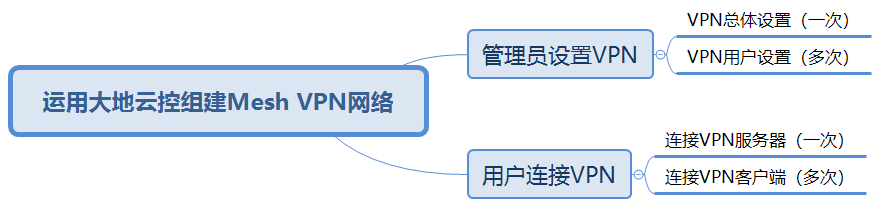
**运用中神通大地云控组建Mesh VPN网络**

武汉中神通信息技术有限公司

在线链接：http://trustcomputing.com.cn/cn/index.php/support/techdocs/zst\_mesh\_vpn

本文下载：http://trustcomputing.com.cn/help/zst\_mesh\_vpn.docx

本文从管理员和用户两个维度描述了如何运用中神通大地云控系统的WireGuard VPN模块组建及运用Mesh VPN网络，步骤如图1所示。

**图1** Mesh VPN设置步骤示意图

## 一、管理员设置WireGuard VPN服务器

### 1.1 WireGuard VPN总体设置

点击左边主菜单“VPN服务器>总体设置”项，在右边页面TAB中点击“WireGuard VPN”，出现“WireGuard VPN>总体设置”界面，如下图2所示：

****

**图2**“WireGuard VPN>总体设置”界面

各参数说明如下：

1）WireGuard VPN：**启用**

启用WireGuard VPN服务器，缺省是“停用”。

2）SNAT-虚拟IP上网：**停用**

VPN虚拟IP能否通过SNAT方式上外网，缺省是“停用”。

如果是组建P2P/Mesh网络，就不需要上外网。

3）服务器端口：52021

WireGuard VPN服务器监听的UDP端口缺省为“52021”，可以更改。

4）虚拟IP地址池：**10.9.0.0/24（缺省配置/自定义）**

WireGuard VPN客户端连接成功后分配的虚拟IP所在的网络，缺省为 “10.9.0.0/24”，IPv4 CIDR格式，根据接入客户端的数量进行更改，“/24”能接入200多客户端。

5）源IP控制：0.0.0.0/0,::/0

允许WireGuard VPN客户端连接的源IPv4及IPv6地址范围，缺省是 “0.0.0.0/0,::/0”，可以更改。

6）目的路由控制：**10.9.0.0/24（自定义）**

允许WireGuard VPN客户端连接的目的IPv4地址范围，缺省是 “0.0.0.0/1,128.0.0.0/1”（需要启用SNAT），可以更改。

如果是组建P2P/Mesh网络，不需要上外网，“目的路由控制”的内容一般就是“虚拟IP地址池”的内容。

7）时间控制：ALL\_time

本服务开放的时间，缺省为“ALL\_time”，一周7天，每天24小时，可以更改。

8）流量控制：停用

统计/限制WireGuard VPN客户端产生的流量，缺省是“停用”，可以更改。

9）服务器公钥：**（自动生成/自定义）**

WireGuard VPN服务器的公钥，用于各客户端的配置文件，是中神通大地云控第一次启动时自动生成的，对应的私钥保密，没有在WEBAdmin上显示。可以点击右边的“更新”按钮更新公私钥对，此前生成的用户的客户端配置文件需要重新下载。

10）客户端认证方法：私钥和公钥认证

WireGuard VPN客户端认证方法和用户名密码无关，缺省是“私钥和公钥认证”，另外可选“私钥和公钥+TOTP动态密码认证”。

11）客户端DNS服务器：**（空）**

设置客户端配置文件中的DNS项，是为了Windows客户端连接成功后自动设置DNS解析服务器，缺省是“8.8.8.8”。

如果是组建P2P/Mesh网络，可以不设置客户端DNS服务器。

### 1.2 WireGuard VPN用户

为了组建一个Mesh VPN网络，至少要新建三个用户。点击“WireGuard VPN>总体设置”界面下方的“用户”按钮，或者点击左边主菜单“VPN服务器>用户管理”项，在右边页面TAB中点击“WireGuard VPN”，出现“WireGuard VPN>用户”列表界面，如下图3所示：

****

**图3**“WireGuard VPN>用户”列表界面

在此界面显示当前的WireGuard VPN用户列表信息及登录状态。点击下方的“新建”按钮，进入用户设置界面，如下图4所示：



**图4**“WireGuard VPN>用户”设置界面

各参数说明如下：

1）登录账号：**（自定义）**

“登录账号”只用于登录、使用WEB用户门户，并不用于客户端软件配置文件，但可以起到标识的作用，以字母开头。

2）用户姓名：（自定义）

“用户姓名”起到标识作用，在用户列表、设置、状态中显示，缺省为空，即“登录账号”的内容，可以更改，可以是中文。

3）用户组：WireGuard\_usergroup

WireGuard VPN用户所在的用户组，用于系统内部区别其它VPN/SSH/WEB用户，此“WireGuard\_usergroup”字符串是内置的、固定的。

