e·quinux

VPN Configuration Guide

LANCOM®

equinux AG and equinux USA, Inc.

© 2009 equinux USA, Inc. All rights reserved.

Under the copyright laws, this manual 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.

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

Created using Apple Pages.

www.equinux.com

Apple, the Apple logo, iBook, Mac, Mac OS, MacBook, PowerBook are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Finder and Mail are trademarks of Apple Computer, Inc. AppleCare is a service mark of Apple Computer, Inc., registered in the U.S. and other countries.

FileMaker is a trademark of FileMaker, Inc.

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

Introduction

This document describes how VPN Tracker can be used to establish a connection between a Mac running Mac OS X and a LANCOM VPN router..

Note This documentation is only a supplement to, not a replacement for, the instructions included with your LANCOM device. Please be sure to read those instructions and understand them before starting.

LANCOM Configuration

The first part of this document will show you how to configure a VPN tunnel on a LANCOM VPN router using a setup that automatically distributes IP addresses to VPN clients through Mode Config.

VPN Tracker Configuration

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

Troubleshooting and Advanced Topics

Troubleshooting and advanced topics are covered in the third part of this document. There you will find:

- instructions for setting up a VPN for a single VPN client using a static IP address
- troubleshooting tips
- an table comparing the various settings on your LANCOM device to those in VPN Tracker

Important Prerequisites

Your LANCOM Device

First make sure to use a recent LANCOM firmware version. The latest release for your LANCOM firewall can be obtained from http://www.lancom-systems.com.

For this document, LCOS 6.32.0021 and 7.28.0031 were used.

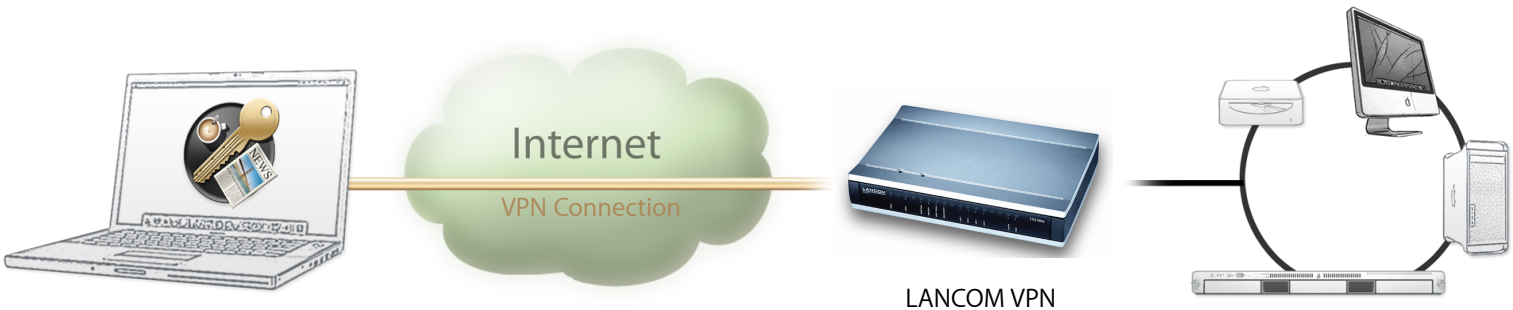
Please note: VPN Tracker has been tested with the LANCOM 1721 VPN device and the above firmware versions. The instructions should also apply to other LANCOM VPN devices with these these firmware revisions.

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 or higher. Make sure to use a recent VPN Tracker version. The latest VPN Tracker release can be obtained from http://www.vpntracker.com
- You will need one VPN Tracker license for each Mac running VPN Tracker

Scenario

In our example, we need to connect an employee's Mac to an office network. The following diagram illustrates this scenario:



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

The LANCOM device has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range 192.168.1.0/24 (which is the same as 192.168.1.0/255.255.255.0). 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.

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.

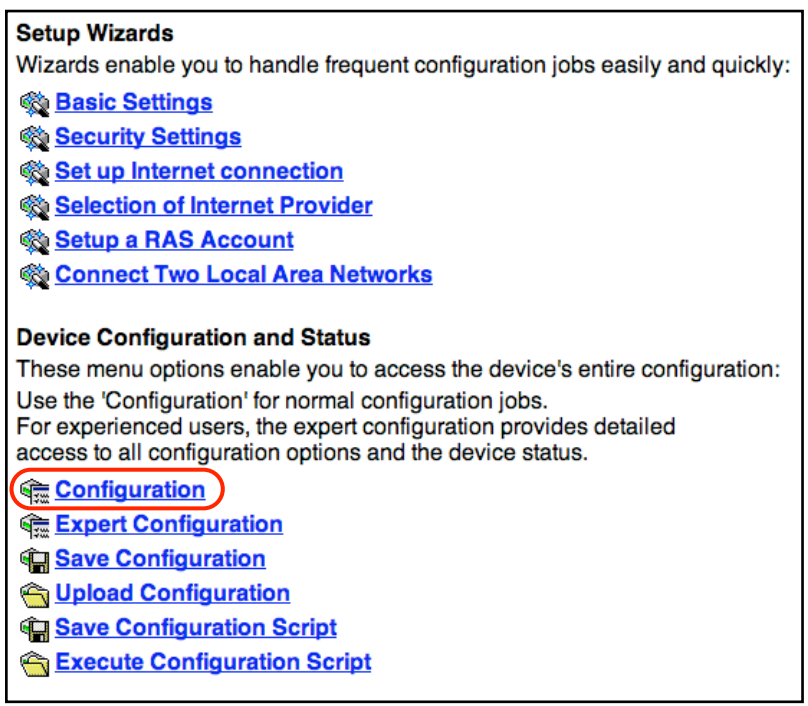
The sample configuration described in this guide is called a "Host to Network" configuration: A single computer, called a "Host" establishes a VPN tunnel to an entire "Network" behind the VPN gateway.

