http://www.fyluo.com/m/?post=198

**OpenVPN Windows 平台安装部署教程**

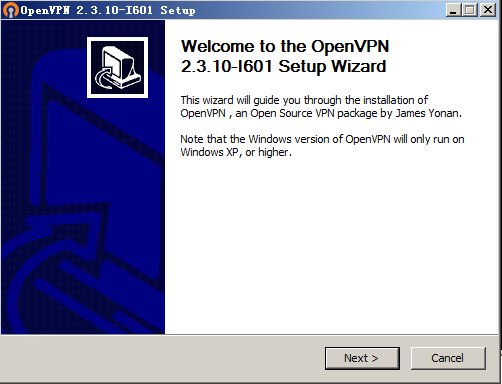
2018-6-5 Eagle

**一、环境准备：**

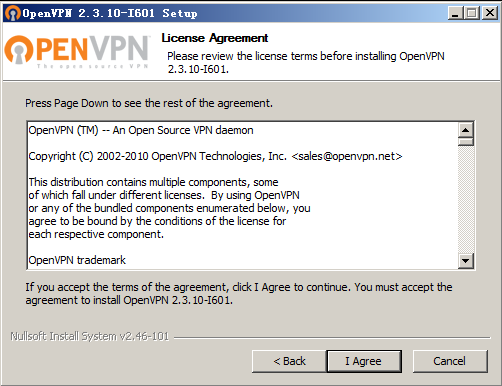
1. 操作系统Windows
2. 服务器IP：192.168.88.123  VPN：192.168.89.1
3. 客户端IP：192.168.78.3
4. 客户端服务端单网卡，路由器做好端口映射
5. 安装包附件下载 [openvpn-install-2.3.10-I601-x86\_64.rar](http://www.fyluo.com/ueditor/php/upload/file/20180607/1528361410428080.rar)

