OpenVPN の Windows Vistaでの設定と実行

2008 年 8 月 4 日　くわむらじゅん

マルチクライアント OpenVPN の Windows Vista でのクライアント設定と実行につきましては、当初の Windows XP と同じ設定ではうまくゆかず、以下のように特筆すべきことが多々ありました。

Windows Vista の場合、まず、up オプションによるスクリプトの実行もだめでした（これは、おそらくルーティング以前の問題）。また、TUN デバイスでは仮想ポートのデバイスが複数できたため、ルーティングに問題が発生しました。最終的に、デバイスを TUN から TAP に変更し、ルーティングの実行（ROUTE コマンド）を外部コマンドに託し、かつ、管理者権限で実行することで解決しました。

1. Windows Vista の場合、ルーティングの設定が失敗

まず、実行エラーの原因を調べるために、ログを確認しました。タスクアイコンを右クリックして、メニューから「ログの表示」を選び、ログを表示して見てみると次のようなメッセージでした。

```
Tue Jul 22 16:31:39 2008 Notified TAP-Win32 driver to set a DHCP IP/netmask of
10.8.0.14/255.255.255.252 on interface {B3DBC69A-FAA7-4F5B-9F0C-398A061A0391}
[DHCP-serv: 10.8.0.13, lease-time: 31536000]

Tue Jul 22 16:31:39 2008 Successful ARP Flush on interface [14] {B3DBC69A-
FAA7-4F5B-9F0C-398A061A0391}

Tue Jul 22 16:31:39 2008 TEST ROUTES: 3/3 succeeded len=3 ret=1 a=0 u/d=up

Tue Jul 22 16:31:39 2008 route ADD 10.8.0.0 MASK 255.255.255.0 10.8.0.13

Tue Jul 22 16:31:39 2008 ROUTE: route addition failed using CreateIpForwardEntry:
間違った引数があります。 [if index=14]

Tue Jul 22 16:31:39 2008 Route addition via IPAPI failed

Tue Jul 22 16:31:39 2008 route ADD 172.16.0.0 MASK 255.255.0.0 10.8.0.13

Tue Jul 22 16:31:39 2008 ROUTE: route addition failed using CreateIpForwardEntry:
間違った引数があります。 [if index=14]

Tue Jul 22 16:31:39 2008 Route addition via IPAPI failed

Tue Jul 22 16:31:39 2008 route ADD 10.8.0.1 MASK 255.255.255.255 10.8.0.13

Tue Jul 22 16:31:39 2008 Warning: route gateway is not reachable on any active
network adapters: 10.8.0.13

Tue Jul 22 16:31:39 2008 Route addition via IPAPI failed

Tue Jul 22 16:31:39 2008 Initialization Sequence Completed
```

2. ROUTE の設定コマンドの実行改善

このエラーは route add コマンドの実行で失敗しているためで、表示されているコマンドを手動で行っても同じエラーになります。原因は権限の問題なので、

[コントロールパネル]-> [ユーザアカウント] -> [ユーザアカウント制御の有効化または無効化]で、**「ユーザアカウント制御（UAC）を使って・・・」**をクリックして無効にして（再起動が必要）、コマンドを実行するとできるようになりました。

しかし、これを一般利用される方々にお願いするのは好ましくありません。

また、もうひとつ別のエラーがありました。前回と同じタイミングの問題です。Push による設定でもインターフェースが構成される前に route が実行されているようでした。

調べたところ、別のルーティング設定方法として、初期構成のオプションの指定にて外部の route コマンドを実行して行うことができることもわかりました。また、実行の遅延を指定することもできることがわかりました。次に示すオプションを初期構成ファイルに挿入することで、遅延させてから外部コマンドの ROUTE.EXE を実行しルーティングの設定をしてくれるようになりました。

```
route-method exe
route-delay 2
```

（参照：http://konstantin.vassilev.name/?p=79）

ROUTE の設定に成功したところで、”route print /4” (/4 は IPv4 の指定、Vista ではこれがなければ冗長な出力となる)を実行し確認はできましたが、ping を実行してみると、実際には届きませんでした。この問題は、デバイスの構成に問題があり、TUN から TAP(dev tap)に変更することで解決ました。もちろん、同時にサーバ側の設定でも、デバイス指定の変更(dev tap)をしました。

※ tun デバイスを使用するとサーバ側クライアント側双方で 2 つづつインターフェースを使ってしまい、ルーティングが複雑になってしまいますが、それ以前に、Vista では、そのうちのインターフェースのひとつがうまく構成できていませんでした。

3. UAC に対する処置の改善

懸案の管理者権限での実行方法ですが、UAC を無効にして実行する以外に、そのプログラムだけを管理者モードで実行する方法がありました。それは、 openvpn-gui.exe を起動する際に、右マウスボタンのメニューから、「管理者として実行」を選択して実行する方法です。これにより、openvpn-gui.exe は管理権限で実行され、route コマンドも正常に実行されることが確認できました。

