

e·quinux



# VPN Configuration Guide

Juniper Networks NetScreen / SSG / ISG Series

equinix AG and equinix USA, Inc.

© 2009 equinix 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 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.

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

[www.equinix.com](http://www.equinix.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.

Juniper Networks, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the U.S. and other countries.

**equinix 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 equinix has been advised of the possibility of such damages.**

<b>Introduction .....</b>	<b>5</b>
Important Prerequisites.....	6
Scenario .....	7
Terminology.....	8
<b>My VPN Gateway Configuration.....</b>	<b>9</b>
<b>Task 1 – Configure Your VPN Gateway .....</b>	<b>10</b>
Step 1– Set up an IP address pool.....	10
Step 2 – Create a Shared IKE User .....	12
Step 3 – Create a Group for the Shared IKE User.....	13
Step 4 – Create Extended Authentication (XAUTH) Users.....	14
Step 5 – Configure the XAUTH Settings.....	15
Step 6 – Configure the Phase 1 Settings (Gateway Settings) .....	16
Step 7 – Configure the Phase 2 Settings (VPN Settings) .....	19
Step 8 – Add a Policy.....	21
Step 9 – Find Your VPN Gateway’s Public IP Address.....	22
<b>Task 2 – Configure VPN Tracker .....</b>	<b>23</b>
Step 1 - Create a New Connection .....	23
Step 2 – Configure the VPN Connection .....	24
<b>Task 3 – Test the VPN Connection .....</b>	<b>25</b>
It’s time to go out!.....	25
Start your connection .....	25
<b>Supporting Multiple Users .....</b>	<b>28</b>
Adding Users on the VPN Gateway .....	28
Deploying VPN Connections to Your Users.....	29
<b>Troubleshooting .....</b>	<b>30</b>
VPN Connection Fails to Establish.....	30

No Access to the Remote Network.....	31
<b>Appendix.....</b>	<b>33</b>
Predefined Security Levels.....	33



# Introduction

This document describes how VPN Tracker can be used to establish a connection between a Mac running Mac OS X and a Juniper Networks firewall/IPsec VPN device running the ScreenOS firmware.

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

## VPN Gateway Configuration

The first part of this guide will show you how to configure a VPN tunnel on your Juniper Networks firewall/IPsec VPN device.

## 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.

## Troubleshooting

Troubleshooting tips can be found in the last part of this guide. We have also included an appendix with additional useful information.

**Tip** If you are setting up VPN on your device for the first time, we strongly recommend you start out with the tutorial-style setup in the first and second part of this document. Your device's configuration has strong interdependencies between settings, so it is recommended to follow the order laid out in this guide when setting up the device.

## Important Prerequisites

### Your VPN Gateway

- ▶ This guide applies to the following Juniper Networks firewall/IPsec VPN devices running ScreenOS (see <http://www.vpntracker.com/interop> for details)
  - SSG series
  - ISG series
  - NetScreen series<sup>1</sup>
- ▶ Make sure you have the newest ScreenOS version installed that is available for your device. This guide is based on ScreenOS 6.2.0<sup>2</sup>

### Your Mac

- ▶ VPN Tracker runs on Mac OS X 10.4 or 10.5
- ▶ The configuration described in this guide requires at least VPN Tracker 6. Make sure you have all available updates installed. The latest VPN Tracker release can always be obtained from <http://www.vpntracker.com>

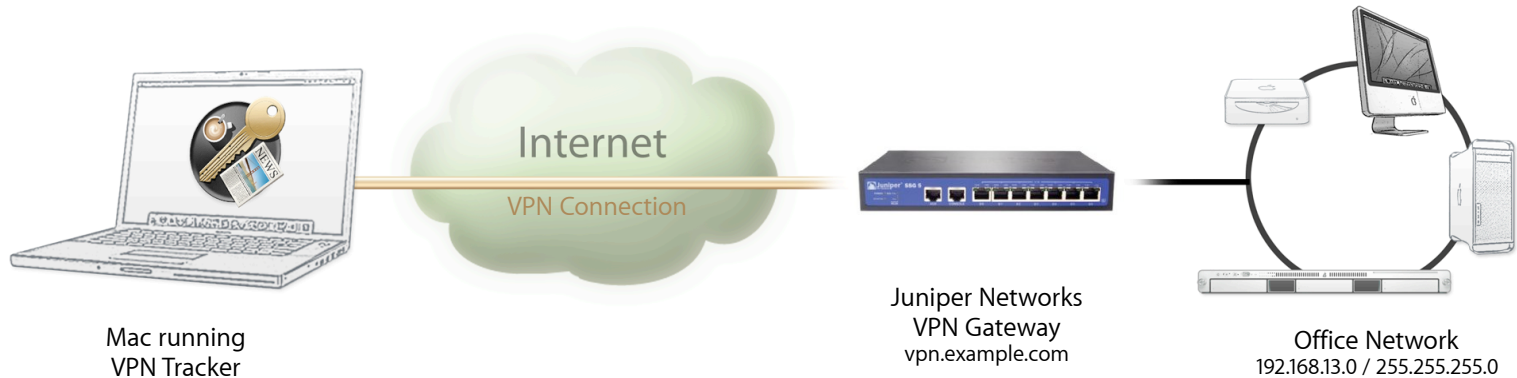
---

<sup>1</sup> The most recent ScreenOS version may not be available for your NetScreen device. In that case, you should be running the latest ScreenOS version available for your particular device.

<sup>2</sup> If you are using a different ScreenOS version, some settings may look different. Wherever we are aware of these differences, we have noted them in *italics* next to the affected setting.

## 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 NetScreen (or SSG, or ISG) 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” (or “peers”). 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.



# 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 form to help keep track of the various settings of your Juniper Networks device.