4）用户端口映射：停用

WireGuard VPN客户端连接成功后，可以通过外网DNAT端口映射功能，将TCP/UDP流量映射到VPN虚拟IP上，缺省为“停用”。

5）用户URL：停用

WireGuard VPN客户端连接成功后，可以通过URL反代功能，将HTTP/HTTPS流量映射到VPN虚拟IP的WEB服务器上，缺省为“停用”。

6）外内URL映射关系：（空）

启用“用户URL”功能后的URL映射关系，缺省为空。

7）客户端认证方法：私钥和公钥认证

即“WireGuard VPN>总体设置”中的“客户端认证方法”的内容，此处只是提示。

8）强制登录用户门户：停用

新创建的WireGuard VPN用户是否需要先登录WEB用户门户，缺省是“停用”，如果改成“启用”，那么用户要先登录WEB用户门户，修改初始口令，才能正常使用。

9）口令/重复口令：**（自定义）**

“口令/重复口令”至少8位，至少是字母和数字的组合，和“登录账号”一样，只用于登录、使用WEB用户门户，并不用于软件的配置文件。如果不填写，实际口令为“12345678”，需要管理员修改或用户登录WEB用户门户修改口令才能正常使用。如果启用了“强制登录用户门户”，则用户要先登录WEB用户门户，修改初始口令，才能正常使用。

10）WireGuard公钥：**（自动生成/自定义）**

WireGuard VPN客户端用户的公钥，用于WireGuard VPN服务器的配置文件，初始内容是新建用户时自动生成的，和WireGuard私钥配对使用。

11）WireGuard私钥：**（自动生成/自定义）**

WireGuard VPN客户端用户的私钥，用于WireGuard VPN客户端的配置文件，初始内容是新建用户时自动生成的，和WireGuard公钥配对使用。

12）绑定IP地址：**（自动生成/自定义）**

“绑定IP地址”是WireGuard VPN客户端软件连接成功后分配的虚拟IP，初始内容是新建用户时自动生成的。

13）创建时间：（自定义）

“创建时间”是管理员新建用户时自动生成的，方便管理员查看。

14）有效期至：**（自动生成/自定义）**

“有效期至”是该用户的有效时间，初始内容是自动生成的，缺省是100年，起始时间为管理员新建用户的时间。另外还可以设置起始时间为用户登录WEB用户门户并修改初始口令后生效，具体查看《中神通大地EDR&DNS&URL&VPN云控管系统-管理员手册》。

15）流量控制：停用

“流量控制”用于统计/控制VPN客户端连接后的流量，即“WireGuard VPN>总体设置”中的“流量控制”的内容，此处只是提示，缺省为“停用”。

16）策略推送：停用

“策略推送”用于自动设置VPN客户端，类似SDN/SD-WAN，达到客户端0配置的目的，缺省为“停用”

17）备注：（自定义）

“备注”的内容是为了方便管理员设置、查看该用户的其它信息。

**注意：**公众版本最多只能创建3个WireGuard VPN用户，且无法使用WEB用户门户及策略推送功能。

## 二、用户连接WireGuard VPN——公众版本

由于公众版本的限制，用户无法使用WEB用户门户，只能在管理员的帮助下进行VPN连接操作。

### 2.1 用户连接WireGuard VPN服务器

#### 2.1.1 用户或管理员下载安装WireGuard VPN客户端软件

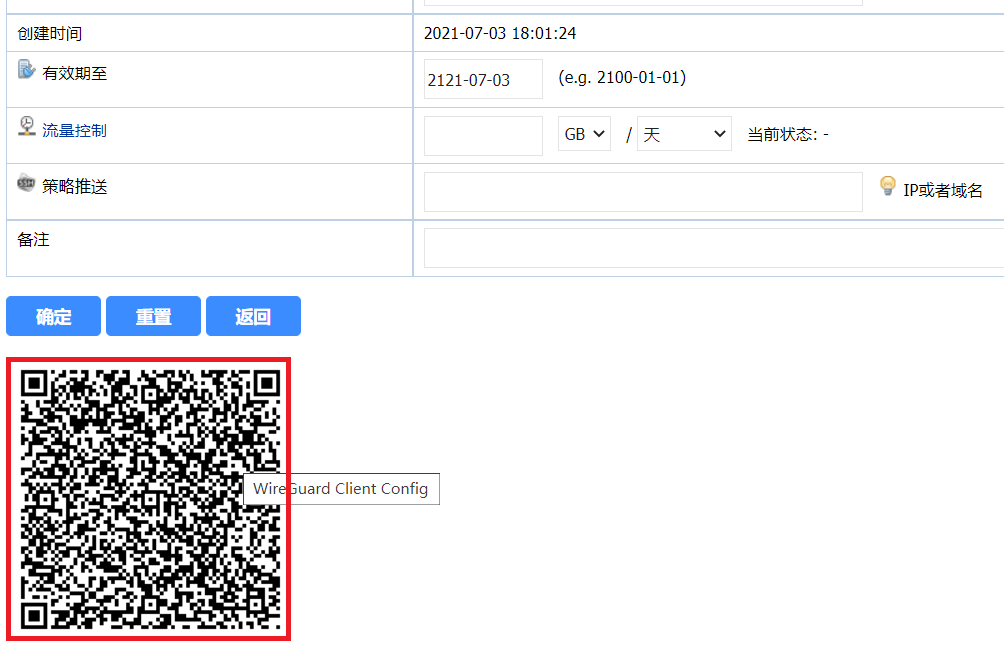
参考“WireGuard软件资源”页面内容，安装Windows客户端软件及优化注册表，网址是“http://trustcomputing.com.cn/bbs/viewthread.php?tid=1815”。对于Linux客户端，最好安装使用大地云控系统，网址是“http://trustcomputing.com.cn/bbs/viewthread.php?tid=1174”。

