OpenVPN Server at Math

Šarūnas Burdulis
Ver. 1, July 2005
Ver. 1.1, 2005.09.01: changed MTU size

Contents

1 Introduction

OpenVPN service is made available at Math Department (MathVPN) as an alternative to the college-wide IPSec-based VPN. The latter type of VPN seems to pose problems for clients using certain Internet providers and from behind NAT routers/firewalls. OpenVPN is based on TLS and has better chances of providing connectivity through firewalls and NAT routers. See [1] and [2] for more on how OpenVPN is different from other VPN technologies.

Authentication scheme used by MathVPN is based on digital certificates issued by the Dartmouth CertAuth1 and therefore is analogous to that used by Dartmouth VPN (Dartmouth VPN also uses DND username and password authentication as an alternative to PKI). Authentication alternatives in OpenVPN are pre-shared secrets (keys) and openvpn-auth-pam. The latter may be of interest when Math LDAP authentication has been introduced.

Our task is to setup OpenVPN service which would allow Linux, Mac OS X and Windows clients to establish a secure tunnel to one of the servers at Math. By establishing such a tunnel, the client should have its IP traffic routed through this secure tunnel, and the connections made to other computers should appear as if they are made from the MathVPN server. To accomplish this we need to: 1) configure the kernel to support virtual TUN/TAP network interfaces, 2) configure Linux netfilter to allow incoming OpenVPN connections and to forward IP traffic in between the physical and virtual network interfaces, 3) get server certificate issued by the Dartmouth CertAuth1 and 4) install and configure OpenVPN.

2 Kernel

Linux kernel has to be configured with:

1. `CONFIG_TUN=y` — virtual network interface driver;
2. `CONFIG_IP_NF_NAT=y` — network address translation (to/from virtual interface, which will be using private IP address space);
3. `CONFIG_IP_NF_TARGET_MASQUERADE=y` — MASQ target used for NAT by netfilter.

If loadable kernel modules are used (`=m`), they have to be loaded on system boot. Add corresponding lines to `/etc/modules`:

```
# echo tun >> /etc/modules
# echo iptable_nat >> /etc/modules
# echo ipt_MASQUERADE >> /etc/modules
```

3 Netfilter

3.1 OpenVPN service

MathVPN will listen on UDP port 1194 (OpenVPN defaults). To open this port in netfilter add to `/etc/iptables.rules`:

```
iptables -A INPUT -p udp --dport 1194 -j ACCEPT
```

3.2 IP forwarding

For its virtual network interface MathVPN will use IP number from the private address space. Clients connecting to the VPN will also be assigned IP addresses from the same address space. Our OpenVPN server therefore will be acting as a router with network address translation (NAT) or ”masquerade”. NAT will occur while forwarding traffic in between the physical server’s network interface `eth0` and the virtual `tun0`. As a result, IP packets coming from the VPN will be rewritten by the router to have headers as if they originated from the server. The following has to be added to the netfilter initialization script `/etc/iptables`:

```
iptables -A INPUT -i tun+ -j ACCEPT
iptables -A OUTPUT -o tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT
iptables -t nat -A POSTROUTING -s 10.7.0.0/24 -o eth0 -j MASQUERADE
```

10.7.0.0/24 is the private network we chose for MathVPN.

4 Certificates

OpenVPN uses TLS, and VPN server therefore needs either 1) its own Certificate Authority (CA) configured via `/etc/ssl/openssl.conf` and a certificate signed by this CA, or 2) server certificate signed by some other CA. We chose the latter and the Dartmouth CertAuth1 as CA — this lets us use Dartmouth personal certificates for client authentication. Certificate procedures are described in more detail in a separate sysadmin document titled ”Math Servers’ Certificates”.

