OpenVPN Server HowTo (Streamlined)

To prevent discombobulation, *please* **follow the format already in place within this Wiki when editing** *(incl. the Table of Contents)*

- *Five things are required for a SSL VPN:*
  - Encryption (Certificates)
  - Network (VPN Interface Creation)
    - Firewall Rules [VPN Traffic]
  - VPN Server [Config]
  - VPN Clients [Config]

Prerequisites

Install Applicable Packages

- `opkg update ; opkg install openvpn-easy-rsa openvpn-openssl luci-app-openvpn`

File Locations

- Firewall Config File: */etc/config/firewall*
- OpenVPN Config File: */etc/config/openvpn*

Folder Locations

- Easy-RSA Root Folder: */etc/easy-rsa/*
- OpenVPN Root Folder: */etc/openvpn/*

Encryption

Edit Vars

- `cd /etc/easy-rsa ; echo > vars ; vi vars`
  - Paste the following *and edit [whatever you'd like]* to show your own custom input
  - ```
    export EASY_RSA="/etc/easy-rsa"

    export OPENSSL="openssl"
    export PKCS11TOOL="pkcs11-tool"
    export GREP="grep"

    export KEY_CONFIG=`/usr/sbin/whichopensslcnf $EASY_RSA`

    export KEY_DIR="$EASY_RSA/keys"

    echo NOTE: If you run clean-all, a rm -rf on $KEY_DIR will be performed

    export PKCS11_MODULE_PATH="dummy"
    export PKCS11_PIN="dummy"

    export KEY_SIZE=2048

    export CA_EXPIRE=3650

    export KEY_EXPIRE=3650

    export KEY_COUNTRY="[2-letter abbreviation]"
    export KEY_PROVINCE="[whatever you like]"
    export KEY_CITY="[whatever you like]"
    export KEY_ORG="[whatever you like]"
    export KEY_EMAIL="[whatever you like]"
    export KEY_OU="[whatever you like]"

    export KEY_NAME="vpnserver"
    ```
    - **Do not use the same Common Name (CN) for two or more clients**
      - The CN (Common Name) is the name you enter when prompted in **uci** after running *build-key-pkcs12*; it should be *unique* to each client

Create SSL Certificates

- ```
  #--- Deletes everything in the "key" directory and starts fresh ---#
  clean-all

  #--- Create's the Certificate Authority (CA) ---#
  build-ca

  #--- Creates Server certificate (DO NOT set a password for THIS SPECIFIC certificate) ---#
  build-key-server my-server

  #--- Converts Server certificate to a PKCS12 certificate (DO NOT set a password for THIS SPECIFIC certificate) ---#
  openssl pkcs12 -export -in keys/my-server.crt -inkey keys/my-server.key -certfile keys/ca.crt -name My-Server -out keys/my-server.p12 ; chmod 0600 keys/my-server.p12

