VPN Configuration Guide

Linksys (Belkin) LRT214 / LRT224 Gigabit VPN Router
Introduction
This configuration guide helps you configure VPN Tracker and your Linksys VPN Gateway to establish a VPN connection between them.

Prerequisites

Your VPN Gateway
This document applies to the following Linksys VPN firewalls

- LRT214
- LRT224

Documentation for other Linksys devices may be available at http://www.vpntracker.com/interop.

Your Mac

- The configuration described in this guide requires VPN Tracker 7. Make sure you have all available updates installed. The latest VPN Tracker updates can be obtained from http://www.vpntracker.com
- Please see the VPN Tracker website for system requirements.

Using the Configuration Guide

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.

Advanced Topics
In the last part of the guide you’ll see how to expand your VPN to multiple users, and how to send all Internet traffic through the VPN.

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.

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.

If you are setting up VPN on your Linksys firewall for the first time, we strongly recommend using the setup proposed in this guide, and making modifications once that is up and running.
**Scenario**

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

This guide assumes that the Mac running VPN Tracker has Internet connectivity. The office’s Linksys firewall (the “VPN gateway”) is also already connected to the Internet and can be accessed through a static IP address (here: 203.0.113.1) or a DNS host name (here: vpn.example.com).

The VPN gateway’s LAN interface is connected to the internal office network. In our example, the office network is 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 Mac through the VPN. It is called the “Remote Network” in VPN Tracker.

**Terminology**

A VPN connection is often called a **tunnel**. A VPN tunnel is established between two **endpoints**. Here one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is the other endpoint’s **peer**.

For each endpoint, the other endpoint’s settings are **remote**, while its own settings are **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 topology shown below is called **Host to Network**: A single computer, a **host**, establishes a VPN to an entire network “behind” the VPN gateway.

Another useful topology is **Host to Everywhere**. A single computer tunnels all its Internet traffic through the VPN so it looks to hosts on the Internet as having originated from the VPN gateway’s network.
My VPN Gateway Configuration

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. You can print out this checklist to help keep track of the various settings of your Linksys VPN gateway. Not all settings are required for every setup, so don’t worry if some stay empty.

IP Addresses

1. Linksys WAN IP Address: _____ . _____ . _____ . _____ or host name ____________________________


3. Linksys LAN Network Address / Subnet Mask: _____ . _____ . _____ . _____ / _____ . _____ . _____ . _____

Identifiers

4. Linksys Remote Client Identifier Type: __________________________

5. Linksys Remote Client Identifier: _____________________________ = Local (!) Identifier in VPN Tracker

Pre-Shared Key

6. Pre-Shared Key: ____________________________
Task 1 – Linksys Configuration

We will first set up VPN on the Linksys firewall. In case you already have VPN in use on your device, you can skip ahead to steps 3 and 4 to verify your settings.

Step 1 – WAN IP Address
- Go to System Status > WAN Status.
- Write down the WAN 1 IP Address as ➊ on your → Configuration Checklist.

Step 2 – LAN Network
- Go to System Status > System Information
- Write down the LAN IPv4/Subnet Mask as ➋ on your → Configuration Checklist.

Before proceeding to make changes in the following steps, please make sure you have a current backup of the device configuration.
Step 3 – Group VPN Setup

- Go to Configuration > VPN > Client To Gateway

Remote Client Setup: These values correspond to the Local (I) Identifier in VPN Tracker.
- Remote Client: Select Domain Name (FQDN).
- Domain Name: Enter an arbitrary non-existent FQDN, e.g. vpntracker.local.

Local Group Setup: The correct settings should already be filled in. The IP address will be similar to the address you wrote down earlier as (2) but it will have zeros in those places where the subnet mask has zeros. Write it down as (3).

Remote Client Setup: These values correspond to the Local (l) Identifier in VPN Tracker.
- Remote Client: Select Domain Name (FQDN).
- Domain Name: Enter an arbitrary non-existent FQDN, e.g. vpntracker.local.

IPsec Setup: We recommend using the values shown above, as they are more secure than the device’s default settings (DES/MD5/DH Group 1).

If you would like to use different algorithms, you’ll need to match these settings in VPN Tracker on the Advanced tab of your VPN connection.
Pre-Shared Key: Choose a long and complex pre-shared key. Write it down and later store the checklist in a secure location.

Advanced:
- Check the box NAT-Traversal.
Task 2 – VPN Tracker Configuration

After finishing Task 1, you should have a completed → Configuration Checklist containing your Linksys settings. We’ll now create a matching setup in VPN Tracker.

