M0n0wall and IPSEC

March 20, 2004
Version 1.1
Francisco Artes
falcor@netassassin.com

Preface: 2
Audience: 2
Assumptions: 2
Subnetting and VLAN routing: 3
VPN tunnels between two IPSEC VPN concentrators: 4
Required Firewall Rules for all VPN tunnels: 9
What if your m0n0wall isn't the main Internet Firewall? 11
Glossary: 12
AH 12
ESP 12
FreeS/WAN 12
IPsec 12

Preface:

This document is intended to give a basic how-to on setting up IPSEC tunnels between the m0n0wall software and other IPSEC compliant VPN devices. We will also cover using roaming IPSEC clients, this is an option and most people prefer it over PPTP tunnels for client to server VPN.

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 IPSEC 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. (Do remember that the WAN interface does not allow ICMP {ping})
3.) You will need to either control or be in contact with the person who does control the other VPN concentrator. If it is another m0n0wall system then share this doc with them, if it isn't then please have them consult the documentation that came with the VPN concentrator they are using.

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

Subnetting and VLAN routing:

Basic networking when you are building a WAN (Wide Area Network.)

1.) If any of the networks you are connecting use the same internal IP range, routing will not work. This includes segments of the other networks.
    a. Make sure your LAN and the LAN you are connecting to are not using the same subnet / network range. Examples of okay combinations: 10.0.0.0/8 and 192.168.100.0/24. 192.168.100.0/24 and 192.168.1.0/24. Examples of bad network ranges: 192.168.100.0/24 and 192.168.100.0/16
    b. Keep in mind the more networks you link together the more important this basic fact becomes. If you have a LAN that you connect to that is 10.0.0.0/8 and another that is 10.254.254.0/24 then the VPN router will send data to the appropriate network as defined. But if the 10.0.0.0/8 network contains a 10.254.254.0/24 network you will not be able to access it as long as there is an IPSEC tunnel specifically pointed at another network using that same subnet.
2.) Application/server level security is going to be a must use item now. With a home LAN you probably don't care who can access your SAMBA server (for example) since it only speaks to your LAN. The IPSEC VPN tunnel will not respond to firewall rules, at the time of this document, so you will not be able to limit what hosts can be accessed from the new connection via the firewall. Thus you will need to pay attention to how your servers are setup.
3.) Pay attention to what you are doing. If you have a VPN to your office, and a VPN to your friend's home network, your friend can now access your company's network. Normally, most companies would fire you if your friend was caught on their network. Best bet here is to use multiple m0n0wall firewalls and use different subnets with local routing / VLAN security.

VPN tunnels between two IPSEC VPN concentrators:

Ok so you have decided you want to build an IPSEC tunnel between your firewall and some other network. This is super cool, if you ask me, and the most common use would probably be connecting your home network to your office, or setting up a private WAN with several of your friends.

There is only one section of the m0n0wall interface that you need to use to do this, ahh see that is the trick. Most people seem to get confused and start setting up Pre-shared keys and Mobile client information and well, that is not needed for this "basic" type of VPN tunnel.

From the main menu click "IPsec" under the "VPN" section of the menu. You will be presented with a page similar to this one:

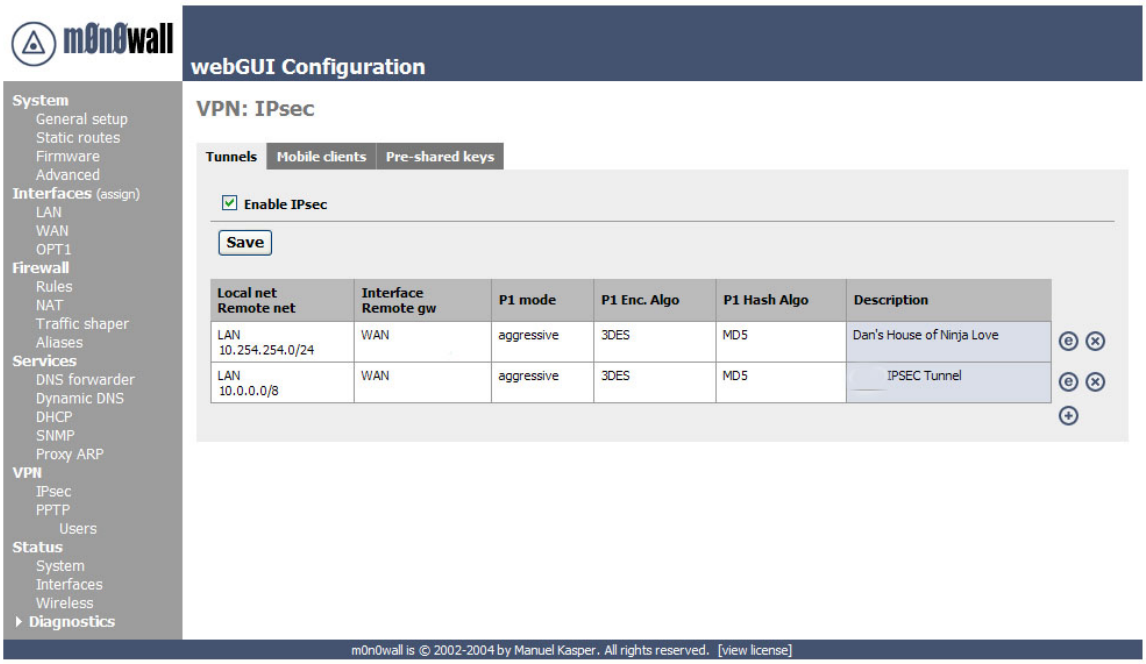


Figure 1 IPSEC server to server

Note: Your screen will probably be blank, I didn't feel much like deleting my configurations or killing my tunnels while writing this so you get to see something of a completed screen. I have erased the remote gw to protect those people's identity. Hehe.

Ok now we need to add a VPN connection, to do this click on the ⊕ icon.

You will be presented with a great form, I will be pasting screen shots of each section as we discuss it.

The first area is the one you use to establish what network ranges will use this IPSEC tunnel.

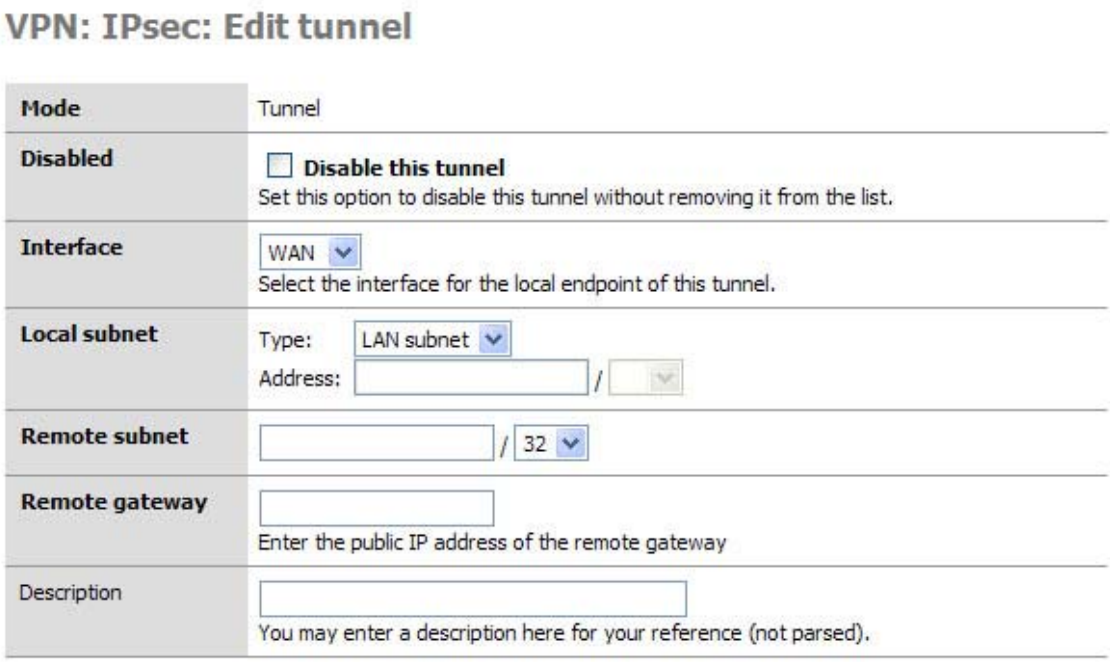


Figure 2 first VPN filed

This is the first set of fields that we need to concentrate on. Later, when testing your tunnel, you can actually fail to establish level 2 connection if this data is incorrect. I will note what to pay particular attention to as we go along.

