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 …

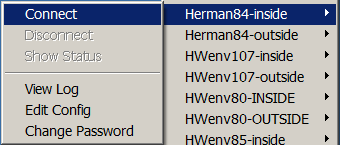
1. Download the 64bit installer from this link <http://openvpn.net/index.php/download/community-downloads.html>
2. Run and install the OpenVPN client
3. The OpenVPN GUI icon will be placed on your desktop…right click and select Properties … Compatibility tab, and check the option “Run this program as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

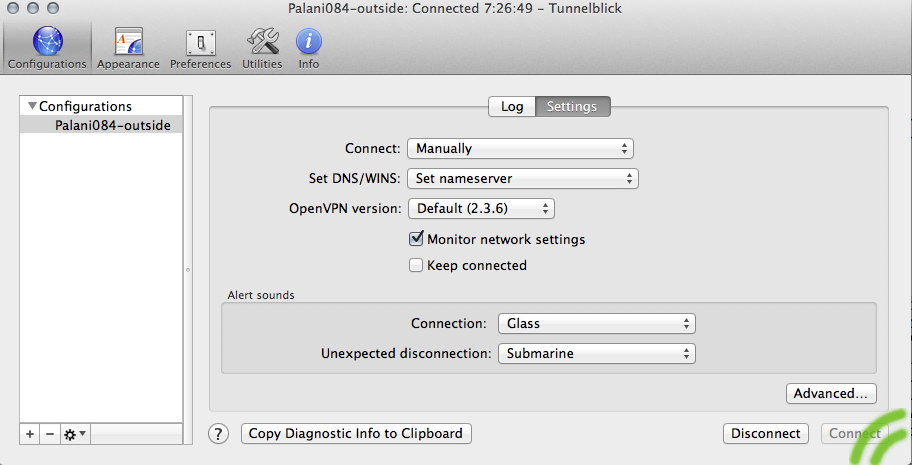
Tunnelblick is a free, open source graphic user interface for OpenVPN on Mac OS X <http://sourceforge.net/projects/tunnelblick/>

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)

Machine generated alternative text: I t4 4)) 4:59PM ISystemAdmiri 

* 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…

Machine generated alternative text: :i ‘t1 4)) 5:05PM ISystemAdmin 
Wired Network fl
Iíupdown (ethO)
Disconnect
I ÇonhigureVPN...  VPN Connections ____
L Disconnect VPN .
___________________ 4/ Enable Networking
Connection Inlormation
L Edit Connections...

* Add

Machine generated alternative text: 000 Network Connections
Wired Wireless Mobile Broadband VPN DSL
Name Last Used [ Add J
EdiL.
DeLete...

* OpenVPN --> Create

Machine generated alternative text: O Choose a VPN Connection Type
SeLect the type of VPN you wish to use for the new connection. if the type of VPN
connection you wish to create does not appear in the list, you may not have the
correct VPN plugin instalLed.
OpenVPN
Compatible with the Open VPN server
Cancel 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.

Machine generated alternative text: Connection name: ENV92
Connect automatically
VPN IPv4 Settings
Ge n e rat
Gateway: 198.175.88183
Au t h e n t ¡ca t Ion
Type: Certilicates (TLS)
User Certilicate:  tlchan-ubul.crt
CA Certificate: j ca.crt
Private Key:  tlchan-ubul.key
Private Key Password:
Show passwords
( Advanced...
Avaitabletoallusers Cancel Save...

* Click on Advanced

General tab

Use custom gateway port: 443

Use TCP connection: checked

Machine generated alternative text: 00 OpenVPN Advanced Options
General Security TLS Authentication Proxies
Usecustomgatewayport: 443
Use custom renegotiation interval: O
Use LZQ data compression
Use a TCP connection
Use a TAP device
Use custom tunnel Maximum Transmission Unit (MTU): 1500
Use custom UDP Iragment size: 1300
Restrict tunnel TCP Maximum Segment Size (MSS)
[__Cancel j [ 0K j

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

Machine generated alternative text: i O OpenVPN Advanced Options
GeneraL Security TLS Authentication Proxies
• Use custom gateway port: 443
Use custom renegotiation interval: O
• Use LZO data compression
• Use a TCP connection
UseaTAP device
Use custom tunnel Maximum Transmission Unit (MTU): 1 500
UsecustomUDPíragmentsize: 1300
Restrict tunnel TCP Maximum Segment Size (MSS)
Cancel j OK j

* Proxies tab

Proxy Type: SOCKS

Server Address: proxy-us.intel.com

Port: 1080

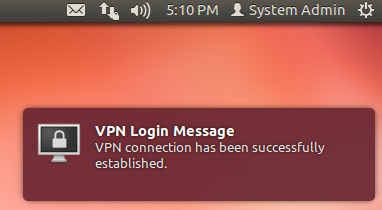
Note that the proxy is only needed when inside the Intel corporate network.

Machine generated alternative text: ØØ OpenVPN Advanced Options
General Security TLS Authentication Proxies
Proxy Type: SOCKS
Select this option ifyour organization requires the
use of a proxy server to access the Internet.
ServerAddress: proxy-us.inteLcom Port: 1080
Retry indelinitely when errors occur
Proxy Username:
Proxy Password:
Fi Show password
[__Cancel__j L__OK j

* OK --> Save…

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

Machine generated alternative text: Pi t4 4)) 5:10PM I System Admin t)
, Iíupdown(etho)
—Th Wired Network
Disconnect
ENV92 VPN Connections
ÇoníigureVPN...  Enable Networking
Connection Informa
Disconnect VPN  Edit Connections... tion



* To disconnect VPN connection:

Machine generated alternative text: t, 4)) 5:11 PM .1 System Admin <
Wired Network
Disconnect
Iíupdown (ethO)
«.? ENV92 VPN Connections
conhigure VPN... 4/ Enable Networking
Disconnect VPN . .
J_________________________

## 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

Machine generated alternative text: citent
remote 198.175.88.183 443
ca /home/sysadritn/tichan-ubul/ca.crt
cert /home/sysadmtn/tichan-ubul/tichan-ubul.crt
key /home/sysadritn/ttchan-ubul/tichan-ubul.key
dey tun
proto tcp
socks-proxy proxy-us.tnteL.con 1080
nobtnd
auth-nocache
scrtpt-security 2
perstst- key
perstst- tun

* 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