Task 1 – Configure your VPN Device

This section describes the configuration of your LANCOM VPN router.

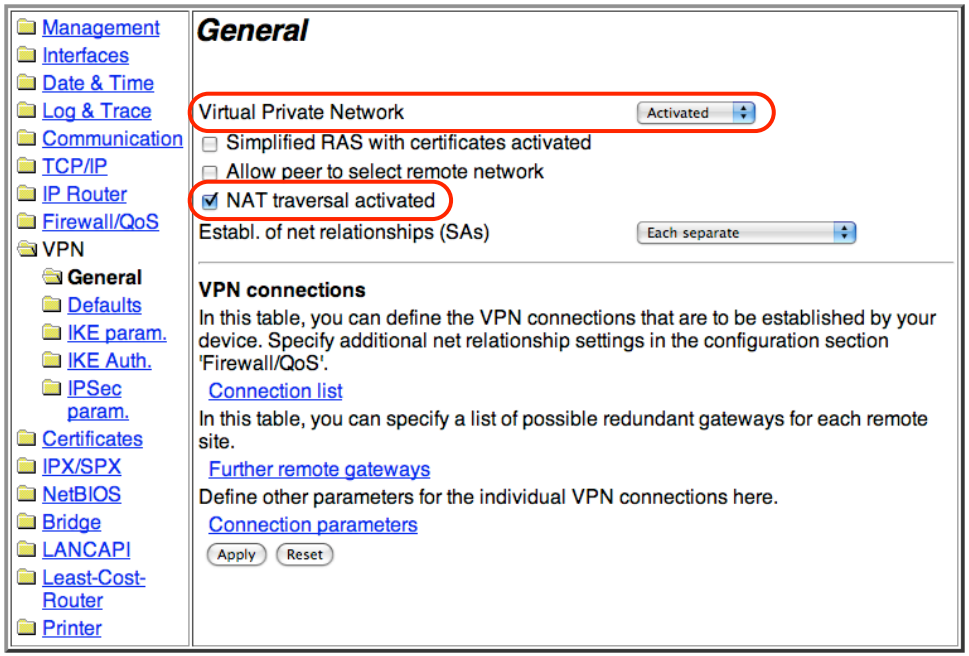
TIP To setup your VPN connection, you'll need to keep track of certain pieces of information. Those details are indicated by red numbers. Throughout this guide we will be referencing those numbers.

Step 1 – Access the Configuration Menu



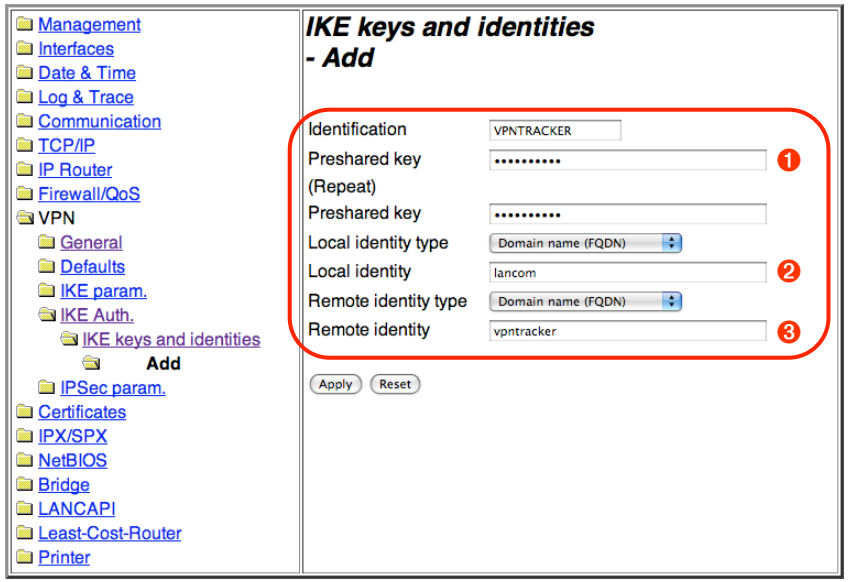
- Access your LANCOM's configuration web interface
- Click on "Configuration"

Step 2 – Activate VPN



- Select "VPN > General"
- **Virtual Private Network:** Select "Activated" from the pop-up list
- **NAT traversal activated**: Please make sure this box is checked
- Click "Apply"