5 OpenVPN Configuration

OpenVPN is available as Debian package `openvpn`. It uses the same executable for both server and client. The role is defined in the configuration file in `/etc/openvpn/`. To install:

```
# apt-get install openvpn
```

MathVPN server configuration file is `/etc/openvpn/server.conf`[1]:

```
# server.conf
#
# IP address to listen on (openvpn will bind to all interfaces if not specified)
local 129.170.28.34

# Use UDP for which openvpn was designed to operate optimally
# See 'man openvpn' for discussion on UDP vs. TCP
proto udp

# Use routed IP tunnel mode ('dev tap' is for Ethernet bridge)
dev tun

# File with Diffie-Hellman parameters for TLS encryption.
# Can be generated with 'openssl dhparam -out dh1024.pem'
dh dh1024.pem

# Cipher algorithm to encrypt packets with
cipher BF-CBC

# Adjustments were necessary to make Starband upload stream work.
# Running client with 'mtu-test' line produced log output:
#   Empirical MTU test completed [Tried,Actual]
#        local->remote=[1541,1237]
#        remote->local=[1541,1437]
# Thus the following settings:
tun-mtu 1500
fragment 1200
mssfix

# Dartmouth CA certificate, MathVPN server certificate and unencrypted private key
ca /etc/ssl/certs/collegeca.pem
cert /etc/ssl/hilbert/hilbert0.pem
key /etc/ssl/hilbert/hilbert0.key

# Allow multiple simultaneous connections with the same client certificate (or Common Name)
duplicate-cn

# Use network 10.7.0.0/24 for MathVPN.
# MathVPN server interface will use 10.7.0.1
server 10.7.0.0 255.255.255.0
```

[1] `openvpn` will find all the config files in `/etc/openvpn/` and will attempt to create VPN server instances or start clients for every config file.

```
# On connection, reconfigure client to have MathVPN server as default gateway
push "redirect-gateway"

# Reconfigure DNS settings on client
push "dhcp-option DOMAIN dartmouth.edu"
push "dhcp-option DNS 129.170.16.4"
push "dhcp-option DNS 129.170.17.4"

max-clients 10

# Connection activity monitoring settings
# (see ping-* options in `man openvpn` for details)
keepalive 10 120
persist-tun
persist-key

# User to run as
user nobody
group nobody

# Logging options
status /var/log/openvpn-status.log
verb 4
log /var/log/openvpn.log
```

6 MathVPN Operation

If installed from the Debian package, OpenVPN should have a start/stop script in `/etc/init.d/` as well as S- and K- symlinks for appropriate runlevels in `/etc/rc*.d/`. The routing table before `openvpn` was started should be:

```
hilbert:# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
129.170.28.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         129.170.28.254  0.0.0.0         UG    0      0        0 eth0
```

To manually start MathVPN:

```
hilbert:# /etc/init.d/openvpn start
Starting OpenVPN daemon: server.
```

Check for `openvpn` process:

```
hilbert:# ps aux|grep vpn
nobody   29166  0.0  0.2   3532  1864 ?        Ss   10:29   0:00 /usr/sbin/openvpn
  --writepid /var/run/openvpn.server.pid --daemon ovpn-server --cd /etc/openvpn
  --config /etc/openvpn/server.conf
```

Check for services listening on UDP:

```
hilbert:# netstat -upln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address         Foreign Address    State     PID/Program name
udp        0      0 129.170.28.34:1194    0.0.0.0:*                    29166/openvpn
udp        0      0 0.0.0.0:631           0.0.0.0:*                    25148/cupsd
... ... ...
```

And the routing table should now have VPN entries (`tun0`, 10.7.0.*):

```
hilbert:# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.7.0.2        0.0.0.0         255.255.255.255 UH    0      0        0 tun0
10.7.0.0        10.7.0.2        255.255.255.0   UG    0      0        0 tun0
129.170.28.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
0.0.0.0         129.170.28.254  0.0.0.0         UG    0      0        0 eth0
```