**二、服务端安装部署：**

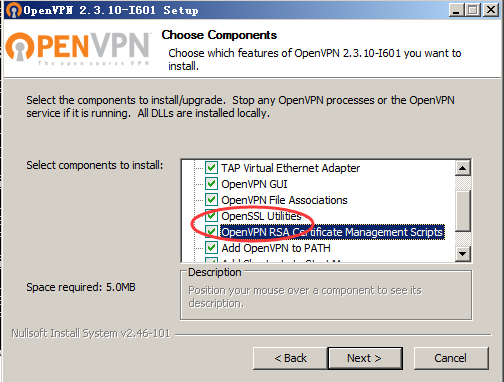
1. 打开安装包进行安装，客户端跟服务器安装方式一样，都需要安装



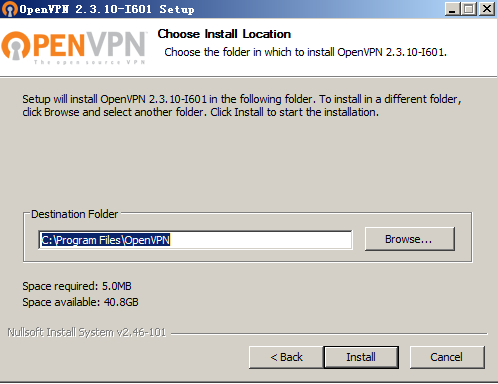
1. 接受下一步



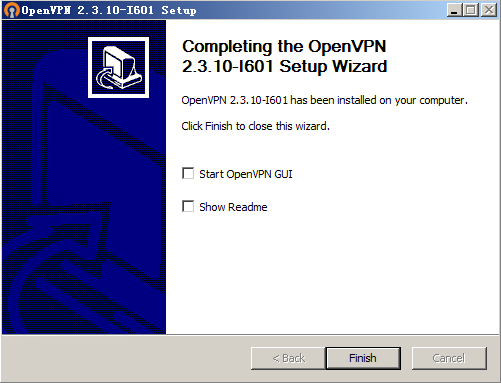
1. 下面两个选项默认不勾选，我们需要勾选不然安装完无法命令行制作证书操作



1. 选择安装目录



1. 安装完成



1. 安装完成后系统会多出一张网卡TAP的 “本地连接2

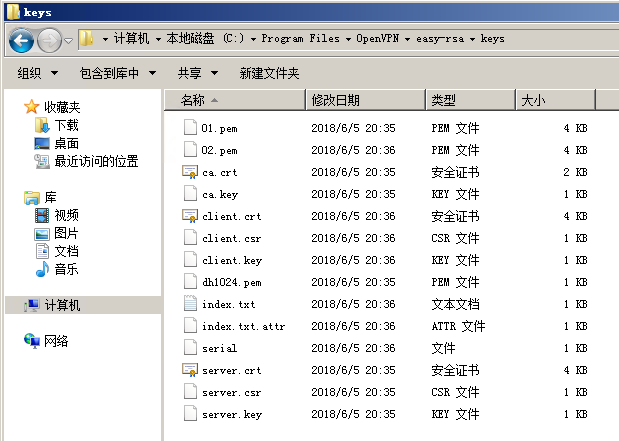


1. 要想客户端能够通过服务端上网需要调整服务端本地网卡共享



**三、服务端配置-生成相关证书配置：**

1. 说明：
2. init-config     # init-config 会把 vars.bat.sample 复制为 var.bat
3. vars        # vars.bat 用来设置一些变量，主要就是配置文件中修改的那部分
4. clean-all     # 会清掉 C: \Program File\OpenVPN\easy-rsa\keys 目录，再把 index.txt 和 serial 文件放进来。
5. build-ca     # 生成根证书
6. build-dh.bat   # 生成 dh1024.pem 文件，Server 使用 TLS(OpenSSL) 必须要有的文件
7. build-key-server server # 生成服务端密钥和证书
8. # server01 是自己定义的参数名，与上相应的就会生成 server01.key、server01.csr 和 server01.crt，也都是在 keys 目录里。
9. # 这一步像 build-dh.bat 一样有些东西要填写，之后就是该回答 y 的 y 一下，关键就一个：
10. # Common Name 必须填，且不能与执行 build-dh 时相同，否则会报：
11. # failed to update database
12. # TXT\_DB error number 2
13. # 找不到 C:\Program Files\OpenVPN\easy-rsa\keys\\*.old
14. # 三个文件 server01.key、server01.csr 和 server01.crt 也会生成，但文件 server01.crt 的大小是 0 字节无效的，就要重新再来，看到 Data Base Updated 才行。
15. # 要生成多个服务端的密钥和证书则继续 build-key-server server02 ......
17. build-key client   #客户端生成密钥和证书
18. # build-ca和build-key-server一样要输入一堆东西，这里注意的是 Common Name 不能与执行 build-key-server 时输入的一样，与 build-ca 的 Common Name 一样我试过没什么关系，否则也是报：
19. # failed to update database
20. # TXT\_DB error number 2
21. # 找不到 C:\Program Files\OpenVPN\easy-rsa\keys\\*.old
22. # 要生成其他的客户端密钥和证书，可以继续 build-key client02 ......
24. ..\bin\openvpn --genkey --secret keys\ta.key
25. # 生成 ta.key 文件
26. 修改文件vars.bat.sample 在C:\Program Files\OpenVPN\easy-rsa 目录下用写字板打开 根据需求修改相关配置信息
27. set KEY\_COUNTRY=CN
28. set KEY\_PROVINCE=FuJian
29. set KEY\_CITY=FuZhou
30. set KEY\_ORG=FYLUO
31. set KEY\_EMAIL=eagle@fyluo.com
32. set KEY\_CN=Eagle
33. set KEY\_NAME=Eagle
34. set KEY\_OU=Eagle
35. set PKCS11\_MODULE\_PATH=Eagle
36. set PKCS11\_PIN=1234
37. 以下进去命令行操作
38. C:\Program Files\OpenVPN\easy-rsa>init-config.bat
39. C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
40. 已复制         1 个文件。
41. C:\Program Files\OpenVPN\easy-rsa>vars.bat
42. C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
43. 系统找不到指定的文件。
44. 已复制         1 个文件。
45. 已复制         1 个文件。
46. C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
47. Loading 'screen' into random state - done
48. Generating a 1024 bit RSA private key
49. .....................++++++
50. ...........++++++
51. writing new private key to 'keys\ca.key'
52. -----
53. You are about to be asked to enter information that will be incorporated
54. into your certificate request.
55. What you are about to enter is what is called a Distinguished Name or a DN.
56. There are quite a few fields but you can leave some blank
57. For some fields there will be a default value,
58. If you enter '.', the field will be left blank.
59. -----
60. Country Name (2 letter code) [CN]:
61. State or Province Name (full name) [FuJian]:
62. Locality Name (eg, city) [FuZhou]:
63. Organization Name (eg, company) [FYLUO]:
64. Organizational Unit Name (eg, section) [Eagle]:
65. Common Name (eg, your name or your server's hostname) [Eagle]:CA
66. Name [Eagle]:
67. Email Address [eagle@fyluo.com]:
68. C:\Program Files\OpenVPN\easy-rsa>
69. C:\Program Files\OpenVPN\easy-rsa>build-dh.bat
70. Loading 'screen' into random state - done
71. Generating DH parameters, 1024 bit long safe prime, generator 2
72. This is going to take a long time
73. .......+.....+.................................................................+
74. ................................................................................
75. .........................+................................+.....................
76. ................................................................................
77. .............................................................+..................
78. ................................................................................
79. .................+.................................................++\*++\*++\*
80. C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server
