

# 目次

サーバ側での作業 ..... 1

**OpenVPN パッケージのインストール** ..... 1

**設定ファイル** ..... 1



# サーバ側での作業

## OpenVPN パッケージのインストール

Ubuntu 18.04 のサーバに、OpenVPN をセットアップします。

```
root@bionic-openvpn:~# apt install openvpn easy-rsa openresolv
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libccid libpcsc-lite libpkcs11-helper1 opensc opensc-pkcs11 pcscl
Suggested packages:
  pcmciautils
The following NEW packages will be installed:
  easy-rsa libccid libpcsc-lite libpkcs11-helper1 openresolv opensc opensc-
pkcs11 openvpn pcscl
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 1749 kB of archives.
After this operation, 5552 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

サーバ側では、[こちら](#) を参照して設定をしておきます。

## 設定ファイル

サーバ側で使用する config は下記のようにしました。

```
#####
# Sample OpenVPN 2.0 config file for                               #
# multi-client server.                                           #
#                                                                 #
# This file is for the server side                               #
# of a many-clients <-> one-server                               #
# OpenVPN configuration.                                         #
#                                                                 #
# OpenVPN also supports                                          #
# single-machine <-> single-machine                               #
# configurations (See the Examples page                          #
# on the web site for more info).                               #
#                                                                 #
# This config should work on Windows                            #
# or Linux/BSD systems. Remember on                             #
```

```
# Windows to quote pathnames and use #
# double backslashes, e.g.: #
# "C:\\Program Files\\OpenVPN\\config\\foo.key" #
# #
# Comments are preceded with '#' or ';' #
#####

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one. You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel if you
# have more than one. On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
```

```
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
# openssl dhparam -out dh2048.pem 2048
dh /etc/openvpn/easy-rsa/keys/dh2048.pem

# Network topology
# Should be subnet (addressing via IP)
# unless Windows clients v2.0.9 and lower have to
# be supported (then net30, i.e. a /30 per client)
# Defaults to net30 (not recommended)
;topology subnet

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
server 10.8.0.0 255.255.255.0

# Maintain a record of client <-> virtual IP address
# associations in this file. If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist /var/log/openvpn/ipp.txt

# Configure server mode for ethernet bridging.
# You must first use your OS's bridging capability
# to bridge the TAP interface with the ethernet
# NIC interface. Then you must manually set the
# IP/netmask on the bridge interface, here we
# assume 10.8.0.4/255.255.255.0. Finally we
```

```
# must set aside an IP range in this subnet
# (start=10.8.0.50 end=10.8.0.100) to allocate
# to connecting clients. Leave this line commented
# out unless you are ethernet bridging.
;server-bridge 10.8.0.4 255.255.255.0 10.8.0.50 10.8.0.100

# Configure server mode for ethernet bridging
# using a DHCP-proxy, where clients talk
# to the OpenVPN server-side DHCP server
# to receive their IP address allocation
# and DNS server addresses. You must first use
# your OS's bridging capability to bridge the TAP
# interface with the ethernet NIC interface.
# Note: this mode only works on clients (such as
# Windows), where the client-side TAP adapter is
# bound to a DHCP client.
;server-bridge

# Push routes to the client to allow it
# to reach other private subnets behind
# the server. Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"

# To assign specific IP addresses to specific
# clients or if a connecting client has a private
# subnet behind it that should also have VPN access,
# use the subdirectory "ccd" for client-specific
# configuration files (see man page for more info).

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
# Then create a file ccd/Thelonious with this line:
#   iroute 192.168.40.128 255.255.255.248
# This will allow Thelonious' private subnet to
# access the VPN. This example will only work
# if you are routing, not bridging, i.e. you are
# using "dev tun" and "server" directives.