Below is a sample of normal MathVPN log taken just after the service start and **before** any client connections:

```
hilbert:# cat /var/log/openvpn.log
Wed Jul 27 10:29:05 2005 us=126975 Current Parameter Settings:
Wed Jul 27 10:29:05 2005 us=127172   config = '/etc/openvpn/server.conf'
Wed Jul 27 10:29:05 2005 us=127191   mode = 1
Wed Jul 27 10:29:05 2005 us=127207   persist_config = DISABLED
Wed Jul 27 10:29:05 2005 us=127222   persist_mode = 1
Wed Jul 27 10:29:05 2005 us=127237   show_ciphers = DISABLED
Wed Jul 27 10:29:05 2005 us=127252   show_digests = DISABLED
Wed Jul 27 10:29:05 2005 us=127266   show_engines = DISABLED
Wed Jul 27 10:29:05 2005 us=127280   genkey = DISABLED
Wed Jul 27 10:29:05 2005 us=127295   key_pass_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=127310   show_tls_ciphers = DISABLED
Wed Jul 27 10:29:05 2005 us=127325   proto = 0
Wed Jul 27 10:29:05 2005 us=127340   local = '129.170.28.34'
Wed Jul 27 10:29:05 2005 us=127356   remote_list = NULL
Wed Jul 27 10:29:05 2005 us=127387   remote_random = DISABLED
Wed Jul 27 10:29:05 2005 us=127403   local_port = 1194
Wed Jul 27 10:29:05 2005 us=127417   remote_port = 1194
Wed Jul 27 10:29:05 2005 us=127434   remote_float = DISABLED
Wed Jul 27 10:29:05 2005 us=127449   ipchange = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=127464   bind_local = ENABLED
Wed Jul 27 10:29:05 2005 us=127479   dev = 'tun'
Wed Jul 27 10:29:05 2005 us=127493   dev_type = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=127507   dev_node = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=127523   tun_ipv6 = DISABLED
Wed Jul 27 10:29:05 2005 us=127538   ifconfig_local = '10.7.0.1'
Wed Jul 27 10:29:05 2005 us=127555   ifconfig_remote_netmask = '10.7.0.2'
Wed Jul 27 10:29:05 2005 us=127570   ifconfig_noexec = DISABLED
Wed Jul 27 10:29:05 2005 us=127585   ifconfig_nowarn = DISABLED
Wed Jul 27 10:29:05 2005 us=127600   shaper = 0
Wed Jul 27 10:29:05 2005 us=127614   tun_mtu = 1500
Wed Jul 27 10:29:05 2005 us=127628   tun_mtu_defined = ENABLED
Wed Jul 27 10:29:05 2005 us=127643   link_mtu = 1500
Wed Jul 27 10:29:05 2005 us=127657   link_mtu_defined = DISABLED
Wed Jul 27 10:29:05 2005 us=127672   tun_mtu_extra = 0
Wed Jul 27 10:29:05 2005 us=127686   tun_mtu_extra_defined = DISABLED
Wed Jul 27 10:29:05 2005 us=127701   fragment = 0
Wed Jul 27 10:29:05 2005 us=127725   mtu_discover_type = -1
Wed Jul 27 10:29:05 2005 us=127740   mtu_test = 0
Wed Jul 27 10:29:05 2005 us=127755   mlock = DISABLED
Wed Jul 27 10:29:05 2005 us=127769   keepalive_ping = 10
Wed Jul 27 10:29:05 2005 us=127784   keepalive_timeout = 120
```

```
Wed Jul 27 10:29:05 2005 us=127799   inactivity_timeout = 0
Wed Jul 27 10:29:05 2005 us=127813   ping_send_timeout = 10
Wed Jul 27 10:29:05 2005 us=127828   ping_rec_timeout = 240
Wed Jul 27 10:29:05 2005 us=127842   ping_rec_timeout_action = 2
Wed Jul 27 10:29:05 2005 us=127857   ping_timer_remote = DISABLED
Wed Jul 27 10:29:05 2005 us=127872   remap_sigusr1 = 0
Wed Jul 27 10:29:05 2005 us=127886   explicit_exit_notification = 0
Wed Jul 27 10:29:05 2005 us=127901   persist_tun = ENABLED
Wed Jul 27 10:29:05 2005 us=127916   persist_local_ip = DISABLED
Wed Jul 27 10:29:05 2005 us=127930   persist_remote_ip = DISABLED
Wed Jul 27 10:29:05 2005 us=127944   persist_key = ENABLED
