Last Update 2013-09-20 14:30

PIA-Tunnel Documentation

Index

Last Update 2013-09-20 14:30

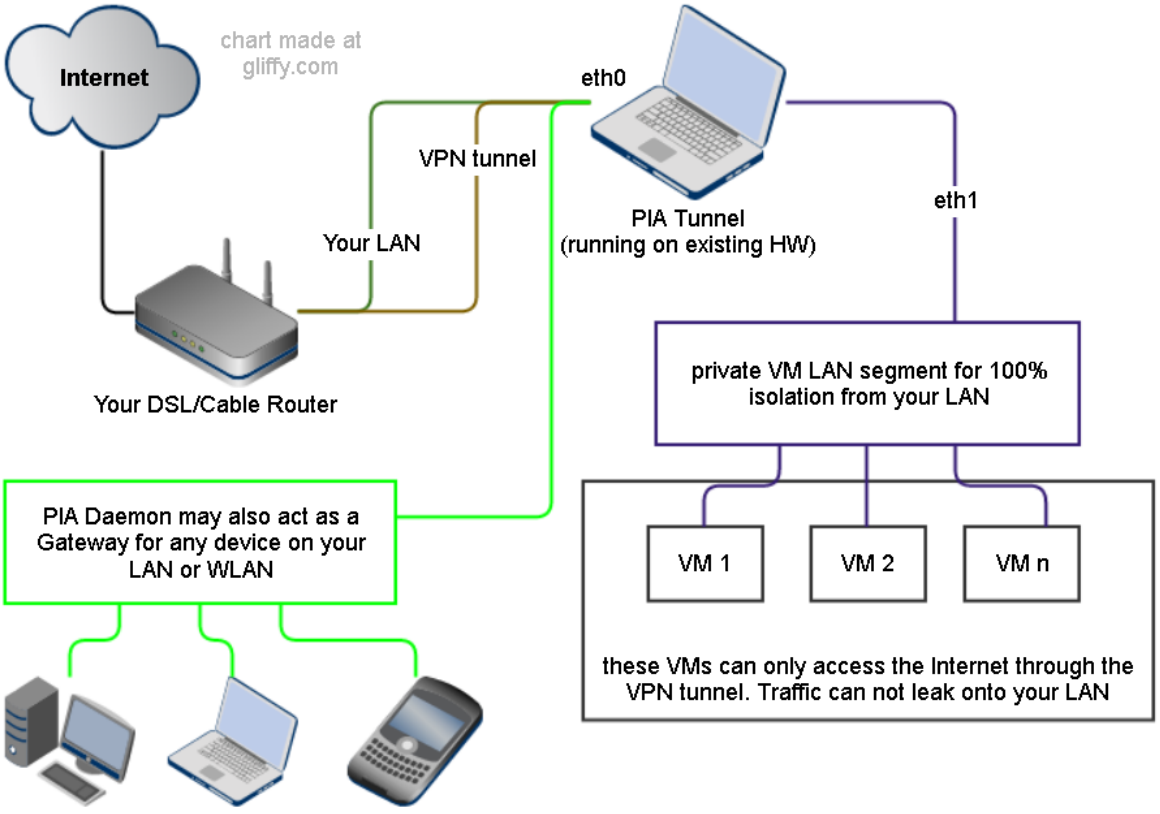
Overview

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 with OVF Template support.

Features

- Open by design. 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.
- Requires 1 CPU core, 92MB RAM and less then 2GB free drive space



