

e·quinux



VPN Quick Configuration Guide

D-Link

© 2010 equinix AG and equinix 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 equinix AG or equinix USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinix logo is a trademark of equinix AG and equinix 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.

equinix 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 equinix 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. equinix is not responsible for printing or clerical errors.

Configuration guide revision 1

Created using Apple Pages.

www.equinix.com

Contents

Introduction.....	5
Using the Configuration Guide	5
Prerequisites	6
Scenario	6
Terminology	7
My VPN Gateway Configuration.....	8
Task 1 – VPN Gateway Configuration.....	9
Step 1 – Address Book Entries	9
Step 2 – Create a Mode Config Pool	10
Step 3 – Add a Pre-Shared Key	10
Step 4 – Add an IPsec Interface	11
Step 5 – Add an XAUTH User	13
Step 6 – Add a User Authentication Rule	13
Step 7 – Add an Access Rule	14
Task 2 – VPN Tracker Configuration.....	15
Step 1 – Add a Connection	15
Step 2 – Configure the VPN Connection	15
Task 3 – Test the VPN Connection.....	16
Troubleshooting.....	18
VPN Connection Fails to Establish	18
No Access to the Remote Network	18
Further Questions?	19

Introduction

This configuration guide helps you configure VPN Tracker and your D-Link router 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 D-Link device.



This guide is a supplement to the documentation included with your 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

Troubleshooting advice 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

- ▶ DFL-200
- ▶ DFL-800
- ▶ Make sure you have installed the newest firmware version available to ensure that you have all security updates and bugfixes.

Your Mac

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

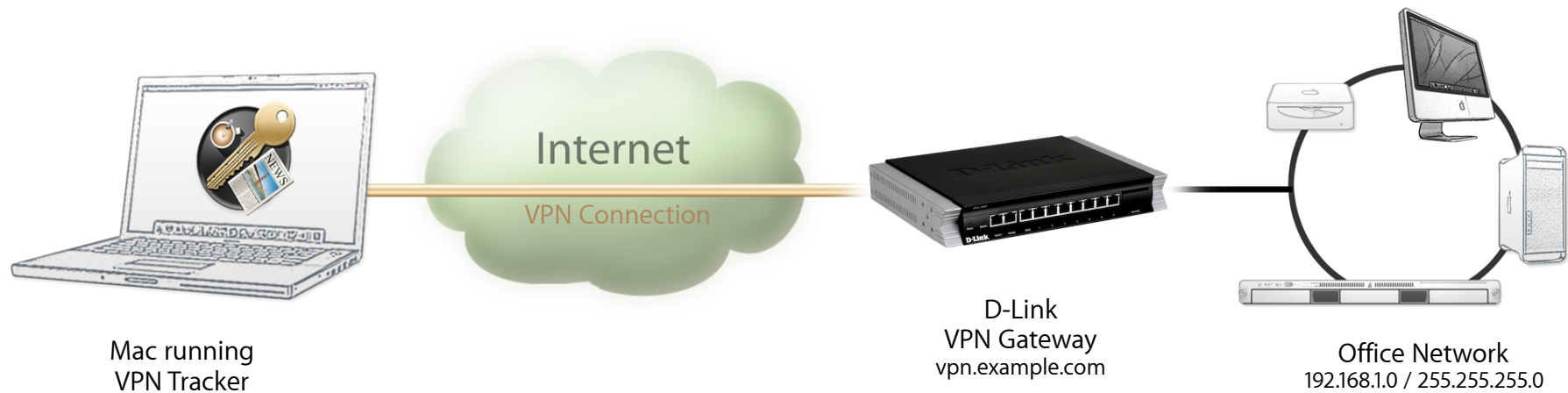
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from <http://www.vpntracker.com>

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 D-Link 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 host name: vpn.example.com.

The VPN gateway has a second network interface which is connected to the internal office network (LAN). In our example, the office network has the IP range 192.168.13.0/24 (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

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 out this checklist to help keep track of the various settings of your D-Link VPN gateway.

