

PIA-Tunnel Documentation

Index

Index	1
Overview.....	3
Features.....	3
Initial Setup.....	4
VMware Workstation and Player	4
ESXi	5
Start PIA-Tunnel	6
PIA-Tunnel Setup Wizard.....	7
PIA-Tunnel Web-based user interface (Management Interface).....	8
Overview.....	8
Network Control	8
Network Status	9
Tools	10
Settings.....	10
General Settings	10
PIA Daemon Settings	11
Advanced Settings	11
DHCP Server Settings.....	13
Configuring your Client PC/Devices to use the VPN.....	14
Hands on with Windows 7.....	15
Running a Server or Torrent Client.....	17
Enable Port Forwarding.....	17
Starting your Torrent client with monitor.vbs	19
Known Issues	20

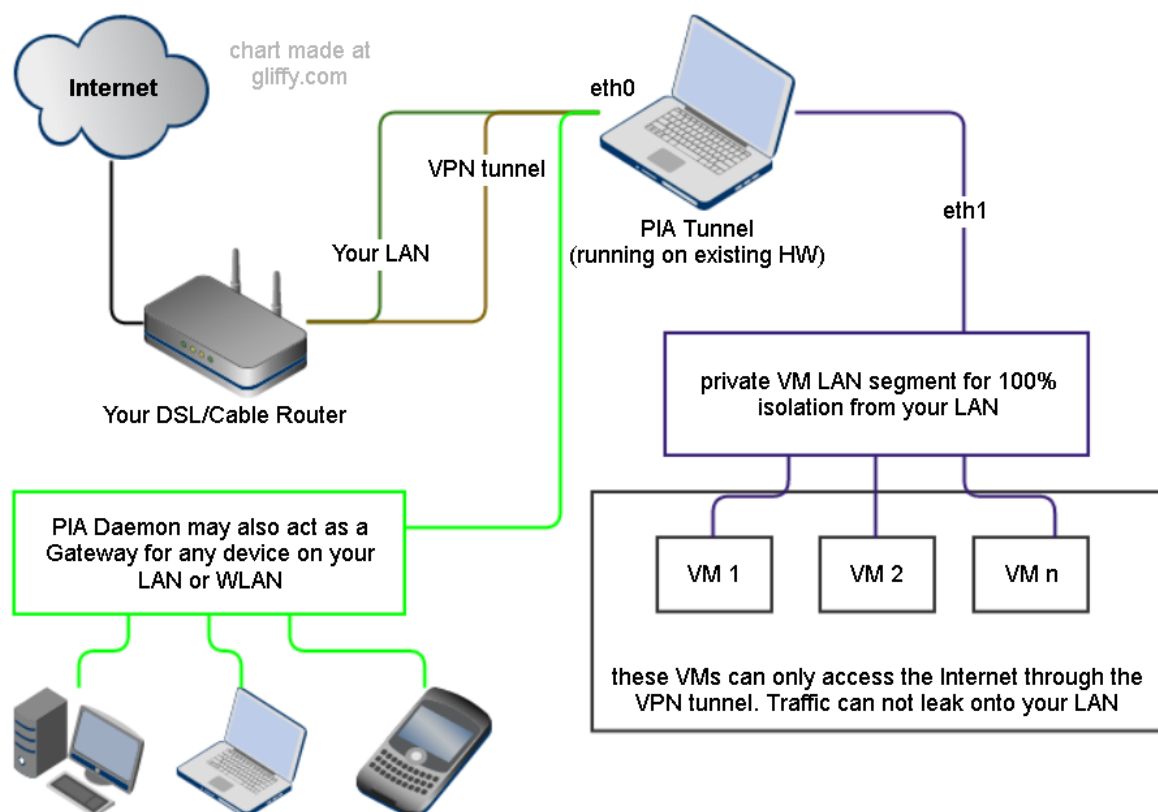
Overview

PIA-Tunnel is a Debian 7 virtual machine which acts as a gateway between your network and the VPN service offered by PrivateInternetAccess.com. The VM will use openvpn to create a connection so it should be compatible with other VPN providers. Get me a test account and I'll implement your provider as well.

The VM has been tested on VMware Workstation, Player and ESXi but should work with any virtual machine solution that supports OVF Templates.