81. Loading 'screen' into random state - done
82. Generating a 1024 bit RSA private key
83. ....++++++
84. ..................................................++++++
85. writing new private key to 'keys\server.key'
86. -----
87. You are about to be asked to enter information that will be incorporated
88. into your certificate request.
89. What you are about to enter is what is called a Distinguished Name or a DN.
90. There are quite a few fields but you can leave some blank
91. For some fields there will be a default value,
92. If you enter '.', the field will be left blank.
93. -----
94. Country Name (2 letter code) [CN]:
95. State or Province Name (full name) [FuJian]:
96. Locality Name (eg, city) [FuZhou]:
97. Organization Name (eg, company) [FYLUO]:
98. Organizational Unit Name (eg, section) [Eagle]:
99. Common Name (eg, your name or your server's hostname) [Eagle]:server
100. Name [Eagle]:
101. Email Address [eagle@fyluo.com]:
102. Please enter the following 'extra' attributes
103. to be sent with your certificate request
104. A challenge password []:201888
105. An optional company name []:
106. Using configuration from openssl-1.0.0.cnf
107. Loading 'screen' into random state - done
108. Check that the request matches the signature
109. Signature ok
110. The Subject's Distinguished Name is as follows
111. countryName           :PRINTABLE:'CN'
112. stateOrProvinceName   :PRINTABLE:'FuJian'
113. localityName          :PRINTABLE:'FuZhou'
114. organizationName      :PRINTABLE:'FYLUO'
115. organizationalUnitName:PRINTABLE:'Eagle'
116. commonName            :PRINTABLE:'server'
117. name                  :PRINTABLE:'Eagle'
118. emailAddress          :IA5STRING:'eagle@fyluo.com'
119. Certificate is to be certified until Jun  2 12:35:53 2028 GMT (3650 days)
120. Sign the certificate? [y/n]:y
121. 1 out of 1 certificate requests certified, commit? [y/n]y
122. Write out database with 1 new entries
123. Data Base Updated
124. C:\Program Files\OpenVPN\easy-rsa>
125. C:\Program Files\OpenVPN\easy-rsa>build-key.bat client
126. Loading 'screen' into random state - done
127. Generating a 1024 bit RSA private key
128. ................++++++
129. ..............................................++++++
130. writing new private key to 'keys\client.key'
131. -----
132. You are about to be asked to enter information that will be incorporated
133. into your certificate request.
134. What you are about to enter is what is called a Distinguished Name or a DN.
135. There are quite a few fields but you can leave some blank
136. For some fields there will be a default value,
137. If you enter '.', the field will be left blank.
138. -----
139. Country Name (2 letter code) [CN]:
140. State or Province Name (full name) [FuJian]:
141. Locality Name (eg, city) [FuZhou]:
142. Organization Name (eg, company) [FYLUO]:
143. Organizational Unit Name (eg, section) [Eagle]:
144. Common Name (eg, your name or your server's hostname) [Eagle]:cli
145. Name [Eagle]:
146. Email Address [eagle@fyluo.com]:
147. Please enter the following 'extra' attributes
148. to be sent with your certificate request
149. A challenge password []:201888
150. An optional company name []:
151. Using configuration from openssl-1.0.0.cnf
152. Loading 'screen' into random state - done
153. Check that the request matches the signature
154. Signature ok
155. The Subject's Distinguished Name is as follows
156. countryName           :PRINTABLE:'CN'
157. stateOrProvinceName   :PRINTABLE:'FuJian'
158. localityName          :PRINTABLE:'FuZhou'
159. organizationName      :PRINTABLE:'FYLUO'
160. organizationalUnitName:PRINTABLE:'Eagle'
161. commonName            :PRINTABLE:'cli'
162. name                  :PRINTABLE:'Eagle'
163. emailAddress          :IA5STRING:'eagle@fyluo.com'
164. Certificate is to be certified until Jun  2 12:36:27 2028 GMT (3650 days)
165. Sign the certificate? [y/n]:y
166. 1 out of 1 certificate requests certified, commit? [y/n]y
167. Write out database with 1 new entries
168. Data Base Updated
169. C:\Program Files\OpenVPN\easy-rsa>
170. C:\Program Files\OpenVPN\easy-rsa>
171. C:\Program Files\OpenVPN\easy-rsa>
172. 生成后文件夹下产生如下文件：



