e·quinux

VPN Configuration Guide

Cisco Small Business (Linksys)
WRVS4400N / RVS4000

© 2010 equinux AG and equinux USA, Inc. All rights reserved.

Under copyright law, this configuration guide may not be copied, in whole or in part, without the written consent of equinux AG or equinux USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinux logo is a trademark of equinux AG and equinux USA, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

equinux shall have absolutely no liability for any direct or indirect, special or other consequential damages in connection with the use of this document or any change to the router in general, including without limitation, any lost profits, business, or data, even if equinux has been advised of the possibility of such damages.

Every effort has been made to ensure that the information in this configuration guide is accurate. equinux is not responsible for printing or clerical errors.

Configuration guide revision 1

Created using Apple Pages.

www.equinux.com

Contents

Introduction

This configuration guide helps you configure VPN Tracker and your Cisco VPN gateway to establish a VPN connection between them.

Using the Configuration Guide

Part 1 – VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your Cisco VPN gateway device using the web configuration interface.

This guide is a supplement to the documentation included with your Cisco VPN gateway device, it can't replace it. Please read this documentation before starting.

Part 2 – VPN Tracker Configuration

In the second part, this guide will show you how to configure VPN Tracker to easily connect to your newly created VPN tunnel.

Part 3 – Troubleshooting and Supporting Multiple Users

Troubleshooting advice and information on supporting multiple users can be found in the final part of this guide.

If you are setting up VPN on your device for the first time, we strongly recommend you keep to the tutorial-style setup in the first and second part of this document and make modifications only after you have tested the basic setup.

Conventions Used in This Document

Links to External Websites

Sometimes you will be able to find more information on external websites. Clicking links to websites will open the website in your web browser:

http://equinux.com

Links to Other Parts of this Guide

A → *Link* will take you to another place in the configuration guide. Simply click it if you are reading this guide on your computer.

Tips and Tricks

This configuration guide contains lots of great tips. You can easily spot them by looking for the light bulb icon.

Warnings

This exclamation mark warns you when there is a setting or action where you need to take particular care.

Getting Help

VPN Tracker makes VPN simple. However, computer networking and VPNs can be complex and tricky at times, so we have also built in tools and helpful features that will assist you if you ever run into problems. Check out → *Troubleshooting* for more information.

Prerequisites

Your VPN Gateway

- This guide applies to Cisco Small Business (formerly Linksys) RVS4000 and WRVS4400N routers
- Make sure you have the **latest firmware** version installed that is available for your device. This configuration guide was created using a Cisco RVS4000 running firmware 1.3.2.0 and a Cisco WRVS4400N running firmware 2.0.0.8

Your Mac

VPN Tracker runs on Mac OS X 10.4, 10.5 and 10.6

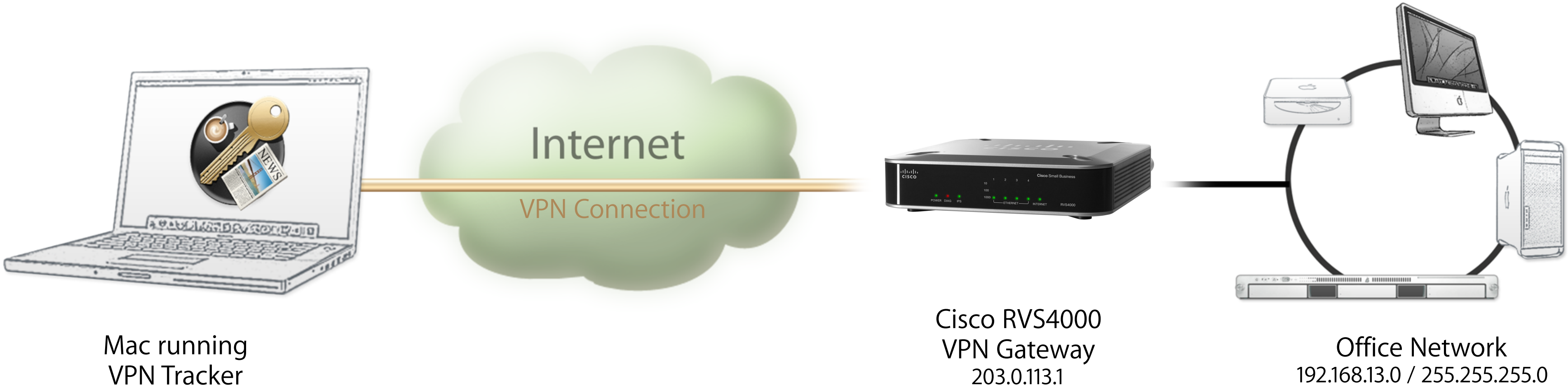
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from http://www.vpntracker.com

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram on the bottom of this page illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has internet connectivity. The office's Cisco VPN gateway device (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address or DNS host name. In our example setup, we will be using a static IP address: 203.0.113.1.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network is using the network 192.168.13.0/24 (which is the same as 192.168.13.0/255.255.255.0). This is the network that will be accessed from the employee's Mac through the VPN. It is called the "Remote Network" in VPN Tracker.



