IPSecuritas 3.x

Configuration Instructions

for

WatchGuard Firebox

June 17, 2009

Legal Disclaimer

Contents
Lobotomo Software (subsequently called "Author") reserves the right not to be responsible for the topicality, correctness, completeness or quality of the information provided. Liability claims regarding damage caused by the use of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected. All offers are not-binding and without obligation. Parts of the document or the complete publication including all offers and information might be extended, changed or partly or completely deleted by the author without separate announcement.

Referrals
The author is not responsible for any contents referred to or any links to pages of the World Wide Web in this document. If any damage occurs by the use of information presented there, only the author of the respective documents or pages might be liable, not the one who has referred or linked to these documents or pages.

Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic or printed publications is not permitted without the author's agreement.

Legal force of this disclaimer
This disclaimer is to be regarded as part of this document. If sections or individual formulations of this text are not legal or correct, the content or validity of the other parts remain uninfluenced by this fact.

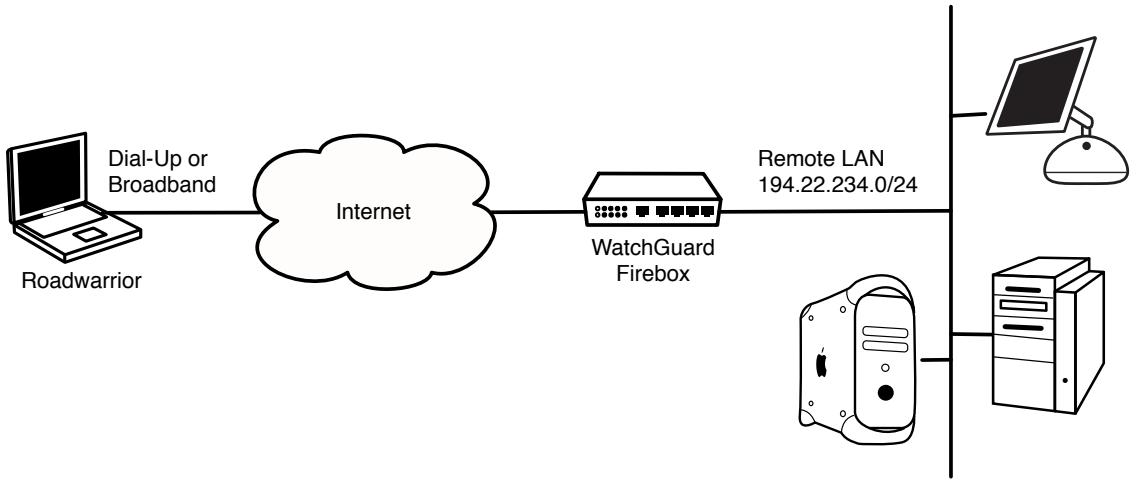
Acknowledgments

Many thanks to Konrad Schnetzler for providing setup information, screenshots and support for writing this document.

Table of contents

Introduction

This document describes the steps necessary to establish a protected VPN connection between a Mac client and a WatchGuard Firebox router/firewall. All information in this document is based on the following assumed network.

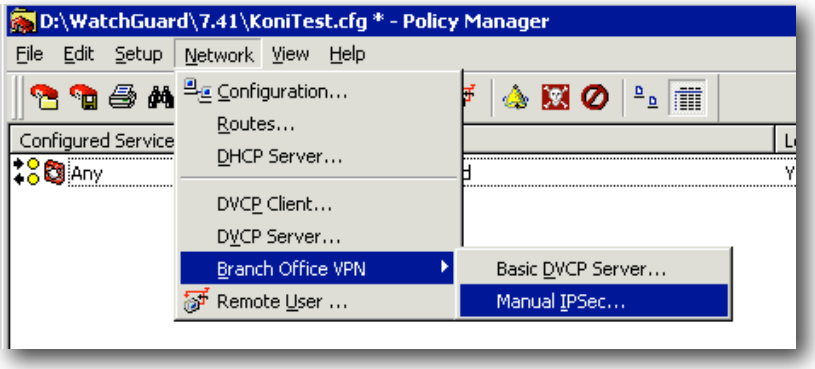


WatchGuard Firebox VPN Setup

This section describes the necessary steps to setup the WatchGuard Firebox to accept incoming connections.

