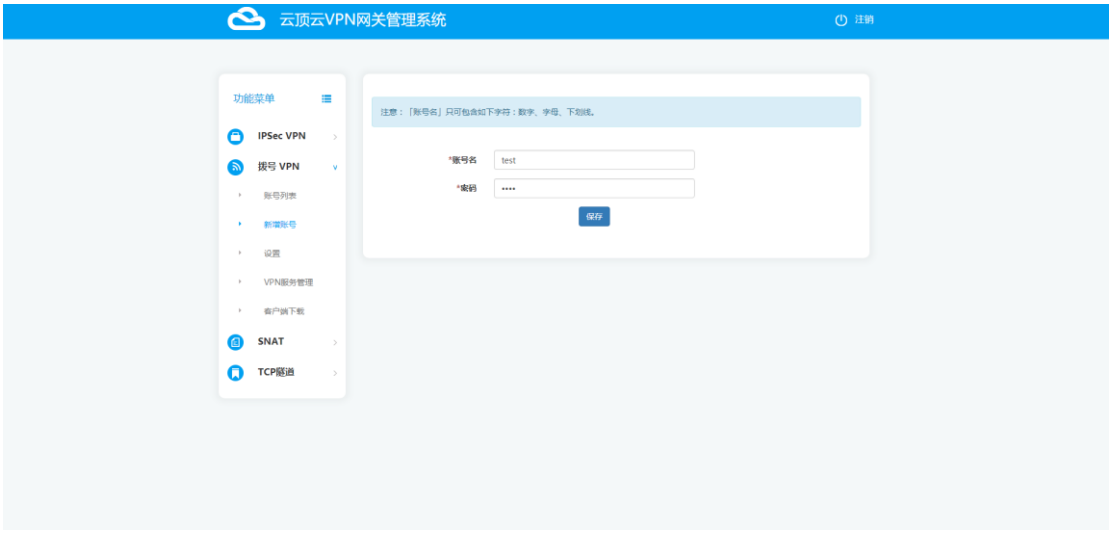


- 通信协议：可选"UDP"、"TCP"。注：每次修改保存后，请重新下载客户端配置文件。
- 虚拟 IP 地址池：即 VPN Server 分配给客户端的虚拟 IP 地址池。本例为：10.8.8.0/24
- 允许 client 间通信：本例子中，这里请选“是”。
- 允许单个账号同时在线：可选“是”或“否”。