1.) Mode, this is a hard set option and frankly you don't need to change it (nor can you.)
2.) Disabled, this is a great "on / off" button if you need to disable the tunnel for what ever reason. Simply select the edit or ✎ from the main VPN: IPsec window and click this checkbox element, then select apply at the bottom of the page. When you need the tunnel again, reverse the process.
3.) Interface, this is how you determine which part of your network will be the termination point (end point) for the VPN Tunnel. If you are connecting to a remote server, then WAN is your option.

4.) Local subnet. This is where you can set which parts, hosts, or the entire LAN can be accessed from the other side of the VPN tunnel. The easiest thing to do is to set the LAN subnet as the option; this means your entire LAN will be accessible from the remote network. IMPORTANT: The other end of the tunnel has this same field, well it probably has 99% of these fields actually, make sure the other end is set exactly as you set this end. E.g. if you said "Single host" in this section and entered the IP address of that host, the other person would set that host in his "Remote Subnet" field. The same goes for you, and with that mentioned we move to the next field.
5.) Remote Subnet. This is more then just labeling which hosts and / or host you want to access on the other network, as mentioned in item 4 it is paramount that you set this exactly like the other end's "local subnet" section. If not, level 2 of the VPN connection will fail and traffic will not pass from one VPN segment to the other.
6.) Description: It is a good practice to always leave notes about why you are doing something. I suggest you enter something about what this VPN tunnel is used for, or about the remote end of the tunnel to remind yourself who/what it is.

Ok all the basic for the routing have been established. Now we move on to phase 1 of the VPN authentication process.

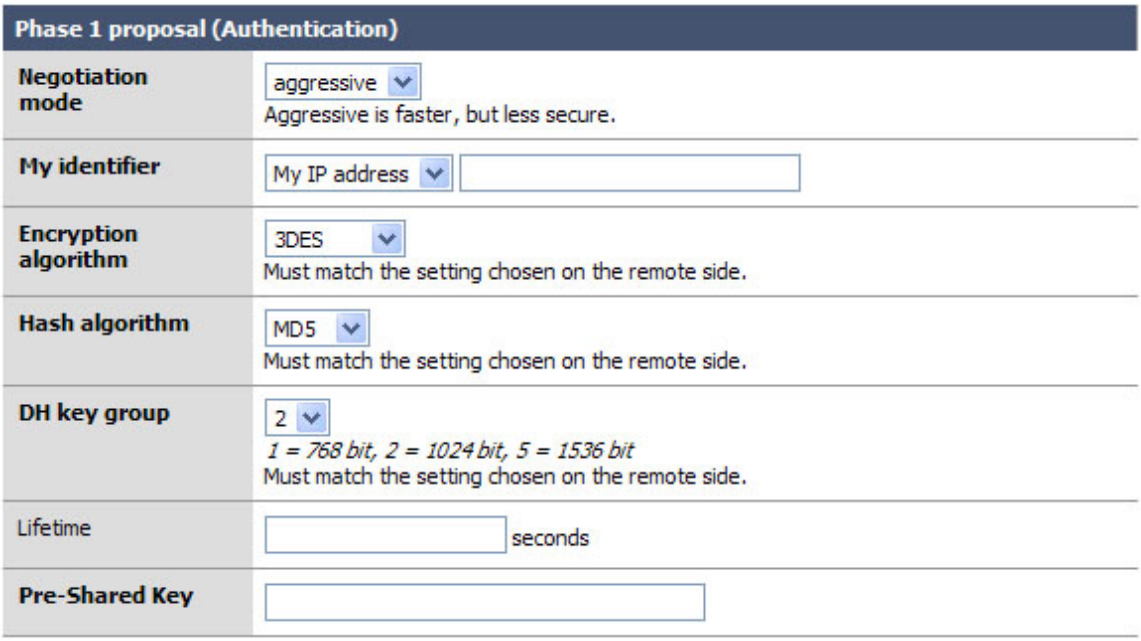


Figure 3 phase 1 of the VPN tunnel

Okay the easy part of the VPN tunnel. The trick here, and even in phase 2, is to make sure that both VPN servers have EXACTLY THE SAME SETTINGS for all of these fields. Well okay, they will have different "My identifier" but make darn sure that they know each others names… more on that later.