其它OS可以下载官方客户端软件，但是只能用于连接VPN服务器，无法进行P2P/Mesh VPN自动组网。

#### 2.1.2 管理员下载客户端配置文件

管理员在“WireGuard VPN>用户”列表界面中，右键点击一行的任意位置或左键点击右边的修改按钮，出现“WireGuard VPN>用户”修改界面，并拉到最下面，找到配置文件的二维码，如下图5所示：

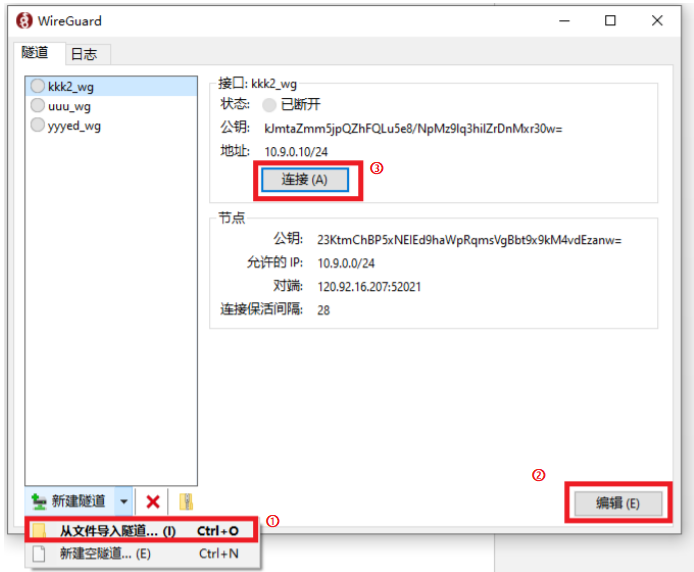


****

**图5**管理员下载WireGuard VPN客户端软件配置文件

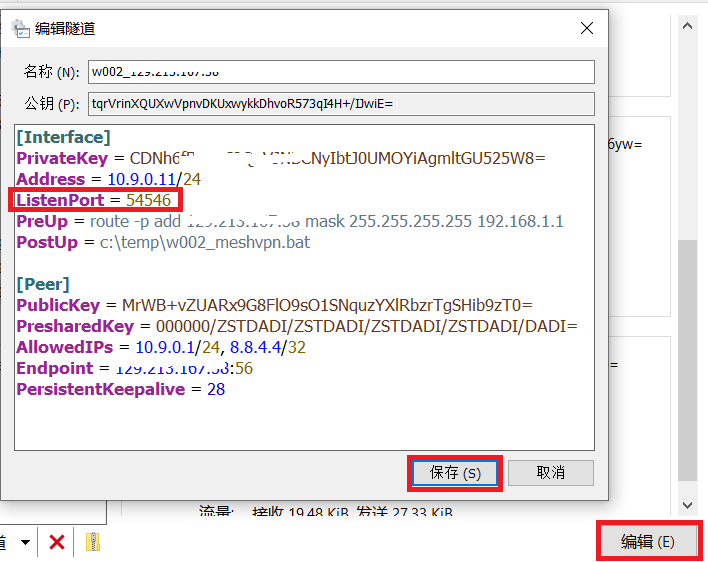
如果是手机用户，可以打开WireGuard VPN APP，点击添加配置按钮，扫描此二维码导入配置文件。

对于Windows用户，点击此二维码图片，下载文件客户端配置文件，文件名格式是“[登录账号]\_[外网地址].conf”。用户或管理员再打开WireGuard VPN客户端软件，按照下图6所示①导入配置文件，根据实际情况②查看、编辑客户端配置文件，再③连接VPN服务器。