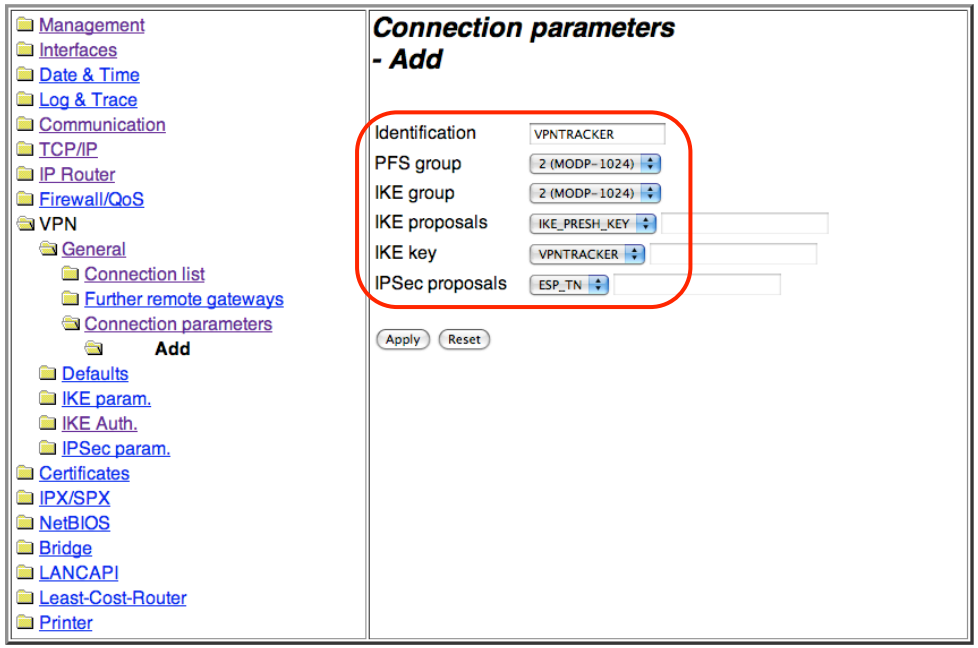
Step 3 – Add an IKE Identity



- Select "VPN > IKE Auth."
- Click "IKE keys and identities"
- Click "Add"
- **Identification**: VPNTRACKER
- Enter a **pre-shared key**. This will be the password for connecting to the VPN 1
- Repeat the pre-shared key
- **Local identity type**: Domain name (FQDN)
- **Local Identity:** Enter an arbitrary identifier (e.g. lancom) 2
- **Remote identity type**: Domain name (FQDN)
- **Remote identity**: Enter an arbitrary identifier (e.g. vpntracker) 3
- Click "Apply"

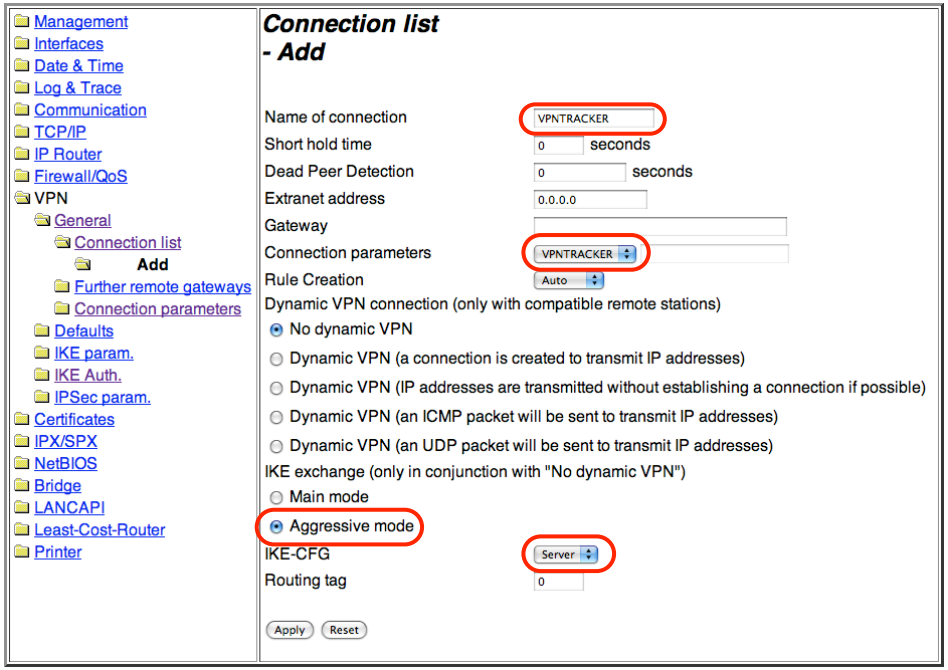
TIP Don't forget to remember (or write down) what you entered for the pre-shared key 1, the local identity 2, and the remote identity 3