Step 1 – Add a Connection

- Open VPN Tracker.
- Click Add Connection (or click the + button in the lower left corner).
- Select Linksys (Belkin) from the list.
- Select your Linksys model (e.g. LRT214).
- Click Create.

Step 2 – Configure the VPN Connection

- Click Configure and switch to the Basic tab if it is not already displayed.
- VPN Gateway: Enter your Linksys’ public IP address or its host name ❼ from your → Configuration Checklist.
- Remote Networks: Enter your Linksys LAN network address and subnet mask. VPN Tracker will automatically convert the mask (e.g. /255.255.255.0) to CIDR notation (e.g. /24) ⩀.
- Local Identifier: Select Fully Qualified Domain Name (FQDN) ⩄ and enter the domain name that you entered on the Linksys ⩅.
- Click Done.
Task 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 Linksys’ network. In order 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, try it out at home. If you are setting up a VPN connection to your home network, try it from an Internet cafe, or go visit a friend.

Connect to your VPN
- Make sure that your Internet connection is working – open your Internet browser and check that you can open http://www.equinux.com
- Open VPN Tracker.
- Click the On/Off slider for your connection.
- If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.
- You will be prompted to enter your pre-shared key 🌐. Optionally, 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.

Connected!
Connecting may take a couple of seconds. If the On/Off button turns blue that’s great – you’re connected!

Now is a great time to take a look at the VPN Tracker Manual. It shows you how to use your newly established VPN and how to get the most out of it.
Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up:

Click the yellow warning triangle to be taken to the log. The log will explain exactly what the problem is. Follow the steps listed in the log.

Press Cmd-L to open the log in a new window. That way, you can have the log side-by-side with your VPN configuration while making changes to troubleshoot a problem.

In most cases, the advice in the log should be sufficient to resolve the issue. However, VPNs are a complex topic and there might be trickier issues with which you need additional help.

VPN Tracker Manual

The VPN Tracker Manual contains detailed troubleshooting advice.

Frequently Asked Questions (FAQs)

Answers to frequently asked questions can be found at

http://www.vpntracker.com/support

Technical Support

If you're stuck, the technical support team at equinux is here to help. Contact information can be found at

http://www.vpntracker.com/support

Please include the following information with any request for support:

- A description of the problem and any troubleshooting steps that you have already taken.
- Linksys model and the firmware version running on it.
- Screenshots of the VPN settings on the Linksys, including what’s under Advanced (please blank out the pre-shared key before sending screenshots).

A Technical Support Report contains the settings and logs necessary for resolving technical problems. Confidential information (e.g. passwords, private keys for certificates) is not included in a Technical Support Report.
Advanced Topics
This chapter covers advanced topics, such as tunneling all Internet traffic through the VPN (Host to Everywhere), supporting multiple VPN users, and setting a fixed local address for VPN Tracker.

Supporting Multiple Users
Once your VPN expands to multiple users, you need to give each user (each copy of VPN Tracker) a distinct Local Address.

The following section on → The Role of the Local Address in VPN Tracker shows you how to choose a suitable IP address for use n

Your VPN gateway supports a limited number of concurrent VPN connections. Please refer to the device’s data sheet for more information.

The Role of the Local Address in VPN Tracker
The local address is the IP address that your Mac uses in the remote network when connected through VPN.

If the Local Address field on VPN Tracker’s Basic tab is left empty, the Mac’s actual local IP address (as shown in System Preferences > Network) is used.

The Local Address is used as the endpoint (on the VPN Tracker end) of the IPsec Security Association (SA) that is established in phase 2 of the connection process.

When to Set the Local Address in VPN Tracker
It can be beneficial to use fixed local addresses in VPN Tracker, instead of leaving the Local Address field empty when you want to ensure that the local address is independent from the Mac’s actual IP address.

There are some cases where you should always set a local address:
▷ Multiple clients (users/computers) connect to the VPN.
▷ The Linksys device is not the default gateway (router) of its LAN network.

Choosing the Local Address
When connecting to a Linksys device, the local address must not be part of the remote network (i.e. the Linksys’ LAN) and the same local address may not be used by two VPN clients at the same time.

If there is only a single user of the VPN, this will automatically be the case if the local address field is simply left empty, and VPN Tracker therefore uses the Mac’s local IP address. However, in all other circumstances, you should configure a specific address.