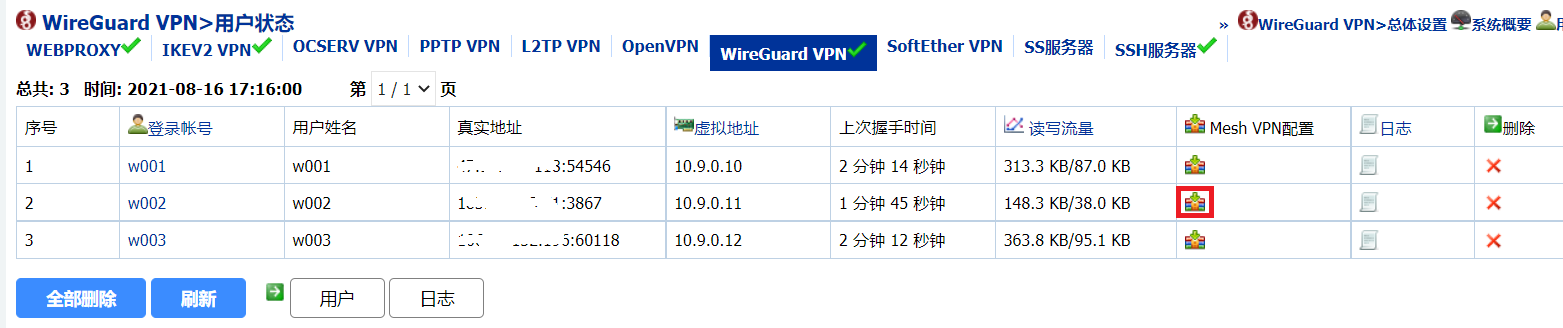
**图6** Windows用户导入使用WireGuard VPN客户端软件配置文件

对于有固定公网IP的WireGuard VPN客户端，为了保持客户端软件监听端口不变，可以启用“**ListenPort** ”，将监听端口设置为一个固定的值，例如：54546，如图7所示。



**图7** 使用WireGuard VPN客户端软件编辑配置文件

全部用户成功连接VPN服务器后，管理员可以在WEBAdmin的“WireGuard VPN>用户状态”界面查看当前连接状态，如下图8所示。



**图8** “WireGuard VPN>用户状态”界面

### 2.2 用户连接其它VPN客户端

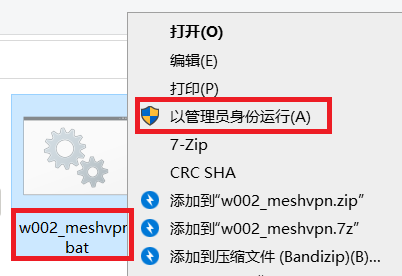
#### 2.2.1 管理员下载Mesh VPN配置文件

全部用户成功连接VPN服务器后，管理员在“WireGuard VPN>用户状态”界面中，点击图符，下载用户的Mesh VPN配置文件，文件格式为“[用户名]\_meshvpn.bat”，主要内容是执行zstnet命令行，类似“zstnet xxx yyy”，适用于Windows和Linux系统。一个Mesh VPN配置文件只能用于一个用户，其他用户无法使用。

#### 2.2.2 用户或管理员运行Mesh VPN配置文件

对于Windows用户，鼠标右键点击bat文件，选择“以管理员身份运行(A)”项，如下图9所示。也可以拷贝bat批处理文件的内容，粘贴到以管理员身份运行的CMD Shell中执行。

zstnet.exe文件下载网址是“http://www.trustcomputing.com.cn/tools/zstnet.exe”，需要拷贝到任一Windows可执行文件目录（ 查看PATH变量）中。

****

**图9** Windows下运行meshvpn批处理文件

对于Linux用户，将bat批处理文件上传到Linux中，再以root身份执行“sh xxx\_meshvpn.bat”。也可以拷贝bat批处理文件的内容，粘贴到Linux Shell中以root身份执行。

安装大地云控系统后，zstnet可执行文件位于/usr/bin/目录下。

当所有参与Mesh VPN组网的用户，都下载相应的xxx\_meshvpn.bat批处理文件并在各自OS下执行后，就构成了绕过VPN服务器的Mesh VPN网络。

组网成功后，如果有一台WireGuard VPN客户端断开后重连，公网IP或监听端口发生了变化，则其它客户端都要重新下载之有关的bat文件，找到对应的“zstnet”命令行程序并执行，可以使用任务计划程序等方式进行自动化监控；如果OS有固定的公网IP，并且监听端口（**ListenPort** ）固定（参考图7），则直接执行对应的“zstnet”命令行程序即可。