# EXAMPLE: Suppose you want to give
```

```
# Thelonious a fixed VPN IP address of 10.9.0.1.
# First uncomment out these lines:
;client-config-dir ccd
;route 10.9.0.0 255.255.255.252
# Then add this line to ccd/Thelonious:
#   ifconfig-push 10.9.0.1 10.9.0.2

# Suppose that you want to enable different
# firewall access policies for different groups
# of clients. There are two methods:
# (1) Run multiple OpenVPN daemons, one for each
#     group, and firewall the TUN/TAP interface
#     for each group/daemon appropriately.
# (2) (Advanced) Create a script to dynamically
#     modify the firewall in response to access
#     from different clients. See man
#     page for more info on learn-address script.
;learn-address ./script

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses. CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by.opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

# Uncomment this directive to allow different
# clients to be able to "see" each other.
# By default, clients will only see the server.
# To force clients to only see the server, you
# will also need to appropriately firewall the
# server's TUN/TAP interface.
;client-to-client

# Uncomment this directive if multiple clients
# might connect with the same certificate/key
# files or common names. This is recommended
# only for testing purposes. For production use,
# each client should have its own certificate/key
```

```
# pair.  
#  
# IF YOU HAVE NOT GENERATED INDIVIDUAL  
# CERTIFICATE/KEY PAIRS FOR EACH CLIENT,  
# EACH HAVING ITS OWN UNIQUE "COMMON NAME",  
# UNCOMMENT THIS LINE OUT.  
;duplicate-cn  
  
# The keepalive directive causes ping-like  
# messages to be sent back and forth over  
# the link so that each side knows when  
# the other side has gone down.  
# Ping every 10 seconds, assume that remote  
# peer is down if no ping received during  
# a 120 second time period.  
keepalive 10 120  
  
# For extra security beyond that provided  
# by SSL/TLS, create an "HMAC firewall"  
# to help block DoS attacks and UDP port flooding.  
#  
# Generate with:  
#   openssl --genkey --secret ta.key  
#  
# The server and each client must have  
# a copy of this key.  
# The second parameter should be '0'  
# on the server and '1' on the clients.  
;tls-auth ta.key 0 # This file is secret  
  
# Select a cryptographic cipher.  
# This config item must be copied to  
# the client config file as well.  
# Note that v2.4 client/server will automatically  
# negotiate AES-256-GCM in TLS mode.  
# See also the ncp-cipher option in the manpage  
cipher AES-256-CBC  
  
# Enable compression on the VPN link and push the  
# option to the client (v2.4+ only, for earlier  
# versions see below)  
;compress lz4-v2  
;push "compress lz4-v2"  
  
# For compression compatible with older clients use comp-lzo  
# If you enable it here, you must also  
# enable it in the client config file.  
comp-lzo
```



```
# The maximum number of concurrently connected
# clients we want to allow.
;max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
#user nobody
#group nogroup

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status /var/log/openvpn/openvpn-status.log

# By default, log messages will go to the syslog (or
# on Windows, if running as a service, they will go to
# the "%Program Files%\OpenVPN\log" directory).
# Use log or log-append to override this default.
# "log" will truncate the log file on OpenVPN startup,
# while "log-append" will append to it. Use one
# or the other (but not both).
;log /var/log/openvpn/openvpn.log
;log-append /var/log/openvpn/openvpn.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages. At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20

# Notify the client that when the server restarts so it
# can automatically reconnect.
explicit-exit-notify 1
```

Last  
update:  
2019/02/25 16:41 mae3xx\_tips:setup\_openvpn:setup\_server:start [https://ma-tech.centurysys.jp/doku.php?id=mae3xx\\_tips:setup\\_openvpn:setup\\_server:start](https://ma-tech.centurysys.jp/doku.php?id=mae3xx_tips:setup_openvpn:setup_server:start)

---

fragment 1426  
mssfix

From:  
<https://ma-tech.centurysys.jp/> - **MA-X/MA-S/MA-E/IP-K Developers' WiKi**

Permanent link:  
[https://ma-tech.centurysys.jp/doku.php?id=mae3xx\\_tips:setup\\_openvpn:setup\\_server:start](https://ma-tech.centurysys.jp/doku.php?id=mae3xx_tips:setup_openvpn:setup_server:start)

Last update: **2019/02/25 16:41**