

## راه اندازی OpenVPN بر روی تلفن های Akuvox

یکی از روش های اتصال به شبکه ی داخلی سازمان و استفاده از منابع سازمان از محیط بیرونی راه اندازی وی پی ان بوده و Openvpn از نرم افزارهای محبوب برای راه اندازی سرور می باشد. این نوع ارتباطات در شبکه ی وی پی VoIP نیز به کاربران سیار و remote اجازه میدهد تا به سیستم تلفنی سازمان خود متصل شوند و بدون نیاز به درگیر شدن با مشکلات مربوط به NAT، تماس های تلفنی خود را برقرار نمایند.

تلفن های تحت شبکه ی آکووکس Akuvox، از جمله تلفن های IP هستند که از openvpn پشتیبانی می کنند و شما می توانید با راه اندازی سرور آن بر روی مرکز تلفن وی پی یا هر سرور دیگری، به کاربران اجازه دهید تا تلفن خود را در شبکه ی داخلی رجیستر نمایند. در ادامه چگونگی تنظیمات در تلفن و سرور را با هم بررسی خواهیم کرد.

### نصب:

پس از نصب openvpn با استفاده از دستور زیر easy-rsa-old را دریافت و نصب نمایید:

```
wget -O /tmp/easyrsa https://github.com/OpenVPN/easy-rsa-old/archive/2.3.3.tar.gz
```

در مرحله بعد فایل را استفاده از دستور زیر untar کنید:

```
tar xzf /tmp/easyrsa
```

در حال حاضر یک دایرکتوری با نام easy-rsa-old-2.3.3 بوجود آمده است.

حال یک دایرکتوری جدید در مسیر openvpn ایجاد کنید و دایرکتوری که در مرحله قبل ساخته شد را به آنجا انتقال دهید:

```
sudo mkdir /etc/openvpn/easy-rsa
```

```
sudo cp -rf easy-rsa-old-2.3.3/easy-rsa/2.0/* /etc/openvpn/easy-rsa
```

سپس owner دایرکتوری را به یک کاربر (غیر از root) بدهید:

```
sudo chown sammy /etc/openvpn/easy-rsa/
```

### تنظیمات سرور:

حال که پکیج های مربوط به Openvpn و easy-rsa نصب شدند. در سرور وارد مسیر /etc/openvpn/server.conf شوید و از وجود مقادیر زیر داخل این فایل اطمینان حاصل نمایید:

```
port 1194
proto udp
dev tun
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /etc/openvpn/keys/server.key
dh /etc/openvpn/keys/dh2048.pem
```

```
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
client-to-client
keepalive 10 120
comp-lzo
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
log openvpn.log
log-append openvpn.log
verb 6
```

سپس داخل فایل `cd /etc/openvpn-2.1.4/easy-rsa/2.0` شده و دستورات زیر را به ترتیب وارد کنید:

```
export D=`pwd`
export KEY_CONFIG=$D/openssl-1.0.0.cnf
export KEY_DIR=$D/keys
export KEY_SIZE=1024
export KEY_COUNTRY=CN
export KEY_PROVINCE=FJ
export KEY_CITY=XM
export KEY_ORG="akuvox.com"
export KEY_EMAIL="admin@akuvox.com"
```

دستورات زیر را برای ساخت CA و Key اجرا نمایید:

```
$ cd /etc/openvpn/easy-rsa
$ source ./vars
$ ./clean-all
$ ./build-ca
```

Country Name (2 letter code) [CN]:

State or Province Name (full name) [FJ]:

Locality Name (eg, city) [XM]:

Organization Name (eg, company) [akuvox.com]:

Organizational Unit Name (eg, section) []:akuvox.com

Common Name (eg, your name or your server's hostname) [akuvox.com CA]:server

Name []:

```
$ ./build-key-server server
```

Country Name (2 letter code) [CN]:

State or Province Name (full name) [FJ]:

Locality Name (eg, city) [XM]:

Organization Name (eg, company) [akuvox.com]:

Organizational Unit Name (eg, section) []:akuvox.com

Common Name (eg, your name or your server's hostname) [server]:server  
Name:[]

Email Address [admin@akuvox.com]:akuvox.com

Please enter the following 'extra' attributes  
to be sent with your certificate request

A challenge password []:abcd1234

An optional company name []:akuvox.com

```
$ ./build-dh
```

```
$ cd /etc/openvpn/easy-rsa/keys
```

```
$ sudo cp dh2048.pem ca.crt server.crt server.key /etc/openvpn
```

```
$ cd /etc/openvpn/easy-rsa
```

```
$ ./build-key client
```

Country Name (2 letter code) [CN]:

State or Province Name (full name) [FJ]:

Locality Name (eg, city) [XM]:

Organization Name (eg, company) [akuvox.com]:

Organizational Unit Name (eg, section) []:akuvox.com

Common Name (eg, your name or your server's hostname) [client]:server  
Name:[]

Email Address [admin@akuvox.com]:

Please enter the following 'extra' attributes  
to be sent with your certificate request

A challenge password []:abcd1234

An optional company name []:akuvox.com

همچنین بررسی نمایید که پارامتر زیر در فایل `/etc/sysctl.conf` وجود داشته باشد:

```
net.ipv4.ip_forward = 1
```

سپس دستورات زیر را برای راه اندازی سرویس `openvpn` اجرا کنید:

```
sudo systemctl -f enable openvpn@server.service
```

```
sudo systemctl start openvpn@server.service
```

```
sudo systemctl status openvpn@server.service
```