1. 创建服务端配置文件

把配置文件server.ovpn放到C:\Program Files\OpenVPN\config目录下

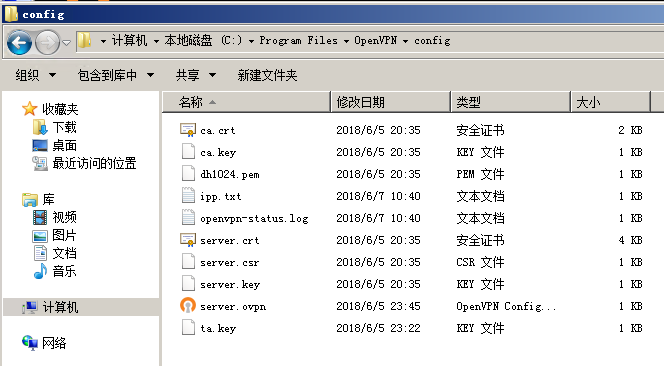
把C:\Program Files\OpenVPN\easy-rsa\keys目录下的

ca.crt、ca.key、server01.crt、server01.csr、server01.key、dh1024.pem、ta.key 复制到

C:\Program Files\OpenVPN\config目录下。

server.ovpn文件内容如下：

1. port 8080
2. proto tcp
3. dev tun
4. ca ca.crt
5. cert server.crt
6. key server.key # This file should be kept secret
7. ;crl-verify vpncrl.pem
8. dh dh1024.pem
9. server 192.168.89.0 255.255.255.0
10. ifconfig-pool-persist ipp.txt
11. push "redirect-gateway def1 bypass-dhcp"
12. push "dhcp-option DNS 218.85.157.99"
13. push "dhcp-option DNS 223.5.5.5"
14. push "route 192.168.88.0 255.255.255.0"
15. client-to-client
16. ;duplicate-cn
17. keepalive 10 120
18. tls-auth ta.key 0 # This file is secret
19. comp-lzo
20. ;max-clients 100
21. user nobody
22. group nobody
23. persist-key
24. persist-tun
25. status openvpn-status.log
26. verb 4
27. 配置文件如下：

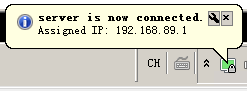


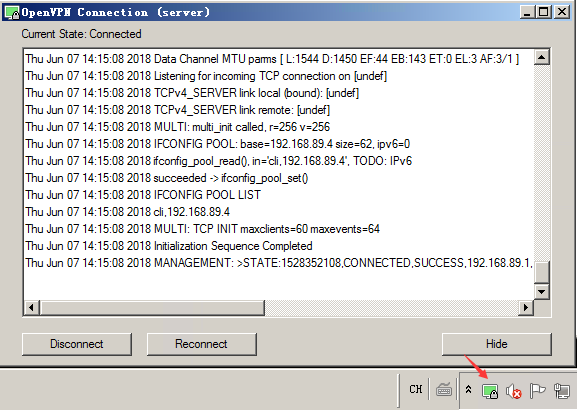
1. 修改注册表：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 将IPEnableRouter改为1

关闭防火墙或将8080端口加入到防火墙允许通过的端口中去

1. 启动服务端





**四、客户端配置：**

1. 创建客户端配置文件：

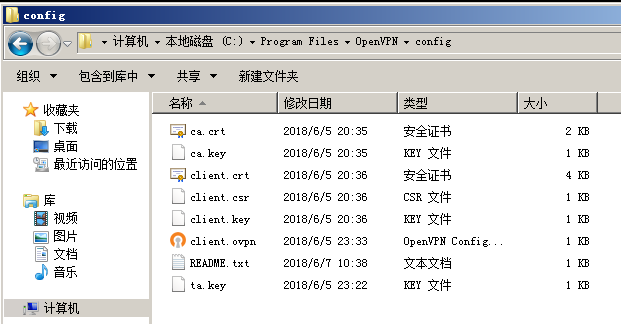
把配置文件client.ovpn放到客户端机器的C:\Program Files\OpenVPN\config目录下，并且把服务器C:\Program Files\OpenVPN\easy-rsa\keys目录下的