Last Update 2013-09-20 14:30

Initial Setup

1. Download the compressed OVF Template from https://mega.co.nz/#!7MYRUQhA!TjQ8FBr2vM1JXGBmTmlHxG2hStIxdvr-JXTBhkmqUr0

2. Extract the 7-Zip archive. 7-Zip is a free compression utility http://www.7-zip.org/

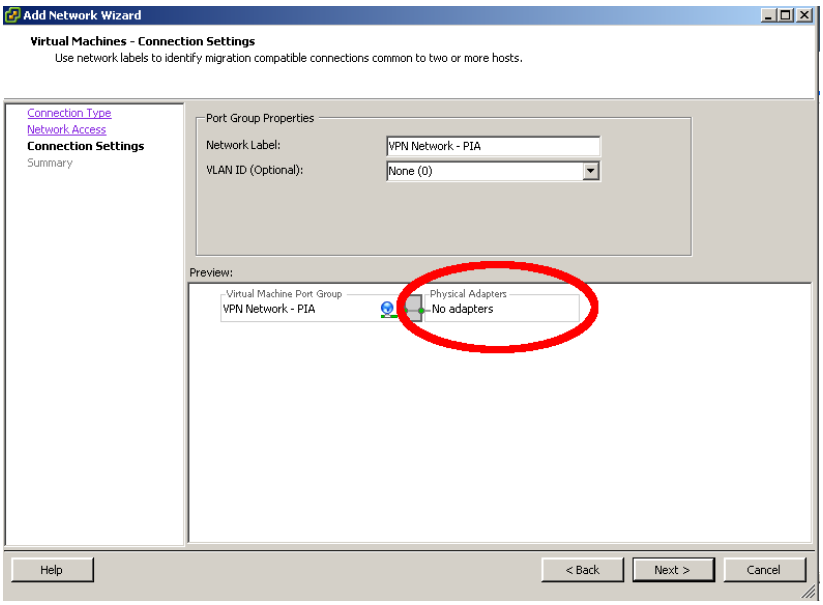
VMware Workstation and Player

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"

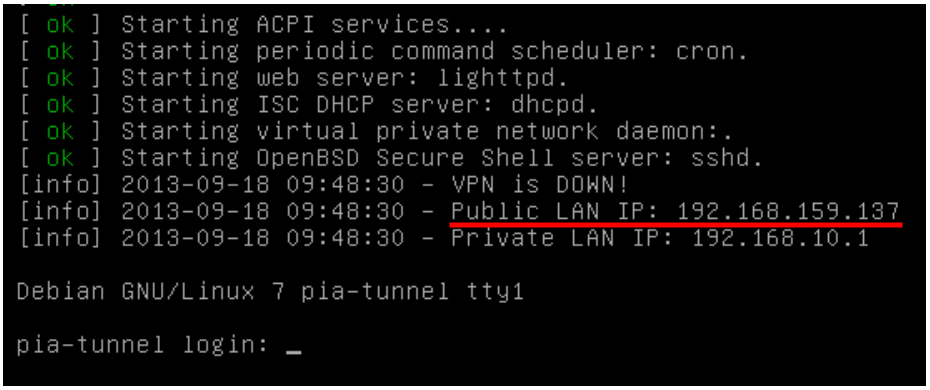
    b. Make sure that "Network adapter 1" is connected to the network with Internet access and that "Network adapter 2" is connected to the private LAN segment you created in step 1 above.

    c. RAM should be set to at least 92MB RAM. I have never seen the VM SWAP so 92MB is tight but enough.

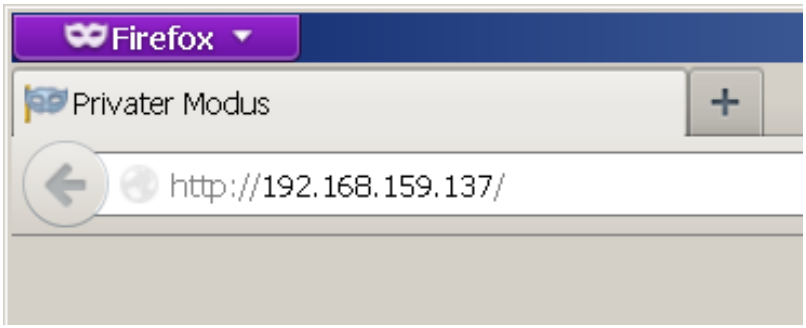
Start PIA-Tunnel

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”



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.

- **Username** and **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

- **Enable Port Forwarding** and **Forward IP**
  Set this option to “yes” if you intend to run a server/torrent client or similar and want to allow incoming connections.
  The **Forward IP** may point to a single IP on your LAN or private LAN segment. The port number will be displayed after a VPN connection is established AND only if the endpoint supports forwarding.

- **Enable pia-daemon**
  starts a background script to reconnect your VPN connection on failure and connect to failover destinations in case of a provider outage.

- **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.

Last Update 2013-09-20 14:30

PIA-Tunnel Management Interface

Overview

The overview is the “Command and Control Center” for PIA-Tunnel.