Features

- Open by design! PIA-Tunnel is script based, so no binaries with hidden features and you may roll your own VM by following the [Clean Installation Steps.txt](#)
- Complete network isolation with private VM LAN segment (leak protection)
- Simple Web-interface
- Port forwarding to 1 IP on your LAN or private VM LAN
- Runs on existing hardware, your Computer, Laptop or Homeserver.
- Requires 1 CPU core, 92MB RAM and less then 2GB free drive space



Initial Setup

1. Download the compressed OVF Template from <http://www.kaisersoft.net/r/?PIAIMG>
2. Extract the 7-Zip archive. 7-Zip is a free compression utility <http://www.7-zip.org/>

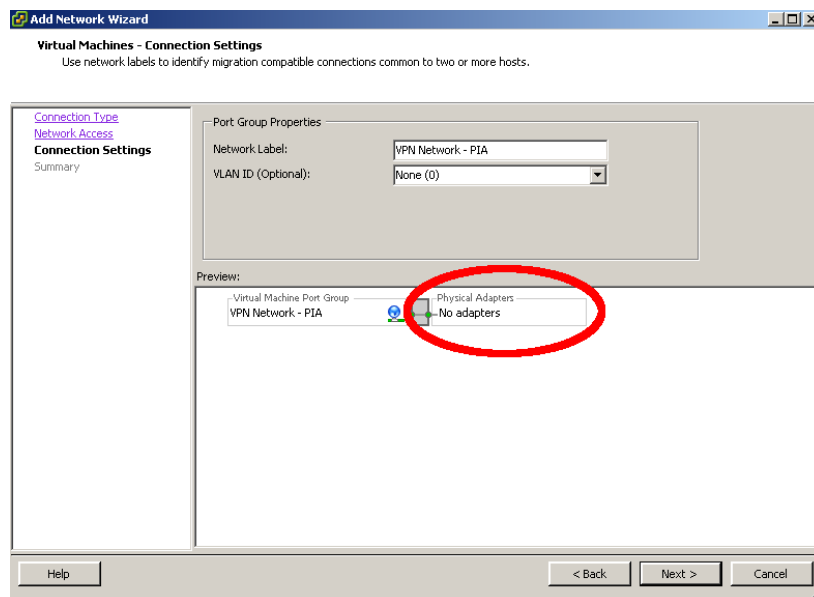
VMware Workstation and Player

1. Add the OVF Template to VMware Workstation or Player
 - a. The easy way:
 - i. Double click on "PIA-Tunnel.ovf" then on "Import" goto step 2
 - b. The hard way:
 - i. Start Player/Workstation and click File => Open...
 - ii. Change file type to "All Files" (lower right corner above OK)
 - iii. Select "PIA-Tunnel.ovf" and click "Open" then "Import"
2. Ensure that the second network adapter is a member of a private LAN segment
 - a. Select "Network Adapter 2"
 - b. Click "LAN Segments" => "Add"
 - c. Enter name of LAN segment. For example: "VPN Bridge"
 - d. Click OK to close
 - e. Use Dropdown to select the LAN segment you just created and click OK

Note: Connect client VMs to this LAN segment and remove or disable their other network cards for complete isolation.

ESXi

1. Setup private VM LAN segment first using vSphere Client
 - a. select your ESXi server and choose "Configuration"
 - b. Click on "Networking" => "Add Networking..."
 - c. "Virtual Machine" => "Create a vSphere standard switch" uncheck any selected interfaces!
NOTE: The preview must list "No adapters" on the "Physical Adapters" side!
 - d. Enter a network name. For example "VPN Network - PIA"



2. Import the OVF Image
 - a. Extract the file you downloaded. You should now have a folder with tree files
 - b. "File" => "Deploy OVF Template..."
 - c. Browse to the extracted files and select "PIA-Tunnel.ovf" => "Next" => "Next"
 - d. Give the VM a name and select a datastore to keep the machine on => "Next"
 - e. Use "Thin Provision" since the VM will not change much
 - f. Select your external Network on the "Network Mapping" screen

- g. Do not auto power the machine once deployment is complete
3. Configure the VM
 - a. Select the VM => "Edit Settings"
 - b. Make sure that "Network adapter 1" is connected to the network with Internet access and that "Network adapter 2" is connected to the private LAN segment you created in step 1 above.
 - c. RAM should be set to at least 92MB RAM. I have never seen the VM SWAP so 92MB is tight but enough.

