M0n0wall and PPTP

January 25, 2006
Version 1.2
Francisco Artes
falcor@netassassin.com
See www.netassassin.com for updates.

Preface: 1
Audience: 1
Assumptions: 2
Subnetting and VLAN routing: 2
Setup of m0n0wall software: 3
PPTP User Setup: 5
PPTP Firewall Rules: 6
Example of filtered PPTP Rules: 9
Setting up a PPTP Client on *Windows XP*™: 11
Testing our PPTP Connection in Windows ™: 14
Some things I have found not to work over the PPTP Connection: 17

Preface:

This document is intended to outline several different PPTP VPN type setups, it includes a how-to on setting up a *Windows XP* ™ PPTO client to connect to the ***m0n0wall*** PPTP VPN server. Later versions of this document will include Linux and other clients.

All Trade Marks ™ are represented in this document, and no intention is made that this document, ***m0n0wall***, or the author are in any way related to any of the companies holding these Trade Marks. All Trade Marks are copy written by their respective companies.

The terms firewall and ***m0n0wall*** are used synonymously in this document. This is mostly because it is easier to say and type "firewall".

Audience:

You need to have a basic understanding of TCP/IP and subnetting to understand this document. The author does make every effort to describe the items being discussed, but let's face it I can only go so far. (And I did include pictures, which apparently are each worth 1,000 words. So that makes this one HUGE document.)

If you have comments, questions, or suggestions in regard to this document please email falcor@netassassin.com. I will try to get back to you as quickly as possible, but please do read this document thoroughly before writing. You may also want to check the ***m0n0wall*** website for email archives on frequently (or even one-time) questions.

Assumptions:

Ok we are going to make several assumptions in this document, if you don't have these assumptions done already you will need to go get them done before PPTP will work correctly.

1.) Your firewall is already setup to do basic NAT and you have tested this, or at least it is doing what ever kind of routing you wanted it to do.
2.) You have configured at least one interface on the firewall so it is working and:
    a. The Client Machine(s) can route to (access) one of the interfaces of your firewall. Make sure of this. If it is an interface that you allow ICMP to access I suggest pinging it.
3.) You have a client machine running some form of VPN client that supports PPTP.

Ok now that we have the basics let's get started on the firewall settings.

Subnetting and VLAN routing:

Ok so this isn't quite true VLAN routing, but we will (quite possibly) be working with a virtual network that doesn't exist until a PPTP connection is made. If you have a better term for this let me know and I will change it. We are however dealing with some virtual subnets, for instance the "Remote Address Range" will be a /28 and PPTP clients will receive a subnet of 255.255.255.255 (ff.ff.ff.ff for all you HEX people out there.) Just ignore that and trust in the magic of the PPTP Tunnel.

You can select (as you will see later) to set the "Sever Address" and "Remote Address Range" to exist inside of the subnet that you defined for the LAN on the firewall. (e.g. Ip Address and subnet bit you set for the LAN under Interfaces → LAN on the ***m0n0wall*** menu.) Our example uses this setup. Pros and Cons? Well the major pro is that the firewall will allow traffic from this VLAN to route to the WAN (in most cases the Internet.) and it is nice and easy. Con's, it allows people to rout to the WAN if you don't want this then read the next paragraph.

You can also setup these two options to have an IP range that is outside of your LAN designation. E.g. LAN = 192.168.1.1/24 (really the 192.168.1.0/24 network) and the PPTP "Server Address" and "Remote Address Range" are set to 192.168.2.254 and 192.168.2.16/28 respectively. This will basically allow those using the PPTP connection

to access the LAN, but the firewall will not route traffic for them to the WAN connection. Opt and WiFi networks will also be isolated depending on how you are routing to those networks and if they are in the same network segment (subnet) as the LAN.

Remember, that when you setup a PPTP connection (especially on *Windows*) all network traffic from that workstation is going to be sent via the PPTP tunnel.

Setup of m0n0wall software:

Most people probably skipped right to this point. If you did, it should be easy enough with these examples if you do run into something go read the parts you skipped you may find the answers there you are looking for.

1.) The first thing we want to do is setup the PPTP server. To do this select PPTP from the VPN section of the ***m0n0wall*** interface. If you clicked the right thing you will have a screen that looks something like **Figure 1**.