1.) Negotiation mode: This is the type of authentication security that will be used. Unless you are under close watch by someone with paranormal like crazyness, just leave this as aggressive. It is indeed far faster and will insure that your VPN tunnel will rebuild itself quickly and probably won't time out an application if the tunnel was down when the resource on the other end was requested. (more about that under Lifetime)
2.) My identifier: This is the key to probably 90% of the email on the list where people seem to not get the VPN tunnel up, or want to know how to do this with dynamic IP addresses, etc. Very simple, set your identifier to something that isn't going to change. So if you leave it as My IP address (* This will be the ip address of the "interface" you listed in the first section. *) then make sure that IP is static and persistent. If you use a DHCP assigned address then I would suggest using domain name instead This is because domain name can be completely your own even if you do not own the domain name. Make yours sexylovemonkey.com just for fun. ;)
3.) Encryption Algorithm: 3DES is the world de facto… if you are connecting to another m0n0wall, or a system that will support it, change this to Blowfish. It is a more secure and about twice as fast! Now of course, if you are trying to connect to a VPN device that only supports DES then you will need to downgrade and hope no one decrypts your key exchange. MAKE SURE BOTH VPN DEVICES ARE USING THE SAME ENCRYPTION ALGORITHM.
4.) Hash Algorithm: this is the hash used for checksum. MD5 is a good choice, SHA1 is the new up and comer and it is more reliable then MD5, but not all things support it. Again make sure you are using the same setting as the other end of the tunnel, and if you can use SHA1 go for it!
5.) DH Key Group: Most systems will support at least up to 1024 bit. This is a good place to stick to, going with more will eat up more resources and less makes your tunnel less-secure.
6.) Lifetime: This field is far more important then it appears. This lifetime, as apposed to the one in phase 2, is how long your end will wait for phase 1 to be completed. I suggest using 28800 in this field.
7.) Pre-Shared Key: Contrary to some suggestions this key must be exactly the same on both VPN routers. It is case sensitive, and it does support special characters. I suggest using both. E.x. f00m0nk3y@BubbaLand

Okay if you managed to coordinate and get both VPN systems set the same all should be good for phase 1. We really don't want to stop here, so let's go right into phase 2.