Wed Jul 27 10:29:05 2005 us=127959   mssfix = 1450
Wed Jul 27 10:29:05 2005 us=127973   passtos = DISABLED
Wed Jul 27 10:29:05 2005 us=127988   resolve_retry_seconds = 1000000000
Wed Jul 27 10:29:05 2005 us=128003   connect_retry_seconds = 5
Wed Jul 27 10:29:05 2005 us=128017   username = 'nobody'
Wed Jul 27 10:29:05 2005 us=128032   groupname = 'nobody'
Wed Jul 27 10:29:05 2005 us=128046   chroot_dir = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128061   cd_dir = '/etc/openvpn'
Wed Jul 27 10:29:05 2005 us=128075   writepid = '/var/run/openvpn.server.pid'
Wed Jul 27 10:29:05 2005 us=128090   up_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128105   down_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128119   down_pre = DISABLED
Wed Jul 27 10:29:05 2005 us=128134   up_restart = DISABLED
Wed Jul 27 10:29:05 2005 us=128148   up_delay = DISABLED
Wed Jul 27 10:29:05 2005 us=128162   daemon = ENABLED
Wed Jul 27 10:29:05 2005 us=128176   inetd = 0
Wed Jul 27 10:29:05 2005 us=128191   log = ENABLED
Wed Jul 27 10:29:05 2005 us=128206   suppress_timestamps = DISABLED
Wed Jul 27 10:29:05 2005 us=128233   nice = 0
Wed Jul 27 10:29:05 2005 us=128249   verbosity = 4
Wed Jul 27 10:29:05 2005 us=128264   mute = 0
Wed Jul 27 10:29:05\subsection{Sever Configuration}
 2005 us=128278   gremlin = 0
Wed Jul 27 10:29:05 2005 us=128293   status_file = '/var/log/openvpn-status.log'
Wed Jul 27 10:29:05 2005 us=128308   status_file_version = 1
Wed Jul 27 10:29:05 2005 us=128322   status_file_update_freq = 60
Wed Jul 27 10:29:05 2005 us=128336   occ = ENABLED
Wed Jul 27 10:29:05 2005 us=128351   rcvbuf = 65536
Wed Jul 27 10:29:05 2005 us=128366   sndbuf = 65536
Wed Jul 27 10:29:05 2005 us=128392   socks_proxy_server = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128407   socks_proxy_port = 0
Wed Jul 27 10:29:05 2005 us=128422   socks_proxy_retry = DISABLED
Wed Jul 27 10:29:05 2005 us=128436   fast_io = DISABLED
Wed Jul 27 10:29:05 2005 us=128451   comp_lzo = DISABLED
Wed Jul 27 10:29:05 2005 us=128466   comp_lzo_adaptive = ENABLED
Wed Jul 27 10:29:05 2005 us=128481   route_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128496   route_default_gateway = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128510   route_noexec = DISABLED
Wed Jul 27 10:29:05 2005 us=128525   route_delay = 0
Wed Jul 27 10:29:05 2005 us=128540   route_delay_window = 30
Wed Jul 27 10:29:05 2005 us=128554   route_delay_defined = DISABLED
Wed Jul 27 10:29:05 2005 us=128570   route 10.7.0.0/255.255.255.0/nil/nil
Wed Jul 27 10:29:05 2005 us=128585   management_addr = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128599   management_port = 0
Wed Jul 27 10:29:05 2005 us=128614   management_user_pass = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128628   management_log_history_cache = 250
Wed Jul 27 10:29:05 2005 us=128643   management_echo_buffer_size = 100
Wed Jul 27 10:29:05 2005 us=128657   management_query_passwords = DISABLED
Wed Jul 27 10:29:05 2005 us=128672   management_hold = DISABLED
Wed Jul 27 10:29:05 2005 us=128687   shared_secret_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128702   key_direction = 0
Wed Jul 27 10:29:05 2005 us=128717   ciphername_defined = ENABLED