Step 4 – Add Connection Parameters



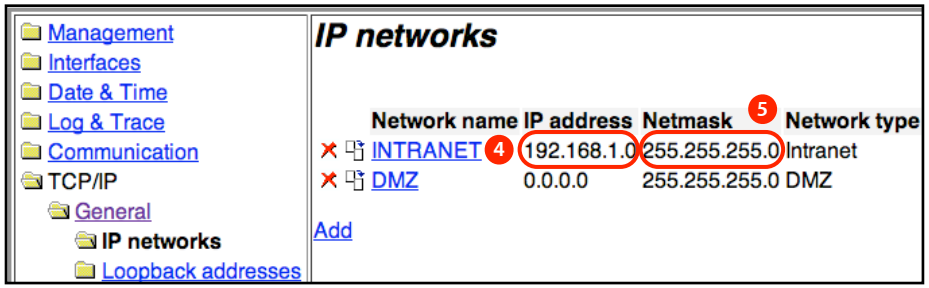
- Select "VPN > General"
- Click "Connection parameters"
- Click "Add"
- **Identification**: VPNTRACKER
- **PFS group**: Select "2 (MODP - 1024)"
- **IKE group**: Select "2 (MODP -1024)"
- **IKE proposals**: Select "IKE_PRESH_KEY"
- **IKE key**: Select "VPNTRACKER"
- **IPSec proposals**: Select "ESP_TN"

Step 5 – Add a VPN Connection



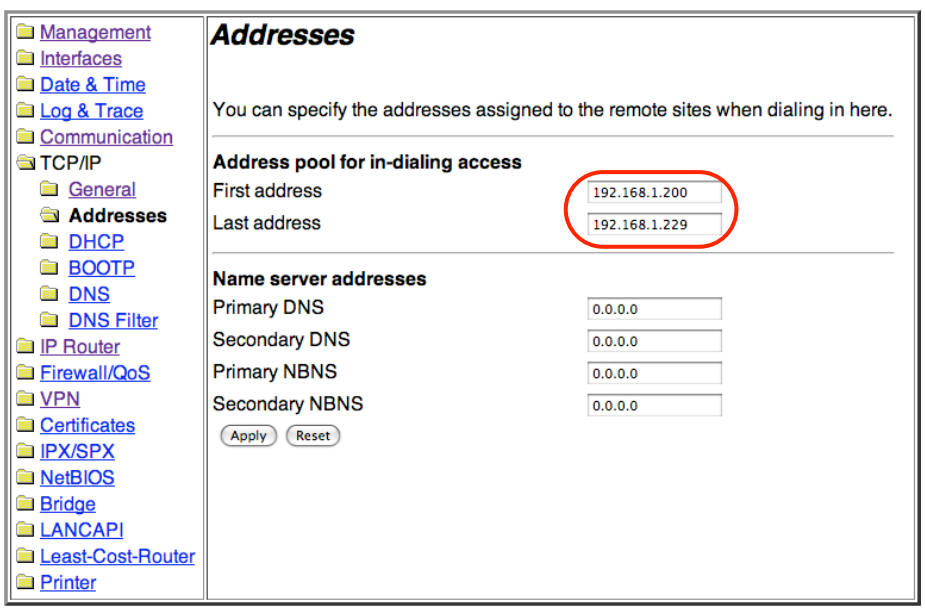
- Select "VPN > General"
- Click "Connection list"
- Click "Add"
- **Name of connection**: VPNTRACKER
- **Connection parameters**: Select "VPNTRACKER" from the pop-up
- **IKE exchange:** Select "Aggressive Mode"
- **IKE-CFG**: Select "Server"
- Click "Apply"

Step 6a – Retrieve your Intranet Information



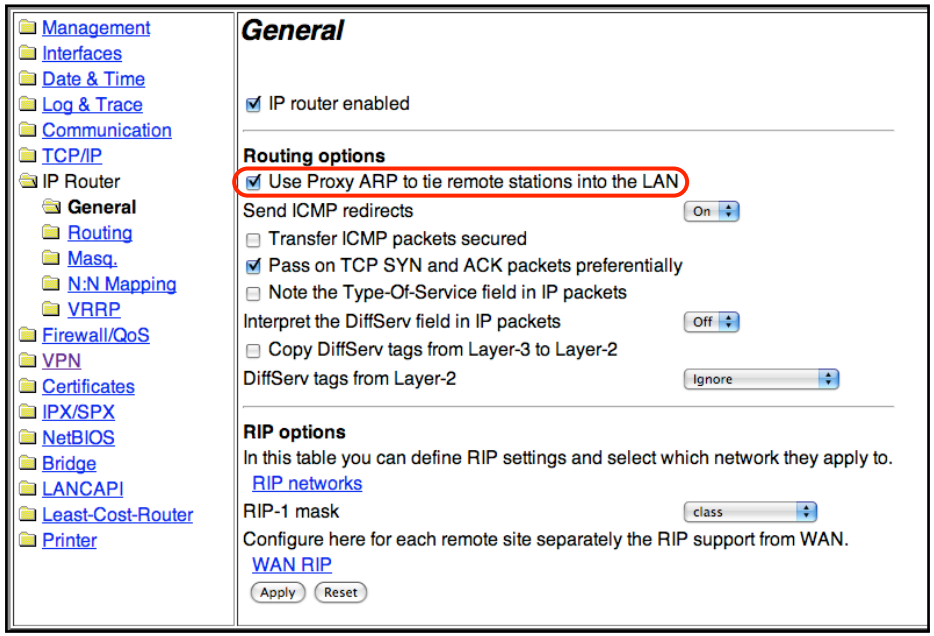
- Select "TCP/IP > General > IP Networks"
- Find the "INTRANET" entry in the list and write down the **IP address** 4 and **netmask** 5