- 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

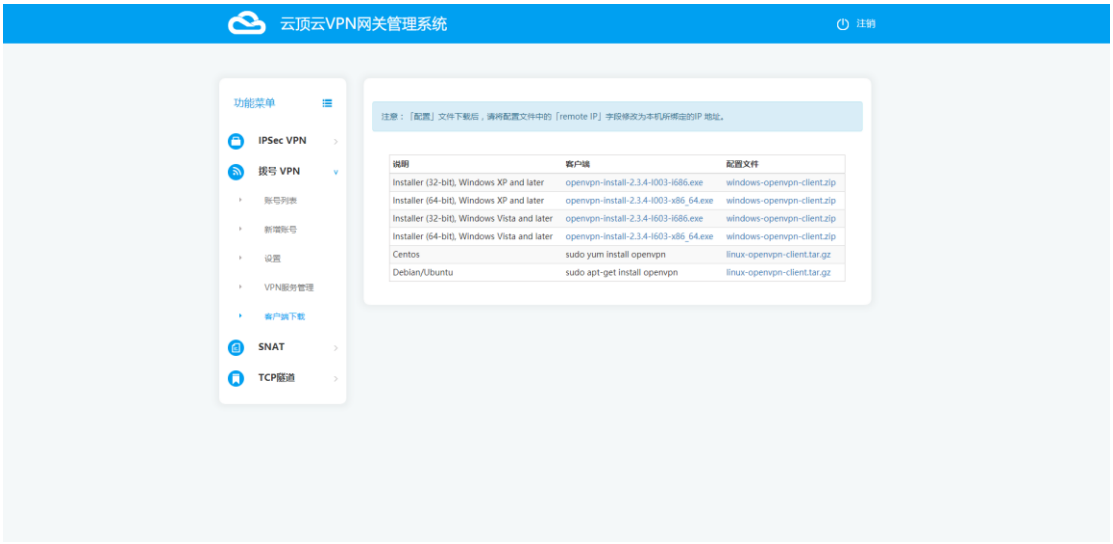
点击新增账号按钮，即可新增账号：



- 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。



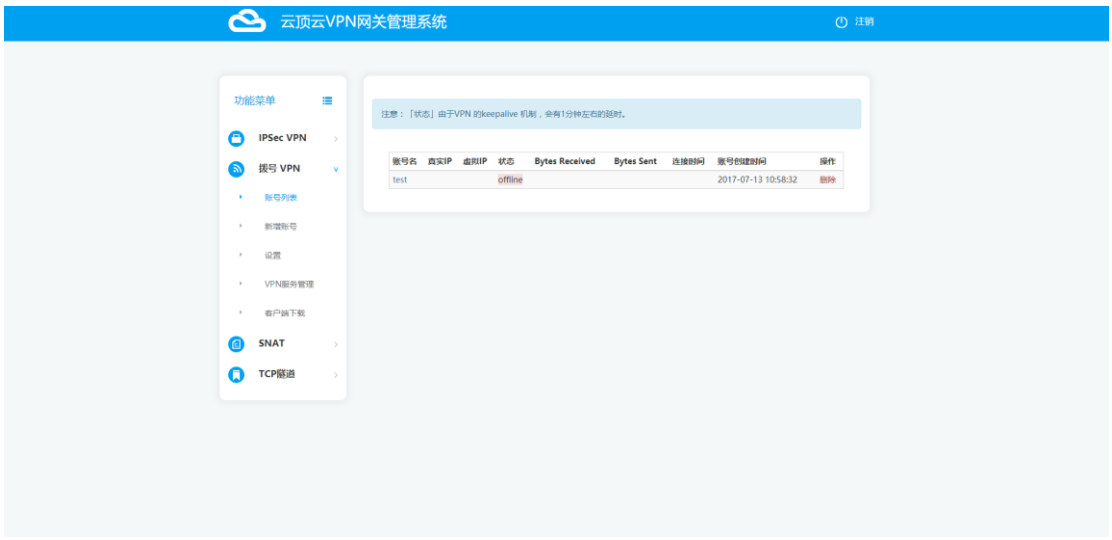
- Windows 平台：安装完客户端后，将配置文件 client.ovpn 和 ca.crt 文件放到安装目录下的 config 文件夹中。然后启动 openvpn-gui.exe，根据提示进行连接。
- Linux 平台 :在配置文件 client.conf 和 ca.crt 的目录下执行命令 :openvpn client.conf，根据提示进行连接。若要以 daemon 形式在后台执行，请执行：openvpn client.conf & 来

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-check-certificate, 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：