Wed Jul 27 10:29:05 2005 us=128732   ciphername = 'BF-CBC'
Wed Jul 27 10:29:05 2005 us=128747   authname_defined = ENABLED
```

```
Wed Jul 27 10:29:05 2005 us=128761   authname = 'SHA1'
Wed Jul 27 10:29:05 2005 us=128776   keysize = 0
Wed Jul 27 10:29:05 2005 us=128791   engine = DISABLED
Wed Jul 27 10:29:05 2005 us=128805   replay = ENABLED
Wed Jul 27 10:29:05 2005 us=128820   mute_replay_warnings = DISABLED
Wed Jul 27 10:29:05 2005 us=128835   replay_window = 64
Wed Jul 27 10:29:05 2005 us=128850   replay_time = 15
Wed Jul 27 10:29:05 2005 us=128865   packet_id_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=128880   use_iv = ENABLED
Wed Jul 27 10:29:05 2005 us=128895   test_crypto = DISABLED
Wed Jul 27 10:29:05 2005 us=128909   tls_server = ENABLED
Wed Jul 27 10:29:05 2005 us=128924   tls_client = DISABLED
Wed Jul 27 10:29:05 2005 us=128939   key_method = 2
Wed Jul 27 10:29:05 2005 us=128954   ca_file = '/etc/ssl/certs/collegeca.pem'
Wed Jul 27 10:29:05 2005 us=128969   dh_file = 'dh1024.pem'
Wed Jul 27 10:29:05 2005 us=128984   cert_file = '/etc/ssl/hilbert/hilbert0.pem'
Wed Jul 27 10:29:05 2005 us=128999   priv_key_file = '/etc/ssl/hilbert/hilbert0.key'
Wed Jul 27 10:29:05 2005 us=129013   pkcs12_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129028   cipher_list = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129042   tls_verify = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129057   tls_remote = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129072   crl_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129086   ns_cert_type = 0
Wed Jul 27 10:29:05 2005 us=129101   tls_timeout = 2
Wed Jul 27 10:29:05 2005 us=129116   renegotiate_bytes = 0
Wed Jul 27 10:29:05 2005 us=129131   renegotiate_packets = 0
Wed Jul 27 10:29:05 2005 us=129146   renegotiate_seconds = 3600
Wed Jul 27 10:29:05 2005 us=129161   handshake_window = 60
Wed Jul 27 10:29:05 2005 us=129176   transition_window = 3600
Wed Jul 27 10:29:05 2005 us=129191   single_session = DISABLED
Wed Jul 27 10:29:05 2005 us=129206   tls_exit = DISABLED
Wed Jul 27 10:29:05 2005 us=129233   tls_auth_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129252   server_network = 10.7.0.0
Wed Jul 27 10:29:05 2005 us=129269   server_netmask = 255.255.255.0
Wed Jul 27 10:29:05 2005 us=129286   server_bridge_ip = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129303   server_bridge_netmask = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129320   server_bridge_pool_start = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129337   server_bridge_pool_end = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129353   push_list = 'redirect-gateway,
                                     dhcp-option DOMAIN dartmouth.edu,
                                     dhcp-option DNS 129.170.16.4,
                                     dhcp-option DNS 129.170.17.4,
                                     route 10.7.0.1,ping 10,ping-restart 120'
Wed Jul 27 10:29:05 2005 us=129426   ifconfig_pool_defined = ENABLED
Wed Jul 27 10:29:05 2005 us=129446   ifconfig_pool_start = 10.7.0.4
Wed Jul 27 10:29:05 2005 us=129462   ifconfig_pool_end = 10.7.0.251