Network

- 1 WAN IP Address: _____ (or DNS host name _____)
- 2 LAN Network Address: _____ / _____

Authentication

- 3 Pre-Shared Key: _____

Extended Authentication (XAUTH)

- 4 Username: _____
- 5 Password: _____

Task 1 – VPN Gateway Configuration

We will first set up VPN on the D-Link. If you already have VPN set up, it's helpful to follow along this tutorial to see how settings on the D-Link fit together with VPN Tracker.

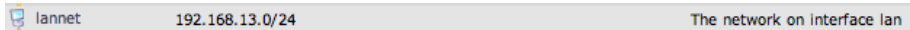
Step 1 – Address Book Entries

▶ Go to **Objects > Address Book > Interface Addresses**

▶ Find the **wan1_ip** entry in the list and write it down on your → *configuration checklist* as ❶



▶ Find the **lannet** entry in the list and write it down on your → *configuration checklist* as ❷

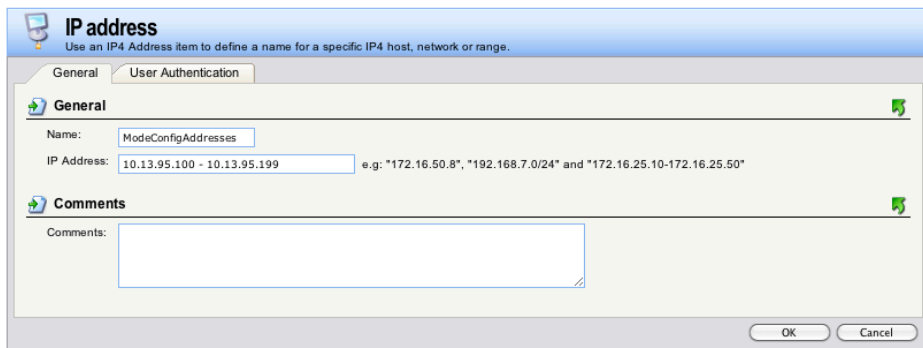


Mode Config Entries

VPN clients will be using Mode Config to automatically receive an IP address to use when connected through VPN. In our setup, we'll be using a pool of addresses that is independent from the D-Link's networks for VPN clients.

▶ Go to **Objects > Address Book**

▶ Click **Add > IP Address**



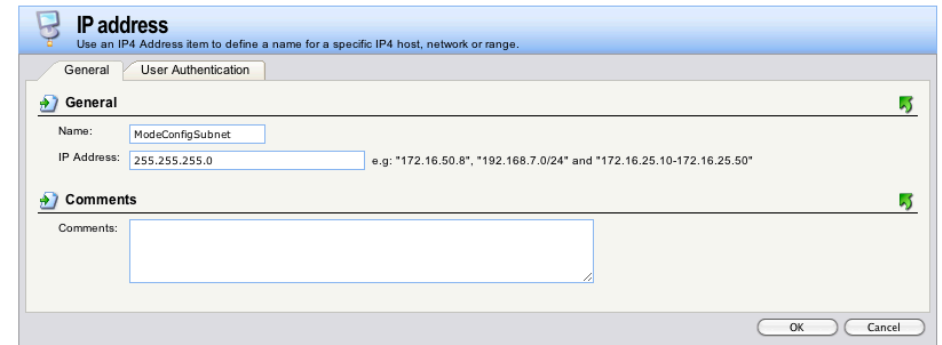
▶ **Name:** Enter a name that allows you to recognize the entry later (e.g. Mode-ConfigAddresses)

▶ **IP Address:** Enter the range of IP addresses that should be assigned to your VPN clients. The IP addresses should come from a [private subnet](#) that is not part of your D-Link's networks. In our example, we're using 10.13.95.100 - 10.13.95.199

▶ Click **OK** to save the entry

For the Mode Config pool, we also need to specify the subnet mask of the network we've chosen.

▶ Click **Add > IP Address**



▶ **Name:** Enter a name that allows you to recognize the entry later (e.g. Mode-ConfigSubnet)

▶ **IP Address:** Enter the subnet mask of the network you have chosen for the address pool (e.g. 255.255.255.0)

▶ Click **OK** to save the entry

Step 2 – Create a Mode Config Pool

- ▶ Go to **Objects > VPN Objects > Config Mode Pool**
- ▶ Click **Add > ConfigModePool**

ConfigModePool
An IKE Config Mode Pool will dynamically assign the IP address, DNS server, WINS server etc. to the VPN client connecting to this gateway.