Start PIA-Tunnel

1. Check that the machine has one CPU and at least 92MB of RAM. The VM will use around 60MB so you should not assign too much.
2. Start the VM and wait until you see "pia-tunnel login:"

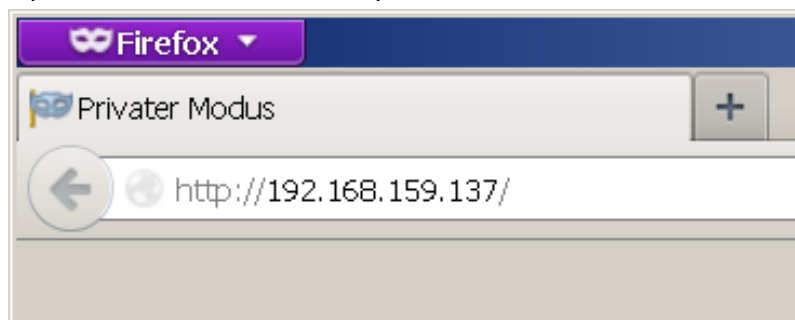
Write down your "Public LAN IP"

```
[ ok ] Starting ACPI services....
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting web server: lighttpd.
[ ok ] Starting ISC DHCP server: dhcpd.
[ ok ] Starting virtual private network daemon:.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[info] 2013-09-18 09:48:30 - VPN is DOWN!
[info] 2013-09-18 09:48:30 - Public LAN IP: 192.168.159.137
[info] 2013-09-18 09:48:30 - Private LAN IP: 192.168.10.1

Debian GNU/Linux 7 pia-tunnel tty1

pia-tunnel login: _
```

3. Open the "Public LAN IP" in your web browser



4. The "PIA-Tunnel Management Interface" should open and prompt you to reset your system. This step is NOT OPTIONAL so click on "Prepare the System and Reboot" to continue.
5. Wait until you see "pia-tunnel login:" again, then refresh the page.
6. The "PIA-Tunnel Setup Wizard" will now open.

PIA-Tunnel Setup Wizard

The “PIA-Tunnel Setup Wizard” will be executed every time the VM is reset. It ensures that the basic configuration options are set properly.

- **Web-UI Username and Web-UI Password**
Access to the Web-UI will be restricted to this user.
- **VPN Username and VPN Password**
Please enter your PIA username and password into these fields
- **VPN Gateway for public LAN**
Set this option to “yes” if you want to share the VPN connection with other computers on your network.
- **VPN Gateway for VM LAN**
Set this option to “yes” if you want to share the VPN connection with a private VM LAN segment
- **root password**
This option will change the default root password from “pia” to something sane. You may enter your own password or accept the randomly generated one.

NOTE: The web GUI is supposed to replace any command line interaction so I recommend that you accept the generated password. You may reset the root password later via the “Tools” menu.

PIA-Tunnel Web-based user interface (Management Interface)

The WebUI should work with any basic HTML5 browser, even with javascript disabled. Enabling javascript will activate the “advanced UI” which will reconfigure some UI elements, enable automatic Network Status updates and make the Settings page easier to use.

Overview

The Overview page is your command and control center.

Network Control

Here you may initiate a VPN connection, terminate an existing connection or execute selected system commands.

- **Start pia-daemon**
 - VPN Disconnected: Will initiate a new VPN connection to “Failover 0”
 - VPN Connected: Will monitor the current connection and attempt to reestablish a connection to “Failover n” on failure
- **Stop pia-daemon**

Stops monitoring the VPN connection but will not terminate it
- **Connect VPN / Connect To**

Establish a VPN connect to the selected location.
- **Disconnect VPN**

Disconnects any active VPN connections
NOTE: pia-daemon will reconnect the VPN if pia-daemon is “running”!
- **Restart Firewall**

reloads the current firewall settings and enable forwarding for configured LAN segments.
- **Stop Forwarding**

reloads the firewall settings and disable any forwarding
- **Restart PIA-VM**

Will reboot the PIA-Tunnel virtual machine
- **Shutdown PIA-VM**

Will shutdown the PIA-Tunnel virtual machine

Network Status

The “Network Status” box will display the current status of your VM. VPN IP and forwarding information will be displayed once the VPN connection has been established.