Wed Jul 27 10:29:05 2005 us=129479   ifconfig_pool_netmask = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129494   ifconfig_pool_persist_filename = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129510   ifconfig_pool_persist_refresh_freq = 600
Wed Jul 27 10:29:05 2005 us=129526   ifconfig_pool_linear = DISABLED
Wed Jul 27 10:29:05 2005 us=129540   n_bcast_buf = 256
Wed Jul 27 10:29:05 2005 us=129555   tcp_queue_limit = 64
Wed Jul 27 10:29:05 2005 us=129570   real_hash_size = 256
Wed Jul 27 10:29:05 2005 us=129584   virtual_hash_size = 256
Wed Jul 27 10:29:05 2005 us=129599   client_connect_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129615   learn_address_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129630   client_disconnect_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129646   client_config_dir = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129660   ccd_exclusive = DISABLED
Wed Jul 27 10:29:05 2005 us=129675   tmp_dir = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129690   push_ifconfig_defined = DISABLED
Wed Jul 27 10:29:05 2005 us=129707   push_ifconfig_local = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129724   push_ifconfig_remote_netmask = 0.0.0.0
Wed Jul 27 10:29:05 2005 us=129738   enable_c2c = DISABLED
Wed Jul 27 10:29:05 2005 us=129753   duplicate_cn = ENABLED
```

```
Wed Jul 27 10:29:05 2005 us=129768   cf_max = 0
Wed Jul 27 10:29:05 2005 us=129783   cf_per = 0
Wed Jul 27 10:29:05 2005 us=129797   max_clients = 10
Wed Jul 27 10:29:05 2005 us=129812   client_cert_not_required = DISABLED
Wed Jul 27 10:29:05 2005 us=129827   username_as_common_name = DISABLED
Wed Jul 27 10:29:05 2005 us=129843   auth_user_pass_verify_script = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129858   auth_user_pass_verify_script_via_file = DISABLED
Wed Jul 27 10:29:05 2005 us=129872   client = DISABLED
Wed Jul 27 10:29:05 2005 us=129886   pull = DISABLED
Wed Jul 27 10:29:05 2005 us=129901   auth_user_pass_file = '[UNDEF]'
Wed Jul 27 10:29:05 2005 us=129921 OpenVPN 2.0 i486-pc-linux-gnu [SSL] [LZO] [EPOLL]
                                   built on Jul  6 2005
Wed Jul 27 10:29:05 2005 us=130012 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 27 10:29:05 2005 us=161083 Diffie-Hellman initialized with 1024 bit key
Wed Jul 27 10:29:05 2005 us=218942 TLS-Auth MTU parms [ L:1541 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed Jul 27 10:29:05 2005 us=221323 TUN/TAP device tun0 opened
Wed Jul 27 10:29:05 2005 us=221457 TUN/TAP TX queue length set to 100
Wed Jul 27 10:29:05 2005 us=221514 /sbin/ifconfig tun0 10.7.0.1 pointopoint 10.7.0.2 mtu 1500
Wed Jul 27 10:29:05 2005 us=271387 /sbin/route add -net 10.7.0.0 netmask 255.255.255.0 gw 10.7.0.2
Wed Jul 27 10:29:05 2005 us=275303 Data Channel MTU parms [ L:1541 D:1450 EF:41 EB:4 ET:0 EL:0 ]
Wed Jul 27 10:29:05 2005 us=276995 GID set to nobody
Wed Jul 27 10:29:05 2005 us=277128 UID set to nobody
Wed Jul 27 10:29:05 2005 us=277186 Socket Buffers: R=[109568->131072] S=[109568->131072]
Wed Jul 27 10:29:05 2005 us=277237 UDPv4 link local (bound): 129.170.28.34:1194
Wed Jul 27 10:29:05 2005 us=277252 UDPv4 link remote: [undef]
Wed Jul 27 10:29:05 2005 us=277284 MULTI: multi_init called, r=256 v=256
Wed Jul 27 10:29:05 2005 us=277380 IFCONFIG POOL: base=10.7.0.4 size=62
Wed Jul 27 10:29:05 2005 us=277463 Initialization Sequence Completed
```