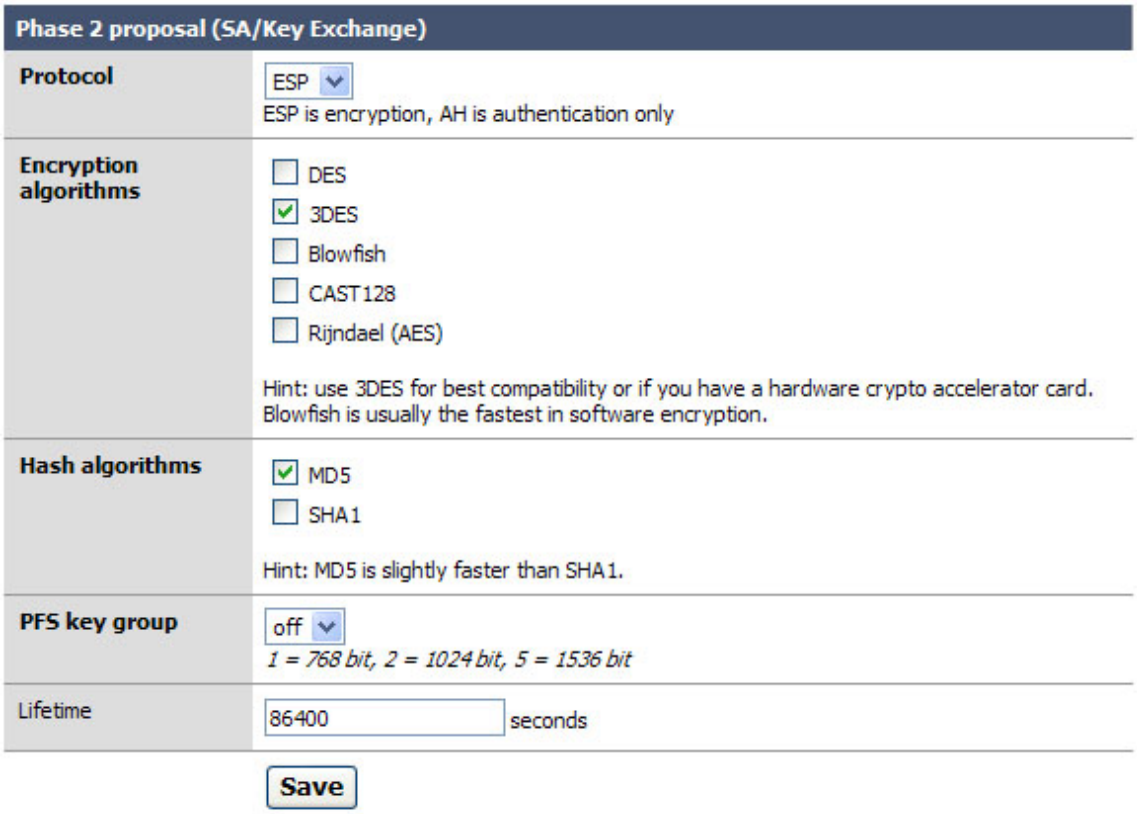


Figure 4 Phase 2 of VPN

Phase 2 is what builds the actual tunnel, sets the protocol to use, and sets the length of time to keep the tunnel up when there is no traffic on it.

1.) Protocol: ESP is the de facto on what most VPN systems use as a transport protocol. I suggest leaving this as is. Note: The system should auto generate a firewall rule for you to allow ESP or AH to the endpoint of the VPN. We will check this later, if it does not you will need to make a firewall rule allowing ESP (or AH if you changed this) traffic to the interface you established as your end point of the tunnel. I will outline that after figure 5.
2.) Encryption algorithms: Ok here is the deal on this. Like before in phase 1, make sure you are setting the algorithm exactly as it is set on the other VPN server. You can use several; when you do so everything you select is available for use. Honestly I like to keep things simple so I recommend only checking the one you are going to use. With m0n0wall to m0n0wall use Blowfish for speed and security over 3DES.
3.) Hash algorithms: again just as in phase 1 you want to make sure your selected hash matches the one on the other end. And like in step 2, don't add things you don't need. SHA1 is the suggestion if you can, but MD5 is always a good alternative.
4.) PFS key group: this works exactly like it does in phase 1. I suggest using 1024 bit, the default is off.

5.) Lifetime: This is the lifetime the negotiated keys will be valid for. Do not set this to too high of a number. E.g. more then about a day (86400) as doing so will give people more time to crack your key. Don't be over paranoid either; there is no need to set this to 20 minutes or something like that. Honestly, one day is probably good.
6.) Click Save
7.) Click Apply Changes

Required Firewall Rules for all VPN tunnels:

Okay the VPN session will now try to establish itself. This should have been done for you, but in testing I have found that it does not always seem to work, well at least for me. So we are going to outline two things in this chapter. One, how to check to see if the firewall rule to allow the VPN was created or not. Two, how to build the rule yourself if there was a problem with the auto rule generator.

We need to make sure the VPN server that we are trying to connect to can establish a connection to us. This means we need to write a rule!