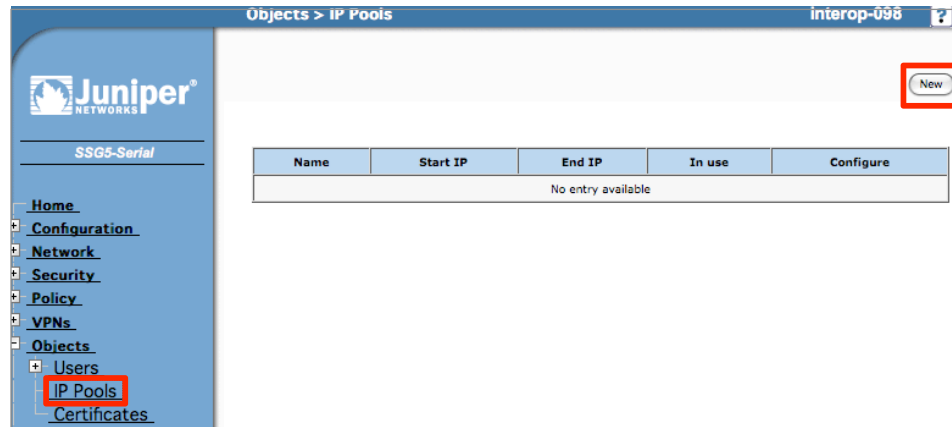
- 1 IKE Identity: \_\_\_\_\_
  
- 2 XAUTH User Name: \_\_\_\_\_
  
- 3 XAUTH Password: \_\_\_\_\_
  
- 4 Pre-Shared Key: \_\_\_\_\_
  
- 5 Remote Network: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ / \_\_\_\_\_  
  
or \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ / \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_
  
- 6 VPN Gateway's Public (WAN) IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ or hostname \_\_\_\_\_

# Task 1 – Configure Your VPN Gateway

The ScreenOS configuration interface is quite complex and may be a bit daunting at first. If you are unfamiliar with the device's configuration, try to keep to these configuration steps as closely as possible, and in the order outlined in this document. They will provide you with a VPN configuration that works well – for one user, or your entire company.

## Step 1– Set up an IP address pool

The “virtual” IP addresses VPN clients use on the device's LAN are distributed from the IP address pool that you will configure in this step.



- ▶ If you have not already done so, log into your device's web configuration interface now.
- ▶ Go to the section “**Objects > IP Pools**”
- ▶ Click “**New**”

**Note** At the time of writing, the ScreenOS web configuration interface did not work very well with the Safari web browser. Should you encounter any problems with the web configuration interface, you might want to try using a different web browser for this task.

<b>IP Pool Name</b>	VPN Client IPs
<b>Start IP</b>	10.13.98.100
<b>End IP</b>	10.13.98.199

- ▶ **IP Pool Name:** Enter a name that will allow you to recognize this IP pool later
- ▶ **Start IP:** Enter the first IP address in the range of IP addresses the IP pool should contain. In our example, we are using the IP address 10.13.98.100. Refer to the guidelines below when selecting a range suitable for your particular scenario.
- ▶ **End IP:** Enter the last IP address in the range of IP addresses the IP pool should contain. In our example, we are using the IP address 10.13.98.199
- ▶ Click **“OK”** to save your new IP address pool

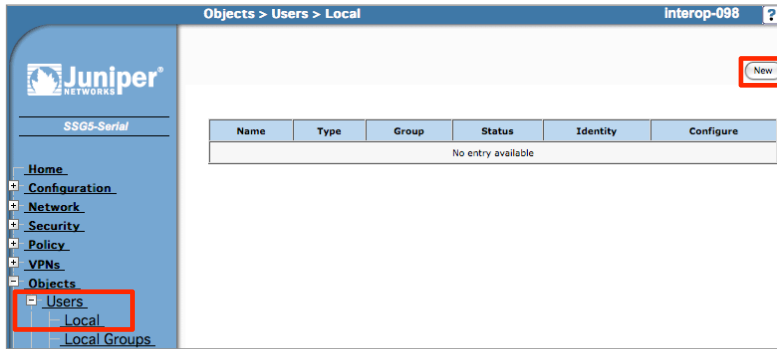
### **Guidelines for selecting a suitable range of IP addresses:**

- ▶ The range of IP addresses **must** come from one of the IP address ranges that are reserved for internal use (“private subnets”)
- ▶ The range of IP addresses **may not** overlap with any of the networks used on your VPN gateway device, in particular, it may not be part of the LAN. It should also not be used by any of the resources (servers etc.) that are being accessed through the VPN
- ▶ The address pool **must** contain enough IP addresses to supply an IP address to each possible user of the VPN connection. If multiple logins for the same user are to be permitted, additional IP addressees must be available. It is usually a good idea to choose the pool to be at least twice as large as the maximum number of expected users.

#### **Private Subnets**

- ▶ 10.0.0.0 - 10.255.255.255
- ▶ 172.16.0.0 - 172.31.255.255
- ▶ 192.168.0.0 - 192.168.255.255

## Step 2 – Create a Shared IKE User



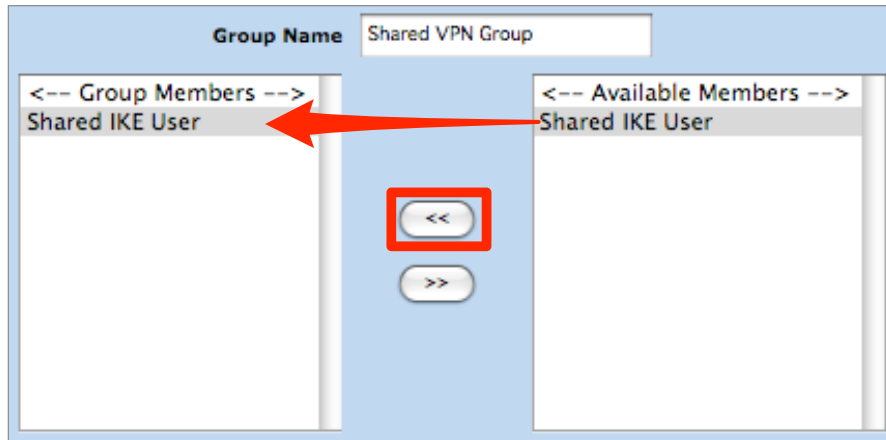
- ▶ Go to the section “**Objects > Users > Local**”
- ▶ Click “**New**”