And a successful client connections shows up in the log as:

```
Wed Jul 27 10:51:08 2005 us=980685 MULTI: multi_create_instance called
Wed Jul 27 10:51:08 2005 us=980835 129.170.28.209:50811 Re-using SSL/TLS context
Wed Jul 27 10:51:08 2005 us=981200 129.170.28.209:50811 Control Channel MTU parms
                                   [ L:1541 D:138 EF:38 EB:0 ET:0 EL:0 ]
                                   Wed Jul 27 10:51:08 2005 us=981231 129.170.28.209:50811
                                   Data Channel MTU parms [ L:1541 D:1450 EF:41 EB:4 ET:0 EL:0 ]
Wed Jul 27 10:51:08 2005 us=981316 129.170.28.209:50811 Local Options String:
                                   'V4,dev-type tun,link-mtu 1541,tun-mtu 1500,
                                   proto UDPv4,cipher BF-CBC,auth SHA1,keysize 128,
                                   key-method 2,tls-server'
Wed Jul 27 10:51:08 2005 us=981332 129.170.28.209:50811 Expected Remote Options String:
                                   'V4,dev-type tun,link-mtu 1541,tun-mtu 1500,
                                   proto UDPv4,cipher BF-CBC,auth SHA1,keysize 128,
                                   key-method 2,tls-client'
Wed Jul 27 10:51:08 2005 us=981380 129.170.28.209:50811 Local Options hash (VER=V4): '239669a8'
Wed Jul 27 10:51:08 2005 us=981407 129.170.28.209:50811 Expected Remote Options hash
                                   (VER=V4): '3514370b'
Wed Jul 27 10:51:08 2005 us=981488 129.170.28.209:50811 TLS: Initial packet from
                                   129.170.28.209:50811, sid=9a293093 fe955833
Wed Jul 27 10:51:09 2005 us=265934 129.170.28.209:50811 VERIFY OK: depth=1,
                                   /DC=edu/DC=dartmouth/C=US/O=Dartmouth_College/
                                   CN=Dartmouth_CertAuth1
Wed Jul 27 10:51:09 2005 us=267164 129.170.28.209:50811 VERIFY OK: depth=0,
                                   /DC=edu/DC=dartmouth/C=US/O=Dartmouth_College/
                                   UID=1503030972/CN=Sarunas_Burdulis/emailAddress
                                   =Sarunas.Burdulis@Dartmouth.edu
Wed Jul 27 10:51:09 2005 us=287430 129.170.28.209:50811 Data Channel Encrypt:
                                   Cipher 'BF-CBC' initialized with 128 bit key
Wed Jul 27 10:51:09 2005 us=287512 129.170.28.209:50811 Data Channel Encrypt: Using 160 bit
                                   message hash 'SHA1' for HMAC authentication
Wed Jul 27 10:51:09 2005 us=287602 129.170.28.209:50811 Data Channel Decrypt:
                                   Cipher 'BF-CBC' initialized with 128 bit key
```

```
Wed Jul 27 10:51:09 2005 us=287621 129.170.28.209:50811 Data Channel Decrypt: Using 160 bit
                                   message hash 'SHA1' for HMAC authentication
Wed Jul 27 10:51:09 2005 us=291273 129.170.28.209:50811 Control Channel: TLSv1,
                                   cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Wed Jul 27 10:51:09 2005 us=291323 129.170.28.209:50811 [Sarunas_Burdulis] Peer Connection
                                   Initiated with 129.170.28.209:50811
Wed Jul 27 10:51:09 2005 us=291410 Sarunas_Burdulis/129.170.28.209:50811 MULTI:
                                   Learn: 10.7.0.6 -> Sarunas_Burdulis/129.170.28.209:50811
Wed Jul 27 10:51:09 2005 us=291432 Sarunas_Burdulis/129.170.28.209:50811 MULTI: primary virtual
                                   IP for Sarunas_Burdulis/129.170.28.209:50811: 10.7.0.6
Wed Jul 27 10:51:10 2005 us=540221 Sarunas_Burdulis/129.170.28.209:50811 PUSH: Received
                                   control message: 'PUSH_REQUEST'Wed Jul 27 10:51:10 2005
                                   us=540359 Sarunas_Burdulis/129.170.28.209:50811 SENT CONTROL
                                   [Sarunas_Burdulis]: 'PUSH_REPLY,redirect-gateway,dhcp-option
                                   DOMAIN dartmouth.edu,dhcp-option DNS 129.170.16.4,dhcp-option
                                   DNS 129.170.17.4,route 10.7.0.1,ping 10,ping-restart
                                   120,ifconfig 10.7.0.6 10.7.0.5' (status=1)
```

MathVPN client setup for Linux, Mac OS X and Windows XP is described in separate user-oriented documents accessible from Computing Resources on Math website.

References

[1] Hans-Cees Speel, Meet OpenVPN, published online in *Linux Journal*, December 15, 2004, http://www.linuxjournal.com/article/7949.

[2] OpenVPN home, http://openvpn.net.