Example: The Linksys’ LAN in this example is the network 192.168.13.0/24 (= 192.168.13.0/255.255.255.0). Take the local addresses from an arbitrary private network that is not part of this network. Here we are using 10.22.13.0/24. Each user is assigned their own IP address from that network:
Local Addresses for the More Curious

Why can’t I use a Local Address from my Linksys’ LAN?

It may seem counter-intuitive to use IP addresses for VPN clients that are not part of the Linksys’ LAN. The reason for this is that the Linksys cannot act as an ARP proxy for its VPN clients (ARP is the protocol used for turning IP addresses into Ethernet addresses). Not having an ARP proxy means that nobody will be responding to ARP requests on behalf of VPN clients (VPN clients themselves won’t see ARP requests because they don’t go through the VPN).

If IP addresses from outside the Linksys’ LAN are being used, computers on its LAN will automatically send replies for VPN clients to the Linksys (assuming that it is their default gateway), and therefore no ARP is required (for VPN client IP addresses).

My users connect from different places, from different IPs. Why do I still need to give them different local addresses?

In most cases, the connecting Macs will be behind routers (DSL routers, wireless access points, ...) that perform Network Address Translation (NAT). The Macs themselves will use a private IP address for their Ethernet or Wi-Fi interface, and this is the IP address that is used by VPN Tracker if the local address field is empty.

The likelihood of two Macs ending up using the same local address is very high: Many NAT routers are by default configured to use the same private networks (192.168.1.0/24 and 10.0.0.0/24 are popular choices), and there is a good chance that two clients connecting from entirely different places will have the same local IP address assigned by their respective local router. It is therefore essential to configure a different local address in VPN Tracker for each VPN user if multiple users connect concurrently.

---

<table>
<thead>
<tr>
<th>User</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>alice</td>
<td>10.22.13.1</td>
</tr>
<tr>
<td>bob</td>
<td>10.22.13.2</td>
</tr>
<tr>
<td>charlie</td>
<td>10.22.13.3</td>
</tr>
<tr>
<td>...</td>
<td>10.22.13._</td>
</tr>
</tbody>
</table>

Why do I have to set a fixed Local Address when my Linksys router is not the default gateway (router) in its LAN?

If the Linksys device is not the default gateway, computers that the VPN clients communicate with do not connect to the Internet through the Linksys. In such an environment, you will have to ensure that those computers (and all other resources accessed through the VPN, such as printers and NAS drives) know where to send replies for VPN clients. This is much easier, if you know what IP addresses your VPN clients will be using, and therefore you should give each VPN client a fixed local address.

Once you know which IP addresses VPN clients will be using, you can either

- set a route to the Linksys device for the VPN clients’ IP addresses on each host that needs to communicate with VPN clients, or
- have the default gateway redirect all traffic for the VPN clients’ IP addresses to the Linksys.
Host to Everywhere

To send all Internet traffic through the VPN, you need a connection that uses a “Host to Everywhere” topology.

Sending all Internet traffic through the VPN can be useful when you are in a location where attacks can easily originate from the local network (e.g. unencrypted/public Wi-Fi networks), or in situations where you would like your web surfing traffic to appear to originate from your company’s network.

To tunnel all Internet traffic through the VPN:

- Set up your Linksys router and your VPN Tracker connection as described in the previous chapters. Make sure the connection works as expected and that you can reach hosts on the Linksys’ LAN via VPN.
- Once you everything is working, change the Local Group Setup on the Linksys router to use 0.0.0.0/0.0.0.0 for IP address and subnet mask:

<table>
<thead>
<tr>
<th>LOCAL GROUP SETUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Security Group Type</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
</tbody>
</table>

If you later go back to edit this Group VPN tunnel, some devices change the subnet mask back to 255.255.255.0. Make sure to set it to 0.0.0.0 before saving anything!

- In VPN Tracker, switch the Topology setting to Host to Everywhere:

With this setup, you should be able to establish the VPN connection. However, your Mac will likely seem cut off from the Internet. In fact, you’re probably not cut off from the Internet, but only from your DNS server, so your Mac can no longer translate hostnames (such as www.google.com) into IP addresses.

To set up remote DNS:

- Check the box Use Remote DNS Server in VPN Tracker and enter a suitable DNS server’s IP address:

These DNS servers should work:

- A DNS server you operate yourself on the Linksys’ LAN (it needs to permit queries from VPN Tracker’s Local Address, see → The Role of the Local Address in VPN Tracker).
- A DNS server operated by the ISP your Linksys router is connected to.
- A public DNS server, such as Google DNS (IP address 8.8.8.8). If unsure, use this IP address.