The screenshot shows the 'Auth/IKE/XAuth/L2TP User' configuration page. The 'User Name' field is set to 'Shared IKE User'. The 'Status' is set to 'Enable'. The 'IKE User' checkbox is checked and highlighted. The 'Simple Identity' radio button is selected. The 'IKE ID Type' is set to 'AUTO'. The 'IKE Identity' field is set to 'vpntracker.local'. The 'Number of Multiple Logins with Same ID' is set to '1'. There are also fields for 'Use Distinguished Name For ID' with 'CN' and 'OU' sub-fields.

- ▶ **User Name:** Enter a user name that you will be able to recognize later
- ▶ Check the box “**IKE User**” and select “**Simple Identity**”
- ▶ **IKE Identity:** Enter an identifier for the VPN connection. This identifier will be the “Local Identifier” in VPN Tracker **1** A good identifier is “vpntracker.local”. However, it is possible to use any host name or an email address. If you do choose to use an email address here, keep in mind that you will have to change the “Local Identifier” type in VPN Tracker to “Email (User FQDN)”.
- ▶ Leave the default values for all other settings.
- ▶ Click “**OK**” to save the new user

**Note** The user object that created in this step is shared by all users of the VPN connection. By separating this shared user object (“IKE user”) from the user objects that we will create later for each individual user (“XAUTH users”), we can prevent complex dependencies when modifying individual users in the future.

### Step 3 – Create a Group for the Shared IKE User



- ▶ Go to the section “**Objects > Users > Local Groups**”
- ▶ Click “**New**”
- ▶ **Group Name:** Enter a group name that you will be able to recognize later
- ▶ In the “**Available Members**” list, select the shared IKE user created in Step 2.
- ▶ Click the “<<” button to move the shared IKE user to the list of group members
- ▶ Click “**OK**” to save the new group

**Note** This group is only for the shared IKE user. Do **not** add any of the XAUTH users that will create in the next step!

## Step 4 – Create Extended Authentication (XAUTH) Users

Auth/IKE/XAuth/L2TP User

User Name  ②

Status  Enable  Disable

IKE User Number of Multiple Logins with Same ID

Simple Identity

IKE ID Type  IKE Identity

Use Distinguished Name For ID

CN

OU

Organization

Location

State

Country

E-mail

Container

Authentication User User Password  ③

XAuth User Confirm Password  ③

L2TP User

L2TP/XAuth Remote Settings ( Remote IP: 0.0.0.0 )

IP Pool  Static IP

Primary DNS IP  Primary WINS IP

Secondary DNS IP  Secondary WINS IP

- ▶ Go to the section “**Objects > Users > Local**”
- ▶ Click “**New**”
- ▶ **User Name:** Enter a user name ②
- ▶ Check the box “**XAUTH User**”
- ▶ **User Password:** Enter a password for the user ③  
Both the user name and the password are case-sensitive
- ▶ **Confirm User Password:** Repeat the password ③
- ▶ Leave all other settings at their default values
- ▶ Click “**OK**” to add the new user