General

Use a pre-defined IPPool Object
IP Pool: (None)

Use a Static IP Pool
IP Pool: ModeConfigAddresses
Netmask: ModeConfigSubnet

Optional

DNS: (None)
NBNS/WINS: (None)
DHCP: (None)
Subnets: (None)

Comments
Comments:

OK Cancel

- ▶ Check the box **Use a Static IP Pool**
- ▶ **IP Pool:** Select the address book entry created in → *Step 1*
- ▶ **Netmask:** Select the address book entry for the subnet created in → *Step 1*
- ▶ Click **OK** to save the Mode Config pool

Step 3 – Add a Pre-Shared Key

- ▶ Go to **Objects > Authentication Objects**
- ▶ Click **Add > Pre-Shared Key**

Pre-shared key
PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

General
Name: VPNTrackerPSK

Shared Secret

Passphrase
Shared Secret: 3
Confirm Secret:

Hexadecimal Key
Passphrase: _____
Generate Random Key

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

Comments
Comments:

OK Cancel

- ▶ **Name:** Enter a name for the pre-shared key object (e.g. VPNTrackerPSK)
- ▶ Select **Passphrase**
- ▶ **Shared Secret:** Enter a password key for the connection and **confirm it** 3
- ▶ Click **OK**



Mode Config pools can also use a reserved pool of addresses from a DHCP server. However, this limits the available VPN client addresses to the number of leases available on the DHCP server, and is more complex. We recommend going with a separate Mode Config pool first. You can always change to a DHCP server based address pool once you have everything working.

Step 4 – Add an IPsec Interface

- ▶ Go to **Interfaces > IPsec**
- ▶ Click **Add > IPsec Tunnel**

General

The screenshot shows the 'General' configuration page for an IPsec tunnel. The 'Name' field is set to 'VPNTracker'. The 'Local Network' is 'lan-net', 'Remote Network' is 'all-nets', and 'Remote Endpoint' is 'all-nets'. The 'Encapsulation Mode' is 'Tunnel' and the 'IKE Config Mode' is 'ConfigModePool'. Under the 'Algorithms' section, 'IKE Algorithms' is 'High', 'IKE Life Time' is '28800 seconds', 'IPsec Algorithms' is 'High', 'IPsec Life Time' is '3600 seconds', and 'IPsec Life Time' is '0 kilobytes'.

- ▶ **Name:** Enter a name for your tunnel (e.g. VPNTracker)
- ▶ **Local Network:** Select **lan-net**
- ▶ **Remote Network:** Select **all-nets**
- ▶ **Remote Endpoint:** Select **all-nets**
- ▶ **Encapsulation Mode:** Select **Tunnel**
- ▶ **IKE Config Mode:** Select **Static** (ConfigModePool)
- ▶ **IKE Algorithms:** Select **High**
- ▶ **IKE Life Time:** We'll be using the default lifetime of 28800 sec. If you ever decide to change this, you'll also need to modify the phase 1 lifetime in VPN Tracker
- ▶ **IPsec Algorithms:** Select **High**

- ▶ **IPsec Life Time (seconds):** We'll be using the default lifetime of 3600 sec. If you ever decide to change this, you'll also need to modify the phase 2 lifetime in VPN Tracker
- ▶ **IPsec Life Time (kilobytes):** The lifetime in kilobytes must be set to 0

Authentication

The screenshot shows the 'Authentication' configuration page. The 'X.509 Certificate' option is unselected. The 'Root Certificate(s)' section shows 'AdminCert' in the 'Available' list. The 'Pre-shared Key' option is selected, with 'VPNTrackerPSK' chosen in the 'Pre-shared Key' dropdown. The 'Local ID Type' is set to 'Auto'.

- ▶ Select **Pre-shared Key**
- ▶ Select the pre-shared key you created in → *Step 3*
- ▶ **Local ID Type:** Select **Auto**

XAUTH

The screenshot shows the 'IKE XAuth' configuration page. The 'Require IKE XAuth user authentication for inbound IPsec tunnels' option is selected. Below this, there are input fields for 'Username:', 'Password:', and 'Confirm Password:'.