#### 2.2.3 用户或管理员验证Mesh VPN网络

P2P/Mesh VPN网络建立后，可以对VPN路由做验证，即在各自OS Shell下ping对方虚拟IP、查看ms值，再traceroute对方虚拟IP。

具体来说，假设w001用户的虚拟IP是10.9.0.10，w002用户的虚拟IP是10.9.0.11。

* 在w001的OS Shell下，测试w002的虚拟IP

ping 10.9.0.11

traceroute -n 10.9.0.11

netstat -nr（Windows）/ ip route get 10.9.0.11（Linux）

* 在w002的OS Shell下，测试w001的虚拟IP

ping 10.9.0.10

traceroute -n 10.9.0.10

netstat -nr（Windows）/ ip route get 10.9.0.10（Linux）

如果ping成功，并且traceroute只有1跳（Hop），则表明P2P/Mesh VPN网络建立成功，如下图10所示，由于是直接连接，绕过了VPN服务器，延时将大幅减少。



**图10** P2P VPN/Mesh VPN建立后的traceoute信息

如果ping成功，但路由有2跳（Hop），则仍然是通过VPN服务器（10.9.0.1）中转而不是VPN客户端之间直接连接，如下图11所示。



**图11**传统拨号VPN建立后的traceoute信息

**注意：**

1）在某些公有云中，必须先主动ping对方的虚拟IP，对方才能ping通该节点的虚拟IP

2）在某些公有云中，或Linux节点下，traceroute可能无法正常显示，可以先运行“ip route get [虚拟IP]”命令查看路由，再通过ping的ms值的变化间接验证，或者在对方Windows节点中做traceroute测试来验证

## 三、用户连接WireGuard VPN——正式版本

正式版本去除了公众版本的限制，用户可以使用WEB用户门户，管理员只负责提供用户初始认证数据，管理员可以通过Email/短信/聊天/办公/发卡系统分发用户初始认证数据，用户自己再通过WEB用户门户完成各项操作。

### 3.1 用户登录WEB用户门户

WEB用户门户网址的格式是“https://[外网地址]/my”，登录账号、初始口令就是管理员在“**1.2 WireGuard VPN用户**”中新建用户时的登录账号和口令。