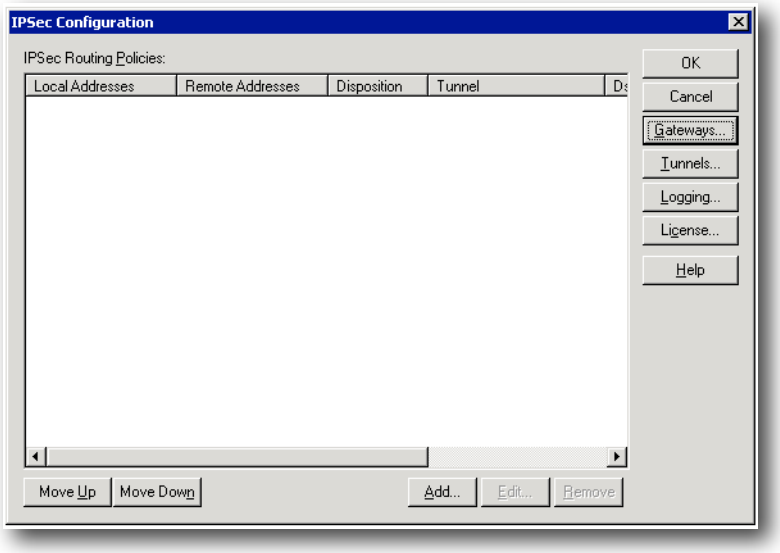
Create New IPSec Configuration

Add a new **manual IPSec** configuration for a **Branch Office VPN** (menu **Network**).

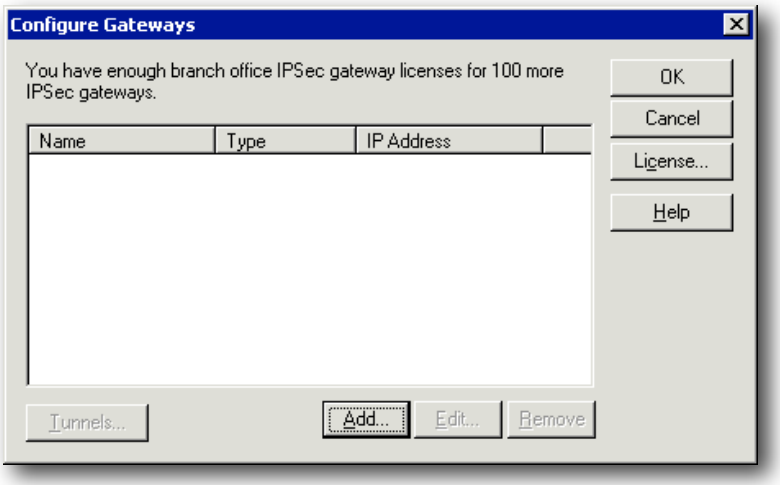


Add a New Gateway

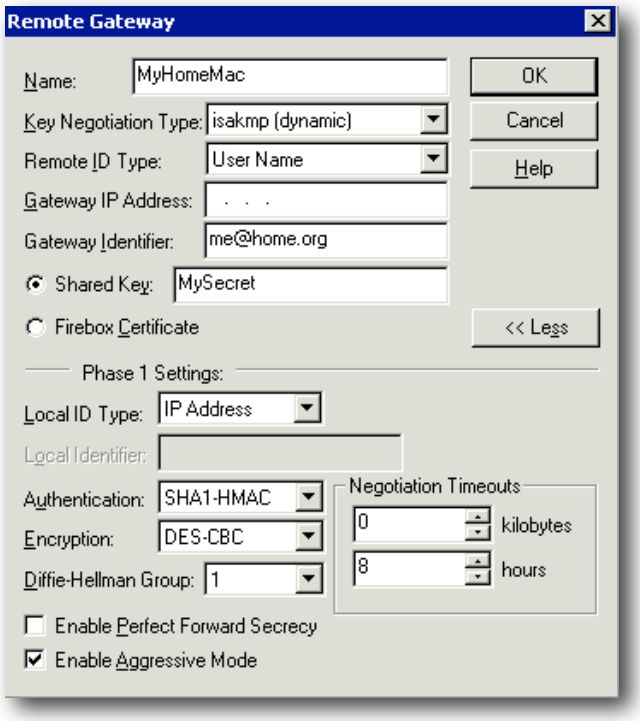
Before IPSec tunnel can be created, a gateway need be added. In the appearing window, press the button **Gateway** to open the gateway editor.