- ▶ Select **Require IKE Xauth user authentication for inbound IPsec tunnels**

Routing

General Authentication XAuth Routing **IKE Settings** Keep-alive Advanced

Automatic Routing

Allow DHCP over IPsec from single-host clients

Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU:

IP Addresses

IP address to use as source IP of the tunnel

Automatically pick the address of a local interface that corresponds to the local net

Specify address manually:

IP Address:

- ▶ **Automatic Routing:** Check **Dynamically add route to the remote network when a tunnel is established**
- ▶ Use the defaults for the remaining settings

General Authentication XAuth Routing **IKE Settings** Keep-alive Advanced

IKE

Main DH Group

Aggressive

Perfect Forward Secrecy

PFS DH Group

Security Association

Per Net

Per Host

Per Port

NAT Traversal

Off

On if supported and NATed

On if supported

Dead Peer Detection

Dead Peer Detection

IKE Settings

- ▶ We will be using the default IKE settings as shown in the screenshot
- ▶ If you make any changes here, you will need to modify the settings in VPN Tracker's Advanced tab to match them

Keep-Alive

General Authentication XAuth Routing **IKE Settings** **Keep-alive** Advanced

Keep-alive

IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuously sending ICMP pings through the tunnel and re-establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP address.

Disabled

Auto

Manually configured IP addresses

Source IP Address:

Destination IP Address:

- ▶ We will be using the default keep-alive settings as shown in the screenshot

Advanced

General Authentication XAuth Routing **IKE Settings** **Keep-alive** **Advanced**

Automatic Route Creation

Automatically add route for remote network.

Add route for remote network

Route Metric:

- ▶ **Uncheck** the box **Add route for remote network**

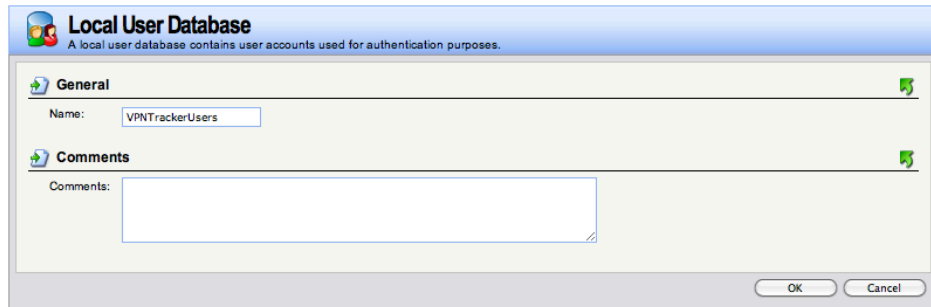


Double-check this step. If you do not uncheck this box, you will cut off your D-Link from the network.

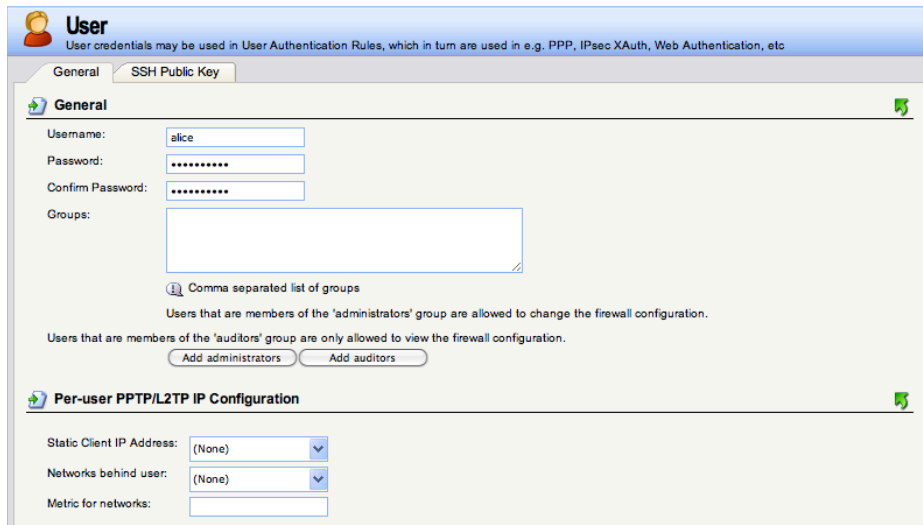
- ▶ Click **OK** to save the IPsec tunnel

