目次

クライアント側の作業

設定

鍵ファイル類のコピー

サーバ側での作業 で生成したca.crt およびクライアント用の **client**.crt, **client**.key ファイルをセキュアな手段で MA-E3xx に持ってきます。

File	内容
ca.crt	ルートCAの証明書
client.crt	クライアントの証明書
client.key	クライアントの秘密鍵

上記ファイルは /etc/openvpn/keys/ 以下に配置します。

```
root@plum:~# ls -l /etc/openvpn/keys/
total 16
-rw-r--r-- 1 root root 1814 Feb 25 15:58 ca.crt
-rw-r--r-- 1 root root 5600 Feb 25 15:59 mae3xx_1.crt
-rw------- 1 root root 1704 Feb 25 15:59 mae3xx_1.key
```

設定ファイルの作成

OpenVPN クライアント用の設定ファイルを作成します。

client.conf

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
```

```
# Use the same setting as you are using on
# the server.
# 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,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

# Are we connecting to a TCP or
# UDP server? Use the same setting as
# on the server.
;proto tcp
proto udp

# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote openvpn-server.example.jp 1194

# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random

# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite

# Most clients don't need to bind to
# a specific local port number.
nobind

# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nobody

# Try to preserve some state across restarts.
persist-key
persist-tun
```

```
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here. See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]

# Wireless networks often produce a lot
# of duplicate packets. Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings

# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/mae3xx_1.crt
key /etc/openvpn/keys/mae3xx_1.key

# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server". This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
# script in the easy-rsa folder will do this.
;ns-cert-type server

# If a tls-auth key is used on the server
# then every client must also have the key.
;tls-auth ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
;cipher x

# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
comp-lzo
```

```
# Set log file verbosity.
verb 3

# Silence repeating messages
;mute 20

fragment 1426
mssfix
```

※ remote openvpn-server.example.jp 1194 の行は、立ち上げたサーバのアドレスおよびポート番号に変更する必要があります。

起動

設定変更を systemd に通知するため“systemctl daemon-reload” を行ってから起動します。

```
root@plum:~# systemctl daemon-reload
root@plum:~# systemctl start openvpn
```

設定がきちんとできていれば tun0 I/F が up して通信ができるようになります。

```
root@plum:~# ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.0.6  netmask 255.255.255.255  destination 10.8.0.5
        inet6 fe80::7031:7640:14c0:272  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen
100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 304 (304.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