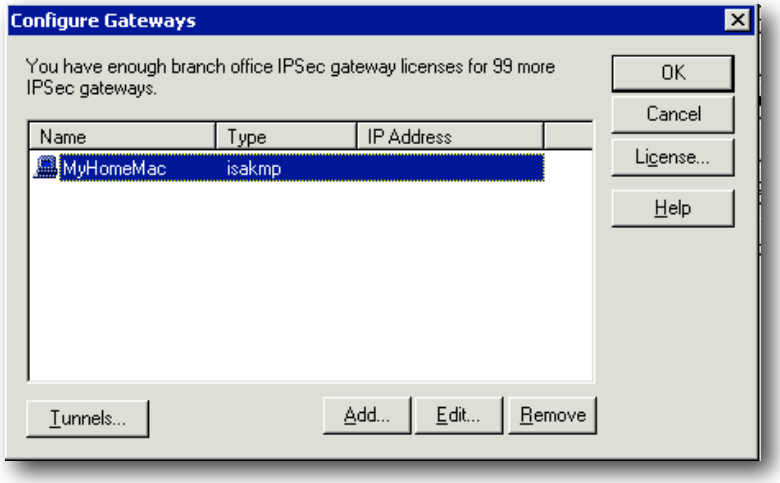
A new window with all available gateways is displayed. Press **Add** to create a new gateway.



Set the properties of the new gateway as depicted below, except for the **Gateway Identifier**, which you may change to your liking, and the **Shared Key**, which you should choose a secure password for. Please keep in mind to set them accordingly when configuring IPSecuritas.

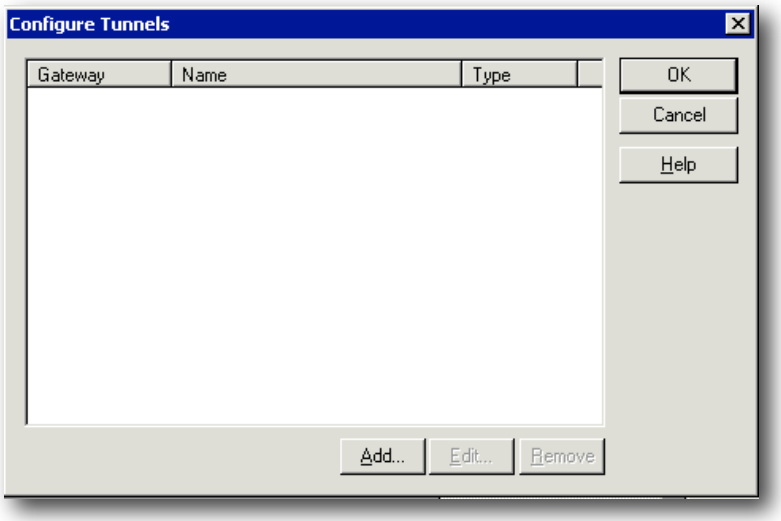


If you're done, press **OK**. The new gateway should now be displayed in the gateway list.