Step 6b – Add an In-Dialing Address Pool



- Select "TCP/IP > Addresses"
- Address pool for in-dialing access: Enter a range of IP addresses from the intranet network that is not used for other purposes (e.g. DHCP or static addresses). Make sure this pool has enough addresses for all clients that you expect to connect.
- Click "Apply"

Step 7 – Enable Proxy ARP

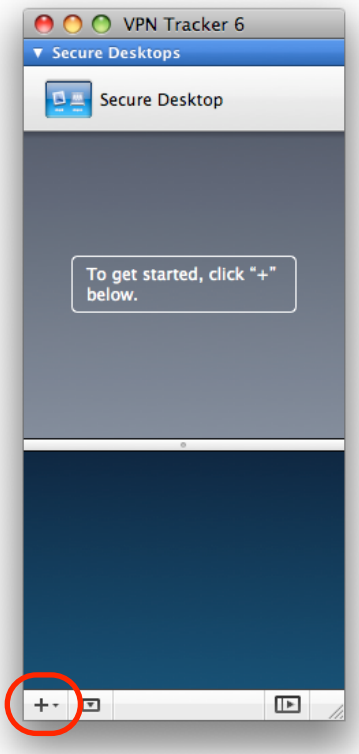


- Select "IP Router > General"
- Check the box **"Use Proxy ARP to tie remote stations into the LAN"**
- Click "Apply"

Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker.

Step 1 - Create a New Connection

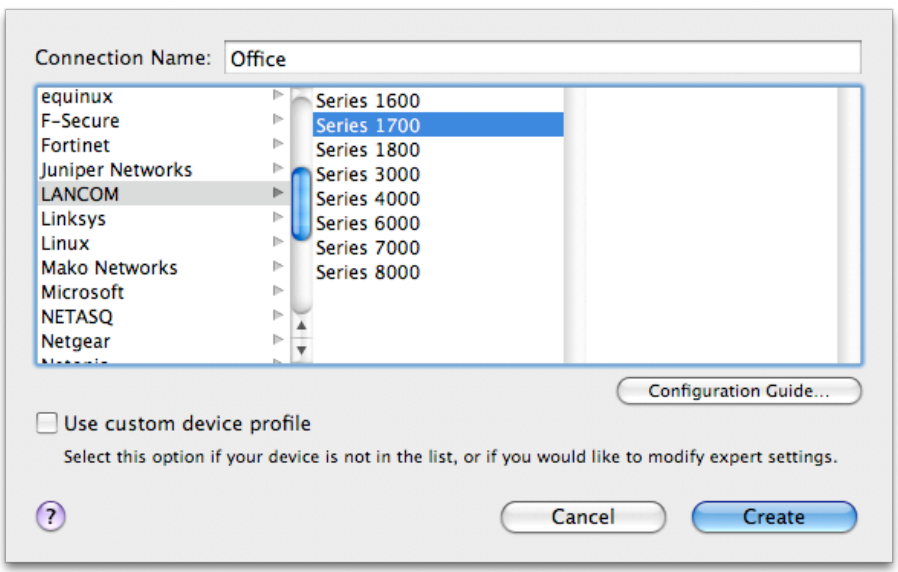


- Start VPN Tracker 6
- Click the "+" button in the main window

Step 2 – Select a VPN Device

For many VPN gateways, VPN Tracker 5 provides pre-defined profiles, based on the device's default settings.

Note If you have changed any of the factory settings while configuring the device (other than as described in this document), you might have to adjust the "Advanced" settings in VPN Tracker. This is explained in detail in the VPN Tracker 5 manual. Please see the appendix of this document for a mapping of LANCOM terms to VPN Tracker terms.

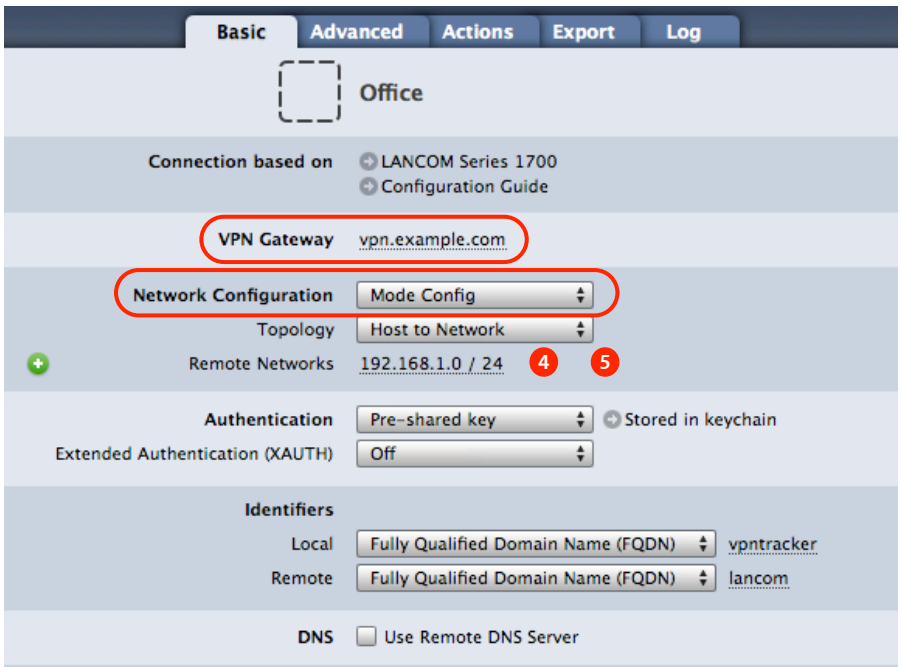


- Select "LANCOM" from the list
- Select your device from the list of LANCOM devices
- **Connection Name**: Choose a name for your connection (e.g. "Office")
- Click "Create"