  #--- Creates Client certificates ---#
  build-key-pkcs12 my-client

  #--- Creates the Diffie Hellman
  build-dh

  #--- Creates the Server's TLS Authorization key ---#
  openvpn --genkey --secret keys/ta.key
  ```
  - The above creates a server certificate named *my-server* (*.crt*, *.csr*, *.key*, and *.p12*) and a client certificate named *my-client* (*.crt*, *.csr*, *.key*, and *.p12*).
    - *.crt:* **signed certificate**
    - *.csr:* **encrypted private key and certificate request**
    - *.key: private key* - **needs to be kept secure at all times**
    - *.p12: PKCS12 certificate* - **needs to be kept secure at all times**
      - Contains the *ca.crt*, *client.crt*, and *client.key*
  - The server certificate cannot be generated as a p12, so the *openssl* command is used to create the p12 certificate
- It is **highly recommended** to keep your *Certificate Authority (CA)* in a secure location
  - **Failure to do so allows anyone who gains access to your Certificate Authority the ability to create client certificates.**
- It is recommended to add a password to *each* client certificate
  - **Failure to do so enables anyone gaining access to your client certificate(s) unfettered access to your VPN**
- You will need to run *build-key-pkcs12* for however many clients you're creating certificates for.
- If using Windows, add your certificate authority (via import) to the *Trusted Root Certificate Authorities* in *Credential Manager*

Create Backup of Certificates

- Once **all** certificates have been created and the Diffie-Hellman certificate (*dh2048.pem*) is generated:
- `cp -R keys /etc/openvpn`

Network

Create VPN interface

- `uci set network.vpn0=interface ; uci set network.vpn0.ifname=tun0 ; uci set network.vpn0.proto=none`
    - You can replace *network*.**vpn0** to *network*.**[whatever you'd like]**
        - If you choose to do so, *network*=**vpn0** will need to be updated accordingly in Allow OpenVPN Tunnel Utilization
    - You can replace *ifname*=**tun0** to *ifname*=**[whatever you'd like]**
        - If you choose to do so, *option dev* '**tun0**' will need to be updated accordingly in Create VPN Server Config

Allow VPN Tunnel Utilization

- `uci add firewall zone ; uci set firewall.@zone[-1].name=vpn ; uci set firewall.@zone[-1].input=ACCEPT ; uci set firewall.@zone[-1].forward=ACCEPT ; uci set firewall.@zone[-1].output=ACCEPT ; uci set firewall.@zone[-1].network=vpn0`

  `uci add firewall forwarding ; uci set firewall.@forwarding[-1].src='vpn' ; uci set firewall.@forwarding[-1].dest='lan' ; uci add firewall forwarding ; uci set firewall.@forwarding[-1].src='lan' ; uci set firewall.@forwarding[-1].dest='vpn'`
    - You can replace *name*=**vpn** with *name*=**[whatever you'd like]**
        - If you choose to do so, *src*='**vpn**' will need to be updated accordingly

Create Firewall Rules

- VPN traffic rules should go as close to the top of the *firewall* config as possible, while interzone forwarding rules are input at the bottom *(iptables is a hierarchical firewall)*
    - After the rules have been committed, verify in **LuCI** the rules are in the order shown below.
- `vi /etc/config/firewall`
- Rule protocol for VPNs should always be both TCP & UDP for troubleshooting purposes
- VPNs should always use the UDP protocol, only utilizing TCP for troubleshooting
    - Allowing both prevents from having to edit the firewall every time troubleshooting is needed
- **It is recommended to use a non-standard port for the VPN** *(i.e. not 1194; VPN port should be >1025 but <10000)*
    - If using a custom port, update VPN Server Config and VPN Client Config accordingly
- ```
  #::: Traffic Rules :::#
  # LuCI: Network - Firewall - Traffic Rules

  #--- Allow initial VPN connection ---#
  # LuCI: From any host in any zone To any router IP at port 1194 on this
  # device (Accept Input)
  config rule
          option target 'ACCEPT'
          option proto 'tcp udp'
          option family 'ipv4'
          option src '*'
          option dest_port '1194'
          option name 'Allow Inbound VPN0'

  #--- Once Assigned a VPN IP, Allow Inbound Traffic to LAN ---#
  # LuCI: From IP range 10.1.1.0/24 in any zone To IP range 192.168.1.0/24
  # on this device (Accept Input)
  config rule
          option target 'ACCEPT'
          option proto 'tcp udp'
          option family 'ipv4'
          option src '*'
          option src_ip '10.1.1.0/24'
          option dest_ip '192.168.1.0/26'
          option name 'Allow Inbound VPN0 Traffic to LAN'

  #--- Once Assigned a VPN IP, Allow Forwarded Traffic to LAN ---#
  # LuCI: From IP range 10.1.1.0/24 in any zone To IP range 192.168.1.0/24
  # on this device (Accept Forward)
  config rule
          option target 'ACCEPT'
          option proto 'tcp udp'
          option family 'ipv4'
          option src '*'
          option src_ip '10.1.1.0/24'
          option dest '*'
          option dest_ip '192.168.1.0/26'
          option name 'Allow Forwarded VPN0 Traffic to LAN'

