

e·quinux



VPN Quick Configuration Guide

Astaro Security Gateway 7.5

© 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 2

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 – WAN IP	9
Step 2 – Create a User	9
Step 3 – Configure the VPN Connection	10
Step 4A – Download Certificates	11
Step 4B – Add a Packet Filter Rule	11
Task 2 – VPN Tracker Configuration.....	12
Step 1 – Add a Connection	12
Step 2 – Configure the VPN Connection	12
Task 3 – Test the VPN Connection.....	15
Troubleshooting.....	17
VPN Connection Fails to Establish	17
No Access to the Remote Network	17
Further Questions?	18

Introduction

This configuration guide helps you configure VPN Tracker and your Astaro Security 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 Astaro.



This guide is a supplement to the documentation included with your Astaro, 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 Advanced Topics

Troubleshooting advice and additional tips can be found in the final part of this guide.



If you are setting up VPN on your Astaro 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 is based on Astaro Security Gateway 7.5
- ▶ Make sure you have installed the newest 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

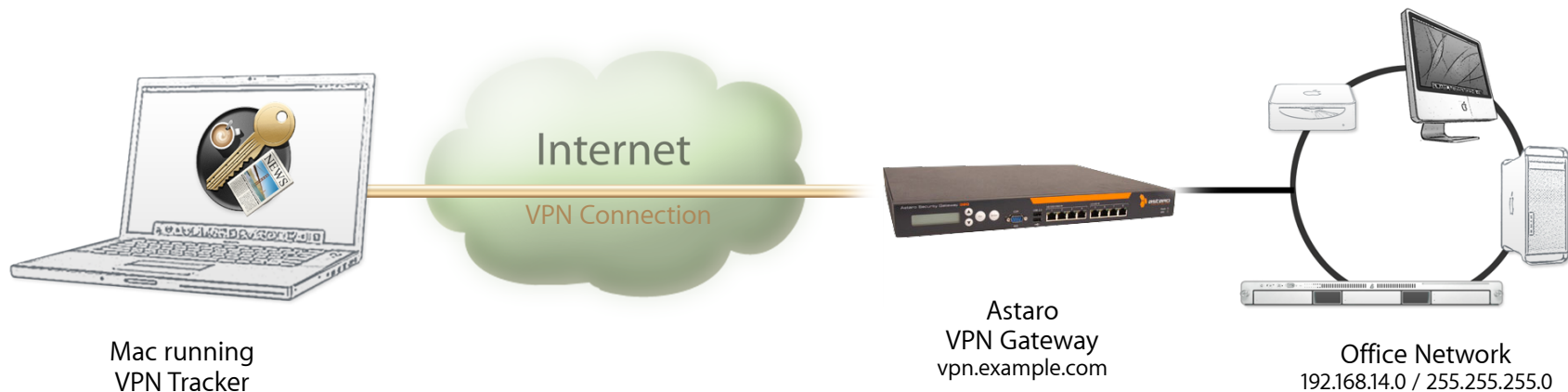
The configuration described in this guide requires VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker updates can always be obtained from <http://www.vpntracker.com>

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 Astaro 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 192.168.14.0/255.255.255.0). 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 Astaro VPN gateway.

IP Addresses

❶ WAN IP Address: _____._____._____._____ or hostname _____

❷ Local Network: _____._____._____._____ / _____

User Authentication (XAUTH)

❸ Username: _____

❹ Password: _____

❺ Email Address: _____ @ _____

❻ IP Address: _____._____._____._____

VPN Connection (for Pre-Shared Key only)

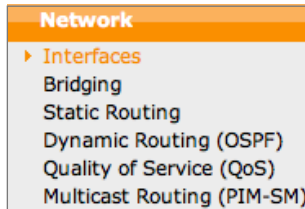
❼ Pre-Shared Key: _____

Task 1 – VPN Gateway Configuration

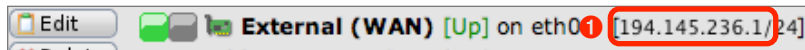
We will first set up VPN on the Astaro. If you already have VPN set up, it's helpful to follow along this tutorial to see how settings on the Astaro fit together with VPN Tracker.