- **Software**
Will offer a link to the Update Client when an update is available.
- **Status**
This is the connection status “VPN Disconnected”, “Connecting to ...” and so on
- **PIA Daemon**
Displays the current state of the pia-daemon script
- **Public LAN IP**
IP of the VM on your network. (default eth0)
- **Private LAN IP**
IP of the VM on the private VM LAN. (default eth1)
- **VPN down**
Only displayed when the VPN is not connected or not connected yet
- **VPN Public IP**
Displayed once the VPN is connected. This is the IP you will use on the Internet.
- **VPN Port**
Displays the port assigned by your VPN provider. The VPN Port is only important if you want to run a server behind your VPN connection. Please see “[Running a Server or Torrent Client](#)” for more details.
- **Port Forwarding**
This option is only shown when “Enable Port Forwarding” is set to “yes”. It will display your Public VPN IP, the VPN Port and the destination IP.
- **FW Interfaces**
If “VPN Gateway for VM LAN” is enabled it will show *eth1 => tun0*
If “VPN Gateway for public LAN” is enabled it will show *eth0 => tun0*

Please note: The information in “Port Forwarding” and “FW Interfaces” is based on your current firewall configuration and does not reflect the active firewall configuration. New Firewall settings are applied after a new VPN connection has been established, by using “Restart Firewall” or by a running pia-daemon.

Tools

This page gives you access to various PIA-Tunnel tools. You may also reset your root password here.

Settings

This is the main configuration page for the PIA-Tunnel VM. Please don't let the number of options scare you off ☺

General Settings

These are the import settings for PIA-Tunnel. Please take a moment to understand what they do.

- **Enable Port Forwarding** : <yes/no> (default: no)
This option enables port forwarding to a computer connected to PIA-Tunnel. Only set this to yes if you intend to run a server or torrent client. Please see "[Running a Server or Torrent Client](#)" for details
- **Forward IP**: <some IP> (default: 192.168.10.100)
This is the target IP of the open port. The option is only available when "Enable Port Forwarding" is set to "yes".
- **VPN Gateway for VM LAN**: <yes/no> (default: yes)
Setting this option to "yes" will share the VPN connection with any computer on your private "VM LAN Segment". The LAN segment is called "VPN Bridge" in the setup portion of this guide.
- **VPN Gateway for public LAN**: <yes/no> (default: yes)
Setting this option to "yes" will share the VPN connection with any computer on your public "LAN Segment". This is your home network, so any computer that may use your current Internet connection will be able to use PIA-Tunnel to access the VPN.
- **Allow web-UI access on**: <eth0> <eth1> (default: both checked)
This option will open port 80 on the selected interfaces. This is needs to be enabled if you want to use the web-UI to mange PIA-Tunnel and if you want to use "Torrent Monitor" client.
Warning: Unchecking both options will prevent you from accessing the web-UI. You may regain access by adding `FIREWALL_IF_WEB[0]='eth0'` back into `/pia/settings.conf`
- **Allow ssh connections on**: <eth0> <eth1> (default: both NOT checked)
Same as "Allow web-UI access" but for port 22, remote SSH access. Don't enable this if you don't know what SSH is or if you don't indent to use it.

- **Web-UI Username and Web-UI Password**

This option specifies the username and password for the Web-UI. **Note:** You may reset the password by setting the following options to nothing in /pia/settings.conf

WEB_UI_USER=""

WEB_UI_PASSWORD=""

- **Remember Me for:** <some integer> (default: 120) days

No login required for this many days. Set to 0 (zero) to disable this feature.

PIA Daemon Settings

PIA Daemon is a script that may be used to keep your network connected to the VPN.

It will test the VPN connection every few minutes, stop all VPN forwarding on error and attempt to reconnect when the connection is down.

- **Start after OS boot:** <yes/no> (default: yes)

PIA-Tunnel VM will attempt to establish a VPN after the operating system has finished booting. Once this option is enabled, you only need to turn on the virtual machine and the VPN connection will be established a few minutes later.

- **Failvoer 0 – n**

These are the locations pia-daemon will use to initiate a VPN connection. Connections are used in sequence so pia-daemon will always create the initial connection with "Failover 0", try "Failover 1" if the connection fails and so on.

Setting "Failover n" to an empty value will remove the Failover setting entirely.

Warning: Locations marked with a * support port forwarding. Keep in mind that the open network port is assigned to you by your VPN provider and will change when you connect to a different location! I provide a monitoring script to detect these port changes, reconfigure your torrent client and restart the application.

Please see "[Starting your Torrent client with monitor.vbs](#)" for details.

Advanced Settings

The advanced settings are below the General Settings. Click on "Show Advanced Settings" to display the options.

WARNING: You can really mess things up in here and may even compromise your security by changing the wrong option.

- **Public LAN interface:** <eth0/eth1/tun0> (default: eth0)

Specifies which interface is connected to your public LAN.

WARNING: Don't change this!

- **VM LAN interface:** <eth0/eth1/tun0> (default: eth1)

Specifies which interface is connected to the private VM LAN segment.

WARNING: Don't change this!