**Note** To create additional users, repeat this step for each user.

## Step 5 – Configure the XAUTH Settings

Juniper®  
SSG5-Serial

VPNs > AutoKey Advanced > XAuth Settings

Reserve Private IP for XAuth User: 480 Minutes

Default Authentication Server: Local

Query Client Settings on Default Server: CHAP

Default Accounting Server: None

Default Accounting Off

IP Pool Name: VPN Client IPs

DNS Primary Server IP: 192.168.13.21

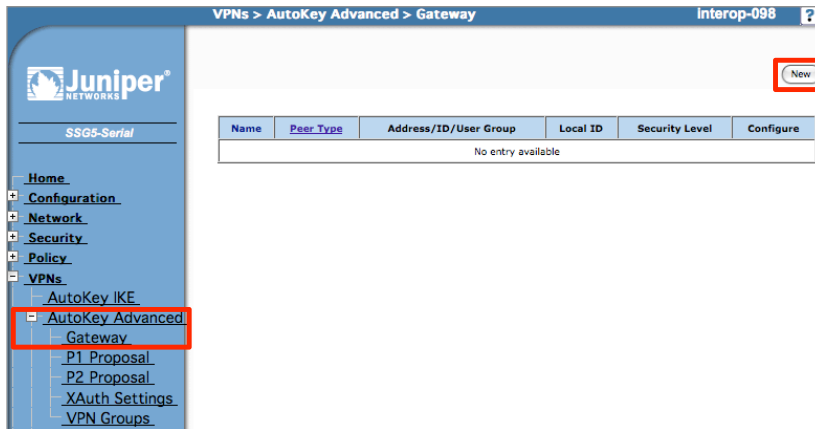
DNS Secondary Server IP: 0.0.0.0

WINS Primary Server IP: 0.0.0.0

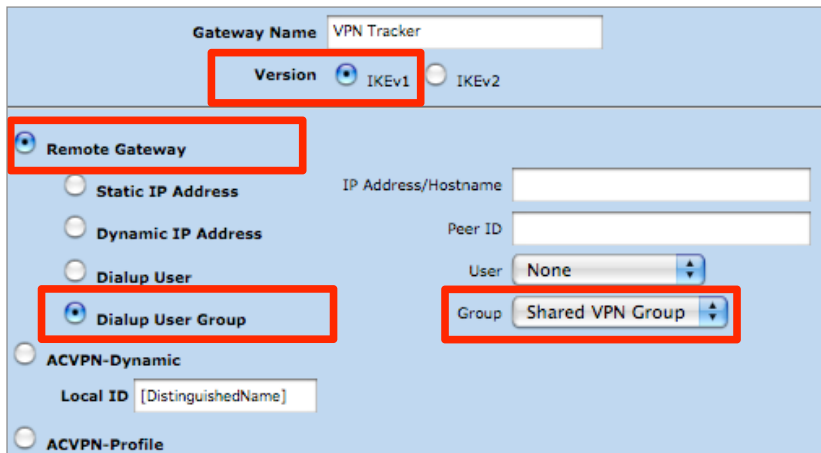
WINS Secondary Server IP: 0.0.0.0

- ▶ Go to the section “**VPNs > AutoKey Advanced > XAuth Settings**”
- ▶ **IP Pool Name:** Select the IP address pool you created in Step 1
- ▶ **DNS Primary Server IP** (optional): If you operate a DNS server in your network, you can enter its IP address here to automatically transmit the DNS settings to your VPN clients.
- ▶ **DNS Secondary Server IP** (optional): If you operate a secondary (backup) DNS server in your network, you can enter its IP address here to automatically transmit the DNS settings to your VPN clients.
- ▶ Click “**Apply**”

## Step 6 – Configure the Phase 1 Settings (Gateway Settings)

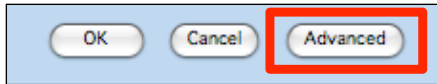


- ▶ Go to the section “VPNs > AutoKey Advanced > Gateway”
- ▶ Click “New”



- ▶ **Gateway Name:** Enter a gateway name that you will be able to recognize later
- ▶ **Version:** Make sure “IKEv1” is selected
- ▶ **Remote Gateway Type:** Set to “Dialup User Group”
- ▶ **Group:** Select the group you created earlier for the shared IKE user





▶ Click **“Advanced”** to edit additional settings

▶ **Preshared Key:** Enter a pre-shared key <sup>4</sup> The pre-shared key is a password that is shared among all users of the connection (individual user passwords are configured for each XAUTH user separately, see Step 4). *If you are running an earlier version of ScreenOS, you will find this and the following two settings among the main settings.*

▶ **Outgoing Interface:** Select the network interface that your VPN connections arrive on. Usually, this will be the “untrust” (WAN) interface.

▶ **Security Level:** Make sure the Security Level is set to “Standard”.

▶ **Mode (Initiator):** Set the mode to **“Aggressive”**

▶ Check the box **“Enable NAT-Traversal”**

▶ Click **“Return”** to leave the advanced settings

▶ Click **“OK”** to save the phase 1 settings

**Advanced Users** **“Standard” security level** means that Diffie-Hellman Group 2 (1024 bit), 3DES or AES-128 encryption, and SHA-1 hashes will be used for phase 1. If you choose a different level, you must match these settings in VPN Tracker (Advanced > Phase 1)

**Advanced Users** While **Main Mode** is considered to be more secure, its dependence on the peer’s IP address makes it unsuitable for use with VPN clients (as opposed to static VPN tunnels between two VPN gateways).

## Enable Extended Authentication (XAUTH)

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure
VPN Tracker	Dialup	Shared VPN Group	-	Standard	<a href="#">Edit</a> <a href="#">Xauth</a> <a href="#">Remove</a>

- ▶ Go to “VPNs > AutoKey Advanced > Gateway”
- ▶ Click “Xauth” in the “Configure” column

None

**XAuth Server**

**Authentication Settings:**

Allowed Authentication Type  Generic  CHAP Only  CHAP & PAP

**Use Default Xauth Settings**

Local Authentication

Allow Any

User

User Group

External Authentication   Query Remote Setting

Allow Any

User

User Group

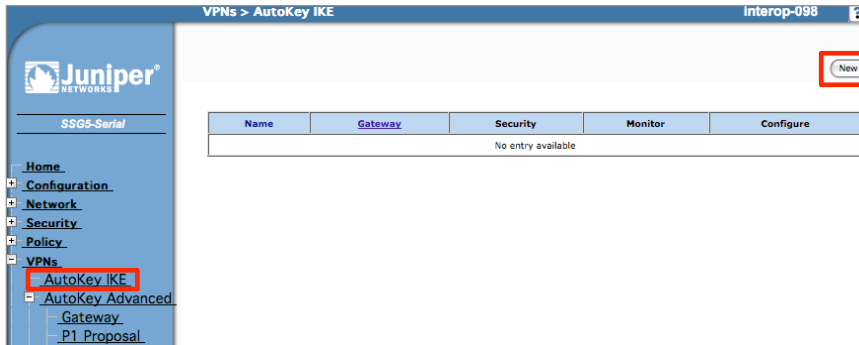
Bypass Authentication

- ▶ Select “XAuth Server”
- ▶ Make sure “Use Default Xauth Settings” is selected to use the settings configured previously (see Step 5)
- ▶ Click “OK” to save your changes

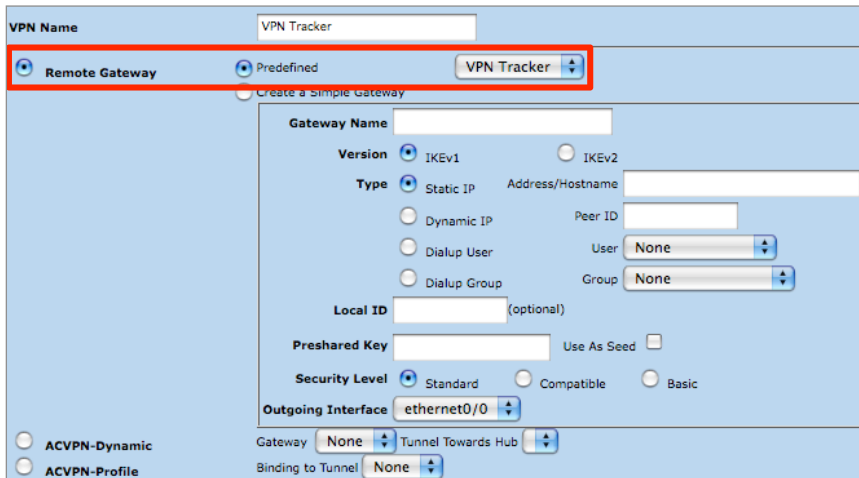
### Advanced Users

Using **CHAP** is more secure, however, not all VPN clients support it. If you are only using VPN Tracker as a client for your VPN connection, you can safely switch to the “**CHAP only**” authentication type.