Step 3 – Configure IP Addresses

There are two important addresses involved in a VPN tunnel:

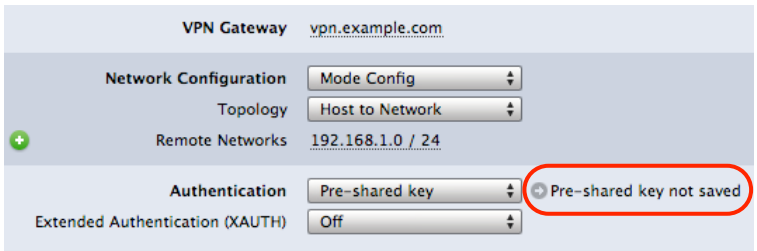
- The VPN gateway's public address (aka WAN IP)
- Your office (intranet) network's IP address at the gateway's end of your VPN tunnel (i.e. the network you want to access through the VPN gateway)



- Make sure the **Mode Config** is selected from the Network Configuration drop-down menu
- **VPN Gateway:** Enter your LANCOM's public IP address (WAN IP) or its host name
- **Remote Networks**: Enter the LANCOM's intranet network address ❹ and network mask ❺, separated by a slash

Step 4 – Configure Authentication

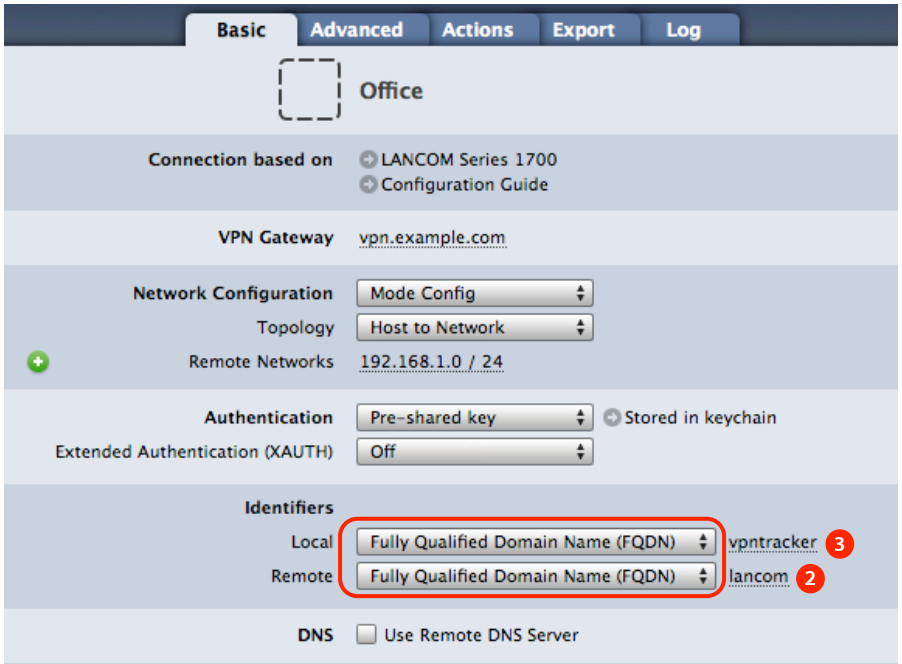
Each VPN tunnel requires mutual authentication of both the client and the gateway. This authentication can be provided by a pre-shared key.



- Click the arrow next to **Pre-shared key**
- Enter the pre-shared key ❶
- Click "Ok"

Step 5 – Configure Identification

In addition to the authentication, client and gateway need to identify themselves. Each identifier has a type and a value.



- **Local Identifier**
  - Select "FQDN" from the pop-up
  - Enter the **remote** identity from the LANCOM ❸
- **Remote Identifier**
  - Select "FQDN" from the pop-up
  - Enter the **local** identity from the LANCOM ❷

You're done! The next task is to test the connection you just configured.

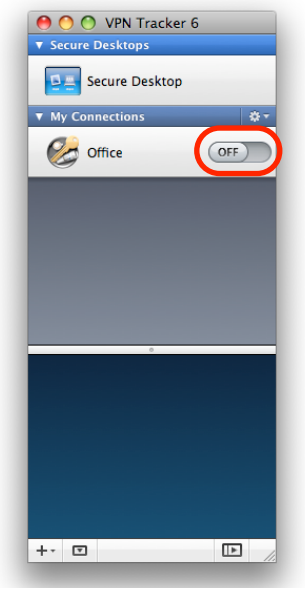
Task 3 – Test the VPN Connection

This section explains how to start and test your VPN connection.

