



VPN Tracker 365

VPN Configuration Guide

Juniper SRX-Series

© 2018 equinix AG and equinix USA, Inc. All rights reserved.

Under copyright law, 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. 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 manual is accurate. equinix is not responsible for printing or clerical errors.

Revised 8. January 2018

Created using Apple Pages.

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

www.vpntracker.com

Contents

- Introduction.....4
- Task 1 – Juniper Configuration5
- Task 2 – VPN Tracker Configuration8
- Task 3 – Test the VPN Connection9

Introduction

This configuration guide will help you connect VPN Tracker to your Juniper SRX-Series VPN Gateway.

My VPN Gateway Configuration

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

IP Addresses

① Juniper WAN IP Address: _____

or host name _____

② LAN Network: _____ / _____

Authentication

③ Pre-Shared Key: _____

Task 1 – Juniper Configuration

First, we'll set up a VPN tunnel on your Juniper gateway.

Step 1 – Find your external gateway address

- ▶ Connect to your Juniper's web interface
- ▶ Go to **Dashboard** or **Monitor** and make a note of your gateway's external WAN IP address as **1**

Step 2 – Start the Juniper VPN Wizard

- ▶ Go to **Configuration Wizards > VPN**
- ▶ Choose **Remote Access VPN**

Step 3 – Configuring Local Settings

- ▶ The default settings here should typically work for most setups
- ▶ Optionally, you can edit the Zone and internal networks your VPN users will be accessing

VPN Wizard

Remote Access VPN: Local Settings

Select VPN Type
Local
VPN
Remote Users
Review & Commit

About this page
On this page you specify the local private network and the public network through which the tunnel passes. The name of the remote access VPN is preset.
If you have previously configured a remote access VPN, you can use this page to edit the existing remote access VPN or click the button at the

Name
VPN Name * wizard_dyn_vpn

Protected Networks
Zone * Internal
Network(s) * 192.168.100.0/24

Public Network
Interface * ge-0/0/0.0
Interface Zone * Internet

Step 4 – Configuring VPN settings

- ▶ Choose IKE Security level **Standard (group2, aes128, sha1)**
- ▶ Enter a pre-shared key
- ▶ Enter "VPNClient" as your Remote Identity
- ▶ Set the IPsec Security Level to **Standard (esp, aes128, sha1)**
- ▶ IPsec Perfect Forward Secrecy should be set to **group5**

VPN Wizard

Remote Access VPN: VPN Settings

Select VPN Type
Local
VPN
Remote Users
Review & Commit

About this page
IKE IPsec tunnel negotiation occurs in two phases. In Phase 1, participants establish a secure channel in which to negotiate the IPsec security association (SA). In Phase 2, participants negotiate the IPsec SA for authenticating traffic that will flow through the tunnel.

VPN Settings
IKE Security Level * Standard (group2, aes128, sha1)
IKE Preshared Key (ASCII) * SecretSharedPassword
Remote Identity * VPNClient
Dead Peer Detection
IPsec Security Level * Standard (esp, aes128, sha1)
IPsec Perfect Forward Secrecy group1 group2 group5

Step 5 – Add VPN users

- ▶ Enter a username and password for each user that will be using this VPN connection

Step 6 – Confirm your settings

- ▶ Review your settings and make a note of the settings so you can enter them in VPN Tracker.
- ▶ Save your new VPN configuration by choosing **Commit**

VPN Wizard

✔ Select VPN Type
✔ Local
✔ VPN
✔ Remote Users
[Review & Commit](#)

About this page
When you edit a configuration, the changes you make do not take effect until you commit them. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file.
This page shows the information you have entered and any errors