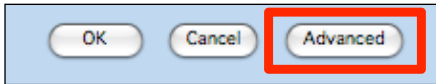
## Step 7 – Configure the Phase 2 Settings (VPN Settings)



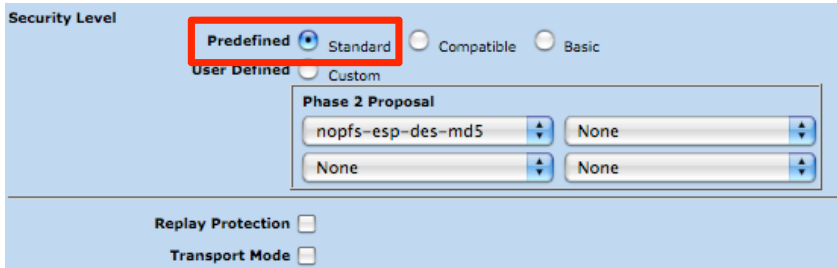
- ▶ Go to the section “VPNs > AutoKey IKE”
- ▶ Click “New”



- ▶ **VPN Name:** Enter a VPN name that you will be able to recognize later
- ▶ **Remote Gateway:** Select “Predefined” and select the gateway you created in Step 6
- ▶ Click “OK” to save the phase 2 settings



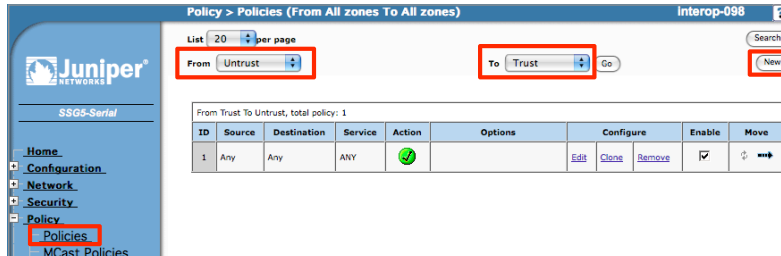
- ▶ Click **“Advanced”** to edit additional settings



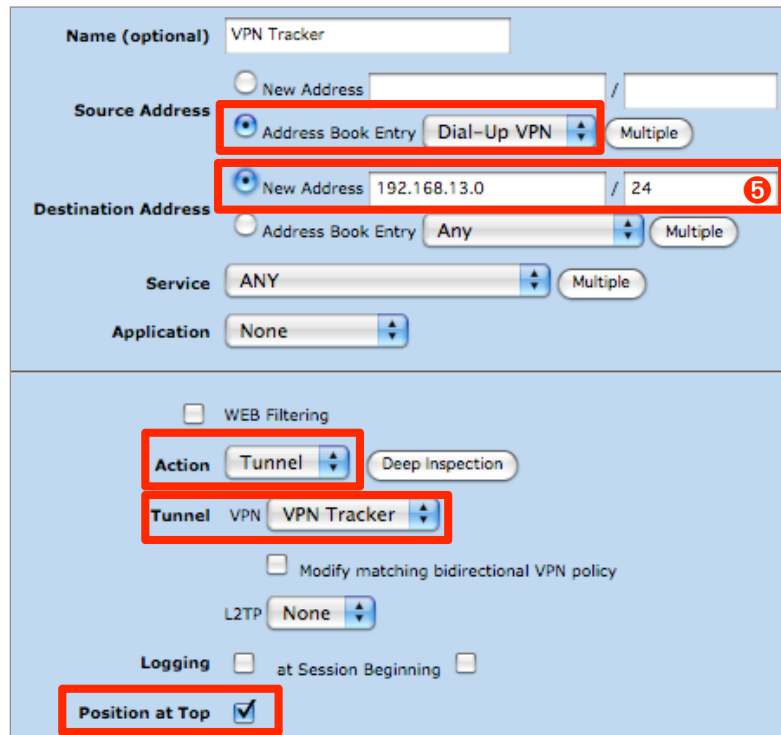
- ▶ **Security Level:** Make sure the security level is set to *“Standard”*. *If you are running an earlier version of ScreenOS, you will find the “Security Level” in the main settings.*

**Advanced Users** **“Standard” security level** means that 3DES or AES-128 encryption, SHA-1 authentication and Perfect Forward Secrecy (PFS) with Diffie-Hellman Group 2 (1024 bit) will be used for phase 2. If you choose a different level, you must match these settings in VPN Tracker (Advanced > Phase 2)

## Step 8 – Add a Policy



- ▶ Go to the section “Policies”
- ▶ **From:** Select “Untrust”
- ▶ **To:** Select “Trust”
- ▶ Click “New”