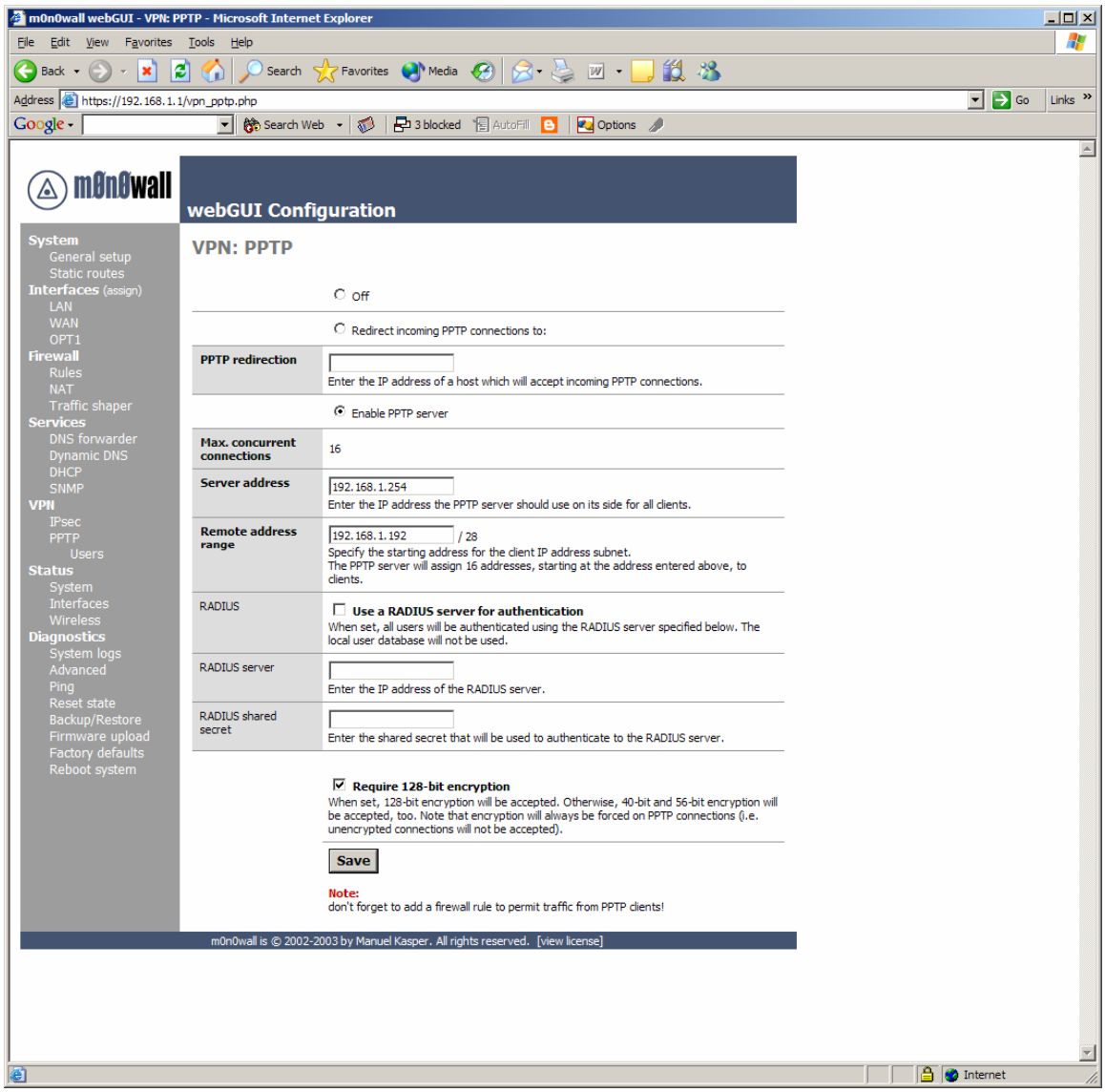


Figure 1

2.) The next step is to enable the PPTP server. Click the "Enable PPTP server" radio button. (It only gets harder from here.)

3.) Now we have to type. (see harder) So enter the "Server Address" next. This can be an unused IP on your LAN, or another locally usable IP address in a separate subnet. It MUST be in the same networking class as the next entry. (NOTE: "Server Address" is really the default route for clients and thus the internal portion of the PPTP network, it is not the IP address you will tell the client to connect to.)

4.) Remote Address range. This is going to be the range of 16 IP addresses that the server will issue to clients. Notice the /28, it is there to remind you there will be 16 hosts. Again, this MUST be in the same subnet class as the IP listed above. (Not in the same /28 though…. If you try to overlap the two the firewall will tell you that you made a mistake.)

In our example we used 192.168.1.254 for the "Server Address" and 192.168.1.192/28 as the "Remote address range." Think of the "Sever Address" as the default route for the IPs you are going to be issuing to the clients. It is also the virtual interface for the PPTP server.

If you are confused here, or in step 3, please go back and read the section named "Subnetting and VLAN routing" as it covered this in more detail.

5.) If you have a RADIUS server of some sort feel free to fill in the next few boxes. I don't so they are blank on this example and frankly go outside of the scope of this document anyway.
6.) If you are really security conscious, and your client software supports it, check the box to require 128-bit encryption.
7.) Click "Save" We are all done setting up the server. Now let's setup some users.

PPTP User Setup:

If you have a RADIUS server and you set it up in the previous section you can either choose to skip this one, or add users here that will be found and used before the PPTP Server sends a request to the RADIUS server.

For the rest of us, this stage is quite important as we need a user account to authenticate to the PPTP Server.

1.) Click on "users" under PPTP in the VPN section of the ***m0n0wall*** interface.
2.) Click the "+" icon and lets fill in some blanks!
3.) Enter a name in the "Username" box.
4.) Enter and then re-enter the password for this account. (You can't use special characters at the time of this document, just FYI.)
5.) Click "Save"
6.) When you get back to the next window you will need to click "Apply Settings" NOTE: This will disconnect any active PPTP connections. Being as we are just setting this up for the first time, and this is our first user, let's hope there aren't any to disconnect.
7.) If everything went well you should have a screen that looks something like **Figure 2**.