- 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

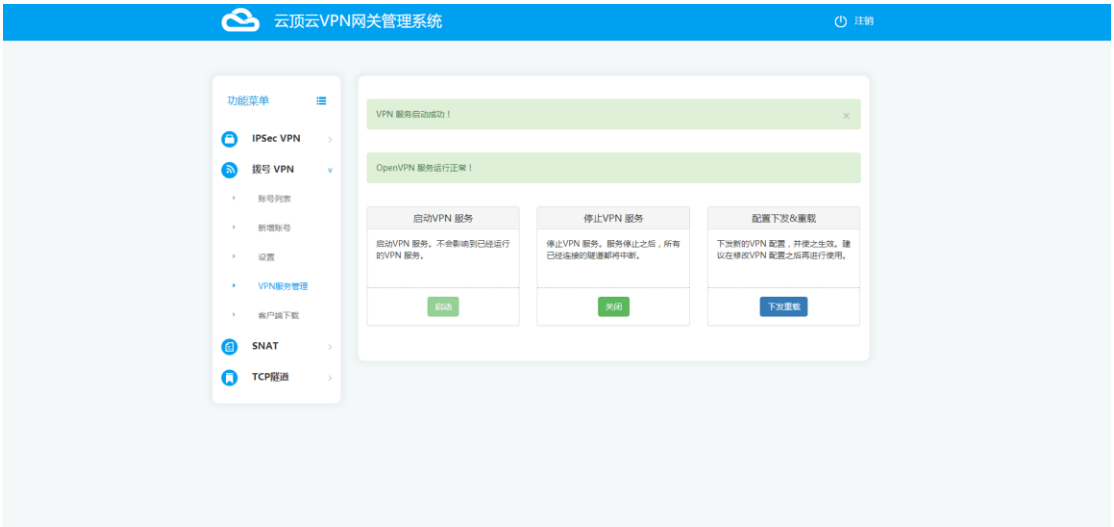
现在，即可使用 VPN 分配的地址 10.8.8.7、10.8.8.9 进行相互通信了。

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

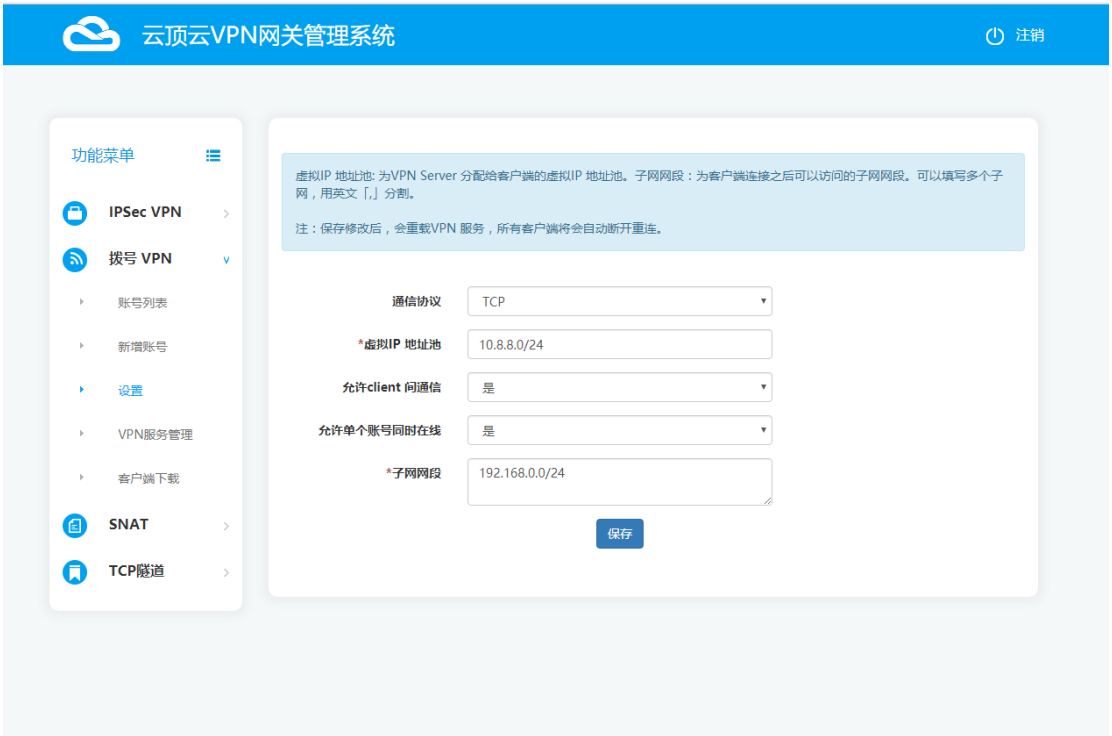
进入拨号 VPN 的 VPN 服务管理页面，确保 GateWay ECS 启动了拨号 VPN 服务。



