ORCA VPN(ソフト型) Ubuntu 接続手順書

2021 年 11 月 08 日

日本医師会 ORCA 管理機構

目次

1 概要

本資料は、VPN サーバーに対して Linux で接続する手順を記載しています。
Linux では現状他の OS が IPsec VPN として設定が省略されている部分を自分で設定する必要があります。

Linux の L2TP/IPSec はおおまかに以下の方法で VPN を実現してます。

- strongswan の ipsec により VPN サーバーとの IPsec 暗号化接続を確立する
- xl2tpd により PPP デバイスを使用して VPN 接続する。

2 動作環境

- Ubuntu 16.04
- Ubuntu 18.04

3 接続アカウントの準備

ORCA VPN(ソフト型)の申込をおこない、事前共有キー、アカウント名、パスワードを入手して下さい。

4 必要ソフトインストール

以下のコマンドでパッケージをインストールします。

```
$ sudo apt-get install strongswan xl2tpd
```

※ xl2tpd の x と 2 の間の l は小文字エル

以下のバージョンがインストールされます。それ以下のバージョンでインストールされない場合は、apt-line を見直して下さい。

Ubuntu 16.04：xl2tpd 1.3.6+dfsg-4ubuntu0.16.04.1
※ xenial-updates universe が必要

Ubuntu 18.04：xl2tpd 1.3.10-1ubuntu1

5 設定

以下の設定を追加していきます。

5.1 IPSec 設定

/etc/ipsec.conf

```
conn gam
        auto=add
        authby=secret
        right=133.110.224.160
        leftprotoport=17/1701
        rightprotoport=17/1701
        ike=3des-sha1-modp1024!
        esp=3des-sha1-modp1024!
        type=transport
        keyexchange=ikev1
```

5.2 事前共有キー設定

/etc/ipsec.secrets

```
133.110.224.160 : PSK "kguWa4I0ir1w"
```

5.3 L2TP 設定

/etc/xl2tpd/xl2tpd.conf に追加します。

ppp を使用するために後述する /etc/ppp/options.l2tpd.client を指定します。

/etc/xl2tpd/xl2tpd.conf

```
[lac gam]
lns = orcamo.iijgw.jp
ppp debug = yes
pppoptfile = /etc/ppp/options.l2tpd.client
length bit = yes
autodial = yes
redial = yes
redial timeout = 10
max redials = 6
```

5.4 接続設定

設定ファイルにアカウントパスワードを記載します。

- name に vs3it0〜 から始まるアカウント名
- password に パスワードを

L2TP 設定で指定したファイルを作成して設定します。

/etc/ppp/options.l2tpd.client

```
name vs3it0xxx
password xxxxxxxxxxxxxxx
usepeerdns
noauth
mtu 1200
mru 1200
persist
```

5.5 ルーティング設定

/etc/ppp/ip-up.d/にルーティング用のシェルスクリプトを設置します。

/etc/ppp/ip-up.d/0001uporcamo

※下記に出てくる「`」はバッククオート(Shift + @キー)

```
#!/bin/sh


VPNSERVER="133.110.224.160"
OROUTE=`ip route|grep default`
LANNW=`echo ${OROUTE} | awk '{print $1}'`
OGW=`echo ${OROUTE} | awk '{print $3}'`
GWDEV=`echo ${OROUTE} | awk '{print $5}'`
echo ${OROUTE} > /etc/ppp/route.original


if [ -n "`echo $1|grep ppp`" ]; then
    # VPN サーバーとの通信は元のデバイスを使用
    ip route|grep -c "${VPNSERVER}" || ip route add ${VPNSERVER} via ${OGW} dev ${GWDEV}
    # 元のネットワーク（LAN)に限定してルーティング
    ip route|grep -c "${LANNW}" || ip route add ${LANNW} via ${OGW} dev ${GWDEV}
    # ルーティングを追加したい場合は以下に追加
    #
    # 元のデフォルトゲートウェイを削除
```

```
    if [ ! -z "${OROUTE}" ]; then
      ip route del ${OROUTE}
    fi
    # 新しいデフォルトゲートウェイの設定
    ip route add default via $PPP_LOCAL dev $1
fi
```

実行権限が必要なので付けます。

```
sudo chmod +x /etc/ppp/ip-up.d/0001uporcamo
```

さらに切断時にルーティングを戻すスクリプトを/etc/ppp/ip-down.d/設置します。

/etc/ppp/ip-down.d/ 0001downorcamo

※下記に出てくる「`」はバッククオート(Shift + @キー)

```
#! /bin/sh

VPNSERVER="133.110.224.160"

if [ -f /etc/ppp/route.original ] ; then
   ip route|grep -c "${VPNSERVER}" && ip route del ${VPNSERVER}
   ip route add `cat /etc/ppp/route.original`
fi
```

実行権限が必要なので付けます。

```
sudo chmod +x /etc/ppp/ip-down.d/0001downorcamo
```

接続方法

```
sudo ipsec restart
sudo ipsec up gam
sudo service xl2tpd restart
```

6 確認

172.16.2.6 に通信可能のはずなので確認します。

```
$ ping 172.16.2.6
PING 172.16.2.6 (172.16.2.6) 56(84) bytes of data.
64 bytes from 172.16.2.6: icmp_seq=1 ttl=60 time=29.2 ms
...
```

ルーティングを確認します。

```
$ ip route
default via 10.255.3.39 dev ppp0
10.255.0.1 dev ppp0  proto kernel  scope link  src 10.255.3.39
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.5 metric 1
202.221.132.144 via 192.168.0.1 dev eth0
203.178.90.32/27 via 192.168.0.1 dev eth0
```

上記の例は、LAN 環境、ハードウェア環境によって異なります。

default の行、10.255.0.1 の行、133.110.224.160 の行、203.178.90.32 の行が存在していることを確認してください。

6.1 名前解決

DNS サーバーが自動で通知されますが、インターネットの DNS が先に設定されている場合、名前が引けないので VPN の DNS を先にくるように設定します。

接続した状態で /etc/resolv.conf を確認し 「nameserver 172.16.2.6」 が一番上の行に無ければ以下を設定します。

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.1.1
nameserver 172.16.2.6
search xxxx
```

/etc/resolvconf/interface-order の ppp* を上位に並べ替えます。

```
# interface-order(5)
o.inet6
lo.inet
lo.@(dnsmasq|pdnsd)
lo.!(pdns|pdns-recursor)
lo
ppp*  # ← 下にあった ppp* を lo の次に移動
tun*
```

xl2tpd を再起動して確認して下さい。

```
sudo service xl2tpd restart
```

sms.orca.orcamo.jp の名前で通信できることを確認して下さい。

```
$ ping sms.orca.orcamo.jp
PING sms.orca.orcamo.jp (172.16.2.11) 56(84) bytes of data.
64 bytes from 172.16.2.11: icmp_seq=1 ttl=60 time=28.9 ms
```

以上で設定完了です。