client01.crt、client01.csr、client01.key、ca.key、ca.crt、ta.key  文件一起复制到

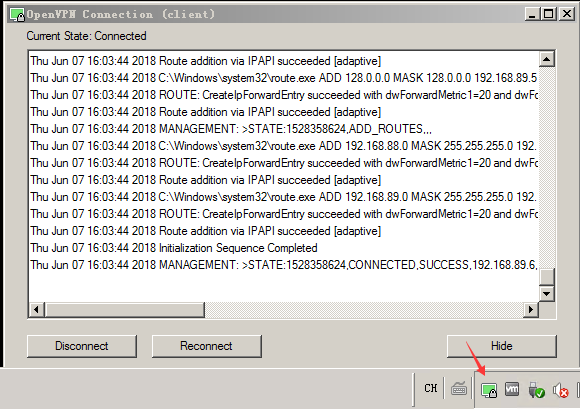
客户端C:\Program Files\OpenVPN\config目录下 （以上文件为服务端生成，客户端需要在服务端拷贝这7个文件过来）

client.ovpn配置文件如下：

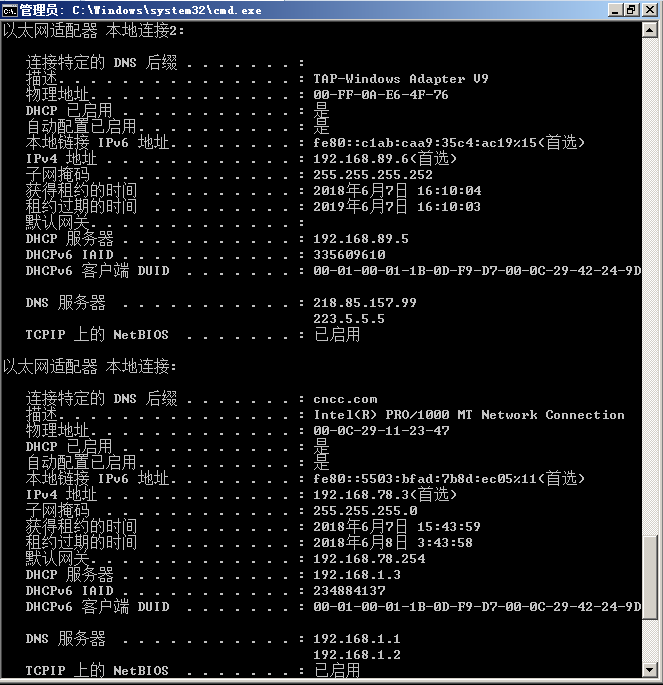
1. client
2. dev tun
3. proto tcp
5. remote 服务端IP 8080
6. ;remote my-server-2 8080
8. ;remote-random
10. resolv-retry infinite
11. nobind
12. user nobody
13. group nobody
14. ;route 192.168.0.0 255.255.252.0
15. persist-key
16. persist-tun
18. ;http-proxy-retry # retry on connection failures
19. ;http-proxy [proxy server] [proxy port #]
21. ca ca.crt
22. cert client.crt
23. key client.key
25. ns-cert-type server
26. tls-auth ta.key 1
27. comp-lzo
28. # Set log file verbosity.
29. verb 4
30. 配置文件如下：



1. 客户端连接后如下：



1. 查看客户端获取的IP

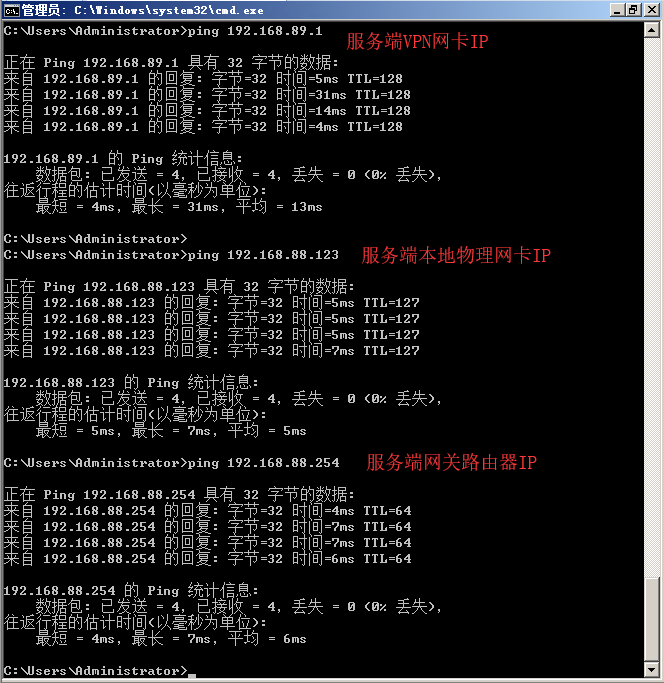


1. 查看客户端获取路由表



**五、网络联通性测试**

1. 以下测试客户端到服务端的内网网络测试



1. 以下是拨号前客户端电脑的出口IP



1. 客户端电脑拨号后的出口IP已经变成了 服务端的出口IP