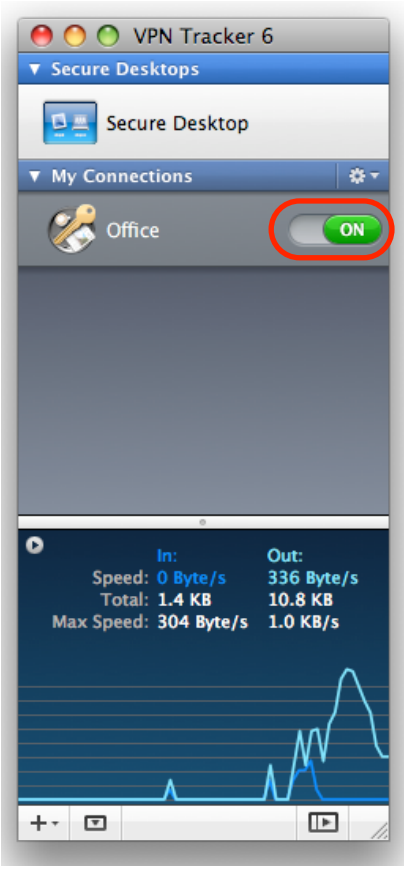
It's time to go out!

You will not be able to test and use your VPN connection from within the intranet that you want to connect to. In order to test your connection, you'll need to connect from a different location. For example, if you are setting up a VPN connection to your office, try it from home. If you are setting up a VPN connection to your home network, try 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 try to connect to http://www.equinux.com
- Start VPN Tracker if it's not already running
- Slide the On/Off slider for the connection you have just configured to **On**



- If the slider goes back to **Off** after starting the connection, 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!

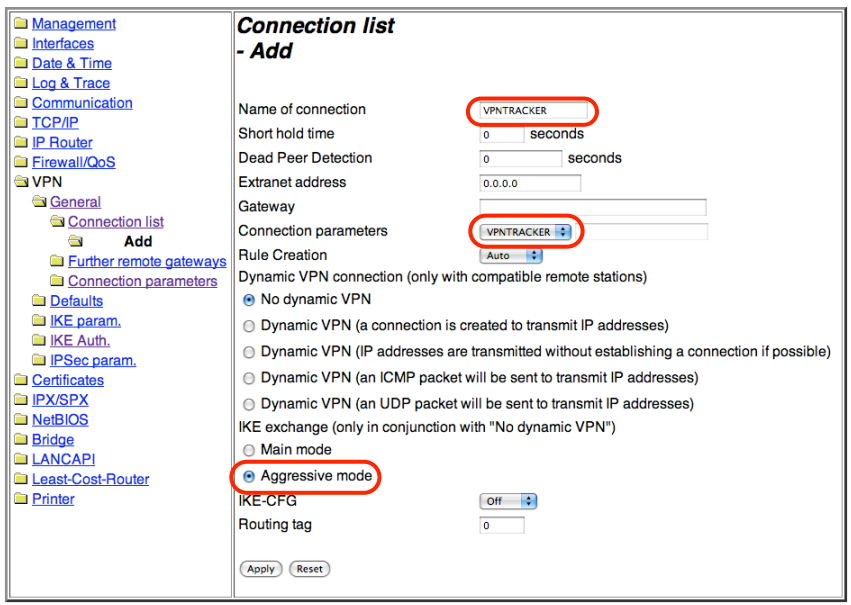
Tip You can re-use this configuration for any additional VPN Tracker clients that need to connect to this VPN . To export connections for other users, VPN Tracker Professional Edition is required.

Setting up a VPN Connection with a Static IP Address

This section explains how to set up a VPN connection that uses a static IP address for use by a single user at a time. The **recommended way** for setting up a VPN connection **is to use the dynamic IP address (Mode Config) setup** described in the previous sections of this document.

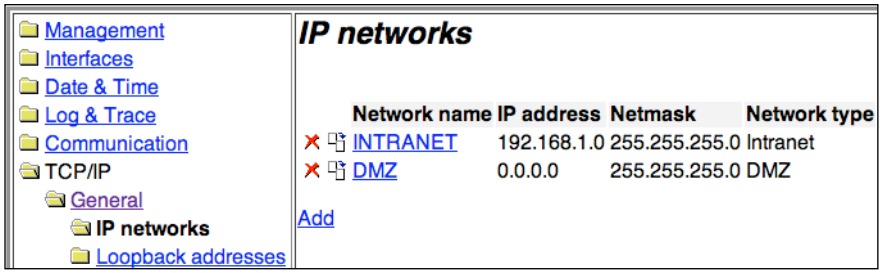
Steps 1 - 4: Follow Steps 1- 4 of "Task 1 – Configure Your VPN Device"