- **VPN interface:** <eth0/eth1/tun0> (default: tun0)
Specifies which interface will be handling the VPN connection.
WARNING: Don't change this!
- **eth0 use DHCP:** <yes/no> (default: yes)
Allows you to configure a fixed IP for eth0 or use an existing DHCP server. This interface will be connected to your LAN where your cable/DSL router is providing DHCP service. Don't change this unless you need to set a static IP.
- **eth0 IP/Subnet/Gateway** (default: all empty)
These options are enabled when "eth0 use DHCP" is set to no.
- **eth1 use DHCP:** <yes/no> (default: no)
Allows you to configure a fixed IP for eth1 or use an existing DHCP server. This interface is connected to your private VM LAN segment without a DHCP server. PIA-Tunnel provides DHCP service for this segment so the IP must be fixed.
I recommend that you don't change this unless you know networking.
- **eth1 IP/Subnet/Gateway** (default: IP:192.168.10.1 Subnet: 255.255.255.0 Gateway: empty)
These options are enabled when "eth1 use DHCP" is set to no.
- **DNS 1-4**
Specifies the DNS servers used by PIA-Tunnel VM. The VM ships with the following defaults:
8.8.8.8 is a public DNS Server hosted by Google.com
208.67.222.222 is a public DNS Server hosted by OpenDNS.com
8.8.4.4 is a public DNS Server hosted by Google.com
208.67.220.220 is a public DNS Server hosted by OpenDNS.com
- **Max allowed packet loss:** <0%-100%> (default: 20%)
Specifies how many ping packets may be lost, per check, before pia-daemon considers the VPN connect as down/bad. Pia-daemon will attempt to connect to Failover 1 through n when the ping failure rate is above this threshold.
- **Verbose / Debug Verbose:** <yes/no> (default: no)
Enables verbose or verbose debug mode on the command line. This option is not used by the web-UI.

DHCP Server Settings

This box gives you access to the configuration file of the DHCP Server running inside PIA-Tunnel. The current UI supports up to two subnets.

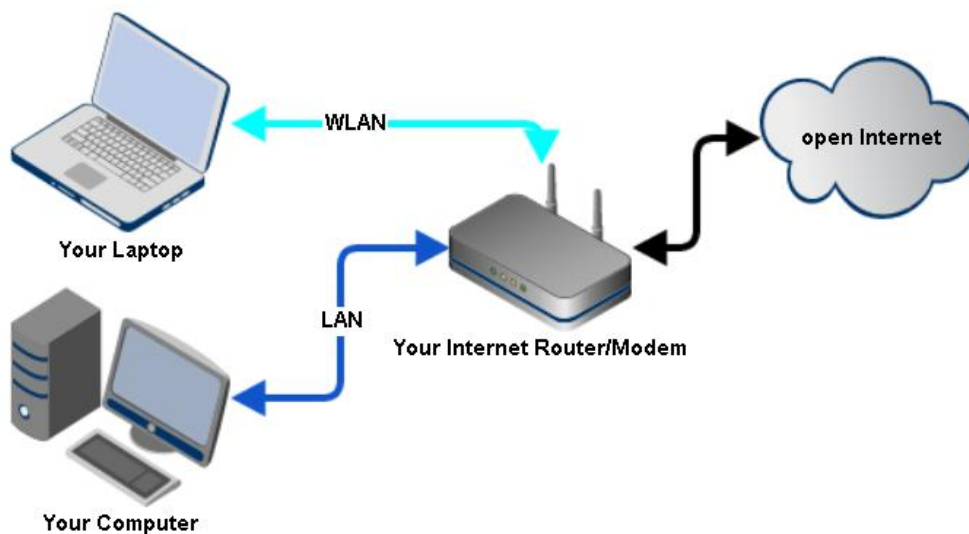
Please contact support (from Tools page) if you require more subnet options.