syslog には下記のように出力されます。

```
Feb 25 16:36:42 plum systemd[1]: Starting OpenVPN service...
Feb 25 16:36:42 plum systemd[1]: Started OpenVPN service.
Feb 25 16:36:42 plum ovpn-client[1328]: OpenVPN 2.4.4 arm-unknown-linux-
gnueabihf [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD]
built on Sep  5 2018
Feb 25 16:36:42 plum ovpn-client[1328]: library versions: OpenSSL 1.1.0g  2
Nov 2017, LZO 2.08
```

```
Feb 25 16:36:42 plum systemd[1]: Started OpenVPN connection to client.
Feb 25 16:36:42 plum ovpn-client[1328]: WARNING: No server certificate
verification method has been enabled.  See
http://openvpn.net/howto.html#mitm for more info.
Feb 25 16:36:42 plum ovpn-client[1328]: TCP/UDP: Preserving recently used
remote address: [AF_INET]xxx.xxx.xxx.xxx:1194
Feb 25 16:36:42 plum ovpn-client[1328]: Socket Buffers: R=[163840->163840]
S=[163840->163840]
Feb 25 16:36:42 plum ovpn-client[1328]: UDP link local: (not bound)
Feb 25 16:36:42 plum ovpn-client[1328]: UDP link remote:
[AF_INET]xxx.xxx.xxx.xxx:1194
Feb 25 16:36:44 plum ovpn-client[1328]: TLS: Initial packet from
[AF_INET]xxx.xxx.xxx.xxx:1194, sid=3dac9839 d72b77f5
Feb 25 16:36:44 plum ovpn-client[1328]: VERIFY OK: depth=1, C=JP, ST=Tokyo,
L=Musashino-shi, O=Century Systems, OU=SW4, CN=Century Systems CA,
name=EasyRSA, emailAddress=kikuchi@centurysys.co.jp
Feb 25 16:36:44 plum ovpn-client[1328]: VERIFY OK: depth=0, C=JP, ST=Tokyo,
L=Musashino-shi, O=Century Systems, OU=SW4, CN=server, name=EasyRSA,
emailAddress=kikuchi@centurysys.co.jp
Feb 25 16:36:44 plum ovpn-client[1328]: WARNING: 'link-mtu' is used
inconsistently, local='link-mtu 1546', remote='link-mtu 1562'
Feb 25 16:36:44 plum ovpn-client[1328]: WARNING: 'cipher' is used
inconsistently, local='cipher BF-CBC', remote='cipher AES-256-CBC'
Feb 25 16:36:44 plum ovpn-client[1328]: WARNING: 'keysize' is used
inconsistently, local='keysize 128', remote='keysize 256'
Feb 25 16:36:44 plum ovpn-client[1328]: Control Channel: TLSv1.2, cipher
TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Feb 25 16:36:44 plum ovpn-client[1328]: [server] Peer Connection Initiated
with [AF_INET]xxx.xxx.xxx.xxx:1194
Feb 25 16:36:46 plum ovpn-client[1328]: SENT CONTROL [server]:
'PUSH_REQUEST' (status=1)
Feb 25 16:36:46 plum ovpn-client[1328]: PUSH: Received control message:
'PUSH_REPLY,route 10.8.0.1,topology net30,ping 10,ping-restart 120,ifconfig
10.8.0.6 10.8.0.5,peer-id 0,cipher AES-256-GCM'
Feb 25 16:36:46 plum ovpn-client[1328]: OPTIONS IMPORT: timers and/or
timeouts modified
Feb 25 16:36:46 plum ovpn-client[1328]: OPTIONS IMPORT: --ifconfig/up
options modified
Feb 25 16:36:46 plum ovpn-client[1328]: OPTIONS IMPORT: route options
modified
Feb 25 16:36:46 plum ovpn-client[1328]: OPTIONS IMPORT: peer-id set
Feb 25 16:36:46 plum ovpn-client[1328]: OPTIONS IMPORT: adjusting link_mtu
to 1629
Feb 25 16:36:46 plum ovpn-client[1328]: OPTIONS IMPORT: data channel crypto
options modified
Feb 25 16:36:46 plum ovpn-client[1328]: Data Channel: using negotiated
cipher 'AES-256-GCM'
Feb 25 16:36:46 plum ovpn-client[1328]: Outgoing Data Channel: Cipher
'AES-256-GCM' initialized with 256 bit key
Feb 25 16:36:46 plum ovpn-client[1328]: Incoming Data Channel: Cipher
'AES-256-GCM' initialized with 256 bit key
```

```
Feb 25 16:36:46 plum systemd-udevd[1330]: link_config: autonegotiation is
unset or enabled, the speed and duplex are not writable.
Feb 25 16:36:46 plum ovpn-client[1328]: ROUTE_GATEWAY ON_LINK IFACE=ppp0
HWADDR=00:00:00:00:00:00
Feb 25 16:36:46 plum ovpn-client[1328]: TUN/TAP device tun0 opened
Feb 25 16:36:46 plum ovpn-client[1328]: TUN/TAP TX queue length set to 100
Feb 25 16:36:46 plum ovpn-client[1328]: do_ifconfig,
tt->did_ifconfig_ipv6_setup=0
Feb 25 16:36:46 plum ovpn-client[1328]: /sbin/ip link set dev tun0 up mtu
1500
Feb 25 16:36:46 plum ovpn-client[1328]: /sbin/ip addr add dev tun0 local
10.8.0.6 peer 10.8.0.5
Feb 25 16:36:46 plum ovpn-client[1328]: /sbin/ip route add 10.8.0.1/32 via
10.8.0.5
Feb 25 16:36:46 plum ovpn-client[1328]: WARNING: this configuration may
cache passwords in memory -- use the auth-nocache option to prevent this
Feb 25 16:36:46 plum ovpn-client[1328]: Initialization Sequence Completed
```

確認

ping で確認してみます。

```
root@plum:~# ping -c 5 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=481 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=501 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=480 ms
64 bytes from 10.8.0.1: icmp_seq=4 ttl=64 time=499 ms
64 bytes from 10.8.0.1: icmp_seq=5 ttl=64 time=530 ms

--- 10.8.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 480.386/498.706/530.023/18.034 ms
```