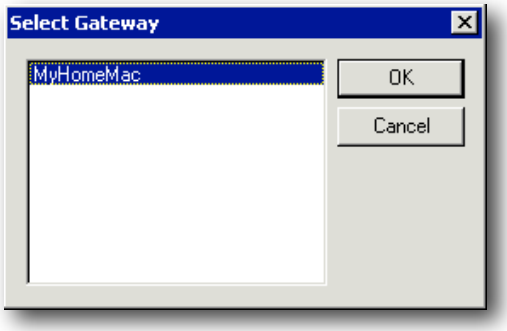


Create New Tunnel

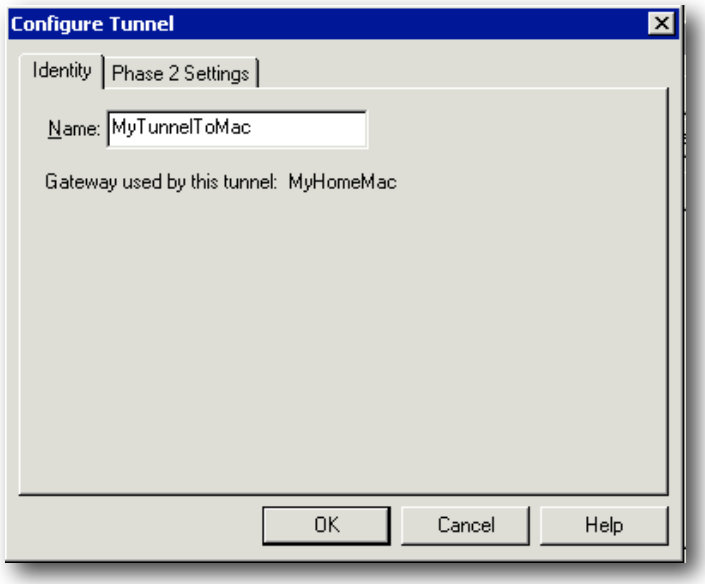
In order to add an IPSec tunnel to the gateway, press the button **Tunnel** at the bottom left side of the window. A new window with an empty tunnel list is displayed.



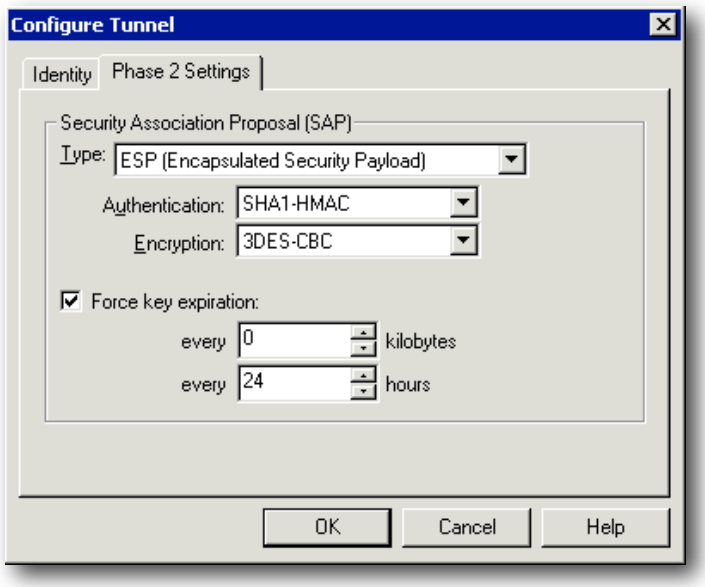
Press the button Add to create a new tunnel for the selected gateway. Select the newly created gateway in the appearing window, then press **OK**.



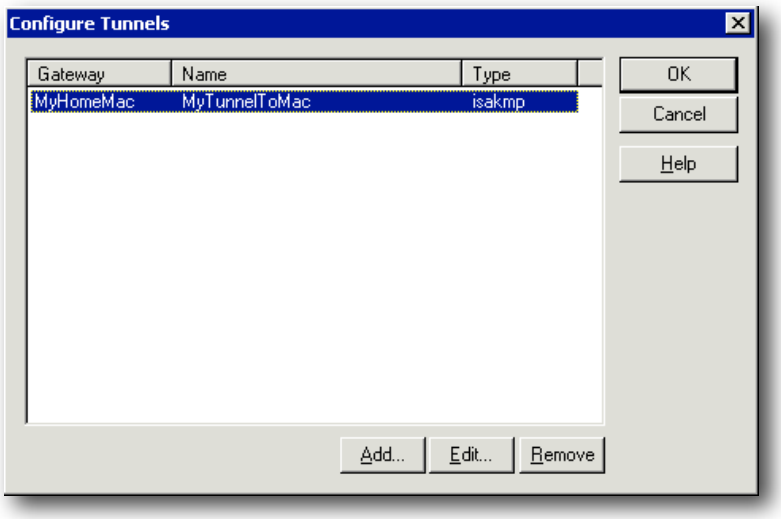
The tunnel configuration window is displayed. Set a descriptive name for future reference of the tunnel.