  #--- Allow Outbound ICMP Traffic from VPN ---#
  # LuCI: ICMP From IP range 10.1.1.0/24 in any zone To any host in lan
  # (Accept Forward)
  config rule
          option target 'ACCEPT'
          option proto 'icmp'
          option src_ip '10.1.1.0/24'
          option src '*'
          option dest 'lan'
          option name 'Allow Inbound ICMP Traffic from VPN0 to LAN'

  #--- Allow Outbound Ping Requests from VPN ---#
  # LuCI: ICMP with type echo-request From IP range 10.1.1.0/24 in any
  # zone To any host in wan (Accept Forward)
  config rule
          option target 'ACCEPT'
          option proto 'icmp'
          option src '*'
          option src_ip '10.1.1.0/24'
          option dest 'wan'
          option name 'Allow Outbound ICMP Echo Request (8) from VPN0'
          list icmp_type 'echo-request'


  #::: Defaults :::#
  # LuCI: Network - Firewall

  #--- Default OpenWRT Rule ---#
  config defaults
          option syn_flood '1'
          option input 'ACCEPT'
          option output 'ACCEPT'
          option drop_invalid '1'
          option forward 'DROP'


  #::: Zones :::#
  # LuCI: Network - Firewall - Zones

  #--- LAN ---#
  config zone
          option name 'lan'
          option input 'ACCEPT'
          option output 'ACCEPT'
          option network 'lan'
          option forward 'DROP'

  #--- VPN ---#
  config zone
          option name 'vpn'
          option input 'ACCEPT'
          option forward 'ACCEPT'
          option output 'ACCEPT'
          option network 'vpn0'
          option family 'ipv4'

  #--- WAN ---#
  config zone
          option name 'wan'
          option output 'ACCEPT'
          option masq '1'
  ```
  ```

```
        option mtu_fix '1'
        option network 'wan wan6'
        option input 'DROP'
        option forward 'DROP'


#::: Firewall.User Rules :::#
# LuCI: Network - Firewall - Custom Rules

config include
        option path '/etc/firewall.user'


#::: InterZone Forwarding :::#
# LuCI: Network - Firewall - Zones - VPN - Edit - Inter-Zone Forwarding

#--- LAN to WAN ---#
config forwarding
        option dest 'wan'
        option src 'lan'

#--- VPN to LAN ---#
config forwarding
        option dest 'lan'
        option src 'vpn'

#--- LAN to VPN ---#
config forwarding
        option dest 'vpn'
        option src 'lan'
```

Commit Changes

- `uci commit network ; /etc/init.d/network reload ; uci commit firewall ; /etc/init.d/firewall restart`
    - *There have been a few instances where rules input in the above order to /etc/config/firewall aren't applied in the same order under LuCI - Network - Firewall - Traffic Rules. If this occurs, delete the problem rule(s) from /etc/config/firewall and add manually via LuCI.*