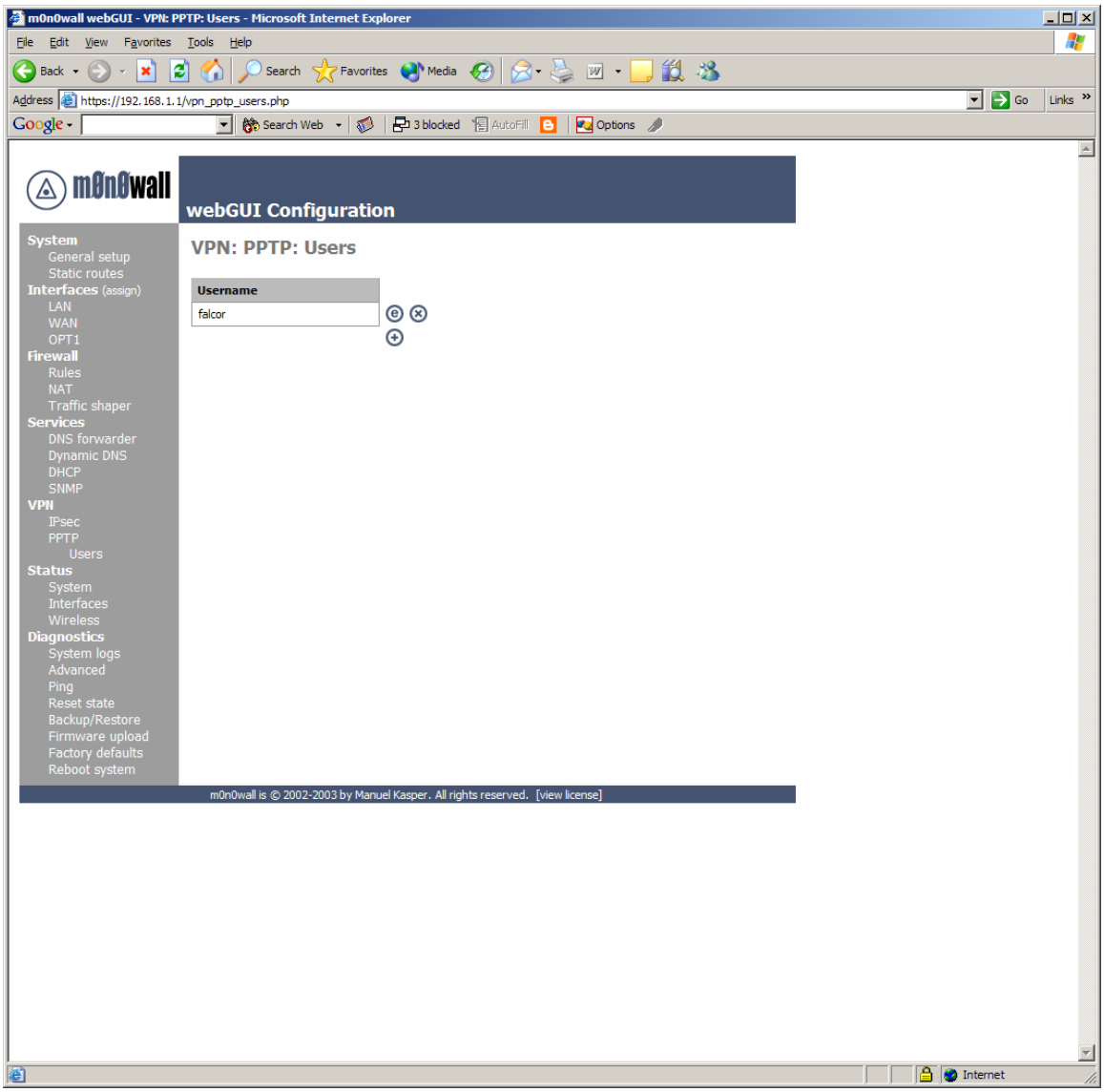


Figure 2

Now we need to setup a firewall rule so people using the PPTP connection can do something with it when they connect.

PPTP Firewall Rules:

Yep you need to do this if you want the darn thing to work. But just like your LAN rule, you can make this as open or as restrictive as you want. Here you can limit the PPTP users to accessing only specific hosts on specific ports, or open it all up. We are going to

assume you want full access for your PPTP users so we are going to setup a firewall rule that is exactly like the default LAN rule.

1.) Start by clicking “Rules” under the firewall section of the ***m0n0wall*** interface.
2.) Next click any of the “+” Icons on the screen so we can add a new rule.