Step 1 – WAN IP

- ▶ Connect to your Astaro's web interface
- ▶ Go to **Network > Interfaces**



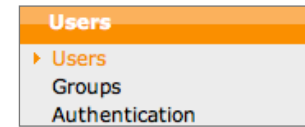
- ▶ Write down the IP address of the **external (WAN) interface** (the part before the forward slash "/") as ❶ on your → *Configuration Checklist*



If your Astaro is reachable through a hostname (permanent DNS entry or using a DynDNS service), you can use its hostname instead of the IP address to contact it.

Step 2 – Create a User

- ▶ Go to **Users > Users**



- ▶ Click **New user...**

- ▶ **Username:** Enter a username for your new user (here: alice) and write it down as ❸
- ▶ **Real Name:** Enter the real name of your user (here: Alice)
- ▶ **Email Address:** Enter an email address ❺
- ▶ **Password:** Enter a password for your user and enter it again in the **Repeat** text field to confirm it ❹
- ▶ **Use static remote access IP:** This is the IP address your user will be using while connected to the VPN. Use a [private IP address](#) that is not used by any other VPN user and is **not** be part of your Astaro's network(s). Here we're using 10.1.2.3 ❻

Step 3 – Configure the VPN Connection

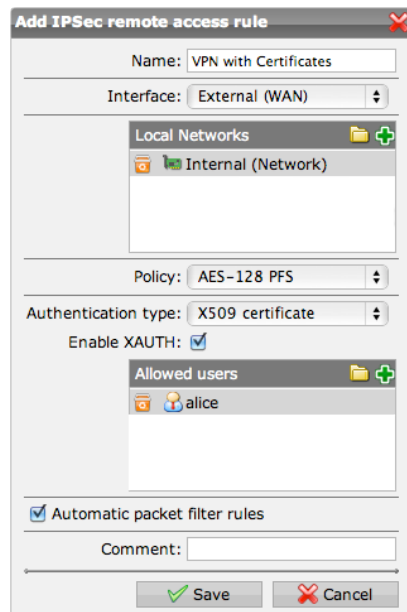
- ▶ Go to **Remote Access > IPsec**



- ▶ Click **New IPsec remote access rule...**

You will have to decide whether to use certificates or whether to use a pre-shared key (a password that is the same for all users of the VPN connection). Certificates are more secure, but need to be distributed to users. In both cases, **users will also have an individual password** in addition to the pre-shared key or certificate.

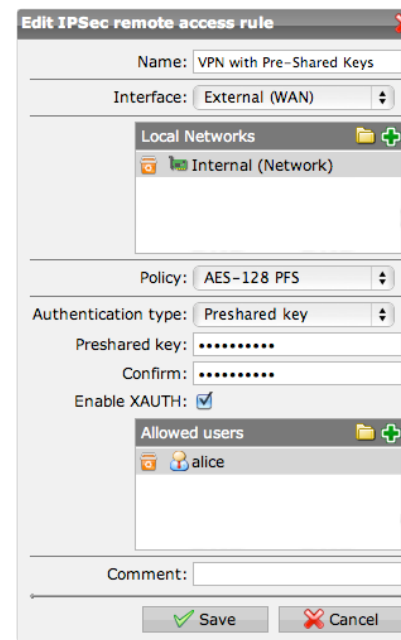
Option A: Certificates



- ▶ **Name:** Enter a name for the connection
- ▶ **Interface:** Select **External (WAN)**
- ▶ **Local Networks:** Add the network your users are to access through VPN. In most cases, this will be your internal network. Write down the network as In our example, the Astaro's LAN is 192.168.14.0/24, and we simply added the built-in address object **Internal (Network)** representing it.
- ▶ **Policy:** Select one of the policies available on your Astaro. If you select a different policy than AES-128 PFS, configure the Advanced settings in VPN Tracker (Phase 1 / 2) to match it.

