Quick-start for Intel HF2 OPNFV Test-bed

# Introduction

The test-bed is physically hosted at Intel’s Hawthorn Farm lab in Hillsboro Oregon. This is a secure facility in which OPNFV engineers can access bare-metal and VM environments for collaboratively working on OPNFV projects. The lab is isolated from Intel’s business network and accessed via OpenVPN (<https://openvpn.net/>) and administered by Intel personnel. The lab network is segregated into “environments” or “PODs” with VLAN subnets.

# VPN Credentials

You will be provided with a VPN certificate that is unique per user. The files sent to you will include …

1. VPN Profile … used for Windows and Mac clients
2. Security certificate … can be used for Linux clients
3. Key file … can be used for Linux clients

# OpenVPN for Windows Client

Install the OpenVPN client …

1. Download the 64bit installer from this link <http://openvpn.net/index.php/download/community-downloads.html>
2. Run and install the OpenVPN client
3. The OpenVPN GUI icon will be placed on your desktop…right click and select Properties … Compatibility tab, and check the option “Run this program as an administrator”

Copy the two config files to the config directory …

1. Copy the two config files to C:\Program Files\OpenVPN\config\ directory

Run the client …

1. Run OpenVPN GUI as Administrator and it’ll place itself on your icon tray
2. Right Click on the OpenVPN GUI on your icon tray…



Select ENV84-INSIDE if you’re connecting from inside Intel network, select ENV84-OUTSIDE if you’re connecting from public network.

Verify connectivity

1. Shortly after selecting connect, a VPN connection will be established..
2. To confirm you have a VPN connection, ping 10.2.84.250, you should get a reply. This is the IP of the VPN server.

# OpenVPN for Mac

Tunnelblick is a free, open source graphic user interface for OpenVPN on Mac OS X <http://sourceforge.net/projects/tunnelblick/>

1. Download Tunnelblick for MAC <http://www.macupdate.com/app/mac/16969/tunnelblick>
2. Install software.   Launch the downloaded software.



1. Launch the application (tunnelblick) and add the configuration file provide by Intel
* Click connect. You should see something as follows



1. Tune the settings as per your need.

# OpenVPN for Ubuntu Linux Client

There are quite a few options on how to establish an OpenVPN client connection on Ubuntu.

## First option is to use the Network Manager graphical user interface

* Copy 3 certs/keys files from network administrator to home directory
* Verify Wired connection is working properly with Network Manager (up/down arrows)

 

* Install the prerequisite packages:

sudo apt-get install network-manager-openvpn-gnome

sudo service network-manager restart

* Define the OpenVPN connection
	+ Click on Network Manager icon --> VPN Connections --> Configure VPN…



* Add



* OpenVPN --> Create



* Fill out the connection details. For the certificates and keys, browse and locate the key/certs in home directory. Private key is not encrypted, so the Private Key Password field is left blank.



* Click on Advanced

General tab

Use custom gateway port: 443

Use TCP connection: checked



* The VPN Server is using compression, also check the box for "Use LZO data compress" option:



* Proxies tab

Proxy Type: SOCKS

Server Address: proxy-us.intel.com

Port: 1080

Note that the proxy is only needed when inside the Intel corporate network.



* OK --> Save…

* Go back to Network Manager and select the created profile to test:





* To disconnect VPN connection:



## Second option on how to establish an OpenVPN connection is to create a connection file and manually run OpenVPN.

* First, create the connection file:
	+ vi ~/env92-client.opvn



* To establish OpenVPN connection, call openvpn and pass it the config file
	+ sudo openvpn --config ~/env92-client.opvn

![Machine generated alternative text: Wed May 29 17:18:48 2013 TCPv4_CLIENT Unk LocaL [undef] Wed May 29 17:18:48 2013 TCPv4_CLIENT Unk remote: [AF_INET]10.1.192.48:1080 Wed May 29 17:18:52 2013 [fwrouter-env92] Peer Connection Initiated with [AF_INE T] 10. 1. 192. 48 : 1080 Wed May 29 17:18:54 2013 TUN/TAP device tunO opened Wed May 29 17:18:54 2013 do_ifconfig, tt->ipv6=O, tt->did_ifconfig_ipvó_setup=O Wed May 29 17:18:54 2013 /sbtn/ifconfig tuno 5.5.5.3 netmask 255.255.255.248 mtu 1500 broadcast 5.5.5.7 - Wed May 29 17:18:54 2013 InitiaUzation Sequence Completed]()