Step 5 – Add an XAUTH User

- ▶ Go to **User Authentication > Local User Databases**
- ▶ Click **Add > Local User Database**



- ▶ **Name:** Enter a name for the user database
- ▶ Click **OK** to save the database
- ▶ Click **Add > User**

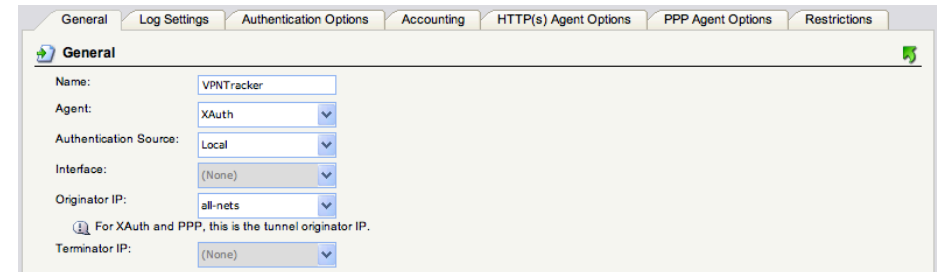


- ▶ **Username:** Enter a name for the user and write it down as 5
- ▶ **Password:** Enter a password for the user and **confirm** it 6
- ▶ Click **OK** to add the user

Step 6 – Add a User Authentication Rule

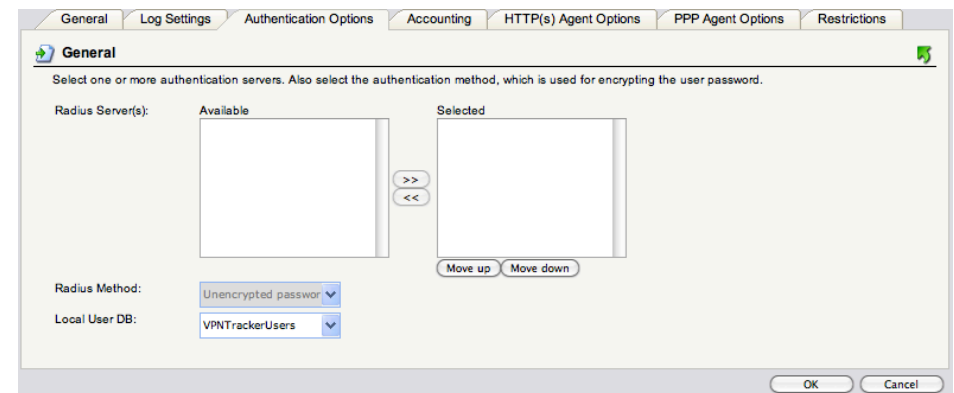
- ▶ Go to **User Authentication > User Authentication Rules**
- ▶ Click **Add > User Authentication Rule**

General



- ▶ **Name:** Enter a name for the authentication rule (e.g. VPN Tracker)
- ▶ **Agent:** Select **XAUTH**
- ▶ **Authentication Source:** Select **Local**
- ▶ **Originator IP:** Select **all-nets**

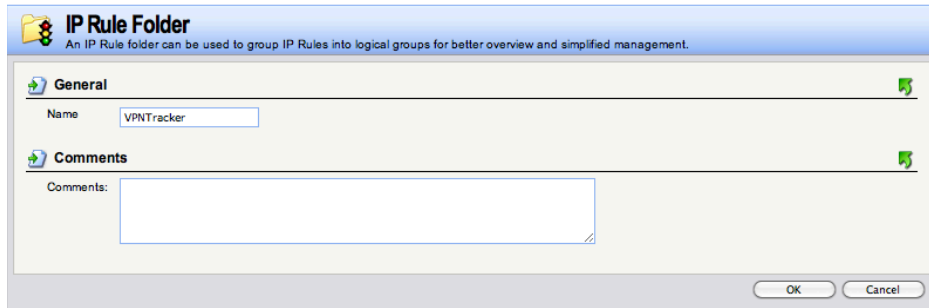
Authentication Options



- ▶ **Local User DB:** Select the database from → Step 5 (e.g. VPNTrackerUsers)
- ▶ All other settings are left at their default values.
- ▶ Click **OK** to add the authentication rule

Step 7 – Add an Access Rule

- ▶ Go to **Rules > IP Rules**
- ▶ Click **Add > IP Rule Folder**



IP Rule Folder
An IP Rule folder can be used to group IP Rules into logical groups for better overview and simplified management.