※権限を変更してコマンドを実行するツールがありました。これについては付録 A にて言及します。

4. その他、運用関連

クライアントモードでは、各利用者毎に証明書と鍵のペアを生成し、認証局の証明書と一緒に配布する必要があります。証明書と鍵のペアを生成するスクリプトはソースアーカイブに含まれています。そのスクリプトで生成したファイルと一緒にクライアント用 OpenVPN 構成ファイルを生成して zip にアーカイブする簡単なスクリプトをつくりました(付録 B)。インターネット接続が可能な利用者は、OpenVPN Windows 版をインストールした後に、この zip ファイルを展開してできたファイルを、所定の場所(**[OpenVPN configuration file directory]**)にコピーして、OpenVPN をクライアントとして起動するだけで、所内 LAN に接続が可能になります。

以下、冗長となりますが、念のために成功時のログを示しておきます。Push オプションの使用により、ROUTE 設定がサーバ側からの Push によって実行されていることも記録に残っています。

```
Wed Jul 23 10:20:22 2008 OpenVPN 2.0.9 Win32-MinGW [SSL] [LZO] built on Oct 1 2006

Wed Jul 23 10:20:22 2008 IMPORTANT: OpenVPN's default port number is now 1194, based on an
official port number assignment by IANA. OpenVPN 2.0-beta16 and earlier used 5000 as the
default port.

Wed Jul 23 10:20:22 2008 WARNING: using --pull/--client and –ifconfig together is probably
not what you want

Wed Jul 23 10:20:22 2008 WARNING: No server certificate verification method has been
enabled. See http://openvpn.net/howto.html#mitm for more info.

Wed Jul 23 10:20:22 2008 LZO compression initialized

Wed Jul 23 10:20:22 2008 Control Channel MTU parms [ L:1574 D:138 EF:38 EB:0 ET:0 EL:0 ]

Wed Jul 23 10:20:22 2008 Data Channel MTU parms [ L:1574 D:1450 EF:42 EB:135 ET:32 EL:0
AF:3/1 ]

Wed Jul 23 10:20:22 2008 Local Options hash (VER=V4): 'd79ca330'

Wed Jul 23 10:20:22 2008 Expected Remote Options hash (VER=V4): 'f7df56b8'

Wed Jul 23 10:20:22 2008 UDPv4 link local (bound): [undef]:1194

Wed Jul 23 10:20:22 2008 UDPv4 link remote: XXX.XXX.XXX.XXX:1194

Wed Jul 23 10:20:22 2008 TLS: Initial packet from XXX.XXX.XXX.XXX:1194, sid=1de553af fcae763a

Wed Jul 23 10:20:22 2008 VERIFY OK:
depth=1,/C=JP/ST=Tokyo/L=Togoshi/O=EXAMPLE.JP/CN=swan.example.jp/emailAddress=admin@example.
jp

Wed Jul 23 10:20:22 2008 VERIFY OK: depth=0,
/C=JP/ST=Tokyo/O=EXAMPLE.JP/CN=server/emailAddress=admin@example.jp

Wed Jul 23 10:20:22 2008 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key

Wed Jul 23 10:20:22 2008 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication

Wed Jul 23 10:20:22 2008 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key

Wed Jul 23 10:20:22 2008 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication

Wed Jul 23 10:20:22 2008 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024
bit RSA

Wed Jul 23 10:20:22 2008 [server] Peer Connection Initiated with XXX.XXX.XXX.XXX:1194

Wed Jul 23 10:20:23 2008 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)

Wed Jul 23 10:20:23 2008 PUSH: Received control message: 'PUSH_REPLY,route 10.8.0.0
255.255.255.0,route 172.16.0.0 255.255.0.0,route-gateway 10.8.0.1,ping 10,ping-restart
120,ifconfig 10.8.0.12 255.255.255.0'

Wed Jul 23 10:20:23 2008 OPTIONS IMPORT: timers and/or timeouts modified

Wed Jul 23 10:20:23 2008 OPTIONS IMPORT: --ifconfig/up options modified

Wed Jul 23 10:20:23 2008 OPTIONS IMPORT: route options modified

Wed Jul 23 10:20:23 2008 TAP-WIN32 device [ローカル エリア接続 2] opened: \\.\Global\{B3DBC69A-
FAA7-4F5B-9F0C-398A061A0391}.tap

Wed Jul 23 10:20:23 2008 TAP-Win32 Driver Version 8.4

Wed Jul 23 10:20:23 2008 TAP-Win32 MTU=1500

Wed Jul 23 10:20:23 2008 Notified TAP-Win32 driver to set a DHCP IP/netmask of
10.8.0.12/255.255.255.0 on interface {B3DBC69A-FAA7-4F5B-9F0C-398A061A0391} [DHCP-serv:
10.8.0.0, lease-time: 31536000]

Wed Jul 23 10:20:23 2008 Successful ARP Flush on interface [11] {B3DBC69A-
FAA7-4F5B-9F0C-398A061A0391}

Wed Jul 23 10:20:25 2008 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up

Wed Jul 23 10:20:25 2008 route ADD 10.8.0.0 MASK 255.255.255.0 10.8.0.1 OK!

Wed Jul 23 10:20:25 2008 route ADD 172.16.0.0 MASK 255.255.0.0 10.8.0.1 OK!

Wed Jul 23 10:20:25 2008 Initialization Sequence Completed

Wed Jul 23 10:21:15 2008 TCP/UDP: Closing socket
```

```
Wed Jul 23 10:21:15 2008 route DELETE 172.16.0.0 MASK 255.255.0.0 10.8.0.1 OK!
Wed Jul 23 10:21:15 2008 route DELETE 10.8.0.0 MASK 255.255.255.0 10.8.0.1 OK!
Wed Jul 23 10:21:15 2008 Closing TUN/TAP interface
Wed Jul 23 10:21:15 2008 SIGTERM[hard,] received, process exiting
```