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**
  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

This will always display the current status of your VM. VPN IP and the open port will be displayed once the VPN connection has been established.

- **Status**
  Displays the current status of your VPN connection. Currently refreshed on page load only.
- **PIA Daemon**
  Displays the current status and setting of pia-daemon
- **Public IP**
  This is your public LAN IP. Configure your network devices to use this IP as the default Gateway.
- **Private IP**
  This is the private VM LAN IP. Configure your network devices to use this IP as the default Gateway.
- **VPN IP**
  This is your IP on the VPN network
- **VPN Public IP**
  This is your public Internet IP. You are hiding behind this IP when you access a resource on the Internet.
- **VPN Port**
  This is the port number someone would use to connect with a server running on your LAN. Keep in mind that this port is assigned by the VPN provider and will change when you switch locations.
- **Forwarding**
  This will show any connections where “VPN Gateway for *“ is set to “yes”

Tools

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

Network Config

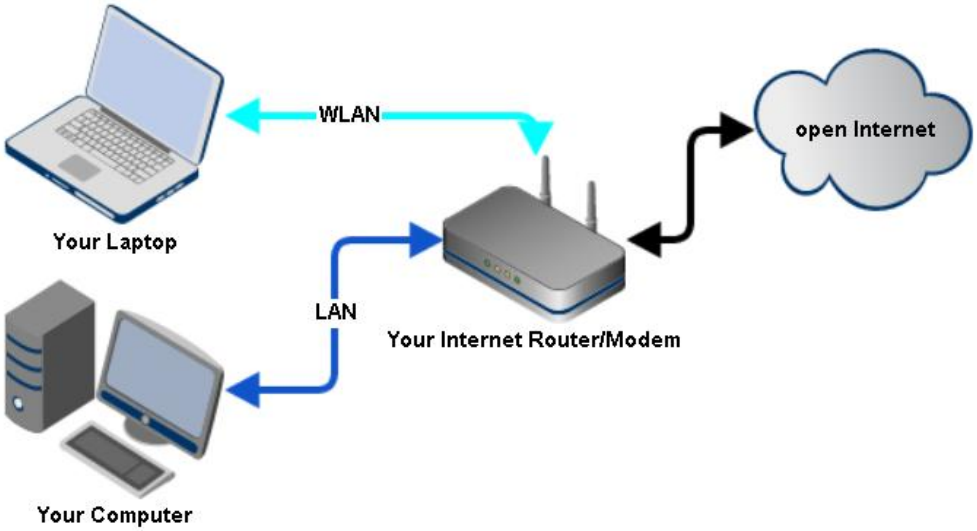
This is the main configuration page for the PIA-Tunnel VM. Here you may find everything from firewall to dhcp server settings.

The page will be reworked soon so I am not going into too much detail. The default settings should work for most people.

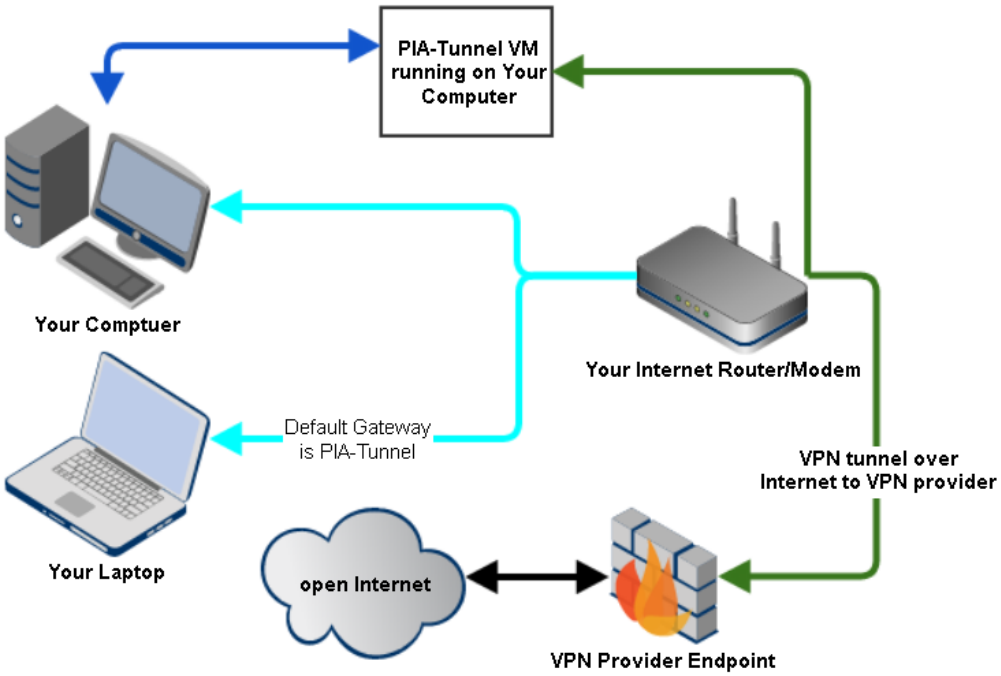
Configuring your Client PC/Devices to use the VPN