Step 5: Add a VPN Connection



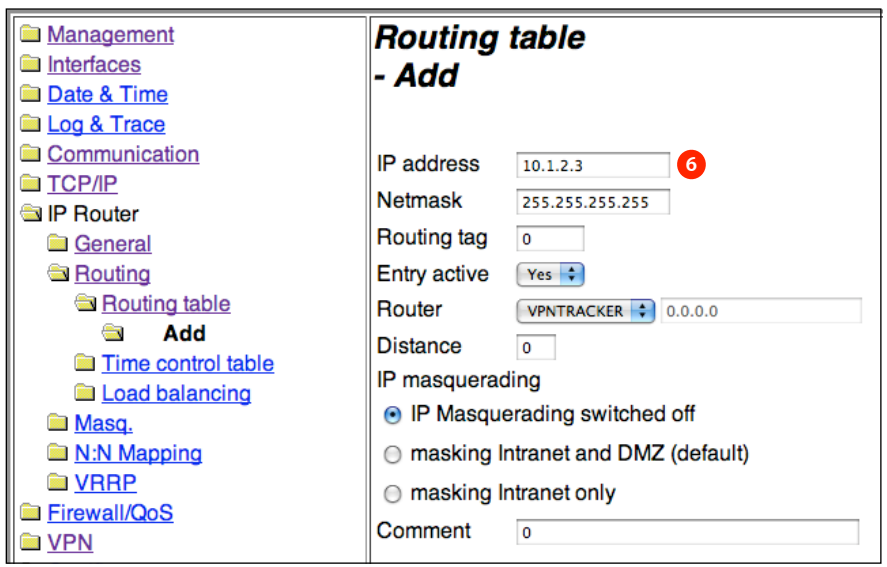
- Select "VPN > General"
- Click "Connection list"
- Click "Add"
- **Name of connection**: VPNTRACKER
- **Connection parameters**: Select "VPNTRACKER" from the pop-up
- **IKE exchange:** Select "Aggressive Mode"
- Click "Apply"

Step 6a: Retrieve your Intranet Information



- Select "TCP/IP > General > IP Networks"
- Find the "INTRANET" entry in the list and write down the IP address and netmask

Step 6b: Add a Route for the Static IP Address



- Select "IP Router > Routing"
- Click "Routing Table"
- Click "Add"
- **IP Address**: Enter an IP address from any private subnet (i.e. 10.x.y.z, 192.168.x.y, 172.16.x.y) that is **not** in the LANCOM's intranet. Here we selected "10.1.2.3" 6
- **Netmask:** Enter 255.255.255.255
- **Router**: Select "VPNTRACKER" from the pop-up
- Click "Apply"

Required Changes in VPN Tracker

Please follow the configuration instructions in "Task 2: Configure VPN Tracker". Then make the following changes:

- **Network Configuration:** select Manual Configuration in the Network Configuration drop-down menu
- A field "Local Address" will appear
- **Local Address**: Enter the IP address that you have configured a route for on the LANCOM ❻

Troubleshooting

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

Can't Establish VPN Connection

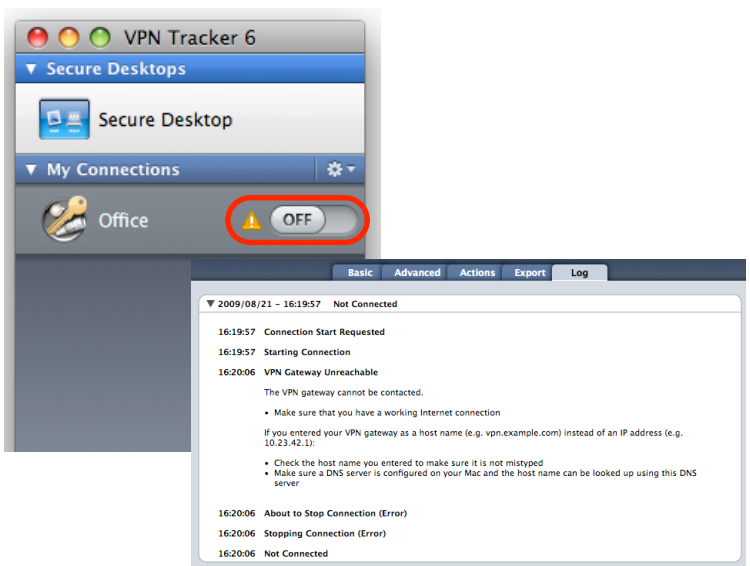
On/Off Slider goes back to "Off" right away

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 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 error (or click the warning triangle to be automatically taken to the "Log" tab).

Depending on the actual problem, VPN Tracker will display detailed suggestions for a solution.



No Access to the Remote Network

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

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

If you are not connecting to the resource by IP address (e.g. 192.168.1.42), but are using a host name (e.g. server.example.com), 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 in VPN Tracker 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 that the IP address you are connecting to is part of the VPN's remote network

Check that the IP address you are connecting to is actually part of the remote network(s). Also double-check the network mask that you have configured for the remote network(s) in VPN Tracker.

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 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 settings
- A detailed description of the problem and the troubleshooting steps you have taken

Appendix: Terminology Matrix

LANCOM	VPN Tracker
Identity	Identifier
IKE-CFG	Mode Config
IKE Exchange	Exchange Mode
IKE Group	Phase 1 Diffie-Hellman (DH) Group
IKE Proposals	Phase 1 Proposals
IPSec Proposals	Phase 2 Proposals
Local	Remote
PFS Group	Perfect Forward Secrecy (PFS) Group
Remote	Local
1 (MODP-768)	Group 1 (768 bit)
2 (MODP-1024)	Group 2 (1024 bit)
5 (MODP-1536)	Group 5 (1536 bit)