VPN Server

Create Config File

- `echo > /etc/config/openvpn ; vi /etc/config/openvpn`
    - Paste the following *and edit* accordingly for custom locations, subnets, port, etc.
    -
```
config openvpn 'VPNserver'

        option enabled     '1'

    # --- Protocol ---#
        option dev         'tun'
        option dev         'tun0'
        option topology    'subnet'
        option proto       'udp'
        option port        '1194'

    #--- Routes ---#
        option server    '10.1.1.0 255.255.255.0'

    #--- Client Config ---#
#       option ccd_exclusive           '1'
#       option ifconfig_pool_persist   '/etc/openvpn/clients/ipp.txt'
#       option client_config_dir       '/etc/openvpn/clients/'
        option ifconfig                '10.1.1.1 255.255.255.0'

    #--- Pushed Routes ---#
        list push    'route 192.168.1.0 255.255.255.0'
        list push    'dhcp-option DNS 192.168.1.1'
        list push    'dhcp-option WINS 192.168.1.1'
        list push    'dhcp-option DNS 8.8.8.8'
        list push    'dhcp-option DNS 8.8.4.4'
        list push    'dhcp-option NTP 129.6.15.30'

    #--- Encryption ---#
        option cipher     'AES-256-CBC'
        option dh         '/etc/openvpn/keys/dh2048.pem'
        option pkcs12     '/etc/openvpn/keys/my-server.p12'
        option tls_auth   '/etc/openvpn/keys/ta.key 0'

    #--- Logging ---#
        option log           '/tmp/openvpn.log'
        option status        '/tmp/openvpn-status.log'
        option verb          '7'

    #--- Connection Options ---#
        option keepalive        '10 120'
        option comp_lzo         'yes'

    #--- Connection Reliability ---#
        option client_to_client '1'
        option persist_key      '1'
        option persist_tun      '1'

    #--- Connection Speed ---#
        option sndbuf           '393216'
        option rcvbuf           '393216'
        option fragment         '0'
        option mssfix           '0'
        option tun_mtu          '24000'

    #--- Pushed Buffers ---#
        list push    'sndbuf 393216'
        list push    'rcvbuf 393216'

    #--- Permissions ---#
        option user     'nobody'
        option group    'nogroup'
```
    - This specific configuration has been designed to give the best performance possible, via MTU [https://community.openvpn.net/openvpn/wiki/Gigabit_Networks_Linux] and buffer [http://winaero.com/blog/speed-up-openvpn-and-get-faster-speed-over-its-channel/] tuning recommendations
        - DNS primary and secondary is Google's [https://developers.google.com/speed/public-dns/docs/using]
        - NTP is garnished from NIST [http://tf.nist.gov/tf-cgi/servers.cgi] (time-c) and can be updated to your NTP server of choice
            - NTP should be specified, but doesn't need to be NIST. When dealing with encryption handshakes, time on both the server and the client must be accurate to within milliseconds.

- The *CCD directives* (under *Client Config*) are commented out, as you will need to read the OpenVPN HowTo [https://openvpn.net/index.php/open-source/documentation/howto.html#policy] to understand what it is and how to use it. The only option under *Client Config* that should *not* be commented out is *option ifconfig*
- **Two or more servers can be run from this config file**
    - To add additional servers, simply copy and paste the first config directly below itself, with a blank line separating the two. Customize the second server config, making sure not to forget to change the second *option dev* (under *Protocol*) to the correct interface name.
- *I strongly encourage taking the 45 min or so to read through the OpenVPN HowTO & OpenVPN Man Page, located in the* **VPN Wiki Links** *section at the bottom of this Wiki; both provide every possible option for the Server and Client Configs, allowing for a truly customizable VPN solution.*

Enable and Start OpenVPN

- `/etc/init.d/openvpn enable ; /etc/init.d/openvpn start ; sleep 2 ; cat /tmp/openvpn.log`