Terminology

A VPN connection is often called a "tunnel" (or "VPN tunnel"). Every VPN tunnel is established between two "endpoints". In our example one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is called the other endpoint's "peer".

Please note that for each endpoint, the settings on the other endpoint are considered to be "remote", while its own settings are considered to be "local". That means a "local" setting from VPN Tracker's perspective, is a "remote" setting from the VPN gateway's perspective, and vice versa.

The sample configuration described in this guide is called a "Host to Network" configuration: a single computer, called a "Host" establishes a VPN tunnel to an entire "Network" behind the VPN gateway.

My VPN Gateway Configuration Checklist

Throughout this guide, there are certain pieces of information that are needed later on for configuring VPN Tracker. This information is marked with red numbers to make it easier to reference it later. You can print this checklist to help keep track of the various settings of your Cisco VPN gateway device.

IP Addresses

❶ WAN IP Address: ______._______._______._______

❷ LAN Network Address / Subnet Mask: ______._______._______._______ / ______._______._______._______

❸ Remote Security Group IP Address: ______._______._______._______

Pre-Shared Key

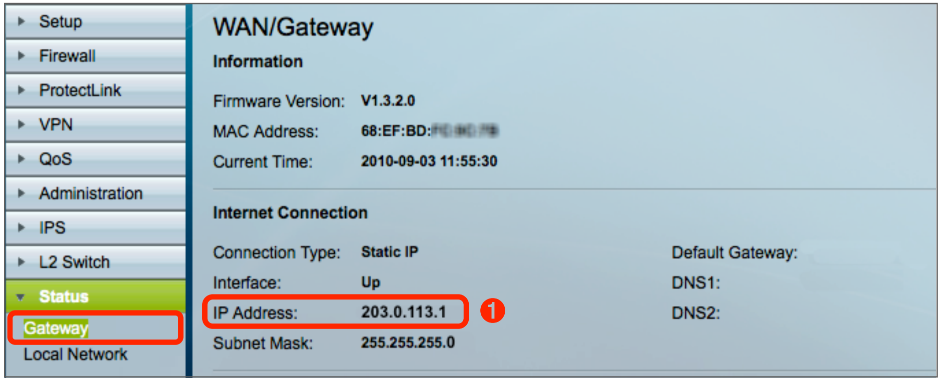
❹ Pre-Shared Key: _____________________________

Task 1 – VPN Gateway Configuration

We will first set up VPN on the VPN gateway. If you already have VPN in place, it’s helpful to follow along this tutorial to see how settings on the device fit together with VPN Tracker.

Step 1 – Retrieve Network Settings

- Connect to your VPN gateway through its web configuration interface
- Go to **Status** > **Gateway**



WAN/Gateway

Information

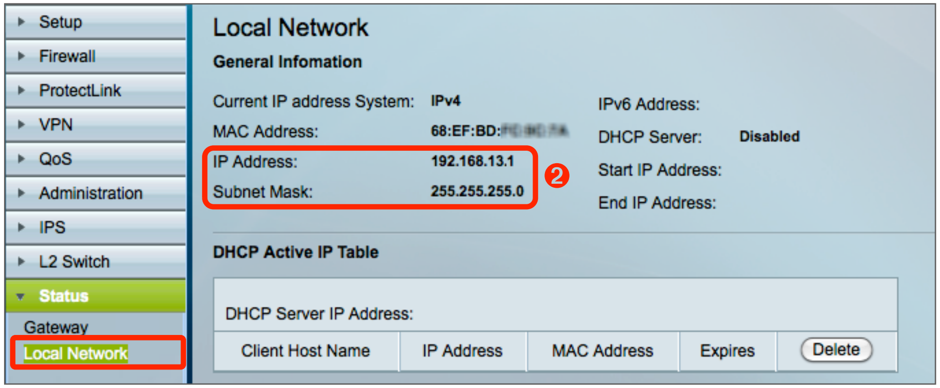
Firmware Version: V1.3.2.0
MAC Address: 68:EF:BD:[redacted]
Current Time: 2010-09-03 11:55:30

Internet Connection

Connection Type: Static IP
Interface: Up
IP Address: 203.0.113.1
Subnet Mask: 255.255.255.0
Default Gateway:
DNS1:
DNS2:

- **Internet Connection:** Write down the **IP address** of your VPN gateway as ❶ on your → *Configuration Checklist* (here: 203.0.113.1)

- Go to **Status** > **Local Network**



Local Network

General Infomation

Current IP address System: IPv4
MAC Address: 68:EF:BD:[redacted]
IP Address: 192.168.13.1
Subnet Mask: 255.255.255.0
IPv6 Address:
DHCP Server: Disabled
Start IP Address:
End IP Address:

DHCP Active IP Table

DHCP Server IP Address:

Client Host Name	IP Address	MAC Address	Expires	Delete

- Calculate your device’s **LAN Network Address** by applying the **Subnet Mask** to the **IP Address** ❷:
  Applying the subnet mask means setting those elements of the IP address to 0 where the subnet mask is 0, and preserving all elements where the subnet mask is 255[1]

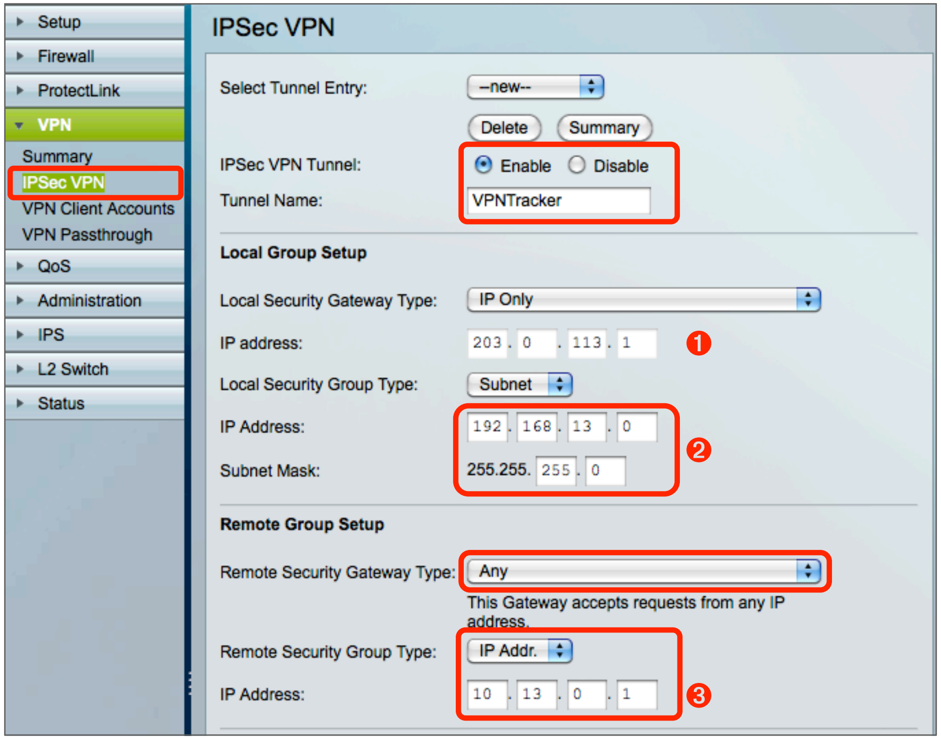
LAN Subnet Mask	255	.	255	.	255	.	0
applied to	↓		↓		↓		↓
LAN IP Address	192	.	168	.	13	.	1
LAN Network Address	192	.	168	.	13	.	0

Write down your calculated LAN network address (here: 192.168.13.0) as ❷ on your → *Configuration Checklist*. This will be your VPN connection’s **Remote Network**.

[1] If you are using a subnet mask with elements that are not 0 or 255, you can use one of the many subnet calculators available online to calculate the correct network address.

Step 2 – Set up VPN

- Go to **VPN** > **IPSec VPN**



IPSec VPN

Select Tunnel Entry: --new--

IPSec VPN Tunnel: ● Enable ○ Disable

Tunnel Name: VPNTracker

Local Group Setup

Local Security Gateway Type: IP Only

IP address: 203 . 0 . 113 . 1 ❶

Local Security Group Type: Subnet

IP Address: 192 . 168 . 13 . 0 ❷

Subnet Mask: 255.255. 255 . 0

Remote Group Setup

Remote Security Gateway Type: Any

This Gateway accepts requests from any IP address.

Remote Security Group Type: IP Addr.

IP Address: 10 . 13 . 0 . 1 ❸

Tunnel Entry

- Choose **--new--** from the tunnel entries
- **IPSec VPN Tunnel**: **Enable** the new VPN tunnel setting
- **Tunnel Name**: Enter a new VPN tunnel name (here: **VPNTracker**)

Local Group Setup

- **Local Security Gateway Type**: Choose **IP Only**
- **IP Address**: This field should already contain your device's WAN IP ❶
- **Local Security Group Type**: Choose **Subnet**
- **IP Address**: Enter the **LAN Network Address** and **Subnet Mask** ❷ from your → *Configuration Checklist*