Remote Access VPN Configuration

VPN Name	
VPN Name	wizard_dyn_vpn
Protected Networks	
Zone	Internal
Networks	192.168.100.0/24 2
Public Network	
Interface	ge-0/0/0.0
Interface zone	Internet
VPN settings	
IKE security level	standard
IKE preshared key	SecretSharedPassword 3
Remote identity	Host name: VPNCClient 4
Dead Peer Detection	Yes
IPsec Security Level	standard
IPsec Perfect Forward Secrecy	group5
Remote user IP settings	
IP pool range/IP	192.168.110.0/24
DNS server	9.9.9.9
WINS server	

[Back](#) [Commit](#)

Step 7 – Configure the Security Zone

- ▶ Go to **Security > Zones/Screens**
- ▶ Choose your external Interface
- ▶ Choose **Edit**
- ▶ Select the tab **Host Inbound Traffic - Interface**
- ▶ Add **ike** to the list of **Selected Services**

SRX / SRX300

Dashboard Configure Monitor Maintain Troubleshoot Commit

Edit Zone

Main Host Inbound Traffic - Zone **Host Inbound Traffic - Interface**

Selected Interfaces
ge-0/0/0.0

Available Services	Selected	Available Protocols	Selected
all	ping	all	
any-service	dhcp	bfd	
bootp	https	bgp	
dhcpv6	ike	dvmrp	
dns		igmp	
finger		ldp	
ftp		mssdp	
http		nhrp	

Cancel OK

Step 8 – Adjust the IKE Gateway Policy

- ▶ Go to **IPSec VPN > VPN Tunnel > Phase I**
- ▶ Select your previously created policy, e.g. “gw_wizard_dyn_vpn” and choose **Edit**
- ▶ As **IKE User Type** choose “shared-ike-id”

That’s it. Now you can set up your new VPN tunnel in VPN Tracker.

The screenshot shows the Juniper SRX300 configuration interface. The left sidebar shows the navigation menu with 'IPSec VPN' expanded to 'VPN Tunnel' and 'Phase I' selected. The main area displays the 'Edit Gateway' dialog for a dynamic VPN tunnel. The 'IKE Gateway' tab is active, and the 'Dynamic VPN configuration tips' section is visible. The 'Name' field is set to 'gw_wizard_dyn_vpn', the 'Policy' is 'ike_pol_wizard_dyn_vpn', and the 'External Interface' is 'ge-0/0/0.0'. The 'Ike Version' is set to '1'. The 'Client Tunnel' radio button is selected. The 'Connections Limit' is set to 50. The 'IKE user type' dropdown is highlighted with a red box and set to 'shared-ike-id'. The 'Remote ID' section shows 'Identity Type' set to 'Host Name' and 'Hostname' set to 'VPNClient'. The 'OK' button is visible at the bottom right of the dialog.



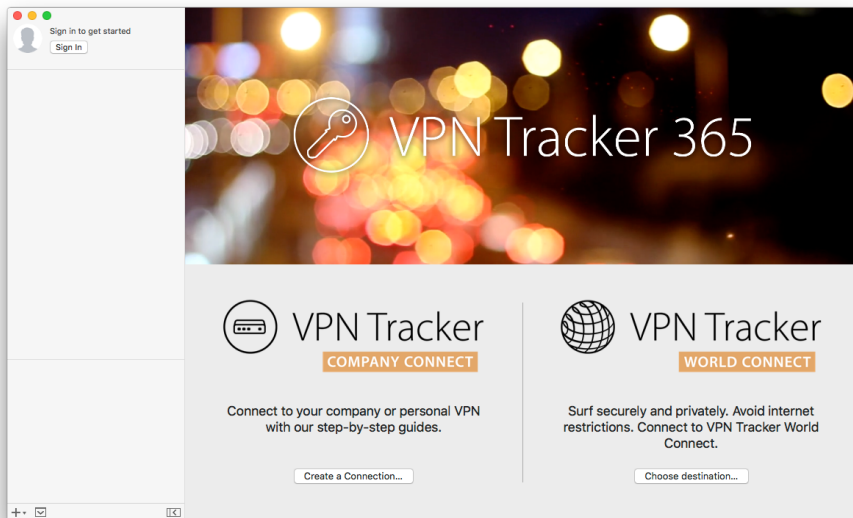
Important This step is crucial, as you will otherwise see a pre-shared key mismatch error when trying to connect from VPN Tracker!