- **Subnet 1:** <enabled/disabled> (default: enabled)
Adds the following settings to the configuration file if “enabled” or removes them when “disabled”.
- **Subnet IP 1:** <IP Address> (default: 192.168.10.0)
IP address of the network
- **Subnetmask 1:** < IP Address > (default: 255.255.255.0)
Subnetmask used by any DHCP clients on your network
- **Broadcast IP 1:** <IP Address> (default: 192.168.10.255)
Broadcast IP used by any DHCP clients on your network
- **Router/Gateway 1:** <IP Address> (default: 192.168.10.1)
Gateway IP used by any DHCP clients on your network
- **IP Range 1:** <IP_Address IP_Address> (default: 192.168.10.101 192.168.10.151)
Range of IPs used by the DHCP server.
Please note the format of “<IP Address><SPACE><IP Address>”
- **Subnet 2:** <enabled/disabled> (default: disabled)
You may setup a second IP Range using the “Subnet 2” option.
Warning: Only use this if you know networking!
- **Subnet IP/Subnetmask/Broadcast IP/Router/Gateway/IP Range**
Same definition as “Subnet 1” but the settings must not define the same range.
Warning: Only use this if you know networking!
- **Fixed IP:** <IP Address> (default: empty)
Specifies one fixed IP that will be assigned to a computer with a MAC address matching the “MAX for IP” setting. You should also enter this IP into “Forward IP” found in “General Settings”
- **MAC for IP:** <MAC Address> (default: empty)
Specifies which computer will receive the Fixed IP specified above.
Please note: The MAC Address must be separated by colons (:). Example: 00:0D:28:A7:3C:45

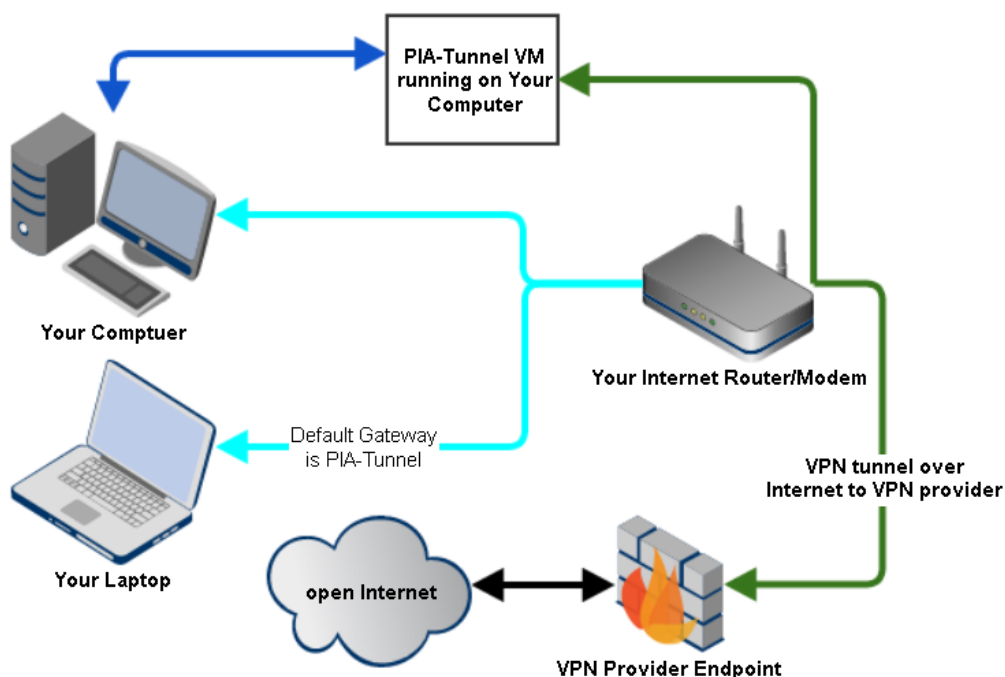
Configuring your Client PC/Devices to use the VPN

PIA-Tunnel acts as a gateway between your LAN and the VPN connection. The operating system of your client devices needs to be configured to use the VPN tunnel as the “Default Gateway”. This will ensure that all network traffic is sent through the VPN and not directly onto the Internet.

This is a typical home/small business network setup. All traffic is directly sent to your router and out onto the Internet.



This is the same setup, all devices are still connected the same way but traffic is first sent to the PIA-Tunnel VM, then to your VPN provider, before it reaches the open Internet.



Hands on with Windows 7

Enough theory, let's get to work.

I will now configure a Windows 7 PC running on my LAN to use the PIA-Tunnel as a default gateway.

I call this the "typical home setup"

1. Start by getting your Internet IP your Inter Service Provider has assigned to you. [Open this page to get your current IP.](#)
2. Open VMware Workstation or Player and ensure that your "Network Adapter" is set to **Bridged** and "Network Adapter 2" is set to **LAN Segment**. (See [Initial Setup](#) if it is not)