Remote Group Setup

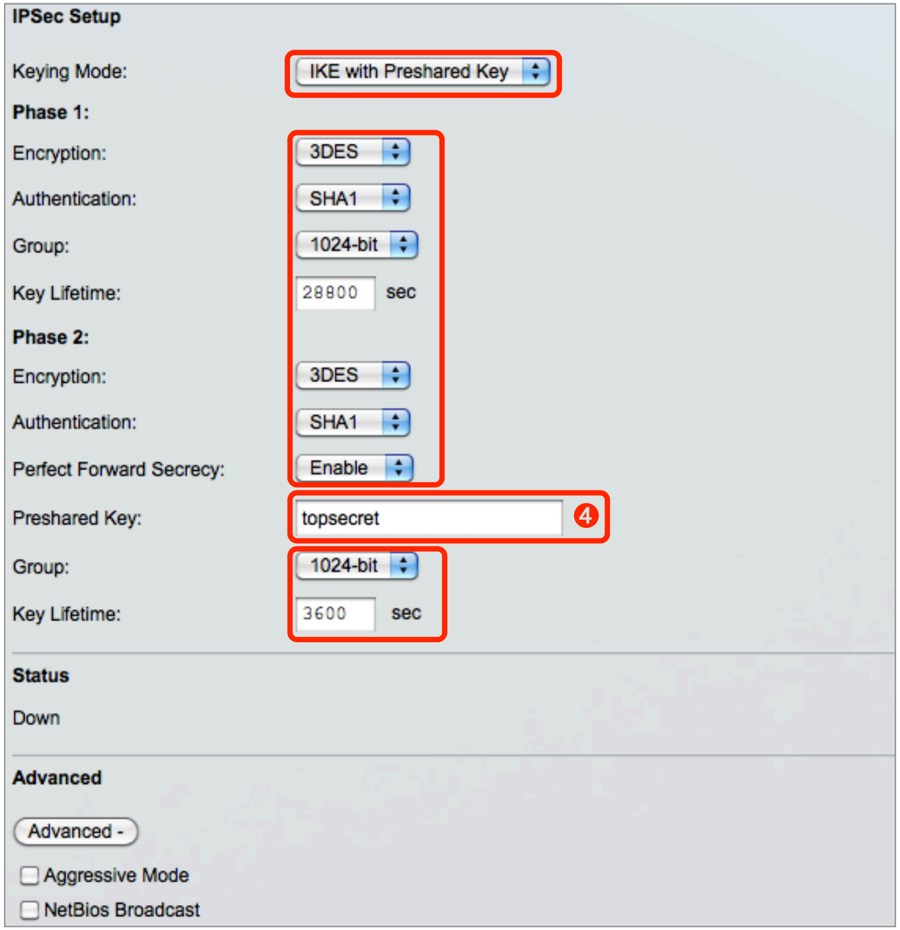
- **Remote Security Gateway Type**: Choose **Any**
- **Remote Security Group Type**: Choose **IP Address**
- **IP Address**: Enter an arbitrary IP address from a private network that is **not** part of the device's LAN network. This IP address will be used as the **Local Address** in VPN Tracker. Write down the IP address as ❸ on your → *Configuration Checklist*

  In our example, the LAN network is 192.168.13.0/24. We can use any IP address from 10.0.0.0/8, as well as from 172.16.0.0/12, and from 192.168.0.0/16 **excluding** IPs from 192.168.13.0/24. We have decided to use 10.13.0.1 here.

This tunnel can be used only by a single user. If you plan to have more than one VPN user, refer to → *Supporting Multiple Users* for more information.

IPsec Setup (Phase 1 / Phase 2)

Please make sure the settings on your device match those shown here:



IPSec Setup

Keying Mode: IKE with Preshared Key

Phase 1:

Encryption: 3DES

Authentication: SHA1

Group: 1024-bit

Key Lifetime: 28800 sec

Phase 2:

Encryption: 3DES

Authentication: SHA1

Perfect Forward Secrecy: Enable

Preshared Key: topsecret ❹

Group: 1024-bit

Key Lifetime: 3600 sec

Status

Down

Advanced

□ Aggressive Mode

□ NetBios Broadcast

- **Preshared Key**: Enter a good password and write it down as ❹ on your → *Configuration Checklist*. This password will be needed to connect to this VPN connection
- Click **Save** to create the new tunnel
- Open the **Advanced** settings and make sure they match the screenshot above. If not, change them and click Save again