1.) Under Firewall: click Rules
2.) Select the ⊕ icon for the interface you want to use as your VPN end point. (In most cases this is the WAN interface)

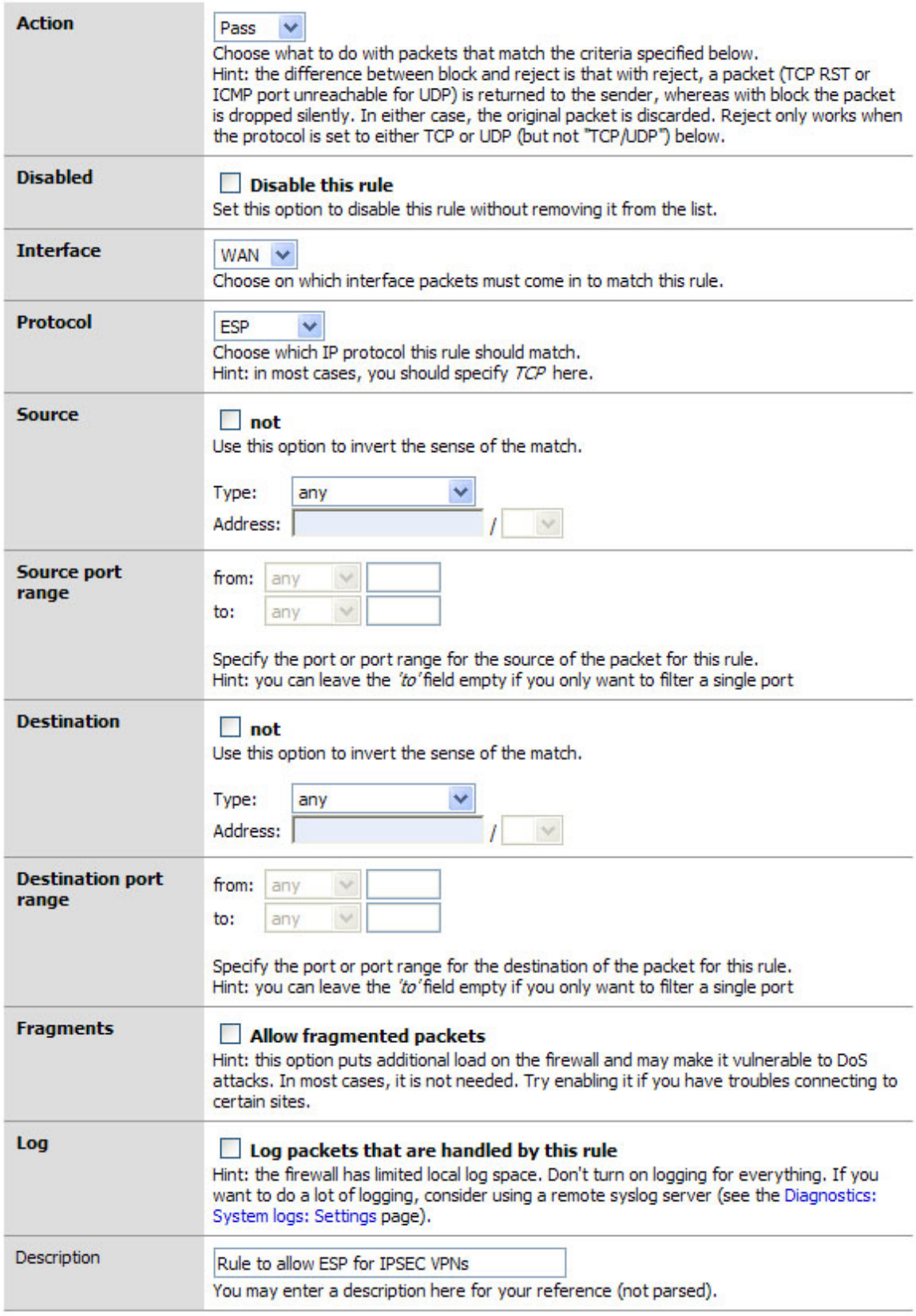


Figure 5 Setting the firewall rule to allow VPN traffic

You will notice this example rule allows ESP connections from any host. This is useful if you are going to use roaming clients to connect to the IPsec VPN, or if you are lazy and don't intend to make a separate firewall rule for every VPN tunnel you build. (I suggest you specify the source and make specific rules for each VPN point-to-point connection you make if you are not using roaming.)

Very quickly: E.g. I am only going to discuss the items you need to do something with.