Set the phase 2 properties as shown in th eimage below.

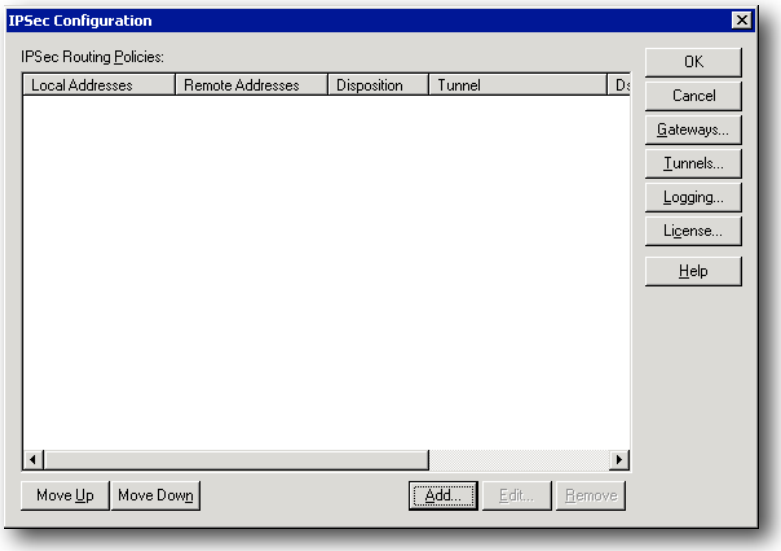


Once you pressed the OK button, the tunnel should be displayed in the tunnel list.



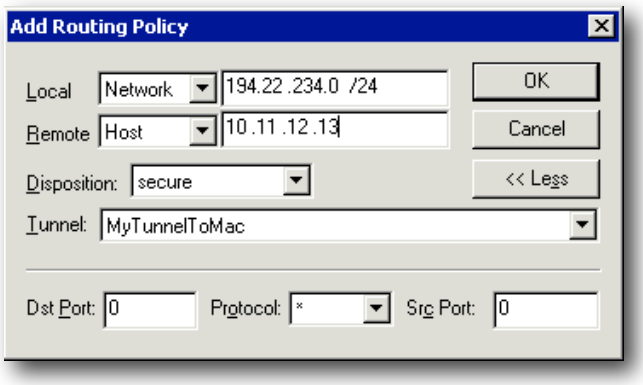
Create a New Routing Policy

In order to tell the router which traffic needs to be routed through the tunnel, you need to add a routing policy. For this, press the button **Add** in the first **IPSec Configuration** window.