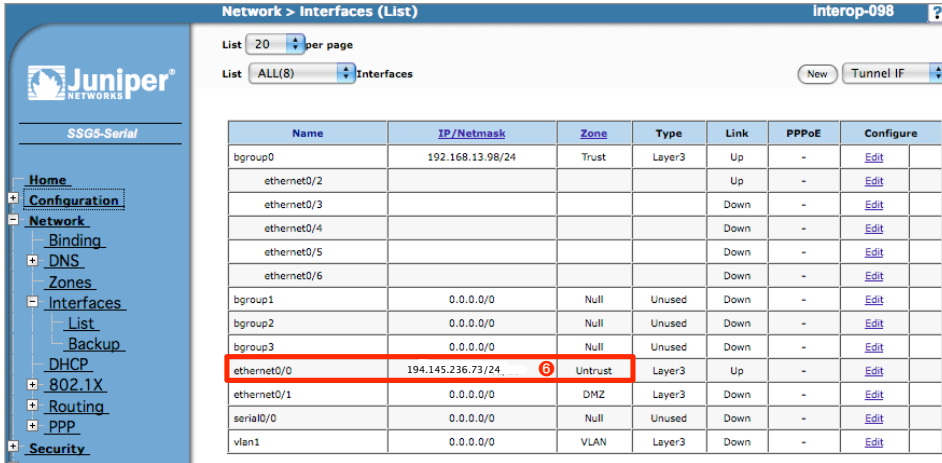


- ▶ **Name:** Enter a name for the new policy (optional, but recommended)
- ▶ **Source Address:** Select “Address Book Entry” and select “Dial-Up VPN” from the popup list
- ▶ **Destination Address:** Select “New Address” and enter the network you want to access through the VPN tunnel 5 Most likely this will be the LAN network of your VPN gateway

**Note** If there is already an entry for the desired network in the device’s address book, please select that entry.

- ▶ **Action:** Select “Tunnel”
- ▶ **Tunnel:** Select the previously created VPN
- ▶ Check the box “Position at Top”
- ▶ Click “OK” to save the new policy

## Step 9 – Find Your VPN Gateway’s Public IP Address



Network > Interfaces (List) interop-098

List 20 per page

List ALL(8) Interfaces New Tunnel IF

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	192.168.13.98/24	Trust	Layer3	Up	-	Edit
ethernet0/2				Up	-	Edit
ethernet0/3				Down	-	Edit
ethernet0/4				Down	-	Edit
ethernet0/5				Down	-	Edit
ethernet0/6				Down	-	Edit
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit
ethernet0/0	194.145.236.73/24	Untrust	Layer3	Up	-	Edit
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	Edit
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit

- ▶ Go to “**Network > Interfaces > List**”
- ▶ Find your public (WAN) interface in the list. In many cases, it will be the “ethernet 0/0” interface, and almost always be assigned to the “Untrust” zone
- ▶ Write down the IP address of the public (WAN) interface as ⑥ Don’t write down the part that comes after the slash (“/”). In our example, we would write down 194.145.236.73

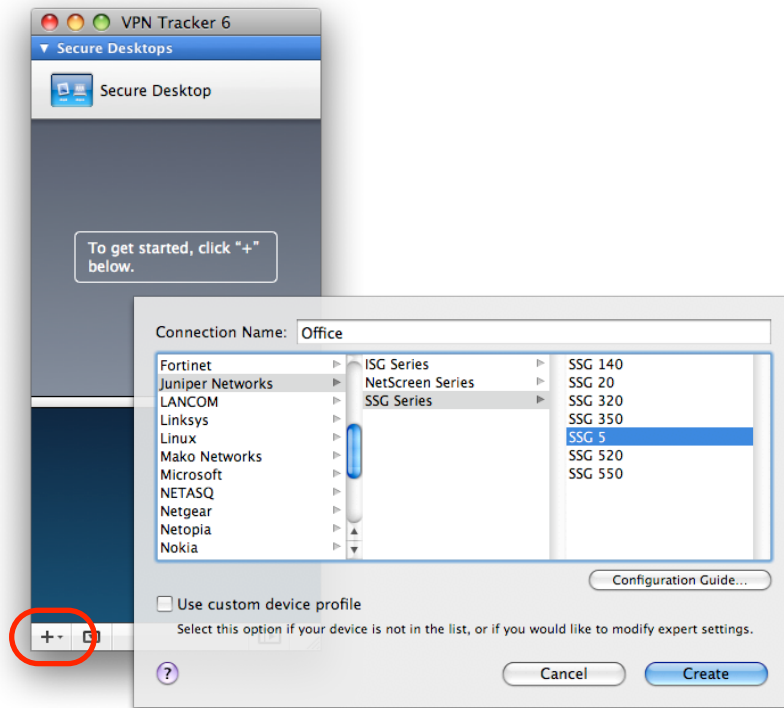
### Advanced Users

If you know your VPN gateway’s public (WAN) IP address or host name, you can skip this step. Write down the IP address or host name as ⑥ on your VPN gateway configuration checklist.

# Task 2 – Configure VPN Tracker

This section describes how to configure VPN Tracker to connect to your Juniper Networks VPN gateway. You will need the configuration information you collected during Task 1. If you are missing any information, please refer back to “Task 1 – Configure your VPN Gateway”.

## Step 1 - Create a New Connection



- ▶ Start VPN Tracker
- ▶ Click the “+” button in the main window

You will be asked to select a device profile for the new connection:

- ▶ Select “**Juniper Networks**” from the list
- ▶ Select your device from the list of Juniper Networks devices
- ▶ **Connection Name:** Choose a name for your connection (e.g. “Office”)
- ▶ Click “OK”

## Step 2 – Configure the VPN Connection

The screenshot shows the configuration page for a VPN connection. At the top, there are tabs for 'Basic', 'Advanced', 'Actions', 'Export', and 'Log'. The 'Basic' tab is selected. The connection is named 'Office'. Below this, there are several sections:

- Connection based on:** Juniper Networks SSG Series (SSG 5) Configuration Guide
- VPN Gateway:** vpn.example.com (6)
- Network Configuration:** Mode Config (dropdown)
- Topology:** Host to Network (dropdown)
- Remote Networks:** 192.168.13.0 / 24 (5)
- Authentication:** Pre-shared key (dropdown) with a note 'Pre-shared key not saved'
- Extended Authentication (XAUTH):** When requested (dropdown) with a note 'Username and password not saved'
- Identifiers:**
  - Local:** Fully Qualified Domain Name (FQDN) (dropdown) with value vpntracker.local (1)
  - Remote:** Remote Endpoint IP Address (dropdown)
- DNS:** Use Remote DNS Server (checkbox)