- ▶ **Authentication Type:** Select **X509 certificate**
- ▶ Check the box **Enable XAUTH** to authenticate each user with their user-name and password in addition to their certificate
- ▶ **Allowed users:** Add the user your created in Step 2
- ▶ Check the box **Automatic packet filter rules** to have the Astaro automatically add rules to permit the user access to the network(s) configured under Local Networks when they connect through VPN.

Option B: Pre-Shared Key



- ▶ **Name:** Enter a name for the connection
- ▶ **Interface:** Select **External (WAN)**
- ▶ **Local Networks:** Add the network your users are to access through VPN. In most cases, this will be your internal network. Write down the network as In our example, the Astaro's LAN is 192.168.14.0/24, and we simply added the built-in address object **Internal (Network)** representing it.
- ▶ **Policy:** Select one of the policies available on your Astaro. If you select a different policy than AES-128 PFS, configure the Advanced settings in VPN Tracker (Phase 1 / 2) to match it.

- ▶ **Authentication Type:** Select **Pre-Shared Key**
- ▶ **Pre-Shared Key:** Enter a strong password and **confirm** it
- ▶ Check the box **Enable XAUTH** to authenticate each user with their user-name and password in addition to their certificate
- ▶ **Allowed users:** Add the user your created in → *Step 2*

Step 4A – Download Certificates



This step applies if you selected **X509 Certificates** in → *Step 3*.
If you selected pre-shared key, go to → *Step 4B*

- ▶ Go to **Remote Access > Certificate Management**



- ▶ Download your **user's certificate** in **PKCS#12** format (i.e. with private key)
- ▶ Download your **Astaro's certificate** in **PEM** format (i.e. without private key). The Astaro's certificate is usually called "Local X509 Cert" in the list.
- ▶ Copy both downloaded certificates to the **Mac running VPN Tracker** and double-click them to **import them into the Mac OS X keychain**:

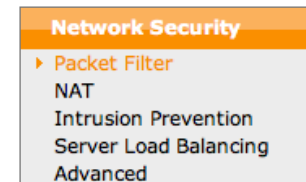
	Alice	certificate
	alice (X509 User Cert)	private key
	astaro	certificate

Step 4B – Add a Packet Filter Rule

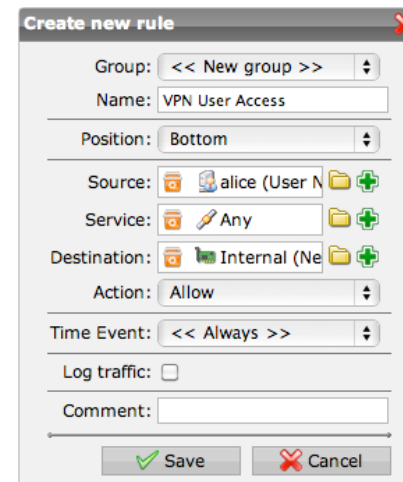


This step applies if you selected **Pre-Shared Key** in → *Step 3*

- ▶ Go to **Network Security > Packet Filter**



- ▶ Click **New rule...**



- ▶ **Group:** Select an existing rule group, or add a new one.
- ▶ **Source:** Add the pre-defined **User Network** for the user created in step 2
- ▶ **Service:** Any
- ▶ **Destination:** Add the same network that you added for the Local Network in Step 3, usually your internal network
- ▶ Click **Save**

- ▶ Click enabled/disabled indicator next to the rule in the list to enable it (the indicator must turn **green**)