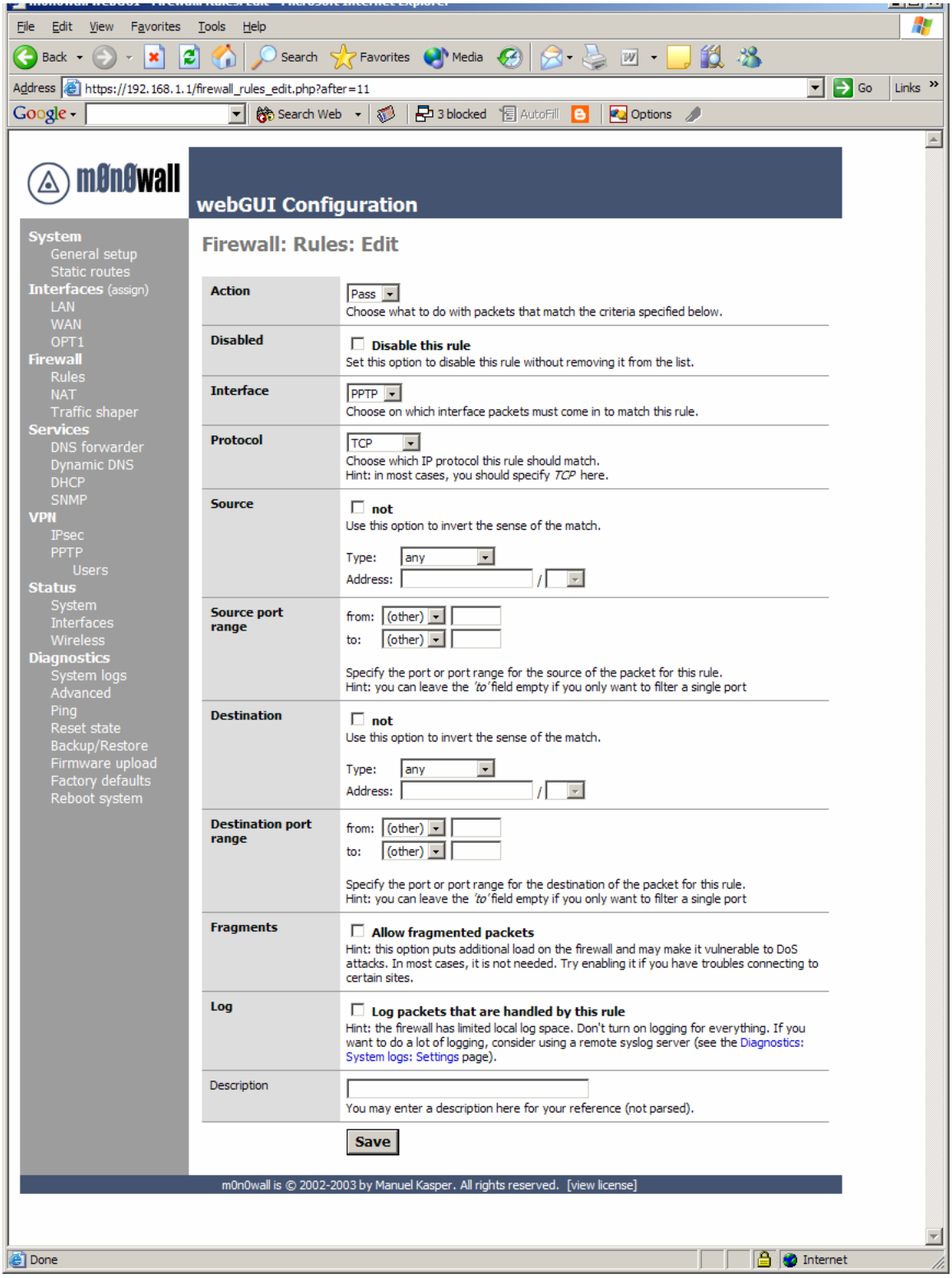


Figure 3

As stated we are going to allow all our PPTP users to access all parts of the LAN, WAN, etc. If you wish to limit this access then you will need to modify things accordingly. I will present one example of such a rule after this default section.

3.) Simply go to the “Interface” section and select PPTP from the drop down. In the Description put something meaningful like “Default PPTP -> any.”
4.) Click Save
5.) You will have to Apply the changes on the next screen.

You are now done setting up the PPTP Server!

Example of filtered PPTP Rules:

In some cases, most for those people who are granting PPTP access to others they do not fully trust, you will want to limit access (Specific Allow Rules) or mitigate specific access with Deny Rules. With specific allow users would be granted explicit permission to access hosts, and sometimes specific ports, and all other traffic is denied. The latter would be done if you wanted the PPTP clients to access the LAN & WAN but did not want them to access your SAMBA server for instance.

Our example is an allow rule granting permission for people on the PPTP network to use SSH on a LAN server with the IP address 192.168.1.151:

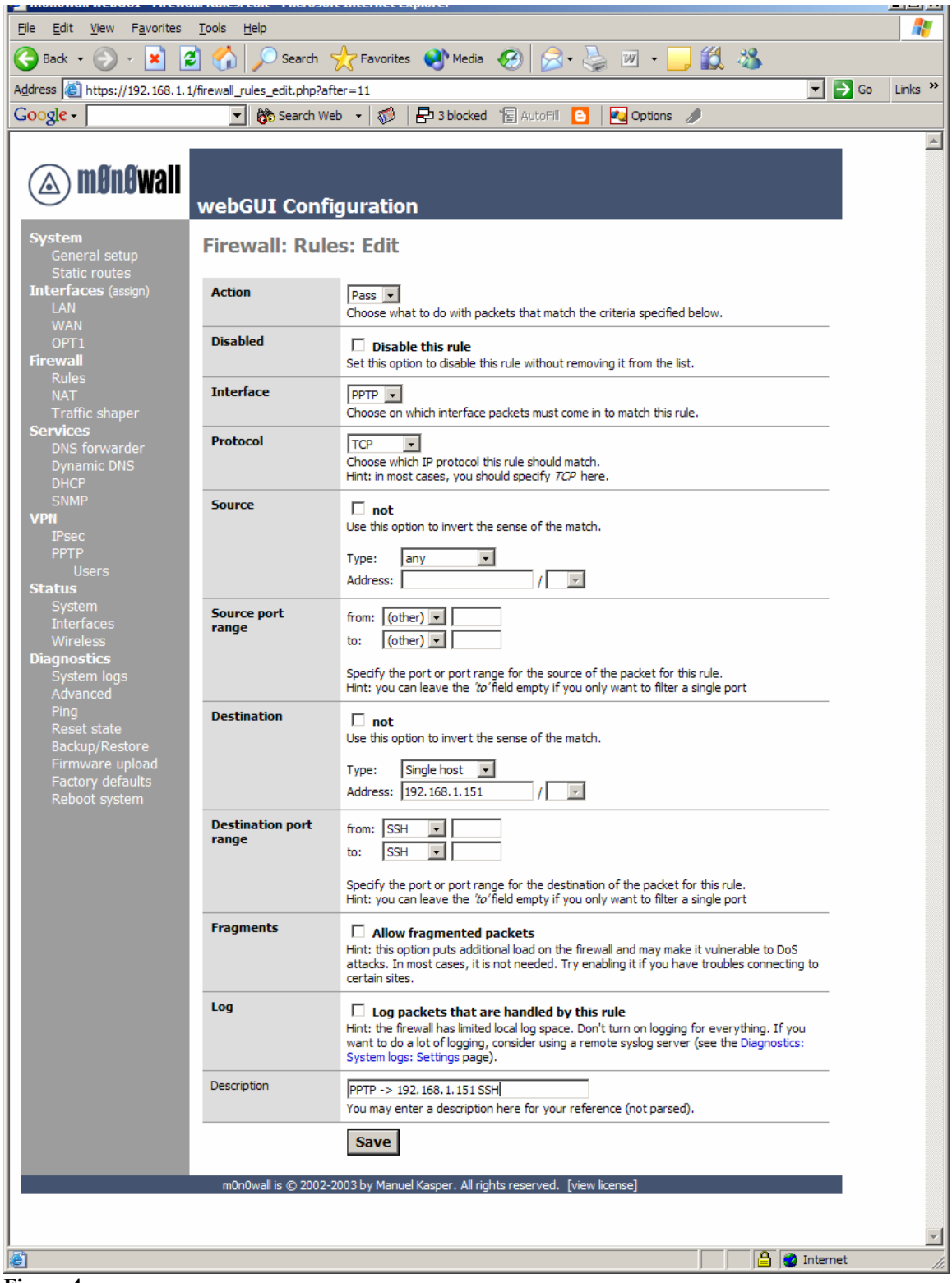


Figure 4

Save and Apply these rules as needed. Test them all to make sure they are working as designed. Most networks are compromised because no one checked the ACLs were activated or even working properly.

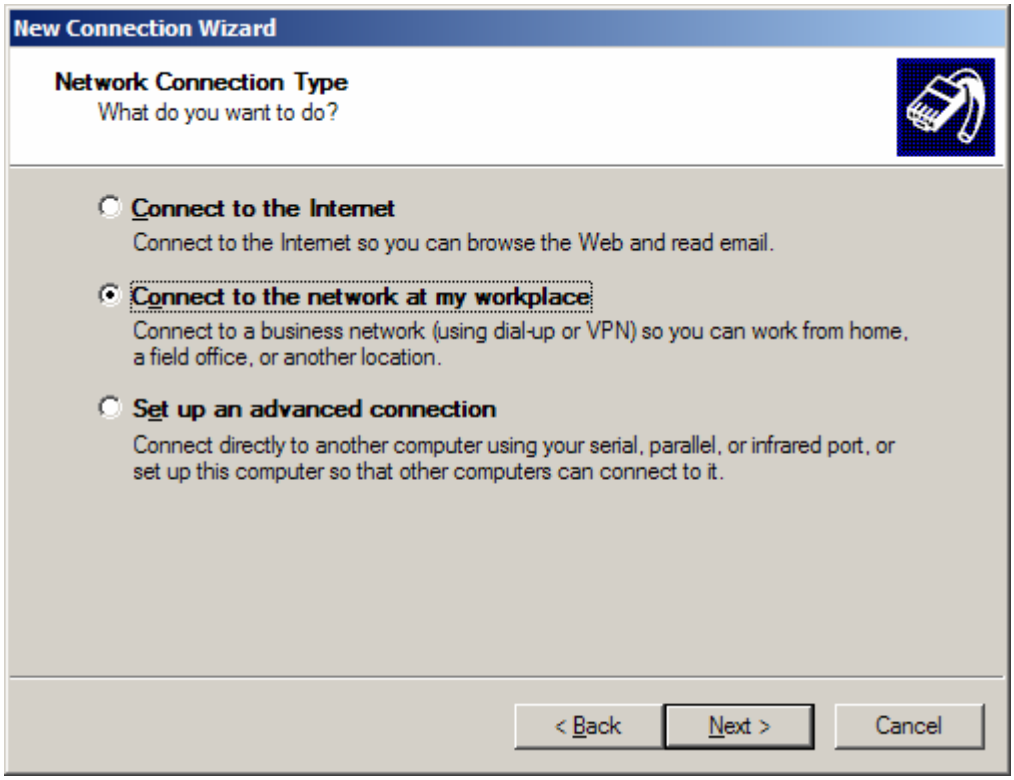
Setting up a PPTP Client on *Windows XP*™:

This is super easy, and you only have to type one piece of information the entire time!

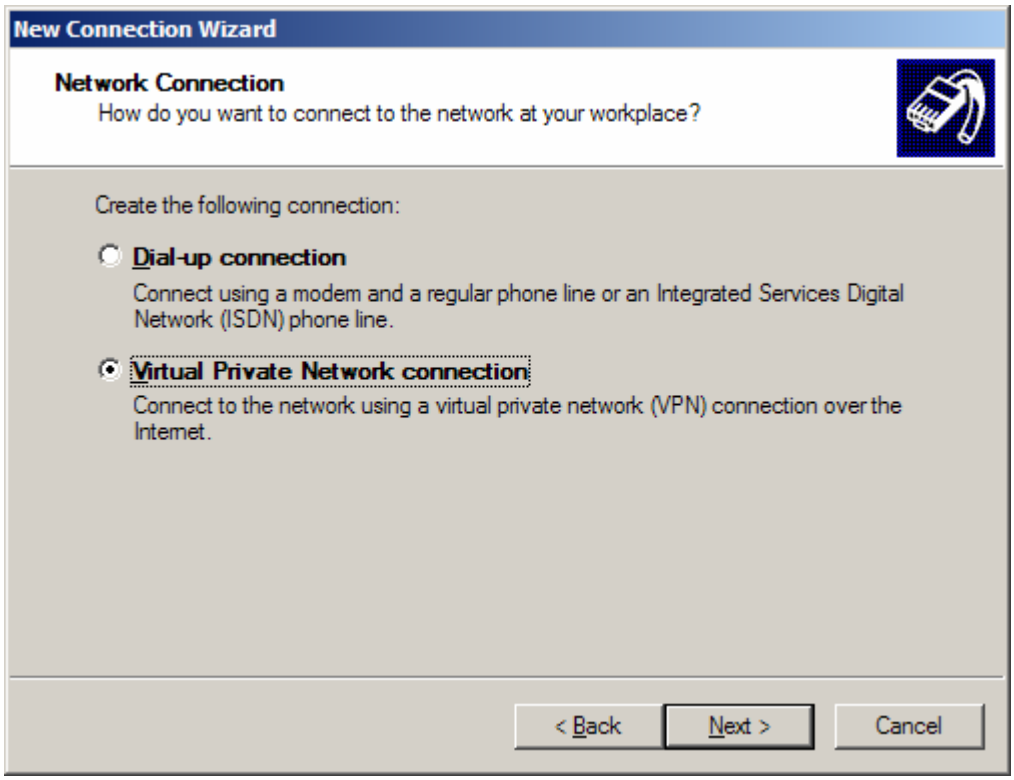
Start by accessing the Network Connections Panel. (do this however you like, I prefer to right click "Network Places" and select Properties.)