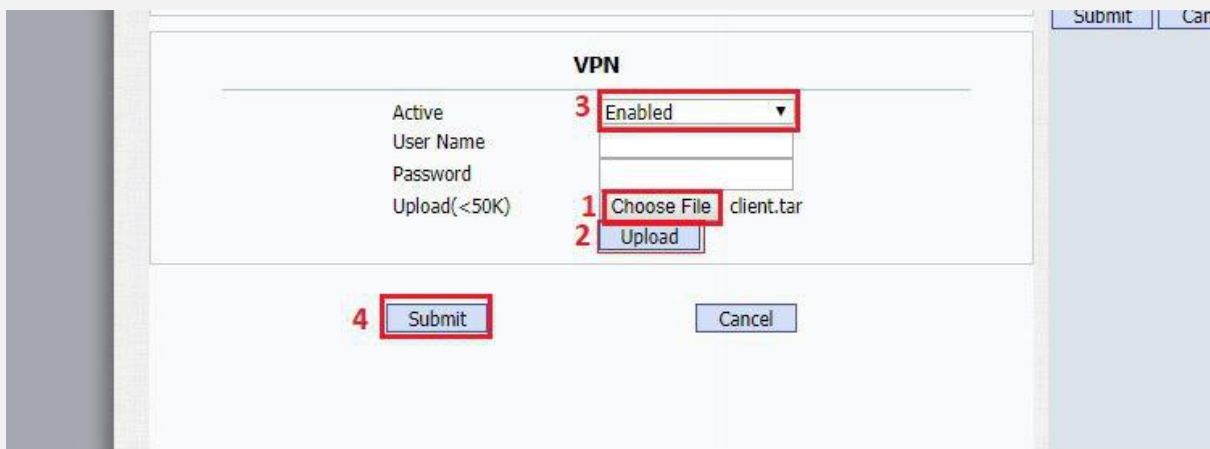
حال فایل‌های زیر را در یک فولدر دلخواه کپی نمایید:

```
/etc/openvpn/easy-rsa/keys/ca.crt
/etc/openvpn/easy-rsa/keys/client.crt
/etc/openvpn/easy-rsa/keys/client.key
```

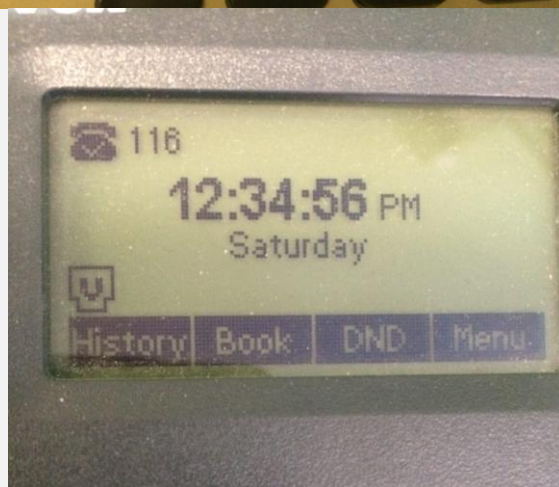
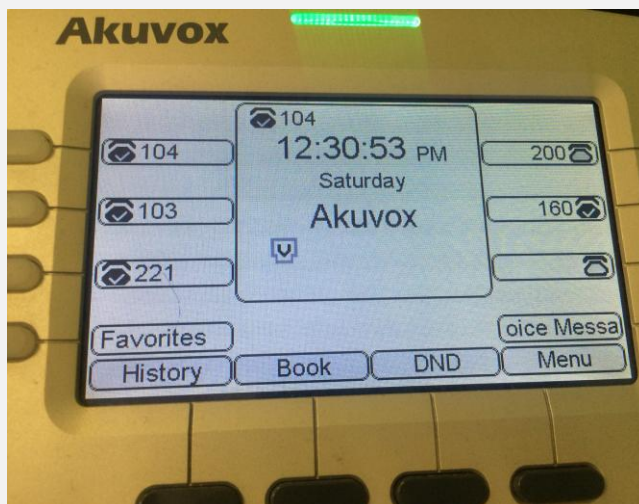
سپس داخل همان فولدر یک فایل به نام `vpn.conf` ساخته و مقادیر زیر را داخل آن کپی کنید:

```
client
setenv SERVER_POLL_TIMEOUT 4
nobind
remote a.b.c.d 1194 udp
dev tun
dev-type tun
ns-cert-type server
reneg-sec 604800
sndbuf 100000
rcvbuf 100000
auth-retry nointeract
comp-lzo no
verb 6
ca /config/openvpn/ca.crt
cert /config/openvpn/client.crt
key /config/openvpn/client.key
```

در نهایت تمام ۴ فایل در این فولدر را در یک فایل زیپ شده به نام `client.tar` قرار داده و این فایل را داخل تلفن در مسیر `Network>Advanced` داخل بخش `VPN` آپلود نمایید. سپس `VPN` را `Enable` کرده، `Submit` کنید. بعد از ریست شدن تلفن، ارتباط از طریق این وی‌پی‌ان برقرار خواهد شد.



توجه: لزومی به وارد کردن نام کاربری و پسورد نمی باشد.



در صورت بروز هرگونه مشکل بهتر است با اجرای دستور `tail -f /etc/openvpn/openvpn.log` لاگ های سرور را بررسی نمایید تا علت بروز خطا را پیدا کنید.