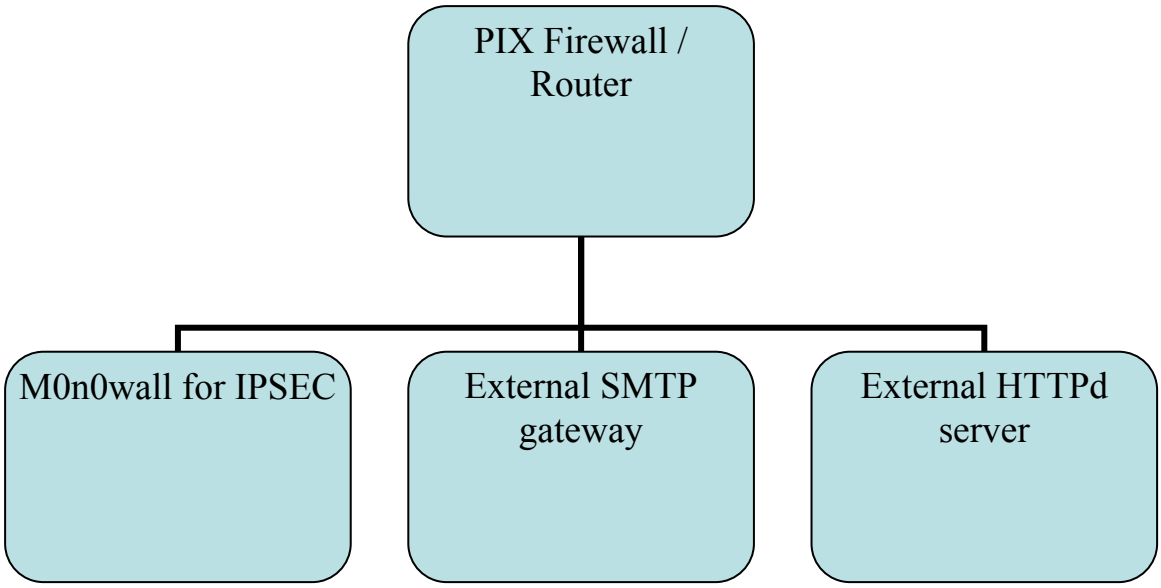
1.) Action, pass unless you want to torture yourself or quickly stop a particular VPN tunnel.
2.) Interface: This needs to be the interface you are using as your end-point of the VPN tunnel. Generally your WAN.
3.) Protocol: For VPN this is normally ESP, some use AH.
4.) Source: Unless you are using roaming clients on this VPN server, specify the static IP of the other end of your VPN tunnel. Create a new rule and repeat this process for every VPN tunnel you build.
5.) Destination: Feel free to leave this as any, makes no difference.
6.) Description: Put something meaningful here please. You will note I put Rule to allow ESP for IPSEC VPNs.
7.) Click Save
8.) Click Apply Changes

Your VPN tunnel should now be working.

What if your m0n0wall isn't the main Internet Firewall?

In some cases you have a firewall or router with layer 2 routing (protocol ACLs) sitting in front of your m0n0wall. If this is the case you will need to port forward ESP or AH (depending on which one you chose) to the m0n0wall. (NOTE: if you are running NAT on that firewall AH will not be an option.)

Example:



Glossary:

AH: Authentication Header Protocol. The Authentication Header is used to provide connectionless integrity and data origin authentication for IP datagrams. Note: AH will not work through NAT, so if you are placing your m0n0wall behind another firewall or layer 2 router that is performing NAT AH will not work. Unless you really have a reason, use ESP.
http://www.networksorcery.com/enp/protocol/ah.htm

ESP: Encapsulating Security Payload. Encrypts and / or authenticates everything above the IPsec layer. ESP, most agree, renders AH completely unnecessary. Best source for ESP information is found at this website:
http://www.networksorcery.com/enp/protocol/esp.htm

FreeS/WAN The magic behind the VPN power of m0n0wall.
http://www.freeswan.org/

IPsec

IPsec is an extension of the IP protocol used for encryption. Encryption occurs at the transport layer of the OSI model, the application doesn't have to support encryption for

the encryption process to work. Therefore, all network traffic generated by applications can be encrypted regardless of the application
http://www.netbsd.org/Documentation/network/ipsec/