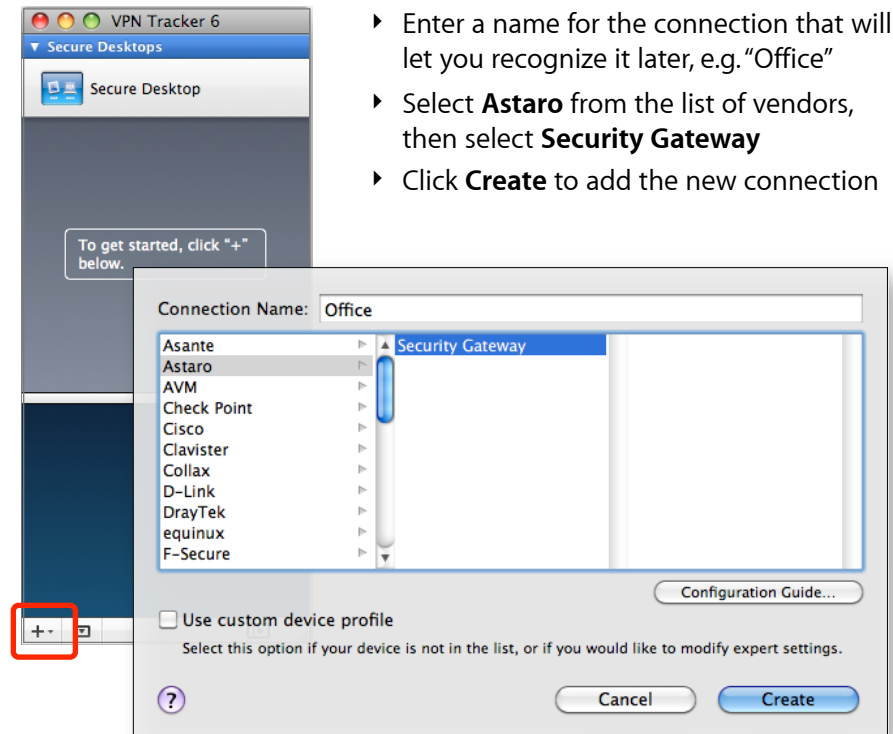


Task 2 – VPN Tracker Configuration

After finishing task 1, you should now have a completed → *configuration checklist* containing your Astaro'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:



- ▶ Enter a name for the connection that will let you recognize it later, e.g. "Office"
- ▶ Select **Astaro** from the list of vendors, then select **Security Gateway**
- ▶ Click **Create** to add the new connection