- 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

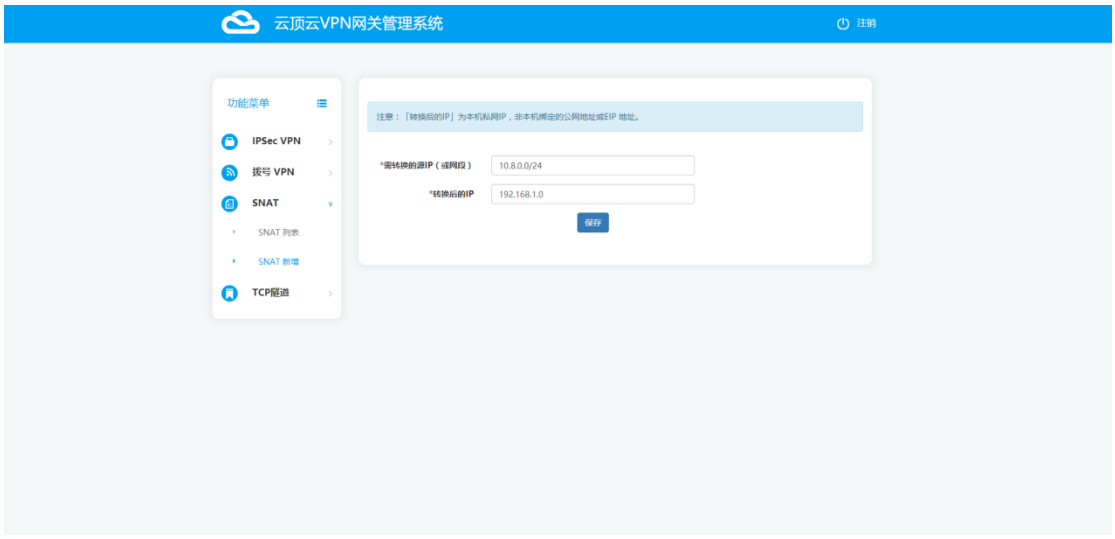


- 通信协议：可选"UDP"、"TCP"。注：每次修改保存后，请重新下载客户端配置文件。
- 虚拟 IP 地址池：即 VPN Server 分配给客户端的虚拟 IP 地址池。
- 允许 client 间通信：可“是”或“否”。

- 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

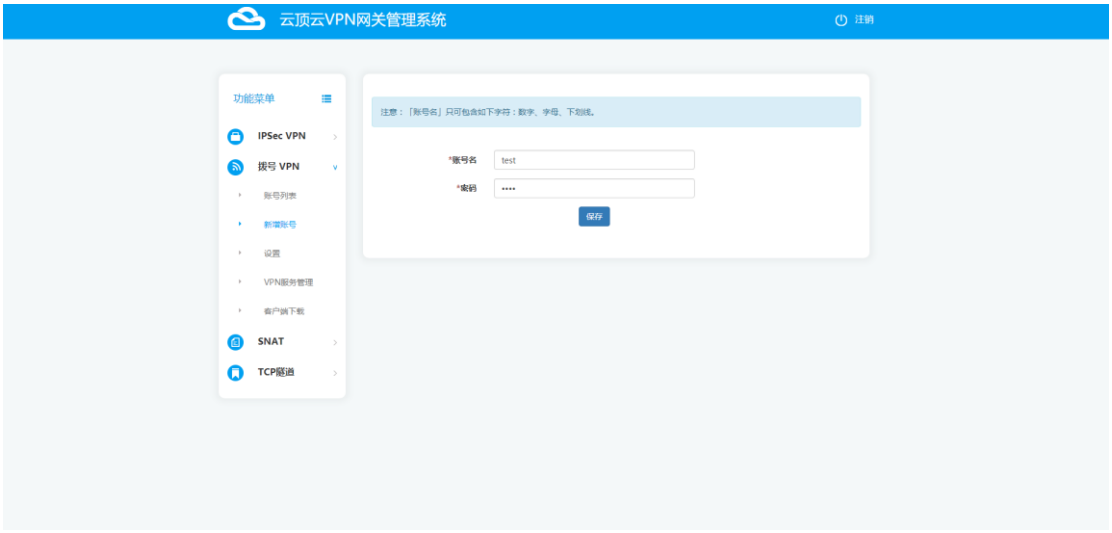
进行拨号 VPN 设置之后，为了让管理员能够访问 VPC2 的私网，需要手工调整相应的 SNAT 设置！