General

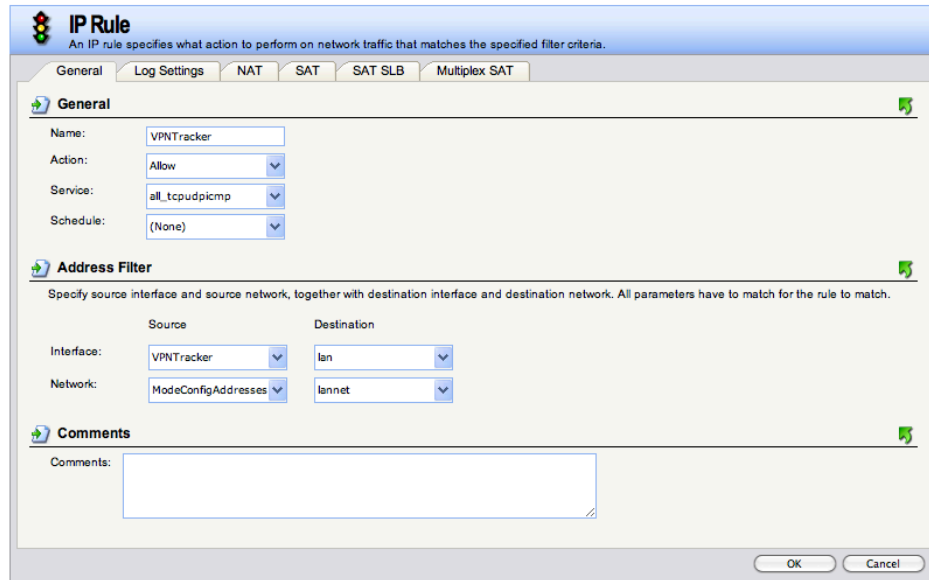
Name:

Comments

Comments:

OK Cancel

- ▶ **Name:** Enter a name for the folder (e.g. VPNTracker)
- ▶ Click **OK** to add the new folder
- ▶ Click **Add > IP Rule**



IP Rule
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT SAT SLB Multiplex SAT

General

Name:

Action:

Service:

Schedule:

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source		Destination	
Interface:	<input type="text" value="VPNTracker"/>	Interface:	<input type="text" value="lan"/>
Network:	<input type="text" value="ModeConfigAddresses"/>	Network:	<input type="text" value="lannet"/>

Comments

Comments:

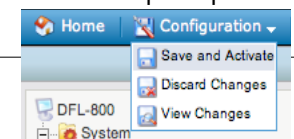
OK Cancel

- ▶ **Name:** Enter a name for the IP rule (e.g. VPNTracker)
- ▶ **Action:** Select **Allow**

- ▶ **Service:** Select the services that VPN users are allowed to access. In most cases, **all_tcpudpicmp** will be a suitable choice
- ▶ **Address Filter**
 - ▶ **Source Interface:** Select the IPsec tunnel interface created in → *Step 4* (e.g. VPNTracker)
 - ▶ **Source Network:** Select the address book entry for your Mode Config IP addresses (e.g. ModeConfigAddresses)
 - ▶ **Destination Interface:** Select the **lan** interface
 - ▶ **Destination Network:** Select the **lannet** network
- ▶ Click **OK** to add the IP rule



Before being able to use your newly set up VPN tunnel, you will need to activate the configuration on the device: Click **Configuration > Save and Activate**, then follow the prompts to save and activate your configuration.