首次登录强制用户修改口令，如下图 12 所示。



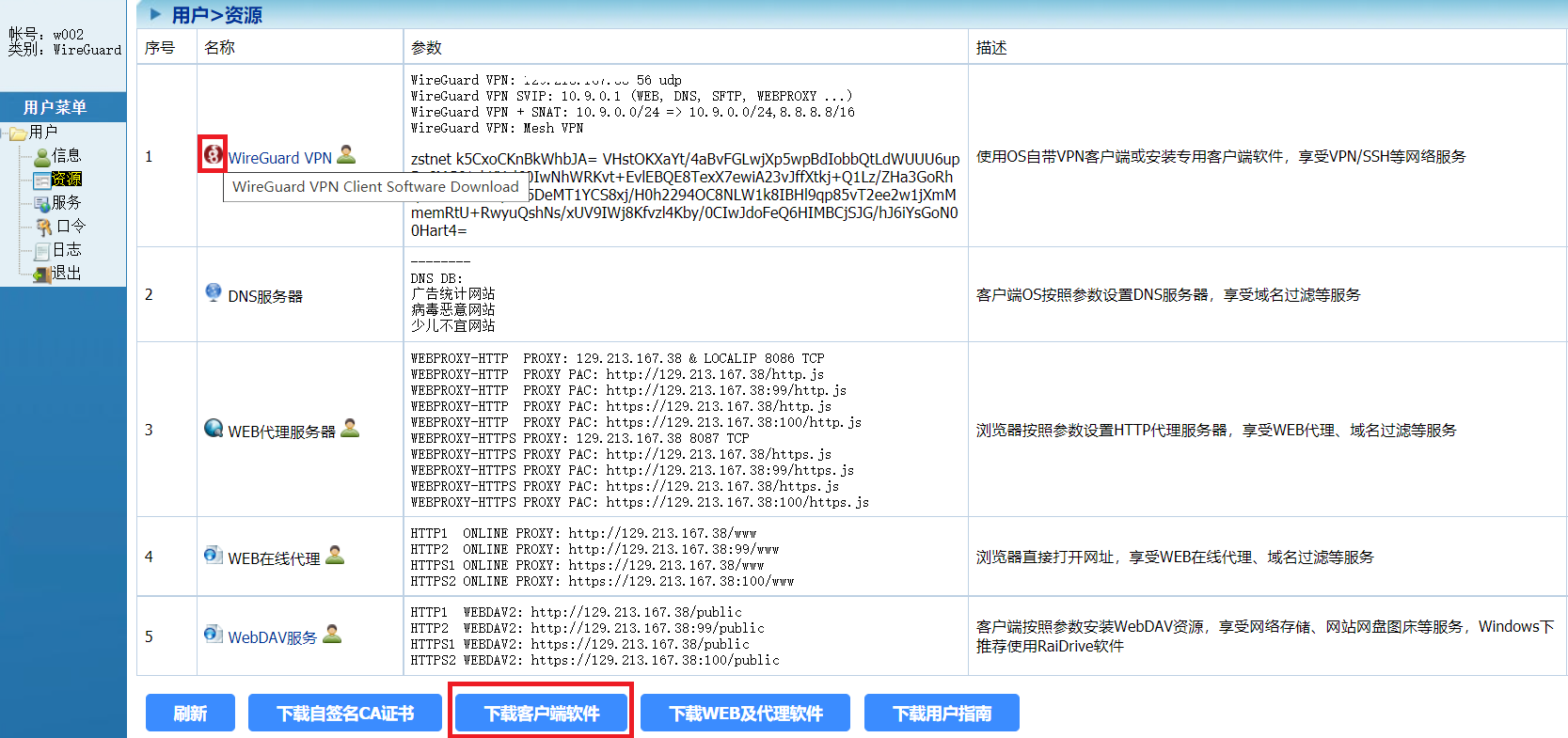
**图12**第一次登录用户门户强制修改口令

之后用户登录使用时，如果 10 分钟内累计三次输入错误的口令，则可能被系统屏蔽 10 分钟，如果忘记了口令只能向管理员求助。退出登录需要关闭整个浏览器，或者通过Chrome 浏览器的“打开新的无痕窗口”功能切换用户。

### 3.2 用户连接WireGuard VPN服务器

#### 3.2.1 用户下载安装WireGuard VPN客户端软件

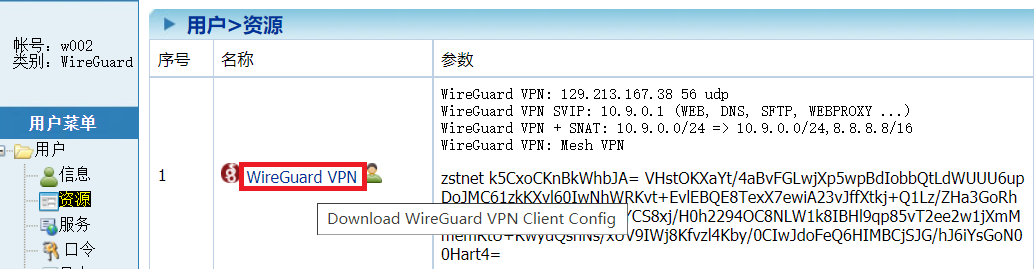
可以直接通过网址“http://www.trustcomputing.com.cn/tools/WireGuard.zip”下载Wireguard VPN客户端软件。或者在 WEB 用户门户的“资源”页面中，点击图符下载，或者点击下方的“下载客户端软件”按钮下载，如下图13所示。



**图13** WEB 用户门户的“资源”页面

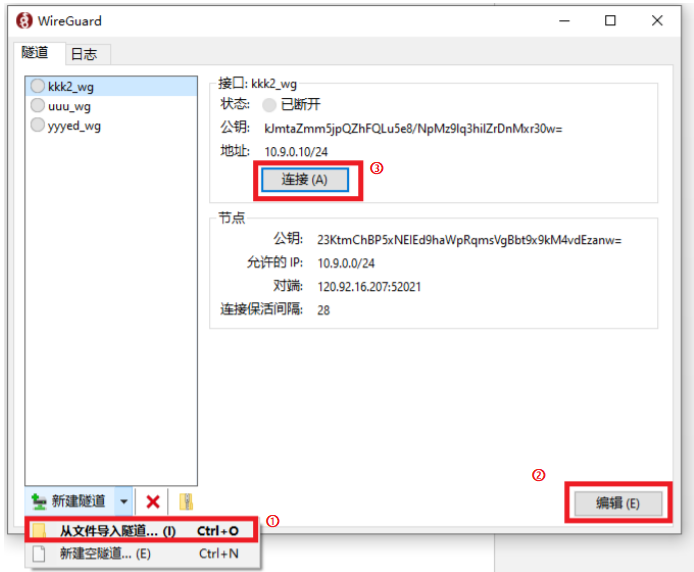
#### 3.2.2 用户下载客户端配置文件

在 WEB 用户门户的“资源”页面中，点击“WireGuard VPN”链接，下载当前账号的 Wireguard VPN客户端配置文件，文件名格式为“[登录账号]\_[外网地址].conf”，如下图14所示。



**图14** 用户下载WireGuard VPN客户端软件配置文件

用户再打开WireGuard VPN客户端软件，按照图6所示①导入配置文件，根据实际情况②查看、编辑客户端配置文件，再③连接WireGuard VPN服务器。



**图6** Windows用户导入使用WireGuard VPN客户端软件配置文件

还可以在 WEB 用户门户的“口令”页面中，点击最下方的二维码图片，如下图15所示，下载当前账号的 Wireguard VPN客户端配置文件。如果是手机用户，可以打开WireGuard VPN APP，点击添加配置按钮，扫描此二维码导入配置文件。如果看不到二维码图片，可能是VPN服务器配置中没有包含此用户，需要管理员重新生成用户数据。