1.) Click "Create New Connection" in the left hand column of the "Network Connections" window.
2.) You are now presented with a Wizard. Click Next to continue.

3.) Select "Connect to the Network at my Workplace" from the menu.

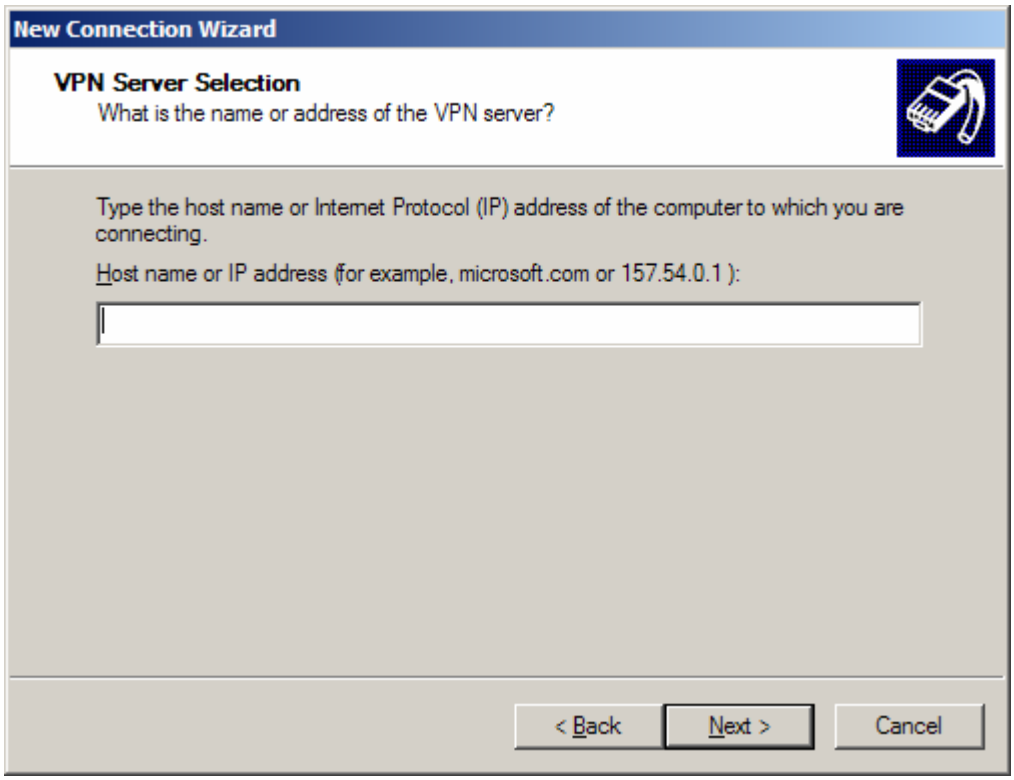


4.) Select Virtual Private Network connection from the next panel.



5.) Name the connection.

6.) Now enter the IP or FQDN of the PPTP Server. (This can be any of the configured interfaces, even the LAN from the LAN.)



7.) If you are the system admin you will be asked if you want this to be for your use only or for anyone's use. I suggest you limit it to your use only unless you want the VPN network to be made available to all user accounts on the workstation.
8.) Next you can either just finish or add a shortcut to the desktop. You are nearly done!
9.) When you launch the client for the first time (hopefully from the icon you asked it to create from the wizard, if not then you will need to access the "Network Connections" window again and double click your new connection.) you will be asked for a username and password. Click connect when you are done with this and if all goes well you will connect to the PPTP Server.

Testing our PPTP Connection in Windows ™:

1.) Start by opening a DOS window. (Command window)
2.) Run ipconfig and you should get something similar to the next figure:

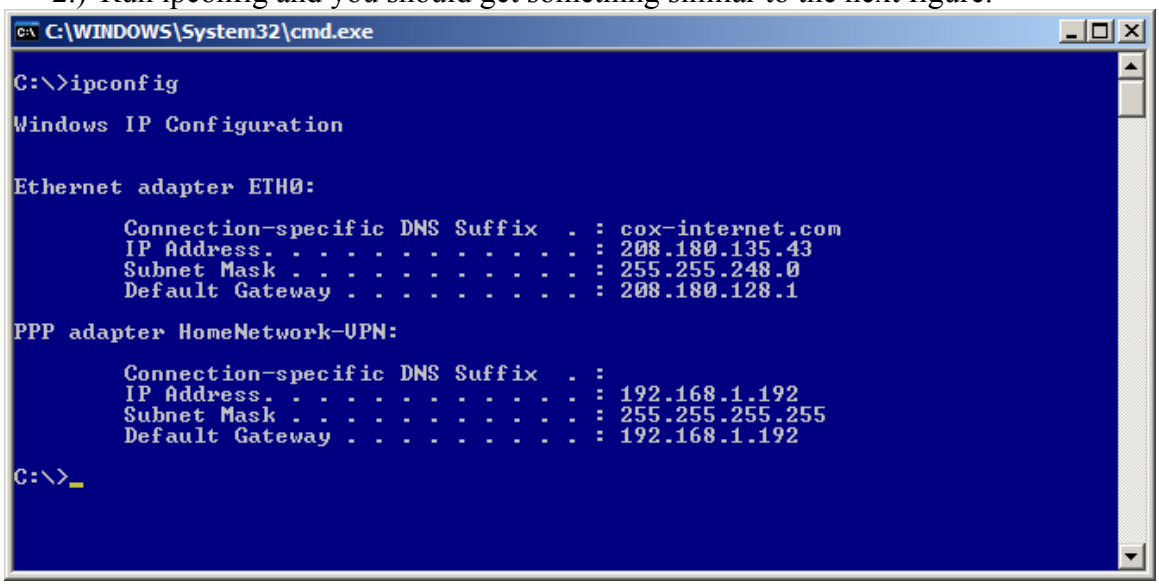


Figure 5

As you hopefully will see you have the settings for your physical adapter (in my case I renamed it to ETH0)
You will also see the PPP Adapter with the name you gave the VPN Connection when performing the steps in the last section. It should have an IP address that is in the range you defined for the PPTP Server. It should also have the subnet of 255.255.255.255 and it will be using itself as the default gateway. Just live with it; it is how it works.

For the more advanced who wish to know if things are all working right, **Figure 6**, displays a full ipconfig on the virtual adapter.

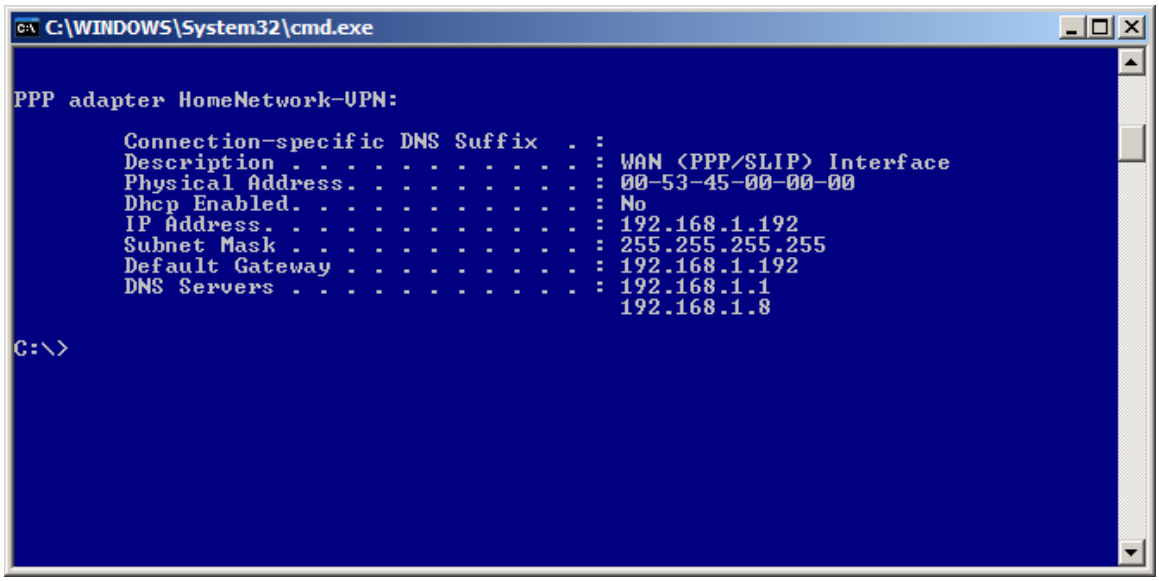


Figure 6

3.) Now lets try doing something. If you followed the setup for this how-to you will have setup full access from the PPTP network to the LAN and WAN. If you setup selective rules you will have to test specifically what you setup. E.g. if you setup rules to only allow SMTP you will need to telnet to the host:25 that you designated in the firewall rule. Or write a new rule allowing ICMP to a host that will echo a reply back.

    We will be sending a ICMP (Ping) to the firewall's internal interface to test the VPN connection.

4.) In my case the firewall is 192.168.1.1 (please use your internal address before writing to me to say pinging 192.168.1.1 didn't work on your 10.x.x.x network. Hehe) If done right (assuming your firewall isn't blocking internal ICMP packets) you are good for LAN access. (If you are blocking ICMP on the internal interface ping some other host on your home network.)