- ▶ **VPN Gateway:** Enter your VPN gateway’s public IP address or its hostname, if available (6) In our example, the device is reachable using the hostname vpn.example.com but we could also use the device’s public IP address (194.145.236.73) from Step 9.
- ▶ **Remote Networks:** Enter the network address of the network that is being accessed through the VPN tunnel (5) Separate the subnet mask with a forward slash (“/”)
- ▶ **Local Identifier:** Enter the **IKE Identity** from your Juniper Networks device (in this example, we configured the device’s IKE identity to be “vpntracker.local”) (1)
- ▶ **DNS (optional):** If you have configured a DNS server during Step 5, check “Use Remote DNS Server” and “Receive DNS Settings from VPN Gateway”



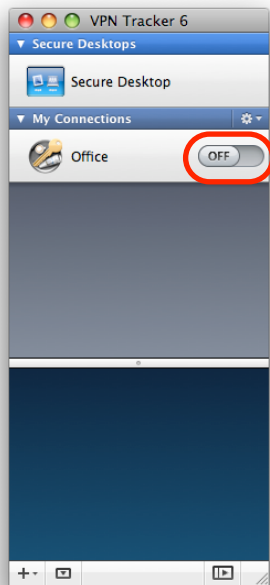
# Task 3 – Test the VPN Connection

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



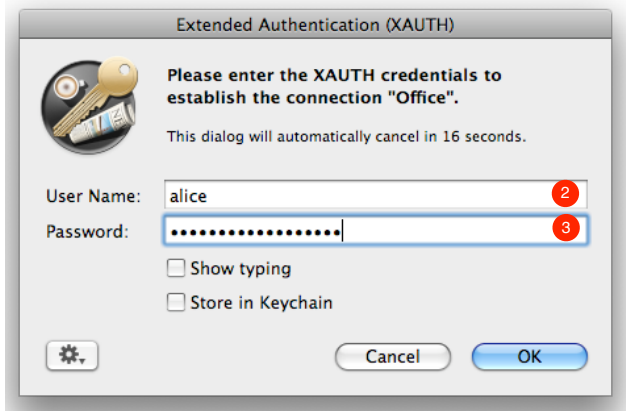
- ▶ Connect to the Internet
- ▶ Make sure that your Internet connection is working – open your Internet browser and try to connect to <http://www.equinux.com>
- ▶ Start VPN Tracker if it's not already running
- ▶ Slide the On/Off slider for the connection you have just configured to **On**

## If you are prompted for your pre-shared key:

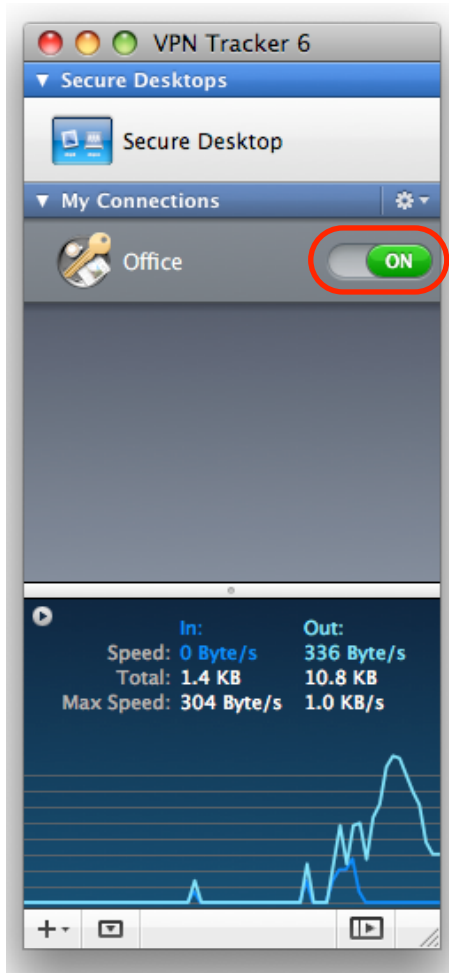


- ▶ **Pre-shared key:** Enter the pre-shared key that you configured on the VPN gateway **4**.
- ▶ Optionally, check the box **"Store in Keychain"** to save the password in your keychain so you are not asked for it again when connecting the next time
- ▶ Click "OK"

## If you are prompted for your Extended Authentication (XAUTH) credentials:



- ▶ **User Name:** Enter the name of the user configured on the VPN gateway **2**
- ▶ **Password:** Enter the password for this user **3**
- ▶ Optionally, check the box **"Store in Keychain"** to save the user name and 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!**

# Supporting Multiple Users

Adding multiple users to your VPN connection on a ScreenOS-based device is easy – simply add more Extended Authentication (XAUTH) users. In addition to purely technical considerations, VPN Tracker makes it easy to distribute pre-configured connections to your users, and prevent the modification of VPN connections and access to confidential data.

**Note** Make sure the IP address pool created in “Step 1 – Set up an IP address pool” is large enough to support the maximum number of concurrent users you expect for the VPN.