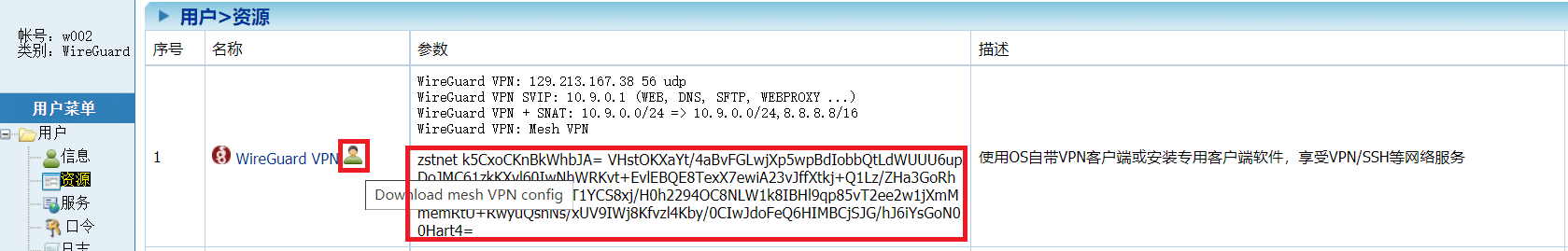
**图15** WireGuard VPN客户端配置文件二维码

### 3.3 用户连接其它VPN客户端

#### 3.3.1 用户下载Mesh VPN配置文件

全部用户成功连接VPN服务器后，用户在 WEB 用户门户的“资源”页面中，点击图符下载当前账号的 P2P VPN/Mesh VPN 配置文件，文件名格式为“[用户名]\_itself.bat”，此批处理文件和管理员在WEBAdmin“WireGuard VPN>用户状态”界面下载的“[用户名]\_meshvpn.bat”不同，不是给此用户使用的，而是给其他用户添加此用户节点用的。

也可以直接拷贝“参数”栏中以“zstnet ”开头的字符串，再发给参与联网的其他用户，如下图16所示；客户端软件没有登录或上次握手超过3分钟，看不到此信息。



**图16** 用户下载Mesh VPN配置文件

在其他用户的客户端配置文件里，为了自动添加xxx用户的Mesh VPN信息，可以编写任务计划程序/定时执行文件（双方都是动态IP或动态端口），或者在WireGuard VPN客户端软件里编辑配置文件，启用PostUp命令，内容类似“PostUp = c:\temp\xxx\_meshvpn.bat”，为了使用PostUp命令需要导入注册表：  
“http://www.trustcomputing.com.cn/tools/wgclient.reg”，再重启客户端软件。

再编辑“c:\temp\xxx\_meshvpn.bat”文件，内容类似：

*REM 使用wget下载xxx\_itself.txt文件*

wget -O c:\temp\xxx\_itself.txt --http-user=xxx --http-password=mypassword --no-check-certificate https://[外网地址]/user\_ex/usercert?type=52021

*REM 执行下载的xxx\_itself.txt*

del c:\temp\xxx\_itself.bat

type c:\temp\xxx\_itself.txt | findstr "^zstnet " | findstr -v "&" | findstr -v "|" | findstr -v ";" | findstr -v "," | findstr -v "(" | findstr -v ")" | findstr -v "\\" | findstr -v "`" | findstr -v "\^" >> c:\temp\xxx\_itself.bat