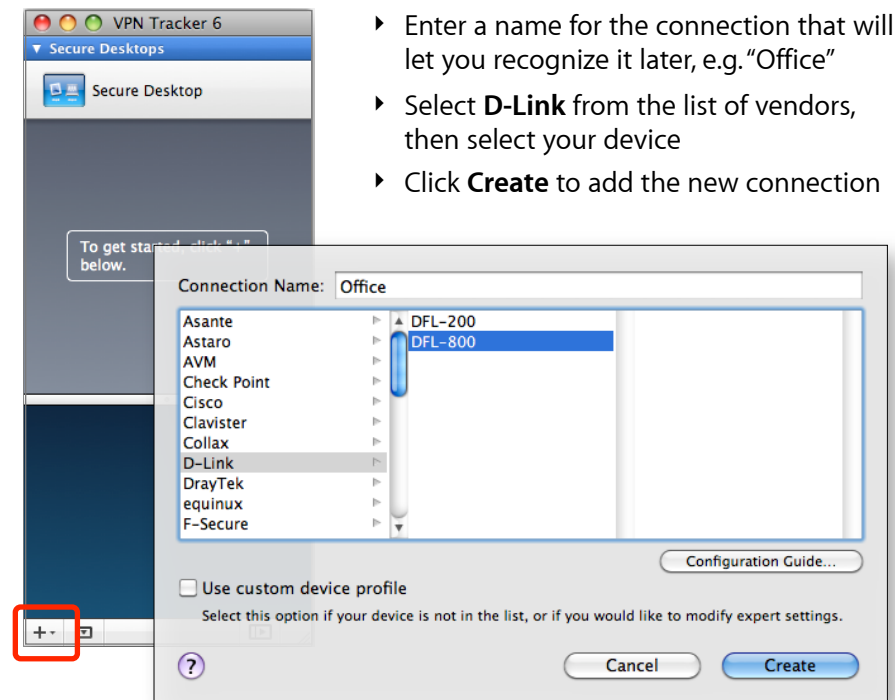


Task 2 – VPN Tracker Configuration

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

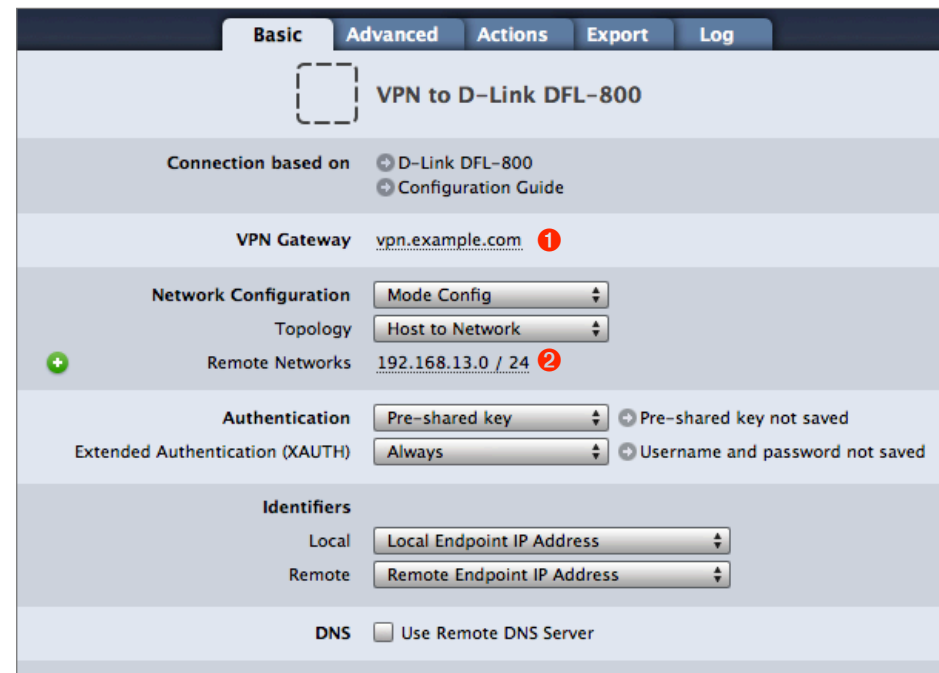
Step 1 – Add a Connection

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



Step 2 – Configure the VPN Connection

Once you have added the new connections, there are a few settings that need to be customized to match what is configured on your D-Link.