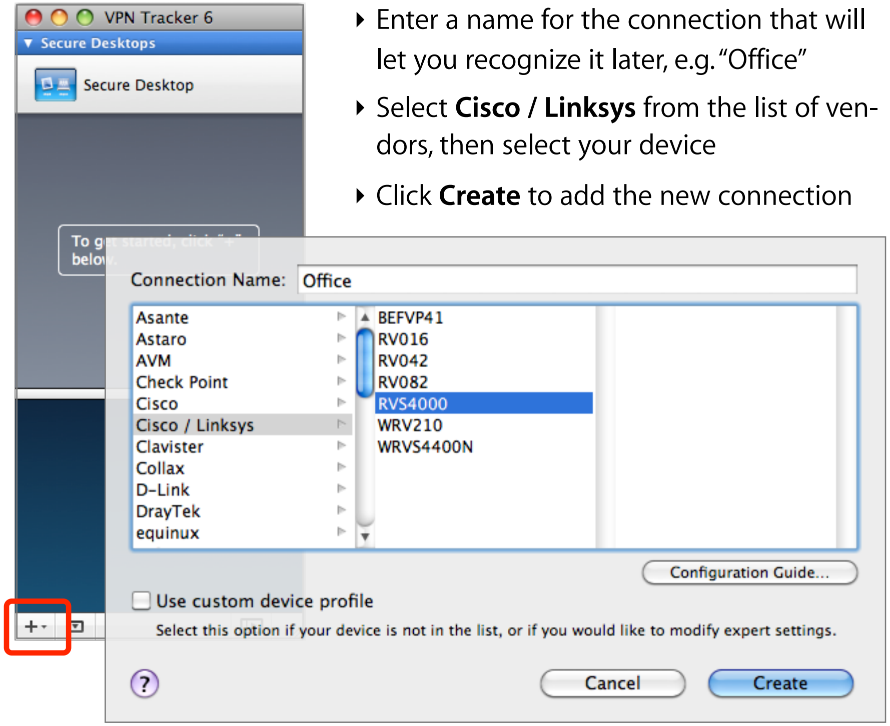
If you wish, you can use other settings than the ones shown for phase 1 and phase 2. If you do so, you must match these settings on VPN Tracker's Advanced tab. **We strongly recommend using the settings shown here for the initial setup, and to make changes only once the connection is working.**

Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed → *Configuration Checklist* containing your VPN gateway's settings. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection

Open VPN Tracker, and click the plus button in the bottom left corner of the window to add a new connection:



Connection Name: Office

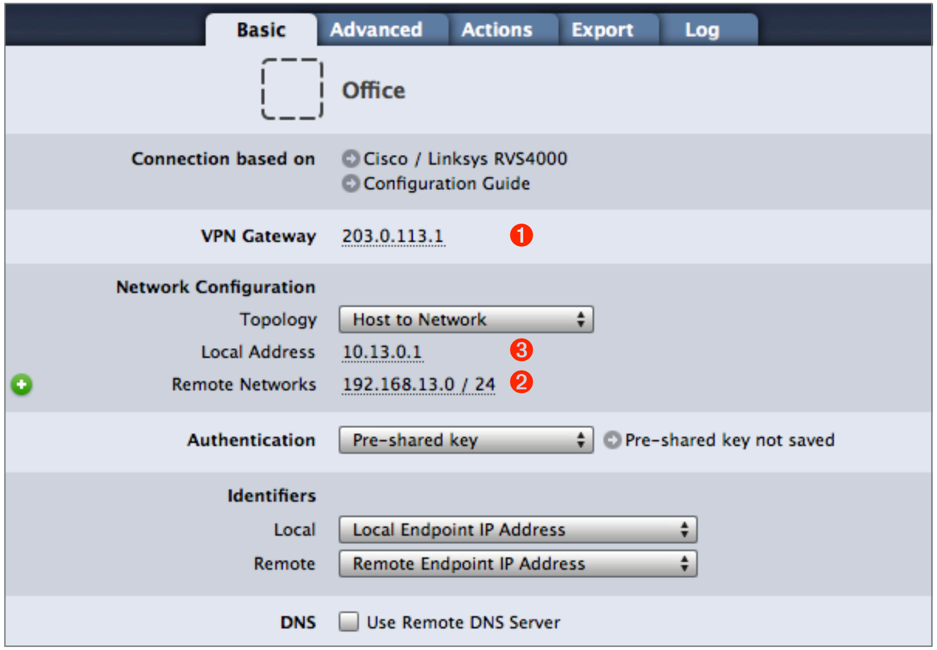
□ Use custom device profile

Select this option if your device is not in the list, or if you would like to modify expert settings.

- Enter a name for the connection that will let you recognize it later, e.g. "Office"
- Select **Cisco / Linksys** from the list of vendors, then select your device
- Click **Create** to add the new connection

Step 2 – Configure the VPN Connection

Once you have added the new connection, there are a few settings that need to be customized to match what is configured on your VPN gateway.



Connection based on: Cisco / Linksys RVS4000, Configuration Guide

VPN Gateway: 203.0.113.1 ❶

Network Configuration

Topology: Host to Network

Local Address: 10.13.0.1 ❸

Remote Networks: 192.168.13.0 / 24 ❷

Authentication: Pre-shared key — Pre-shared key not saved

Identifiers

Local: Local Endpoint IP Address

Remote: Remote Endpoint IP Address

DNS: □ Use Remote DNS Server

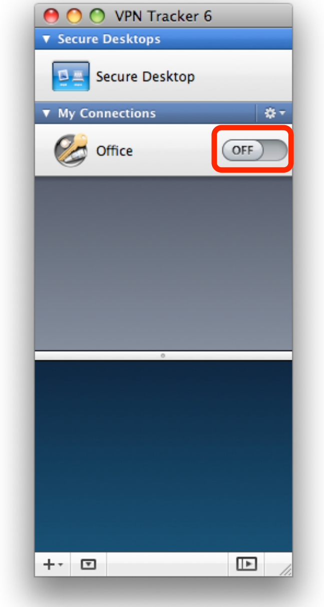
- **VPN Gateway**: Enter the WAN IP address of your VPN gateway you wrote down as ❶ on your → *Configuration Checklist*
- **Local Address**: Enter the Remote Security Group IP Address you wrote down as ❸ on your → *Configuration Checklist*
- **Remote Network**: Enter the network address of the network that is being accessed through the VPN tunnel ❷. Separate the subnet mask with a forward slash („/")

Step 3 – Test the VPN Connection

It 's time to go out!