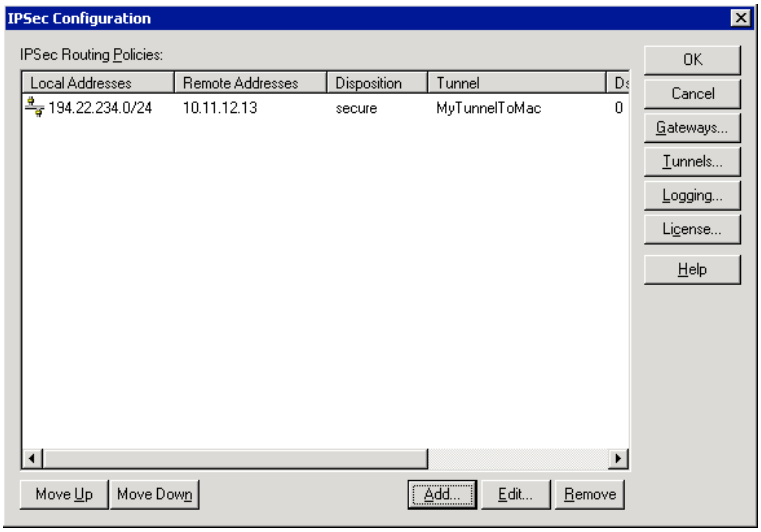


In the appearing window, set the two endpoints you want to connect. The local enpoint is a single address or more commonly a network that you want to access remotely.
Specify a single address for the remote endpoint. It is recommened to use addresses from the private address spaces defined in **RFC 1918** for the client address.

Fille the other parameter as shown in the image below (chosse the tunnel you just created).



Once you pressed the OK button, the new policy should be shown in the policy list. You may add more policies for each network that you want make remotely available and for each additional remote client.



You may now proceed with the setup of IPSecuritas described in the next chapter.

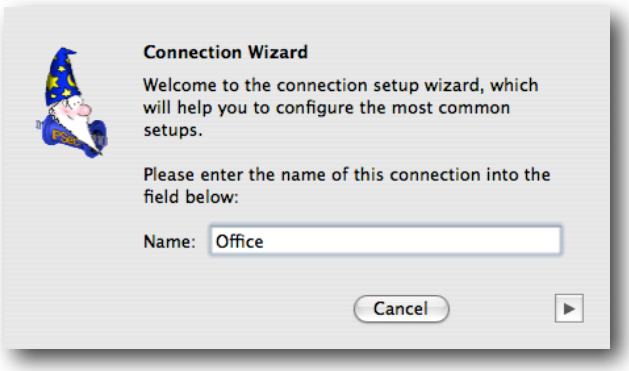
IPSecuritas Setup

This section describes the necessary steps to setup IPSecuritas to connect to the WatchGuard Firebox router.

Start Wizard

Unless it is already running, you should start IPSecuritas now. Change to **Connections** menu and select **Edit Connections** (or press ⌘-E). Start the Wizard by clicking on the following symbol: 

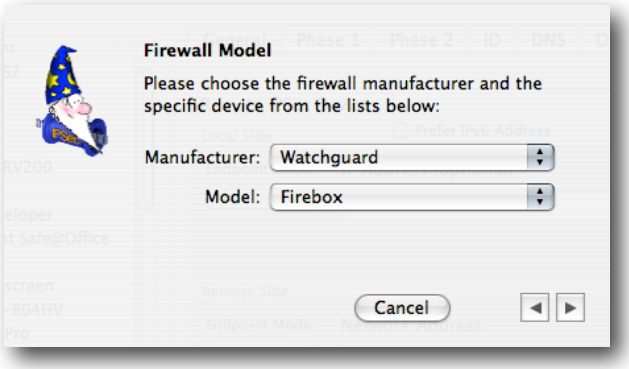
Enter Name of New Connection



Enter a name for the connection (any arbitrary name).

Click on the right arrow to continue with the next step.

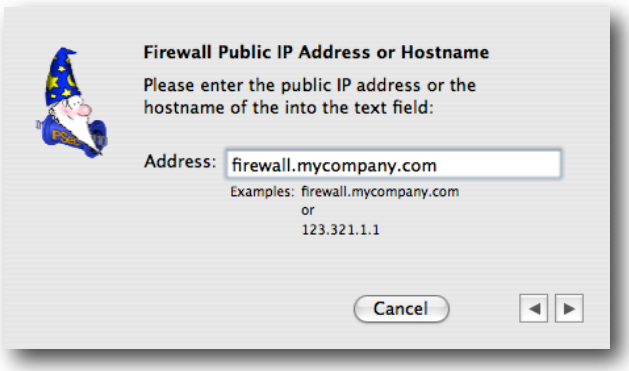
Select Router Model



Select **WatchGuard Firebox** from the manufacturer list and **Firebox** from the model list.