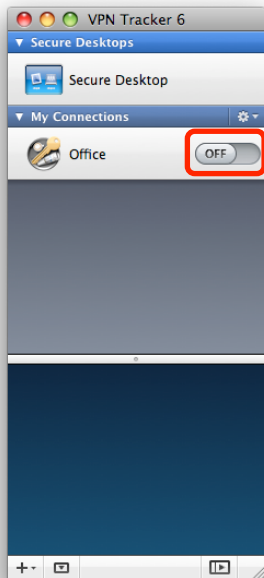
Task 3 – Test the VPN Connection

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 internal network that you want to connect to. 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, 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 try to 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:

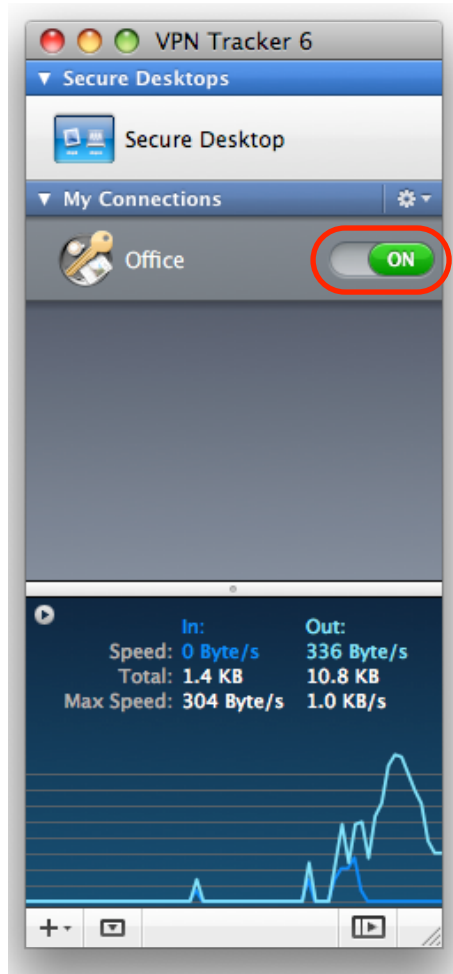


- ▶ **Pre-shared key:** Enter the pre-shared key that you configured on the VPN gateway **3**
- ▶ Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- ▶ Click **OK**

When prompted for your Extended Authentication (XAUTH) credentials:



- ▶ **User Name:** Enter the name of the user you have added on the device **4**
- ▶ **Password:** Enter the password for the user **5**
- ▶ 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**



- ▶ If the slider goes back to **Off** after starting the connection, or after entering your pre-shared key or your XAUTH credentials, 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.

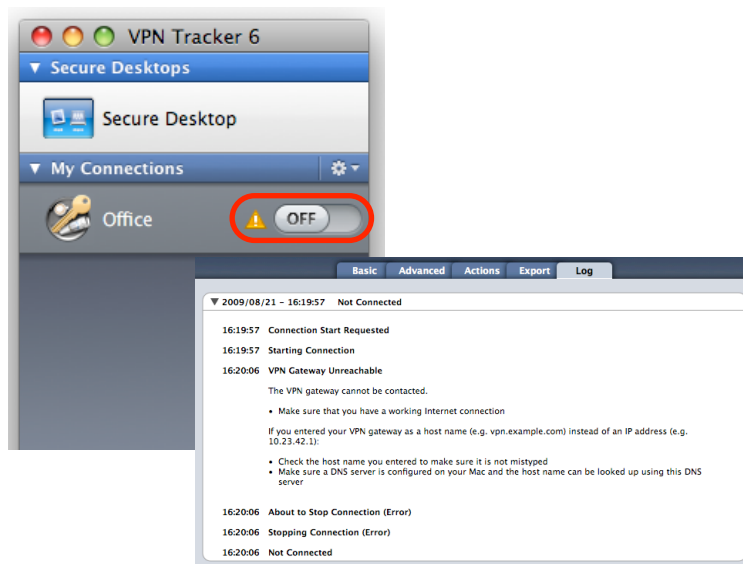
VPN Connection Fails to Establish

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 error (or click the warning triangle to be automatically taken to the “Log” tab). 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. 192.168.13.42), 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 network(s) permitted for VPN Access

Check that the IP address you are connecting to is actually part of the remote network(s) in VPN Tracker, and make sure this network matches the Local Network configured for the IPsec tunnel interface on the D-Link, and make sure you have completed → Step 7 to add an appropriate access rule.

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