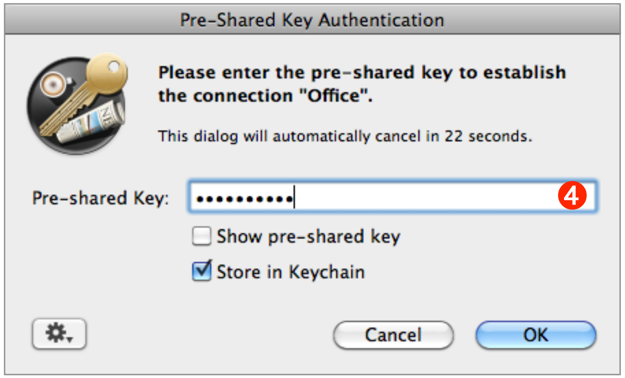
You will not be able to test and use your VPN connection from within the internal network that you want to connect to. To test your connection, you will need to connect from a different location. For example, if you are setting up a VPN connection to your office, test it from home. If you are setting up a VPN connection to your home network, test it from an Internet cafe, or go visit a friend.

Start your connection



- Connect to the Internet
- Make sure that your Internet connection is working – open your Internet browser and connect to http://www.equinux.com
- Open VPN Tracker if it’s not already running
- Slide the ON/OFF slider for the connection you have just configured to **ON**

When prompted for your pre-shared key:


Pre-Shared Key Authentication

Please enter the pre-shared key to establish the connection "Office".

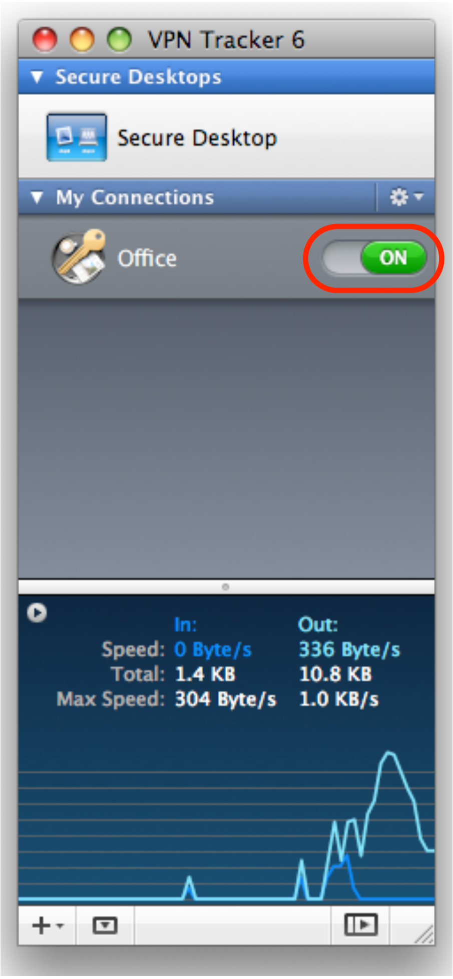
This dialog will automatically cancel in 22 seconds.

Pre-shared Key: •••••••••• ❹

□ Show pre-shared key

☑ Store in Keychain

- **Pre-shared key**: Enter the pre-shared key that you configured on your VPN gateway ❹
- Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- Click **OK**



```
           In:            Out:
    Speed: 0 Byte/s       336 Byte/s
    Total: 1.4 KB         10.8 KB
Max Speed: 304 Byte/s     1.0 KB/s
```

- If the slider goes back to **OFF** after starting the connection, or after entering your pre-shared key, please read the → *Troubleshooting* section of this document
- If the slider goes to **ON** and turns green after a while, you have successfully established a connection
- **Congratulations**!

Troubleshooting

In most cases, your connection should work fine if you follow the instructions above. If you cannot connect, please read on.