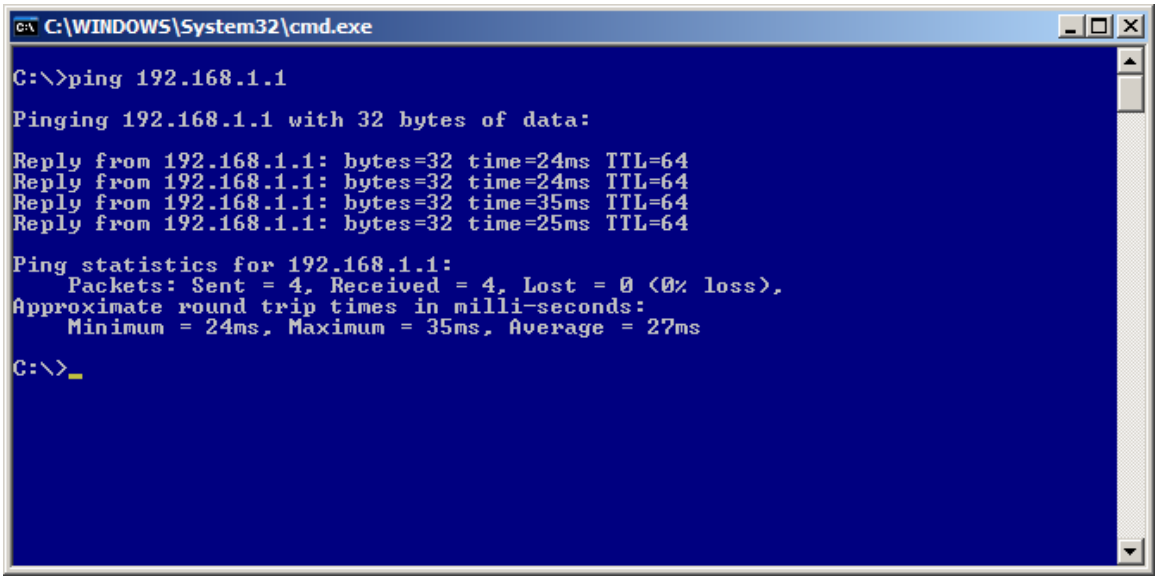


Figure 7

5.) Now lets test beyond the firewall. Ping isn't so good to use here as more and more people are blocking ICMP packets. So we will use tracert to check we are 1.) Routing via the PPTP tunnel and 2.) That we successful. Of course if you told the firewall to not allow WAN access then this step can be skipped.

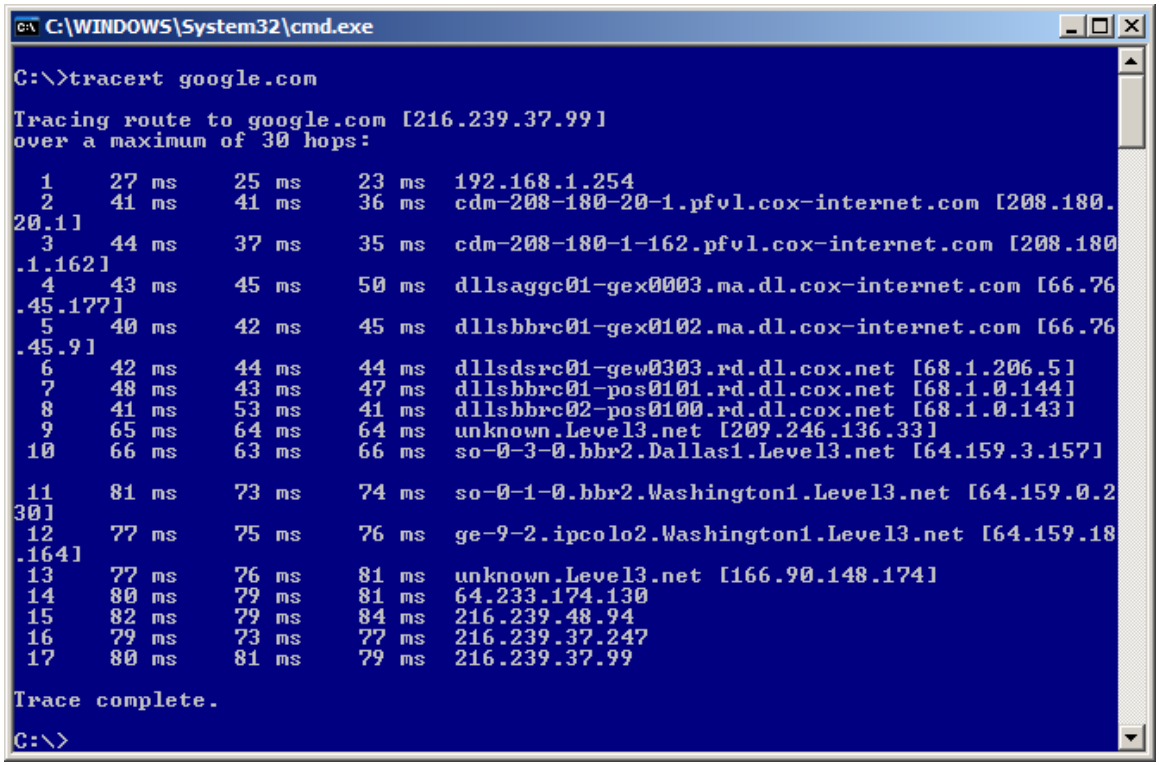


Figure 8

As seen in the last figure, the first hop is the PPTP "Server Address" as this is the gateway/interface for the PPTP Network.

Now check things like HTTP, etc. If you have this much and followed the directions you should be able to do everything.

Some things I have found not to work over the PPTP Connection:

These are more limits of PPTP then anything else.

- NAT sometimes does not play nice with PPTP. The m0n0wall seems to have this licked, and it works rather well.
- UPnP packets from your LAN do not make it to the PPTP network. This is more then likely because the current version of m0n0wall does not support UPnP. (In English: those of use having dreams of accessing our ReplayTV ™ or other media devices that use UPnP can dream of other things for now. It is actually more secure to not have UPnP on a firewall, but some people overlook that so they can use voice chat software and DVRs.)
- Major "Gotcha!" If you are visiting a remote network where the network range is the same as the network range on the PPTP Network (your LAN network in most cases) then the PPTP tunnel will not work. E.g. You are using a WiFi connection in a local coffee shop and the network range it has put you in is 192.168.1.0/24. You try to connect to your home network via PPTP, but your home also uses 192.168.1.0/24. The tunnel/authentication to the PPTP server will happen, but no traffic will go across that tunnel due to the "confusion" in the TCP/IP stack on your workstation. To get around this use some odd network range at home. E.x. 192.168.88.0/24. Most people use 10.0.0.1 and 192.168.1.0 so try to set your home network differently. This will also help when you setup IPSEC tunnels between your house and say your friend's house.
- Don't make the WAN network and the LAN or worse yet the PPTP network the same network range. I know most people would realize this, but I have receive a lot of email from people wanting to know why things don't work and the WAN and PPTP network are the same network range.

I haven't really beaten the PPTP tunnel that much yet, so if you find more items that don't seem to work right let me know and I will add them here so people don't go crazy trying to figure out something that just won't work. ;)