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

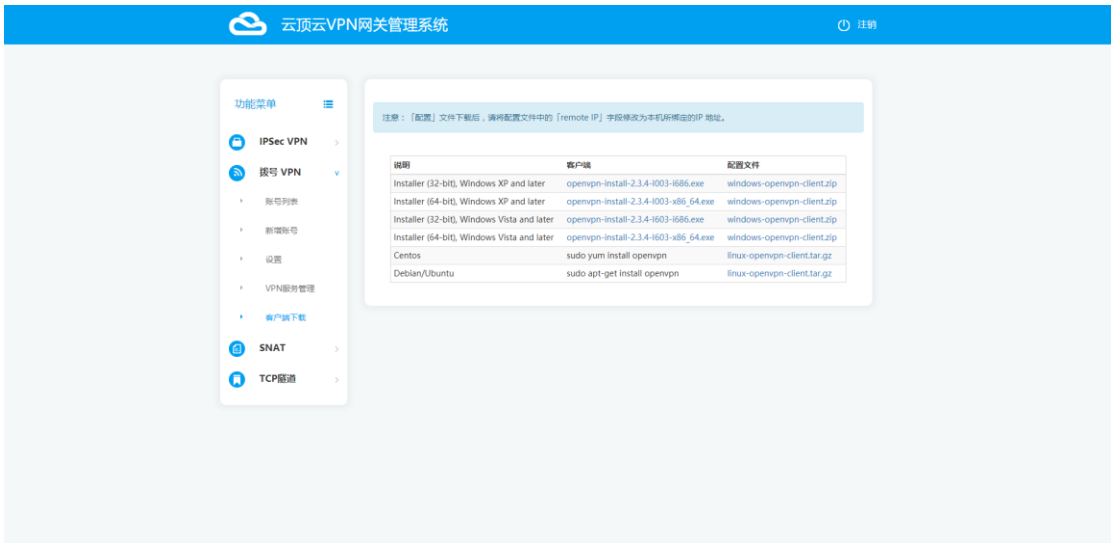
点击新增账号按钮，即可新增账号：



- 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

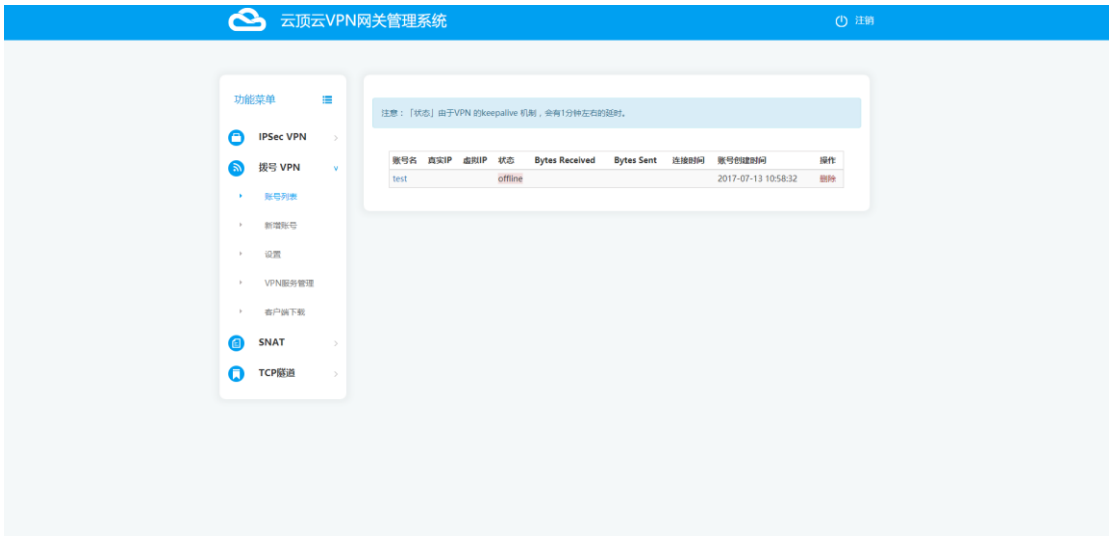
点击客户端下载按钮，可以下载 VPN 客户端和相应的配置文件。



- 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-check-certificate, 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：