call c:\temp\xxx\_itself.bat

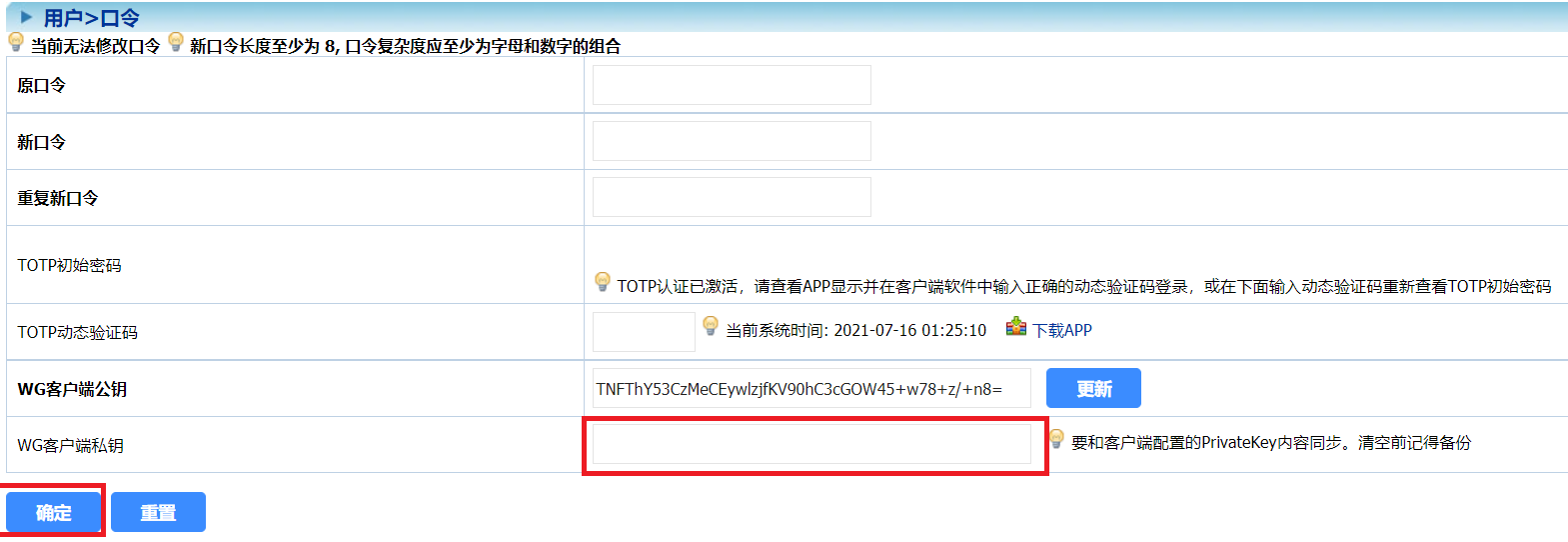
*REM 最后返回值为0*

echo

**注意：**

1、客户端软件连接后，查看客户端软件的“日志”，了解执行bat批处理文件的情况。

2、由于下载xxx\_itself.bat文件用到了用户名口令，为了方便其他用户直接下载xxx\_itself.bat文件的同时防止其他用户借机登录用户门户，进而修改口令或下载wireguard客户端配置文件，需要事先在用户门户的“口令”界面，把“WG客户端私钥”栏的内容清空（VPN服务器只需要公钥），之前记得保存（即WireGuard客户端软件“编辑”内容的**PrivateKey**值），如下图17所示。管理员也可以在用户管理设置界面中清空“WireGuard私钥”栏的内容，达到同样的目的。



**图17** 清空“WG客户端私钥”栏的内容防止信息泄露

#### 3.3.2 用户运行Mesh VPN配置文件

双方分别在自己的 PC 上以管理员/root身份执行对方的xxx\_itself.bat 文件后，即构成 P2P VPN/Mesh VPN。

假设有N个用户参与组网，则每个用户都要得到其他N-1个用户的xxx\_itself.bat 文件（相当于管理员在WEBAdmin“WireGuard VPN>用户状态”界面下载的“xxx\_meshvpn.bat”文件），并执行才能完成全部的组网；也可以有选择的执行，但需要双方都执行对方的xxx\_itself.bat文件才有效。

组网成功后，如果有一台WireGuard VPN客户端断开后重连，公网IP或监听端口发生了变化，则其它客户端都要重新下载之有关的bat文件，找到对应的“zstnet ”命令行程序并执行，可以使用任务计划程序等方式进行自动化监控；如果OS有固定的公网IP，并且监听端口（**ListenPort** ）固定（参考图7），则直接执行对应的“zstnet ”命令行程序即可。

#### 3.3.3 用户验证Mesh VPN网络

P2P/Mesh VPN网络建立后，可以对VPN路由做验证，即在各自OS Shell下ping对方虚拟IP、查看ms值，再traceroute对方虚拟IP。如果traceroute只有1跳（Hop）就表明P2P/Mesh VPN组网成功，如果有2跳（Hop），则表明仍是通过VPN服务器中转的。

如果由于种种原因P2P VPN/Mesh VPN失效，数据传输将还原为传统客户端服务器模式的VPN连接，即要通过VPN服务器中转，此时，需要检查更新连接信息，重新建立P2P VPN/Mesh VPN。建立好P2P VPN/Mesh VPN之后，最好新开一个CMD命令窗口，一直ping对方的虚拟IP，防止中间路由设备因为超时等原因中断此连接。

**zstnet用法**

* zstnet xxx yyy

根据本机WireGuard VPN状态，连接其它客户端

* zstnet xxx yyy 1

无条件删除已建立的连接

* zstnet xxx yyy 2

无条件连接其它客户端

**参考资料**

1、运用Mesh VPN自建去中心化网络基础设施服务

http://trustcomputing.com.cn/cn/index.php/support/techdocs/122-p2p-mesh-vpn

2、中神通大地EDR&DNS&URL&VPN云控管系统（简称大地云控）

http://www.trustcomputing.com.cn/cn/index.php/product/dns-url

3、中神通大地EDR&DNS&URL&VPN云控管系统-管理员手册：http://www.trustcomputing.com.cn/help/zst\_dadi\_adm.doc

4、中神通大地EDR&DNS&URL&VPN云控管系统-用户指南：http://www.trustcomputing.com.cn/help/zst\_dadi\_userguide.pdf