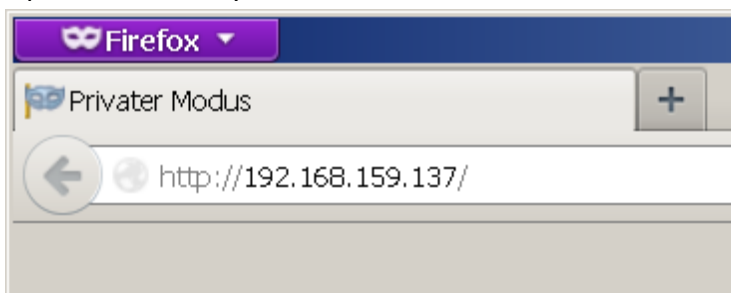


3. Start the VM and wait until you see "pia-tunnel login:"
Write down the "Public LAN IP", 192.168.159.137 in this example

```
[ ok ] Starting ACPI services...
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting web server: lighttpd.
[ ok ] Starting ISC DHCP server: dhcpd.
[ ok ] Starting virtual private network daemon:.
[ ok ] Starting OpenBSD Secure Shell server: sshd.
[info] 2013-09-18 09:48:30 - VPN is DOWN!
[info] 2013-09-18 09:48:30 - Public LAN IP: 192.168.159.137
[info] 2013-09-18 09:48:30 - Private LAN IP: 192.168.10.1

Debian GNU/Linux 7 pia-tunnel tty1
pia-tunnel login: _
```

4. Open the IP with your webbrowser



5. Goto "Network Config" and make sure that "VPN Gateway for public LAN" is set to "yes".
6. Goto "Overview" and click "Connect VPN". Wait a little while then refresh the page until the "Status" field changes to "Connected to YourLocation".
7. This is it for the PIA-Tunnel. Next time you just boot the VM and click "Connect VPN"
8. On your Windows 7 Computer, open the "Network and Sharing Center" found in the Control Panel.
9. Click "Change adapter settings" in the top left corner
10. Ignore the VMware Network Adapters. Right click on your "LAN Connection" and select "Properties".
11. Click on "Internet Protocol Version 4" => "Properties"
 - a. If "Obtain an IP address automatically" is selected
 - i. Click "Advanced"
 - ii. Click on "Add" under "Default gateways:" and enter the "Public LAN IP" of the PIA-Tunnel (Step 2).
 - iii. OK to close the Form
 - iv. You should see the IP in the "Default gateway" box now. The settings will override the Information sent by your router but will still use the IP and Subnetmask provided.
 - v. Select "Use the following DNS server addresses" and enter
Preferred DNS server: 8.8.8.8
Alternate DNS server: 208.67.222.222
 - vi. Click OK until all forms are closed
 - b. If "Use the following IP address" is selected
 - i. Enter the "Public LAN IP" of the PIA-Tunnel (Step 2) into the "Default gateway" box.
 - ii. Select "Use the following DNS server addresses" and enter
Preferred DNS server: 8.8.8.8
Alternate DNS server: 208.67.222.222
 - iii. Click OK until all forms are closed

12. That is it. All traffic should now be routed through the VPN tunnel. Double check by opening a [website that will display your public IP](#).

The IP must not be the same one from step 1 and has to match the “VPN Public IP” displayed on the “Overview” page.

Running a Server or Torrent Client

Some PIA VPN endpoints support port forwarding so you may run any kind of server behind the VPN connection. This section will refer to this computer as your **server**.

Keep in mind that PIA will assign the open port so you need to reconfigure your server software when you change VPN endpoints or if PIA assigns you a new port.

The PIA-Tunnel VM comes with a client script that can detect port changes and reconfigure your torrent client using the new port. The script is currently only available for Windows and supports [Deluge](#) or [qBittorrent](#)

Enable Port Forwarding

Port forwarding works by redirecting traffic for a specific port number to a single IP on your network. Other computers will be able to share the same VPN connection but incoming requests on the “open port” will always go to the computer you specify below.

- 1) Open “Settings” and locate the “PIA Network Settings” section
- 2) Ensure that “Enable Port Forwarding” is set to yes
- 3) Enter the IP of your server into the “Forward IP” field. This should be a static IP.
- 4) Confirm your changes with “Store Settings”
- 5) Go back to the main “Overview” and connect with any locations marked with a *
- 6) You should see a “VPN Port” and “Port Forwarding” entry once the connection is established. The “VPN Port” is the port someone would use to connect to the server running behind your VPN IP.
- 7) Go to your server, open the PIA Tunnel Web-GUI, go to “Tools” and download the “Torrent Monitor for Windows”
- 8) Extract the archive
- 9) Double click on pskill.exe to accept the license. You only need to accept the license once.