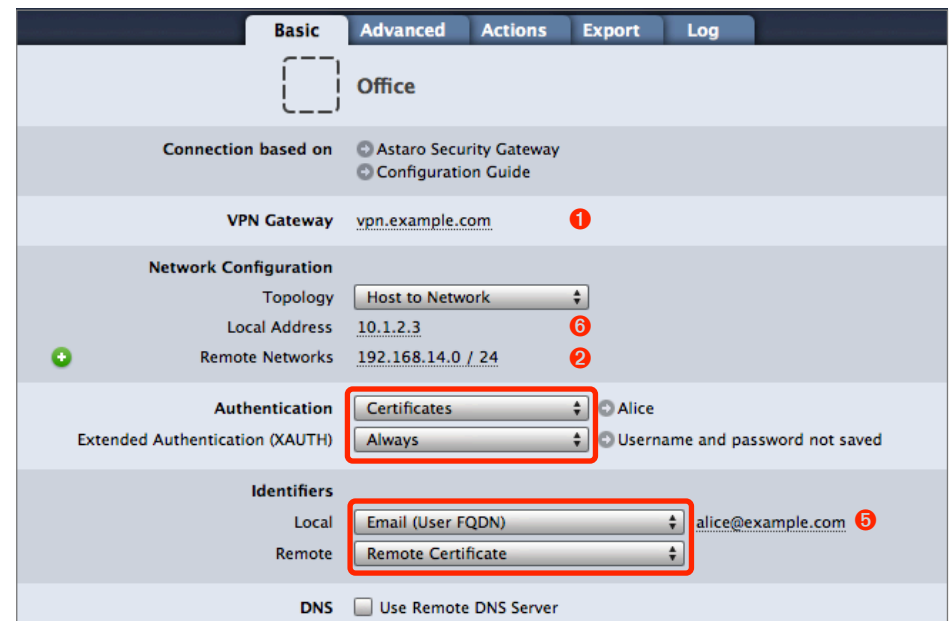
Step 2 – Configure the VPN Connection

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

Basic Settings (Certificates)



This step applies if you selected **X509 Certificates** in → *Step 3*. If you selected pre-shared key, go to → *Basic Settings (Pre-Shared Key)*.



Basic | Advanced | Actions | Export | Log

Office

Connection based on Astaro Security Gateway Configuration Guide

VPN Gateway vpn.example.com 1

Network Configuration

Topology Host to Network

Local Address 10.1.2.3 6

Remote Networks 192.168.14.0 / 24 2

Authentication Certificates Alice

Extended Authentication (XAUTH) Always Username and password not saved

Identifiers

Local Email (User FQDN) alice@example.com 5

Remote Remote Certificate

DNS Use Remote DNS Server

VPN Gateway

Enter the **external (WAN) IP address of your Astaro** that you wrote down as 1. If your Astaro has a DNS host name (such as vpn.example.com in our example), you can use it instead.

Local Address

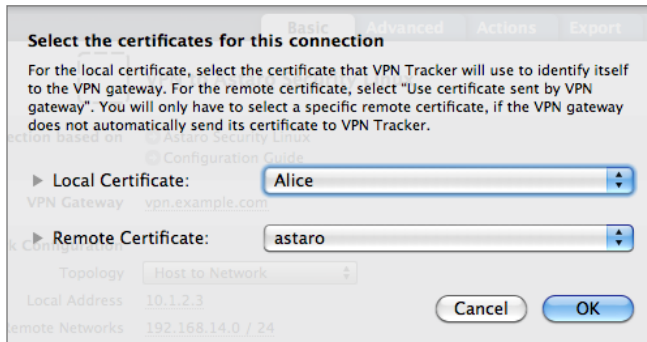
Enter the **static IP address configured for your user** 6

Remote Networks

Enter the network configured as the **local network of the VPN connection** ②

Authentication

Switch the authentication to **Certificates**. You will get prompted to select your certificate. Select your user's certificate as the **Local Certificate**, and your Astaro's certificate as the remote certificate.



Extended Authentication (XAUTH)

Select **Always**.

Local Identifier

Select **Email (User FQDN)** and enter the email address you configured for your user on the Astaro ⑤

Remote Identifier

Select **Remote Certificate**.

Continue with → *Advanced Settings (Certificates and Pre-Shared Key)*

Basic Settings (Pre-Shared Key)



This step applies if you selected **Pre-Shared Key** in → *Step 3*. For **Certificates**, continue with → *Advanced Settings (Certificates and Pre-Shared Key)* on the next page.



VPN Gateway

Enter the **external (WAN) IP address of your Astaro** that you wrote down as ①. If your Astaro has a DNS host name (such as vpn.example.com in our example), you can use it instead.

Local Address

Enter the **static IP address configured for your user** ⑥


Remote Networks

Enter the network configured as the **local network of the VPN connection** ②

Extended Authentication (XAUTH)

Select **Always**.