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.



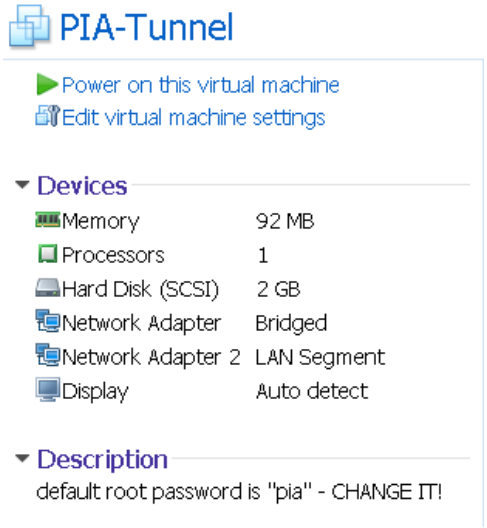
Hands on with Windows 7

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.

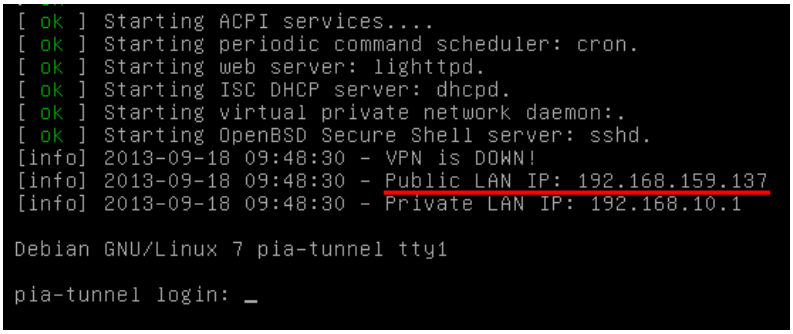
I call this the "typical home setup"

1. Start by getting your Internet IP your Inter Service Provider has assigned to you. Open this page to get your current IP.

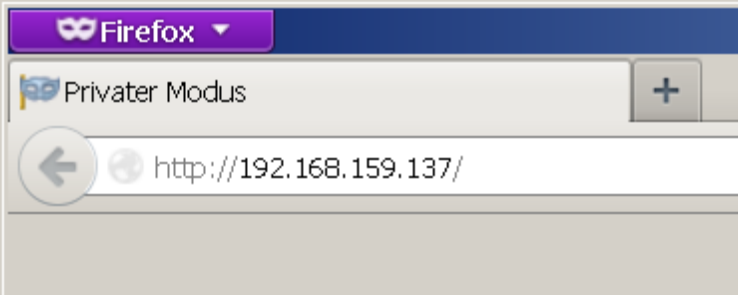
2. Open VMware Workstation or Player and ensure that your "Network Adapter" is set to **Bridged** and "Network Adapter 2" is set to **LAN Segment**. (See Initial Setup if it is not)



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



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.

Known Issues

- pia-daemon needs a 100% success rate to detect the VPN as „up“. This may cause the VPN to be disconnect/reconnect if you max out the upload capacity of your Internet connection without going through the VPN.
  I can only reproduce this by uploading something over an encrypted connection from a PC that is not connected to the VPN. This will be fixed soon by updating the ping function to not only accept 100% success rate.

- PIACommands.php calls “sudo bash –c ‘command’” to start the connection scripts in the background. www-data has “no password” sudo rights for bash. This must be changed soon!

- The WebUI is not password protected yet