- 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

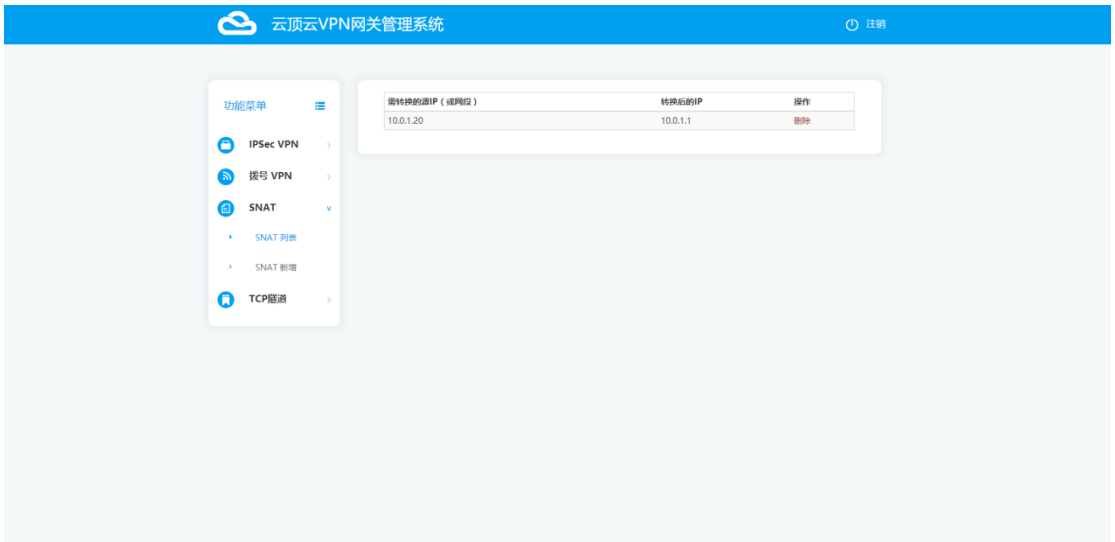
1、添加 SNAT 条目

进入 SNAT 的 SNAT 新增页面：

- 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：

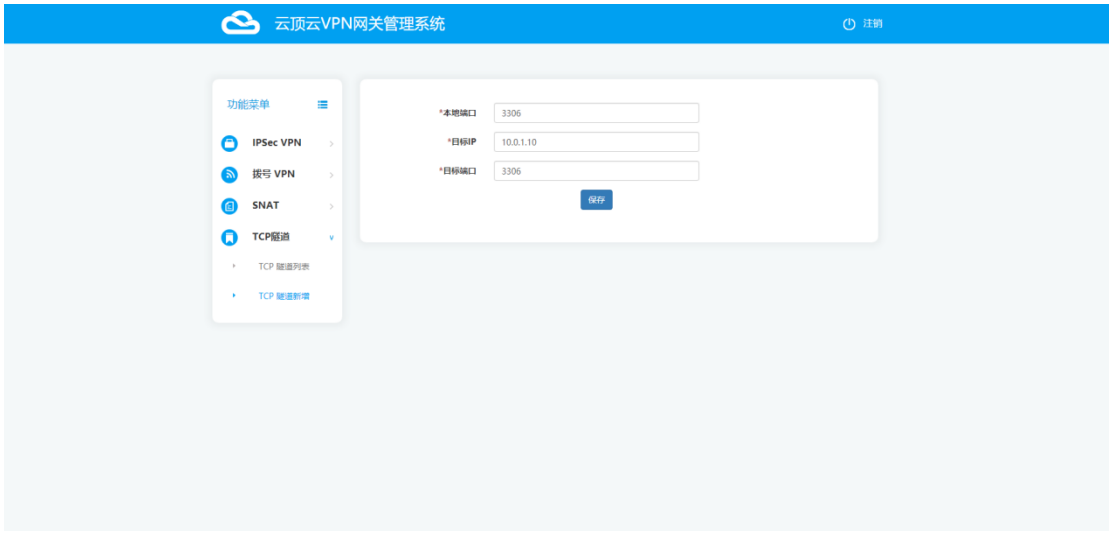


- 需转换的源 IP（或网段）：为 VPC 中需要访问公网的私网网段。本例中为：10.0.1.20