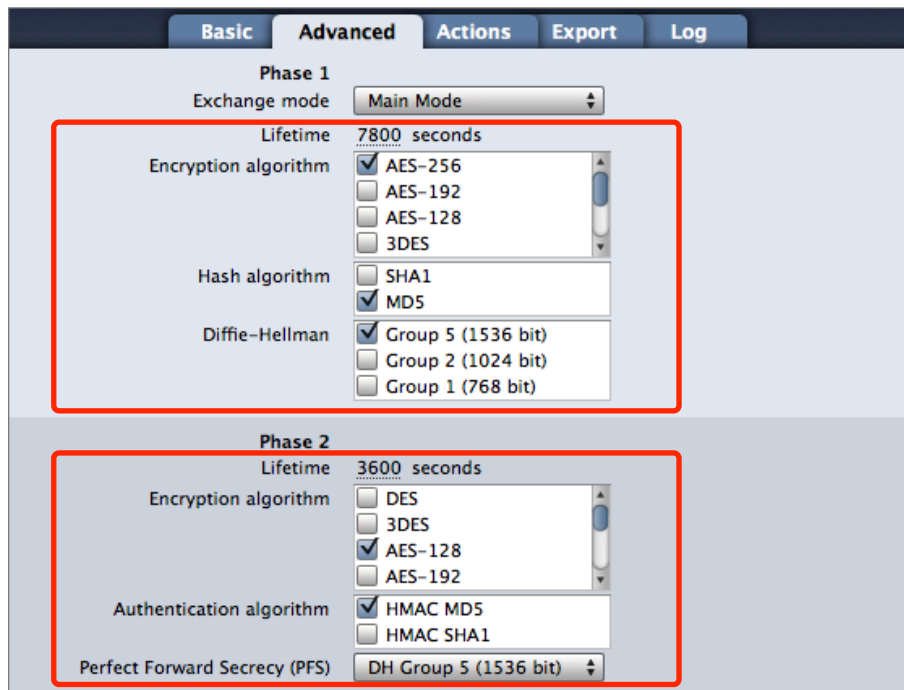
Local Identifier

Select **Email (User FQDN)** and enter the email address you configured for your user on the Astaro 

Remote Identifier

Select **Remote Endpoint IP Address**.

Advanced Settings (Certificates and Pre-Shared Key)



- ▶ Select only those algorithms for phase 1 and 2 that are part of the policy selected for your VPN connection on the Astaro. In our example, we selected

the **AES-128 PFS** policy. We can easily see what exactly this policy requires when looking at **Remote Access > IPsec > Policies** on the Astaro:

Policy Name	IKE Settings	IPSec Settings	Lifetime
AES-128 PFS	AES 256 / MD5 / Group 5: MODP 1536	AES 128 / MD5 / Null (None)	7800 seconds / 3600 seconds
	Compression off, not using strict policy.		
AES-256	AES 256 / MD5 / Group 5: MODP 1536	AES 128 / MD5 / Group 5: MODP 1536	7800 seconds / 3600 seconds
	Compression off, not using strict policy.		

- ▶ For the **AES-128 PFS** policy we selected in → *Step 3* this means
 - ▶ **Phase 1:** 7800 seconds / AES-256 / MD5 / DH Group 5 (1536 bit)
 - ▶ **Phase 2:** 3600 seconds / AES-128 / HMAC MD5 / DH Group 5 (1536 bit)



AES-256 requires VPN Tracker Professional Edition or Player Edition*. If you are using **VPN Tracker Personal Edition**, you can use AES-128 instead, even though the policy specifies AES-256 as long as the policy does not strictly enforce encryption algorithms (option **Strict Policy** on the Astaro).

* VPN Tracker Player Edition cannot be used to set up connections. Connections for use with Player Edition must be exported from VPN Tracker Professional Edition.