Click on the right arrow to continue with the next step.

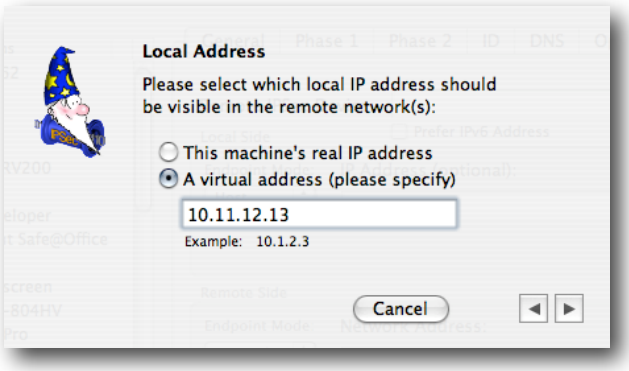
Enter Router's Public IP Address



Enter the public IP address or hostname of your WatchGuard Firebox router. In case your ISP assigned you a dynamic IP address, you should register with a dynamic IP DNS service (like http://www.dyndns.org).

Click on the right arrow to continue with the next step.

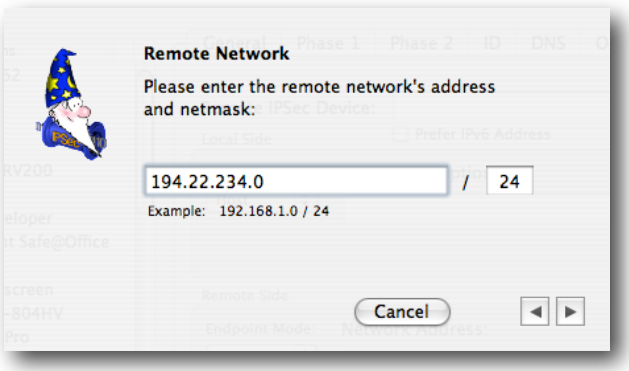
Enter a Virtual IP Address



Enter the virtual local IP address you used for the remote endpoint in the routing policy configuration while setting up the WatchGuard router (see **Create a New Routing Policy** above).

Click on the right arrow to continue with the next step.

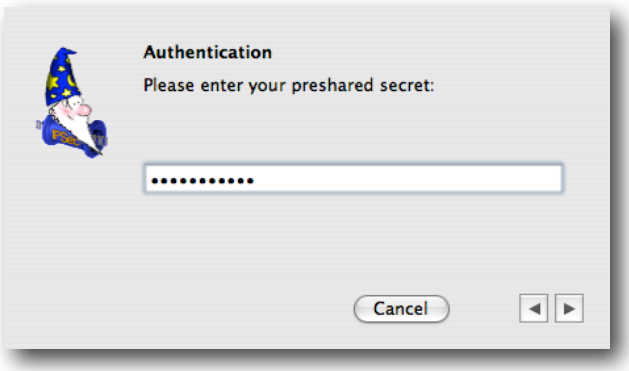
Enter Remote Network



Enter the remote network address and netmask (please note that the netmask needs to be entered in **CIDR** format). This has to match with the routing policy settings of the WatchGuard Firebox.

Click on the right arrow to continue with the next step.

Enter Preshared Key



Enter the same **Preshared Key** that you used for the WatchGuard Firebox.

Click on the right arrow to finish the connection setup.

Diagnosis

Reachability Test

To test reachability of the remote host, open an **Terminal Window** (Utilities -> Terminal) and enter the command **ping**, followed by the WatchGuard Firebox **local IP address**. If the tunnel works correctly, a similar output is displayed:

```
[MacBook:~] root# ping 194.22.234.1
PING 194.22.234.1 (194.22.234.1): 56 data bytes
64 bytes from 194.22.234.1: icmp_seq=0 ttl=64 time=13.186 ms
64 bytes from 194.22.234.1: icmp_seq=1 ttl=64 time=19.290 ms
64 bytes from 194.22.234.1: icmp_seq=2 ttl=64 time=12.823 ms
```