- 转换后的 IP：为 VPC 中 GateWay ECS 的私网 IP，而非 EIP。本例中为：10.0.1.1
- 删除：点击删除按钮，即可删除该 SNAT 条目，且立即生效。

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。

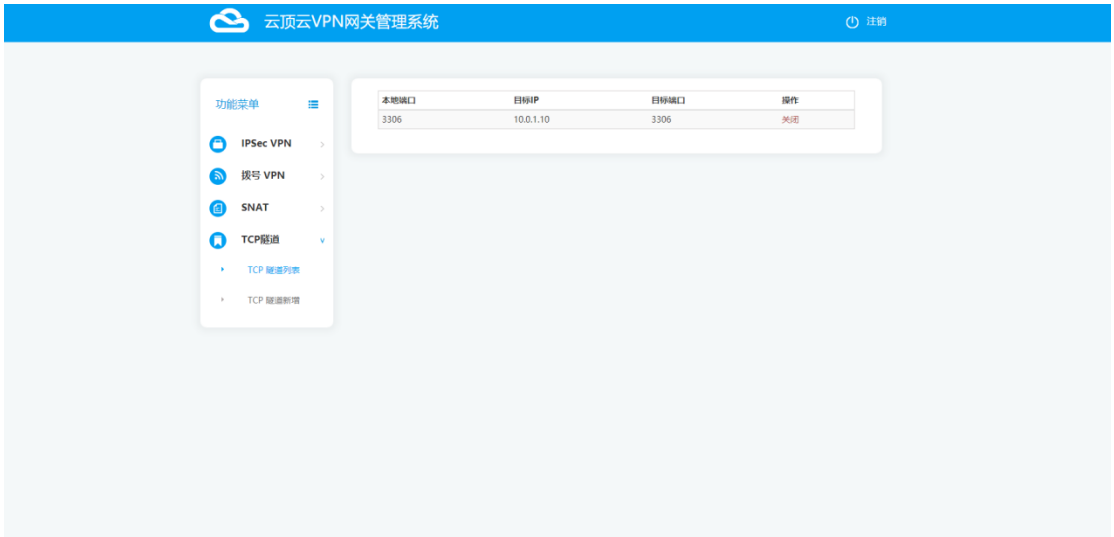
1、添加 TCP 隧道



- 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：



- 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。