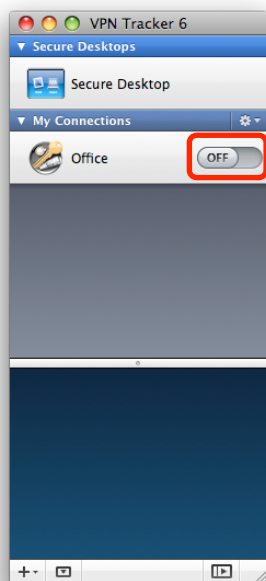
Task 3 – Test the VPN Connection

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**

(Pre-Shared Key only) When prompted for your pre-shared key:

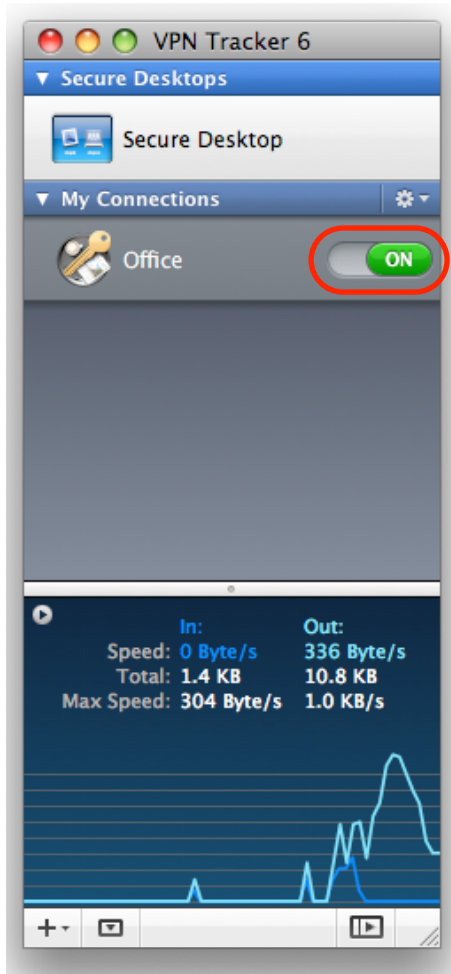


- ▶ **Pre-shared key:** Enter the passphrase that you configured on the Astaro for the VPN connection 7
- ▶ Optional: Check the box **Store in Keychain** to save the password in your keychain so you are not asked for it again when connecting the next time
- ▶ Click **OK**

When prompted for your Extended Authentication (XAUTH) credentials:



- ▶ User Name: Enter the name of the user you have added on the Astaro 2
- ▶ Password: Enter the password for the user 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**



- ▶ 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.

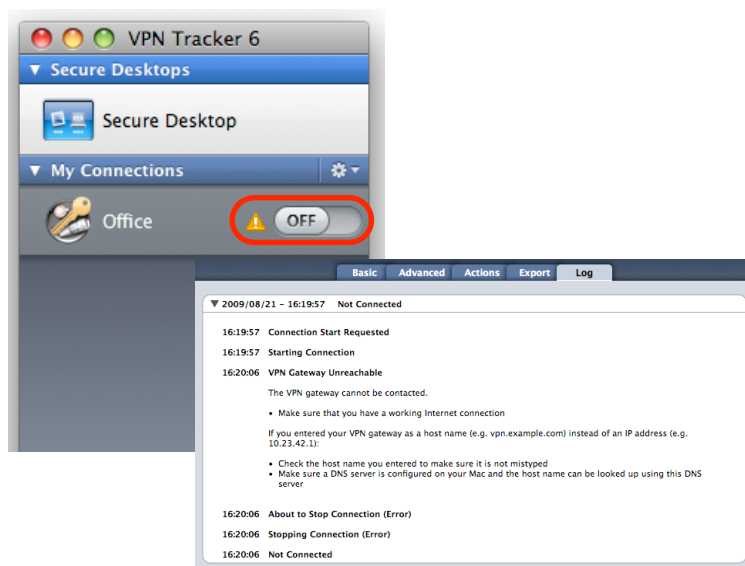
VPN Connection Fails to Establish

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 VPN connection on the Astaro. Also ensure that the checkbox **Automatic packet filter rules** is checked (if using certificates) or that you have created the appropriate packet filter rules yourself (if using pre-shared key, see → *Step 4B*)

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