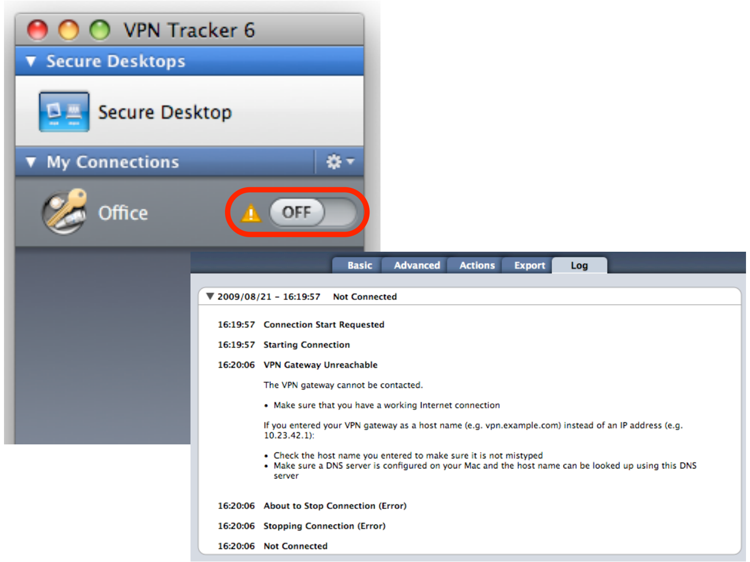
VPN Connection Fails to Establish

ON/OFF slider goes back to OFF right away

If the slider goes back to **OFF** right away, please make sure you have entered all the required information. VPN Tracker will highlight fields that are missing or obviously incorrect information.

ON/OFF slider goes back to OFF after a while

If the connection **ON**/**OFF** slider goes back to **OFF** a while after attempting to start the connection, please go to the **Log** tab to get more information about the issue (or click the warning triangle to be automatically taken to the **Log** tab). VPN Tracker will display detailed suggestions for a solution:



```
▼ 2009/08/21 – 16:19:57    Not Connected

    16:19:57   Connection Start Requested

    16:19:57   Starting Connection

    16:20:06   VPN Gateway Unreachable

               The VPN gateway cannot be contacted.

               • Make sure that you have a working Internet connection

               If you entered your VPN gateway as a host name (e.g. vpn.example.com) instead of an IP address (e.g.
               10.23.42.1):

               • Check the host name you entered to make sure it is not mistyped
               • Make sure a DNS server is configured on your Mac and the host name can be looked up using this DNS
                 server

    16:20:06   About to Stop Connection (Error)

    16:20:06   Stopping Connection (Error)

    16:20:06   Not Connected
```

No Access to the Remote Network

If the connection slider goes to **ON** and turns green, but you cannot access resources (servers, email, etc.) through the VPN connection please check the following points.

Connect to an IP address (instead of a host name)

If you are using a host name (e.g. server.example.com) instead of an IP address (e.g. 192.168.13.42) to connect to a resource , please try using the resource's IP address instead. If the connection works when using the IP address, but not when using a host name, please make sure that your Mac's DNS server or the "Remote DNS" server that you have configured on your VPN gateway is able to resolve this host name to an IP address.

Test VPN Availability again

In many networks your Mac will be behind a router that performs Network Address Translation (NAT). For a VPN connection to be established through such a router, VPN Tracker can use different methods, but not all of them may be supported by your local router or your VPN gateway.

VPN Tracker automatically runs a test to detect the proper method for your particular Internet connection when you first connect using this Internet connection. However, test results could become outdated by changes to the local router, so it is a good idea to test again if there are problems.

- Select **Tools** > **Test VPN Availability** from the menu
- Click **Test Again** and wait until the test has completed
- Try connecting again

Check the Local Address setting

In order for replies to reach VPN Tracker, make sure that the **Local Address** (Basic tab) is **not** part of the remote network.

Further Questions?

You can find the latest news and compatibility information on our support and FAQ website:

http://www.equinux.com/support

If you need to contact equinux Technical Support

If you can't resolve your issue with the information available on our website or in this guide and would like to contact Technical Support through our website, please be sure to include at least the following information:

- The manufacturer and model and firmware revision of the VPN gateway
- A Technical Support Report from VPN Tracker (Help > Generate Technical Support Report)
- Screenshots of what you have configured on your VPN gateway, in particular all VPN-related settings
- A description of the problem and the troubleshooting steps you have taken

Supporting Multiple Users

To add another user, you'll need to add a new tunnel. The tunnel must share the phase 1 settings and pre-shared key of the first tunnel, but needs to use a different IP address for the VPN client.

Tunnel Name

The tunnel name must be **different** from the first tunnel set up on the device. Here, we have used VPNTracker2.

Local Group Setup

The Local Group Setup must be the **same** as the first tunnel's settings

Remote Group Setup

The IP address must be **different** from the one(s) used in any other tunnel(s) on the device. For our first tunnel, we have already used 10.13.0.**1**, so we now use 10.13.0.**2** for the second tunnel.