Task 2 – VPN Tracker Configuration

From Task 1, your → *Configuration Checklist* will have all your Juniper settings. We will now create a matching configuration in VPN Tracker.

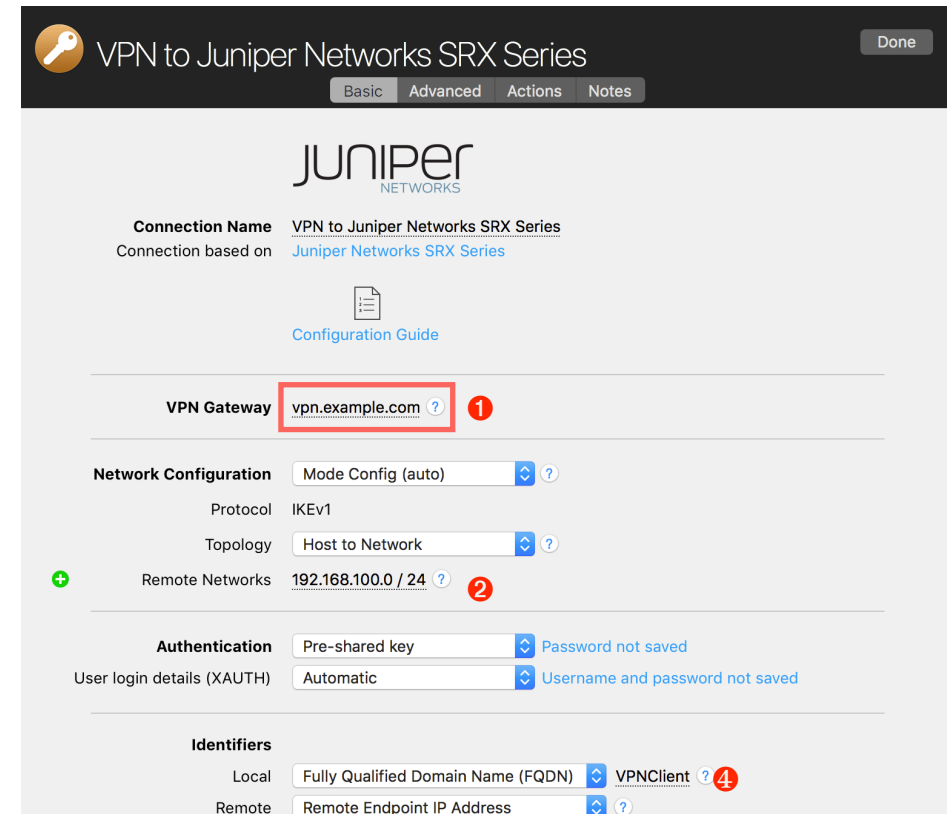
Step 1 – Add a Connection

- ▶ Open VPN Tracker.
- ▶ Click **“Create a Connection”** (or click the + button in the lower left corner).
- ▶ Select **“Juniper”** from the list.
- ▶ Select your Juniper series (e.g. SRX series).
- ▶ Click **“Create”**.



Step 2 – Configure the VPN Connection

- ▶ Click **“Configure”** and switch to the **“Basic”** tab
- ▶ **VPN Gateway:** Enter your Juniper’s public IP address or its host name **1** from your → *Configuration Checklist*.
- ▶ **Network Configuration:** Enter the Remote Network from **2**
- ▶ **Identifiers:** Enter the FQDN Local Identifier from **4**
- ▶ Click **“Done”**



Task 3 – Test the VPN Connection

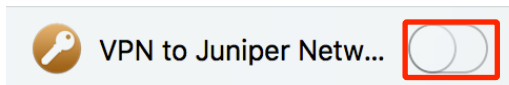
It's time to go out!