* Hit Control-C to kill the VPN connection

## Third option on how to establish an OpenVPN connection is to embed the certificates and key into the client configuration file and then call OpenVPN manually

This step is the same as option 2, except the configuration file contains all necessary certs and key:

sudo vi ~/env92-aio.opvn

![Machine generated alternative text: cUent remote 198.175.88.183 443 dey tun proto tcp socks-proxy proxy-us.tnteL.com 1080 nobtnd auth - nocache scrtpt-securtty 2 persist-key perstst-tun <ca> BEGIN CERTIFICATE  MI IDQDCCAqmgAWIBAgIJAK-i-1n9LZajGqMAOGCSqGSIb3DQEBBQUAMHQxCzAJBgNV BAVTAtVTMQ5wCQVDVQQI EwJPUj ESMBAGA1UEBxMJSETMTFNCT1JPMQ4WDAYDVQQK EwVFflY5Mj ERMA8GA1UEAxMIRUSWOTIgQOExITAfBqkqhktG9wOBCQEWEr1FkbWLu QG1udGVsZWljLmNvbTAeFw0xMzA1*4 - F “H c1MjVyMjMyNTZaMHQx CzAJBgNVBAYTA1VTMQswtQVDVQQIEwJPUjESMi IU iXAIJSE’ . .CT1JPMQ4W DAVDVQQKE  ‘“r4fsnhktG94oBCQEw 019KORDc ,   CFRWQEYZgILLL4WRcÇJuNsvIInRWÙN-î+kVrj3” Ÿ’ ÇJ- lKoóoHfvgx9M uXuppVSMdppVdNDS2kyt  _rti  ‘f-eos 2TCB1jAdBgNV HQ4EFgQIY ‘mj3IQPoLuF.MN’AMv]a+)  >r’CBm4AUk9mj3IQP 8LU1..MnANvja’ ,‘Qx94úyh P2MHQxCzAJSg BAYTA1w’ÇswCf DVQQIEWJPUjES MBAGA1UEBxMJStZh 1PMQ4wDAYDVQÇr.Ew “‘HjERMA8GA1UEAxMIRU5W OTIgQOExITAi 1hktG9w0BCQEWEmFkbWù3., tuucivsZWlJLmNvbVIJAK+1n9LZ ajGqMAWGA1UoEWQFMAMBAf8wDQVJK0ZIhvcNAQEFBQADqYEAVh5t8Scqd9aQ3L/V xhez÷1+bdPHttogsuDsAtuwpctDPbsM1lBvMupPks2tVcTLCl8AvrMt4JoamtMw 1//WykCw/3WCLvqKnztfkTnW9VXmWSU5VaTVWtZ4mJdh6XZmYCFDhn79A89JZqGV / 2BDOwb LohyzxVdvzlu EAp j b9lw= END CERTIFICATE  <cert> BEGIN CERTIFICATE  MI IDtzCCAvSgAwIBAgIBAzANBgkqhktG9wOBAQUFADBOMQswCQVDVQQGEwJVUzEL MAkGA1UECBMCT1IxEjAQBgNVBAcTCUhJTExTQk9STzEOMAwGA1UEChMFRU5WOTIx FTAPBnNVBAMTCFVOVIkvT FNRMSFwHwV.]Kn7ThvrNAflkRFh]h7C1 nhkBnhnRl beNn]()

The content of the ca certificate is embedded between the <ca> </ca> tag

The content of the user certificate is embedded between the <cert> </cert> tag

The content of the user private key is embedded between the <key> </key> tag

* To establish OpenVPN connection, call openvpn and pass it the config file

sudo openvpn --config ~/env92-aio.opvn

* Hit Control-C to kill the VPN connection