IPsec Setup

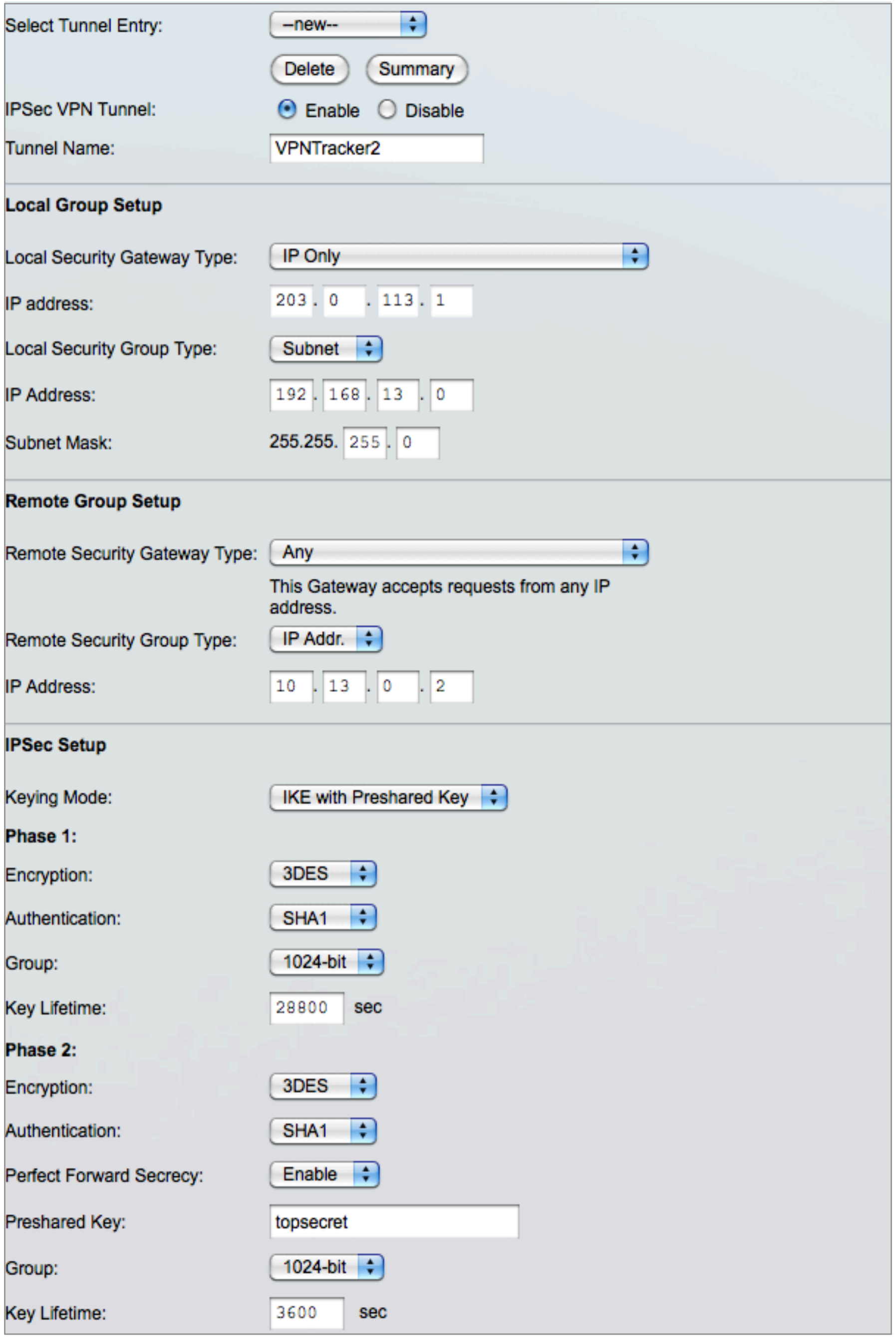
Phase 2

The Phase 1 settings must the **same** as the first tunnel's phase 1 settings. This is because the VPN gateway cannot distinguish this tunnel from other tunnels at the beginning of phase 1.

Phase 2

While you could use different settings for phase 2 (encryption, authentication, lifetime, group, and perfect forward secrecy), we recommend using the same settings as for the first tunnel.

The **Preshared Key** must be the **same** as the first tunnel's key!



Select Tunnel Entry:	--new--
	Delete Summary
IPSec VPN Tunnel:	● Enable ○ Disable
Tunnel Name:	VPNTracker2
Local Group Setup	
Local Security Gateway Type:	IP Only
IP address:	203 . 0 . 113 . 1
Local Security Group Type:	Subnet
IP Address:	192 . 168 . 13 . 0
Subnet Mask:	255.255. 255 . 0
Remote Group Setup	
Remote Security Gateway Type:	Any This Gateway accepts requests from any IP address.
Remote Security Group Type:	IP Addr.
IP Address:	10 . 13 . 0 . 2
IPSec Setup	
Keying Mode:	IKE with Preshared Key
Phase 1:	
Encryption:	3DES
Authentication:	SHA1
Group:	1024-bit
Key Lifetime:	28800 sec
Phase 2:	
Encryption:	3DES
Authentication:	SHA1
Perfect Forward Secrecy:	Enable
Preshared Key:	topsecret
Group:	1024-bit
Key Lifetime:	3600 sec