Settings for Deluge

- 1) Open monitor.ini in a text editor and configure the following settings

- a. STATUS_IP=192.168.10.1
This is either the "Private LAN IP" or "Public LAN IP" of the PIA Tunnel VM.
- b. SOFTWARE=deluge
Set this option to deluge
- c. PROCESS_NAME=
Optional: Specifies the process name as seen by the Windows Taskmanager. This should not be required when SOFTWARE is set to deluge or qBittorrent
- d. EXE_PATH= C:\My Custom Path\Deluge\deluge.exe
Optional: Specify the location of executable if not installed in a default location.
- e. CONFIG_PATH=C:\My Custom Path\deluge\core.conf
Optional: Specify the location of the deluge config file IF not in the default location of: %APPDATA%\deluge\core.conf

Settings for qBittorrent

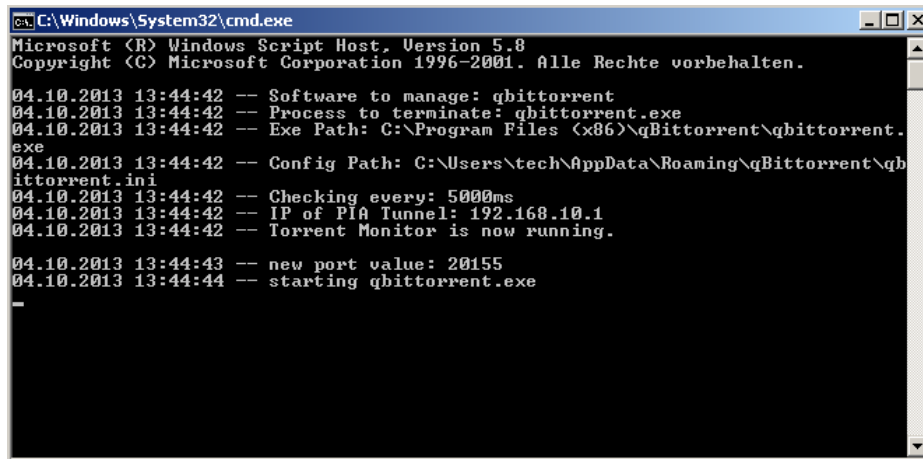
- 1) Open monitor.ini in a text editor and configure the following settings
 - a. STATUS_IP=192.168.10.1
This is either the "Private LAN IP" or the "Public LAN IP" of the PIA Tunnel VM.
 - b. SOFTWARE=qbittorrent
Set this option to qbittorrent
 - c. PROCESS_NAME=
Optional: Specifies the process name as seen by the Windows Taskmanager. This should not be required when SOFTWARE is set to deluge or qBittorrent
 - d. EXE_PATH=C:\My Custom Path\qbittorrent \ qbittorrent.exe
Optional: Specify the location of executable if not installed in a default location.
 - e. CONFIG_PATH=C:\My Custom Settings Path\qbittorrent \qBittorrent.ini
Optional: Specify the location of the deluge config file IF not in the default location of: %APPDATA%\ qbittorrent \qBittorrent.ini

Starting your Torrent client with monitor.vbs

The monitoring script isn't very smart so you should always use it to start your torrent client.

Simply double click on "monitor.vbs" to get the latest port info and update the configuration before starting your torrent client.

You should see a window similar to this screenshot. You may stop the script at any time by closing the command window.



```
C:\Windows\System32\cmd.exe
Microsoft (R) Windows Script Host, Version 5.8
Copyright (C) Microsoft Corporation 1996-2001. Alle Rechte vorbehalten.

04.10.2013 13:44:42 -- Software to manage: qbittorrent
04.10.2013 13:44:42 -- Process to terminate: qbittorrent.exe
04.10.2013 13:44:42 -- Exe Path: C:\Program Files (x86)\qBittorrent\qbittorrent.
exe
04.10.2013 13:44:42 -- Config Path: C:\Users\tech\AppData\Roaming\qBittorrent\qb
ittorrent.ini
04.10.2013 13:44:42 -- Checking every: 5000ms
04.10.2013 13:44:42 -- IP of PIA Tunnel: 192.168.10.1
04.10.2013 13:44:42 -- Torrent Monitor is now running.

04.10.2013 13:44:43 -- new port value: 20155
04.10.2013 13:44:44 -- starting qbittorrent.exe
```

Known Issues

You may contact support at <http://www.kaisersoft.net/r/?HELPME>

- The “Overview” page may not show the correct “Connecting to XXX” location when the system is rebooted while connecting and if “Start after OS boot” is set to “yes”.
This is only a label/caching bug and will correct itself once a VPN connection has been established.