Log File Output

Correct Log Output w/o CCD

- root@OpenWRT:/# cat /tmp/openvpn.log
  Tue Jul 7 19:57:02 2015 us=55343 OpenVPN 2.3.6 arm-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6] built on Jun 2 2015
  Tue Jul 7 19:57:02 2015 us=55674 library versions: OpenSSL 1.0.2a 19 Mar 2015, LZO 2.08
  Tue Jul 7 19:57:02 2015 us=454270 Diffie-Hellman initialized with 2048 bit key
  Tue Jul 7 19:57:02 2015 us=546774 Control Channel Authentication: using '/etc/openvpn/keys/ta.key' as a OpenVPN static key file
  Tue Jul 7 19:57:02 2015 us=547010 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
  Tue Jul 7 19:57:02 2015 us=547197 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
  Tue Jul 7 19:57:02 2015 us=547412 TLS-Auth MTU parms [L:48058 D:166 EF:66 EB:0 ET:0 EL:0]
  Tue Jul 7 19:57:02 2015 us=547644 Socket Buffers: R=[163840->327680] S=[163840->327680]
  Tue Jul 7 19:57:02 2015 us=567559 TUN/TAP device tun0 opened
  Tue Jul 7 19:57:02 2015 us=567788 TUN/TAP TX queue length set to 100
  Tue Jul 7 19:57:02 2015 us=567990 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
  Tue Jul 7 19:57:02 2015 us=568318 /sbin/ifconfig tun0 10.1.1.1 netmask 255.255.255.0 mtu 48000 broadcast 10.1.1.255
  Tue Jul 7 19:57:02 2015 us=608940 Data Channel MTU parms [L:48058 D:48058 EF:58 EB:135 ET:0 EL:0 AF:3/1]
  Tue Jul 7 19:57:02 2015 us=609448 GID set to nogroup
  Tue Jul 7 19:57:02 2015 us=609690 UID set to nobody
  Tue Jul 7 19:57:02 2015 us=609897 UDPv4 link local (bound): [undef]
  Tue Jul 7 19:57:02 2015 us=610077 UDPv4 link remote: [undef]
  Tue Jul 7 19:57:02 2015 us=610251 MULTI: multi_init called, r=256 v=256
  Tue Jul 7 19:57:02 2015 us=610560 IFCONFIG POOL: base=10.1.1.2 size=252, ipv6=0
  Tue Jul 7 19:57:02 2015 us=614653 Initialization Sequence Completed

Correct Log Output w/ CCD enabled

- root@OpenWRT:/# cat /tmp/openvpn.log
  Tue Jul 7 19:57:02 2015 us=55343 OpenVPN 2.3.6 arm-openwrt-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [MH] [IPv6] built on Jun 2 2015
  Tue Jul 7 19:57:02 2015 us=55674 library versions: OpenSSL 1.0.2a 19 Mar 2015, LZO 2.08
  Tue Jul 7 19:57:02 2015 us=454270 Diffie-Hellman initialized with 2048 bit key
  Tue Jul 7 19:57:02 2015 us=546774 Control Channel Authentication: using '/etc/openvpn/keys/ta.key' as a OpenVPN static key file
  Tue Jul 7 19:57:02 2015 us=547010 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
  Tue Jul 7 19:57:02 2015 us=547197 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
  Tue Jul 7 19:57:02 2015 us=547412 TLS-Auth MTU parms [L:48058 D:166 EF:66 EB:0 ET:0 EL:0]
  Tue Jul 7 19:57:02 2015 us=547644 Socket Buffers: R=[163840->327680] S=[163840->327680]
  Tue Jul 7 19:57:02 2015 us=567559 TUN/TAP device tun0 opened
  Tue Jul 7 19:57:02 2015 us=567788 TUN/TAP TX queue length set to 100
  Tue Jul 7 19:57:02 2015 us=567990 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
  Tue Jul 7 19:57:02 2015 us=568318 /sbin/ifconfig tun0 10.1.1.1 netmask 255.255.255.0 mtu 48000 broadcast 10.1.1.255
  Tue Jul 7 19:57:02 2015 us=608940 Data Channel MTU parms [L:48058 D:48058 EF:58 EB:135 ET:0 EL:0 AF:3/1]
  Tue Jul 7 19:57:02 2015 us=609448 GID set to nogroup
  Tue Jul 7 19:57:02 2015 us=609690 UID set to nobody
  Tue Jul 7 19:57:02 2015 us=609897 UDPv4 link local (bound): [undef]
  Tue Jul 7 19:57:02 2015 us=610077 UDPv4 link remote: [undef]
  Tue Jul 7 19:57:02 2015 us=610251 MULTI: multi_init called, r=256 v=256
  Tue Jul 7 19:57:02 2015 us=610560 IFCONFIG POOL: base=10.1.1.2 size=252, ipv6=0
  Tue Jul 7 19:57:02 2015 us=610897 ifconfig_pool_read(), in='OpenWRT-VPNclient1,10.1.1.5', TODO: IPv6
  Tue Jul 7 19:57:02 2015 us=612378 succeeded -> ifconfig_pool_set()
  Tue Jul 7 19:57:02 2015 us=612581 ifconfig_pool_read(), in='OpenWRT-VPNclient2,10.1.1.6', TODO: IPv6
  Tue Jul 7 19:57:02 2015 us=612747 succeeded -> ifconfig_pool_set()
  Tue Jul 7 19:57:02 2015 us=612912 IFCONFIG POOL LIST
  Tue Jul 7 19:57:02 2015 us=613077 OpenWRT-VPNclient1,10.1.1.5
  Tue Jul 7 19:57:02 2015 us=613349 OpenWRT-VPNclient2,10.1.1.6
  Tue Jul 7 19:57:02 2015 us=614653 Initialization Sequence Completed