付録 A 権限昇格ツール

探してみると、権限の昇格を簡単にするツールとして、「Vista のエレベータ」というのがありました。

（http://homepage3.nifty.com/t-sugiyama/にダウロード用のリンクがある）これをダウンロードして解凍すると3つの実行プログラムが出てきます。

これらを任意の場所に置いて、事前に一回は、VETray.exe を起動します。権限昇格要求が出ますので許可をするとタスクトレイにアイコンができます。

昇格要求不要な（昇格した状態で実行する）コマンドを生成するには、アイコンを右クリックして、メニューから「昇格要求不要なDOSコマンド生成(M)」を選択し、現れたダイアログで実行ファイル名として openvpn-gui.exe のパスを参照から選んで指定し、「デスクトップに起動アイコンの生成」のボタンを押すとできあがります（詳細は Readme.txt を参照）。

この操作で生成された、ショートカットを実行してもうまくゆくことを確認しました。

付録 B　MakeClientCKZip.sh

```
#!/bin/sh -f

if test $# -ne 1; then
  echo "Usage: $0 <client?>"
  exit
fi
cd /usr/local/etc/openvpn/easy-rsa/keys

cat >$1.ovpn<<__EOF__
client

dev tap         # tun | tap
proto udp       # udp | tcp
port 1194

remote swan.example.jp 1194
;remote my-server-2 1194

ca   ca.crt
cert $1.crt
key  $1.key

comp-lzo

persist-tun
persist-key

route-delay 2


# redirect-gateway def-1

;verb 3
;mute 20
__EOF__

zip /tmp/sample-$1.zip ca.crt $1.crt $1.key $1.ovpn
chmod 600 /tmp/sample-$1.zip
```

付録 C　マルチクライアントプラットホームでの OpenVPN

マルチクライアントプラットホームでの OpenVPN 接続では、今後は Windows Vista の対応も必要になることを見越して設定しテストを行い、問題点に改善対処しました。そして、Windows 2000, Windows XP、そして Linux での接続テストを行い、結果は次の表にまとめました。

OS	接続形態	結果	備考
Linux-2.6.23	ADSL NAPT ルータ経由	○	ISP は EAccess
Windows2000	ADSL NAPT ルータ経由	○	ISP は EAccess
WindowsXP	直接ダイアルアップ	○	ISP は EMobile
WindowsXP	ADSL NAPT ルータ経由	○	ISP は EAccess
WindowsXP	ADSL NAPT 無線 LAN	○	ISP は EAccess、Fon ルータ
WindowsXP	ADSL NAPT ルータ経由	×	FortiNet 等別の VPN インストール済み
WindowsVista	ADSL NAPT ルータ経由	○	ISP は EAccess

この結果から、接続形態は、直接ダイアルアップでも、NAPT ルータ経由でも大丈夫でした。また、Windows 2000/XP/Vista,Linux(kernel 2.6.2x)でも可能な共通の設定ファイルをつくることができました。この設定ファイルと証明書と鍵を、配布用の ZIP にまとめる簡易スクリプトを作ってみました（添付）。テストを行ったうち、1 台だけどうしてもうまくゆかなかった PC がありましたが、この PC には FortiClient, 商用 SSH など複数の VPN クライアントソフトウェアがインストールされていたために、そのうちのなにかが影響を及ぼしていることが想像できますが、原因を特定することはできませんでした。

改訂履歴

2008 年 08 月 04 日　初版。

2008 年 10 月 15 日　ログ内の固有名を変更、内容の一部を付録 C へ移動。

© 2008 Jun Kuwamura