In order to test your connection, you will need to connect from a different location.

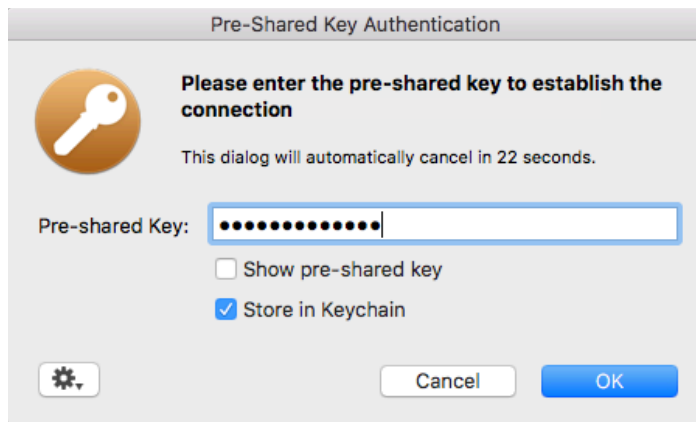
For example, if you are setting up a VPN connection to your office, try it out at home, or from an Internet cafe, or go visit a friend.

Connect to your VPN

- ▶ 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 **3**. 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 VPN and how to get the most out of it.

Troubleshooting

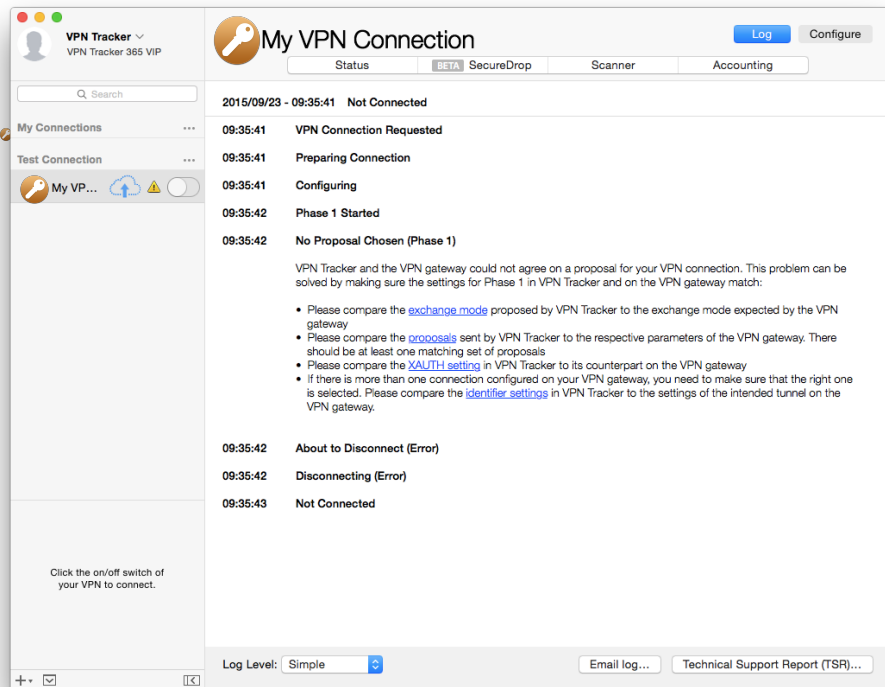
In case there's a problem connecting, a yellow warning triangle will show up:



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.



Pre-Shared Key Hash Mismatch Error?

If you're seeing a pre-shared key error, double-check you have configured the IKE user type to **Shared-IKE-ID** as described in Section 1, Step 8.

Other Issues

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 equinix is here to help. Contact us via

<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.
- ▶ A VPN Tracker Technical Support Report (Log > Technical Support Report).
- ▶ Juniper model and the firmware version running on it.
- ▶ Screenshots of the Client VPN settings on your Juniper.



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.