VPN Clients

- The server's TLS key (text from *ta.key*) goes in the blank xml space between *Begin* and *End*

Windows Config

- client
  dev tun
  tun-mtu 24000
  fragment 0
  mssfix 0
  proto udp
  remote your.ddns.com 1194
  float
  resolv-retry infinite
  nobind
  persist-key
  persist-tun
  pkcs12 OpenWRT-VPNclient1.p12
  key-direction 1
  <tls-auth>
  -----BEGIN OpenVPN Static key V1-----
  #---PASTE KEY HERE---#
  -----END OpenVPN Static key V1-----
  </tls-auth>
  remote-cert-tls server
  cipher AES-256-CBC
  auth-nocache
  verb 5
  comp-lzo
  - In Windows, if the p12 certificate isn't stored in the same directory as the ovpn config file, you will need to reference the path to the p12 cert
    - In Windows you must use double backslashes, i.e. *"C:\\Program Files\\OpenVPN\\Config\\"*

Android Config

- client
  dev tun
  tun-mtu 24000
  fragment 0
  mssfix 0
  proto udp
  remote your.ddns.com 1194
  float
  nobind
  persist-key
  persist-tun
  key-direction 1
  <tls-auth>
  -----BEGIN OpenVPN Static key V1-----
  #---PASTE KEY HERE---#
  -----END OpenVPN Static key V1-----
  </tls-auth>
  remote-cert-tls server
  cipher AES-256-CBC
  auth-nocache
  verb 5
  comp-lzo
  - OpenVPN for Android [https://play.google.com/store/apps/details?id=de.blinkt.openvpn&hl=en] is the best app for VPNs on Android
  - There's no need to reference a p12 cert as it's installed into the *Android Keychain*; a security feature will cause a warning toast to always appear in the notification area due to user installed certs.
    - This warning can be removed if you have a rooted or bootloader unlocked device by following this [http://forum.xda-developers.com/google-nexus-5/help/howto-install-custom-cert-network-t2533550] tutorial on XDA Developers. It involves a minor edit and permissions change, transferring the p12 cert from userland to system trusted.
  - If you choose to reference the *ta.key*, instead of utilizing XML
    - *Remove:*
    - key-direction 1
      <tls-auth>
      -----BEGIN OpenVPN Static key V1-----

      -----END OpenVPN Static key V1-----
      </tls-auth>
    - *Add:*
    - tls-auth /path/to/ta.key 1
  - *There is an issue with some Android devices not being able to convert PKCS12 certs to X509 certs*
    - *If you've verified your device is one of the ones affected, and you're having issues connecting to your VPN on Android, you may need to reference your individual certs in your Server Config:*
      - *Remove:*
      - #--- Encryption ---#

```
        option pkcs12     '/etc/openvpn/keys/my-server.p12'
```