## Adding Users on the VPN Gateway

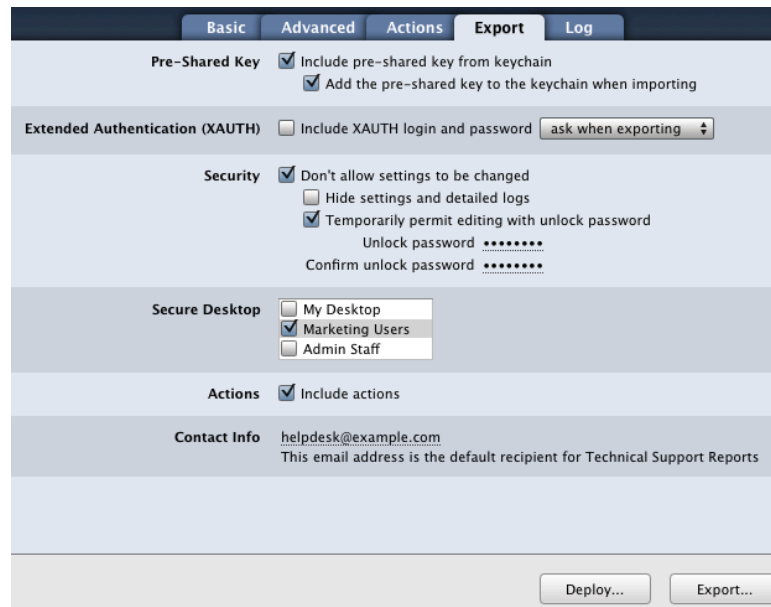
To add more users on the VPN gateway, simply follow “Step 4 – Create Extended Authentication (XAUTH) Users” of “Task 1 – Configure Your VPN Gateway”. Choose a different user name and password for each user. There is no need to modify the actual connection settings, all you’ll need to change in VPN Tracker is the XAUTH user name and password.

**Note** The total number of users and concurrent VPN connections on your VPN gateway may be limited by the hardware’s capabilities and firmware restrictions. Please refer to your device’s data sheet for specific information.

## Deploying VPN Connections to Your Users

VPN Tracker Professional Edition offers a number of ways to easily distribute pre-configured connections to users. It is even possible to create a custom VPN Tracker application that contains a pre-configured connection and a license voucher for your users.

Further information on deploying connections to users is available in the VPN Tracker manual.



The screenshot shows the 'Export' tab of the VPN Tracker configuration interface. The tabs at the top are 'Basic', 'Advanced', 'Actions', 'Export', and 'Log'. The 'Export' tab is active and contains the following sections:

- Pre-Shared Key:**  Include pre-shared key from keychain  
 Add the pre-shared key to the keychain when importing
- Extended Authentication (XAUTH):**  Include XAUTH login and password
- Security:**  Don't allow settings to be changed  
 Hide settings and detailed logs  
 Temporarily permit editing with unlock password  
Unlock password: .....  
Confirm unlock password: .....
- Secure Desktop:**  My Desktop  
 Marketing Users  
 Admin Staff
- Actions:**  Include actions
- Contact Info:** helpdesk@example.com  
This email address is the default recipient for Technical Support Reports

At the bottom right, there are two buttons: 'Deploy...' and 'Export...'.

**Tip** To deploy VPN Tracker to many users, you can create a custom VPN Tracker application with a pre-configured connection and a license voucher. Simply click "Deploy..." to get started.

# 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

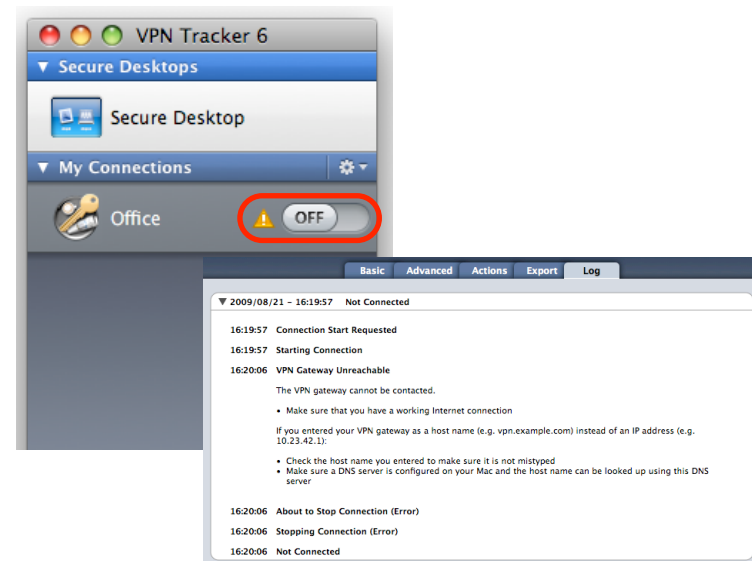
### On/Off Slider goes back to “Off” right away

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).

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.

## Make sure the VPN gateway is the default gateway in the remote network

If it is not, you will have to ensure that responses to all IP addresses in the address pool (see Step 1) are routed to the VPN gateway, either by adding a general route on the network's default gateway, or by adding individual routes on each host that VPN clients need to communicate with.

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



# Appendix

## Predefined Security Levels

	Standard (recommended)	Compatible	Basic
Phase 1	<ul style="list-style-type: none"><li>▶ 3DES or AES-128</li><li>▶ SHA-1</li><li>▶ Diffie-Hellman Group 2 (1024 bit)</li></ul>	<ul style="list-style-type: none"><li>▶ 3DES or DES</li><li>▶ SHA1 or MD5</li><li>▶ Diffie-Hellman Group 2 (1024 bit)</li></ul>	<ul style="list-style-type: none"><li>▶ DES</li><li>▶ SHA1 or MD5</li><li>▶ Diffie-Hellman Group 1 (768 bit)</li></ul>
Phase 2	<ul style="list-style-type: none"><li>▶ 3DES or AES-128</li><li>▶ HMAC SHA-1</li><li>▶ Perfect Forward Secrecy (PFS) with Diffie-Hellman Group 2 (1024 bit)</li></ul>	<ul style="list-style-type: none"><li>▶ 3DES or DES</li><li>▶ HMAC SHA1 or HMAC MD5</li><li>▶ no Perfect Forward Secrecy (PFS)</li></ul>	<ul style="list-style-type: none"><li>▶ DES</li><li>▶ HMAC SHA1 or HMAC MD5</li><li>▶ no Perfect Forward Secrecy (PFS)</li></ul>