- *Add:*

-
```
 #--- Encryption ---#
        option ca         '/etc/openvpn/keys/ca.crt'
        option cert       '/etc/openvpn/keys/my-server.crt'
        option key        '/etc/openvpn/keys/my-server.key'
```

Optional:

Redirect Gateway (Same Subnet)

- Routing All Client Traffic (Including Web-Traffic) through the VPN [https://openvpn.net/index.php/open-source/documentation/howto.html#redirect]

Server VPN Config

- Pushed Routes
  - *Remove:*

  - ```
    list push    'dhcp-option DNS 8.8.8.8'
    list push    'dhcp-option DNS 8.8.4.4
    ```

  - *Add:*

  - ```
    list push    'redirect-gateway def1 local'
    list push    'dhcp-option DNS 10.1.1.1'
    ```

Server Firewall Config

- InterZone Forwarding

- ```
  #::: InterZone Forwarding :::#
  # LuCI: Network - Firewall - Zones - VPN - Edit - Inter-Zone Forwarding

  #--- Allow forwarding from VPN to WAN ---#
  config forwarding
          option dest 'wan'
          option src 'vpn'
  ```

- Zone Masquerading

- ```
  #::: Zones :::#
  # LuCI: Network - Firewall - Zones

  #--- Add: option masq '1' ---#
  config zone
          option name 'lan'
          option input 'ACCEPT'
          option output 'ACCEPT'
          option network 'lan'
          option forward 'DROP'
          option masq '1'
  ```

Apply Changes

- ```
  /etc/init.d/firewall restart ; /etc/init.d/openvpn restart
  ```

VPN Wikis

OpenSSL

- OpenSSL Documents [https://www.openssl.org/docs/]
- OpenSSL HowTo [https://www.openssl.org/docs/HOWTO/]
- OpenSSL Man Page [https://www.openssl.org/docs/apps/openssl.html]

OpenVPN

- OpenVPN on Android [https://docs.openvpn.net/docs/openvpn-connect/openvpn-connect-android-faq.html]
- OpenVPN Forum [https://forums.openvpn.net/] *<---- For Help*
- OpenVPN HowTo [https://openvpn.net/index.php/open-source/documentation/howto.html] *<---- Highly Recommended*
- OpenVPN Man Page [https://community.openvpn.net/openvpn/wiki/Openvpn23ManPage] *<---- Highly Recommended*
- OpenVPN Tuning [https://community.openvpn.net/openvpn/wiki/Gigabit_Networks_Linux]

OpenWRT

- OpenWRT Forum [https://forum.openwrt.org/]
- VPN Guide for Beginners [http://wiki.openwrt.org/doc/howto/vpn.openvpn]
- VPN Server HowTo [http://wiki.openwrt.org/inbox/vpn.howto]
- VPN TUN Server [http://wiki.openwrt.org/doc/howto/vpn.server.openvpn.tun]

Random Info

- Deploying a VPN with PKI on GNU/Linux [http://archive.oreilly.com/pub/a/security/2004/10/21/vpns_and_pki.html?page=1]

WinAero

- Buffer Tunning [http://winaero.com/blog/speed-up-openvpn-and-get-faster-speed-over-its-channel/]

XDA Developers

- Remove "Your Network Could be Monitored" Toast [http://forum.xda-developers.com/google-nexus-5/help/howto-install-custom-cert-network-t2533550]
- Trust CAcert's Root Certificate [http://wiki.cacert.org/FAQ/ImportRootCert#Android_Phones]

Questions (Please Help Yourself)

- *Please take the time to read*
  - *If you refuse to help yourself, don't expect someone else to help you*

- *The answer to any question one could possibly have about an OpenVPN Client or Server configuration is contained within this Wiki or the VPN Wiki Section*
  - *If, after reading, one still is unable to find a solution to their question, please post a question in the applicable thread on OpenWRT's [https://forum.openwrt.org/] or OpenVPN's [https://forums.openvpn.net/] Forum*

  ```