



VPN Configuration Guide

Ubiquiti EdgeRouter

© 2019 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 16 October 2018

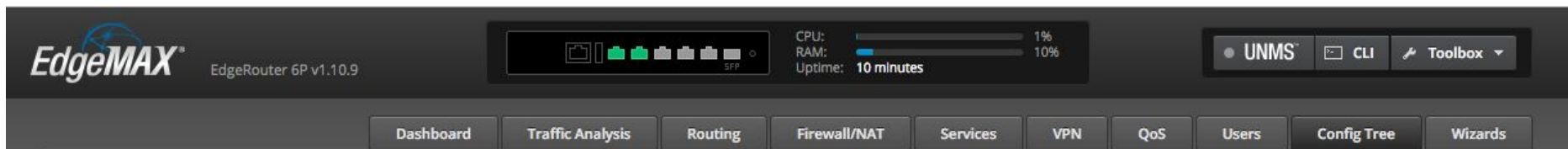
Apple, the Apple logo, iBook, Mac, Mac OS, MacBook, PowerBook are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

www.equinix.com

Task One - Setting up L2TP

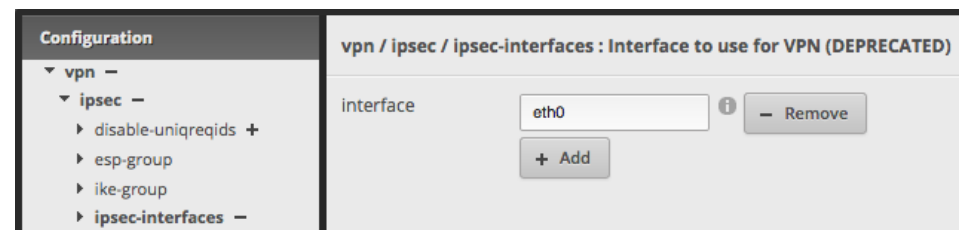
Step One: Open the Config Tree

- From any device connected to a LAN port of your router, open the router setup page in Safari or any browser of your choice.
- Log in with an administrator user account.
- Select the tab "Config Tree".



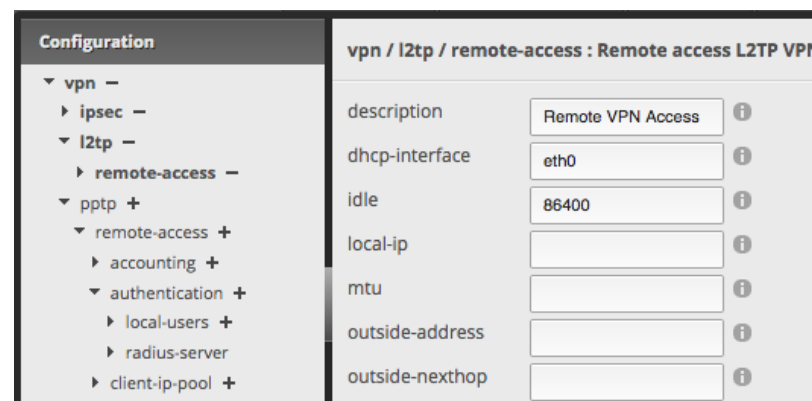
Step Two: Setting up an IPSec interface

- Open up the branch "vpn > ipsec > ipsec-interfaces".
- Enter the name of the interface to that VPN users will be connecting, e.g. "eth0".



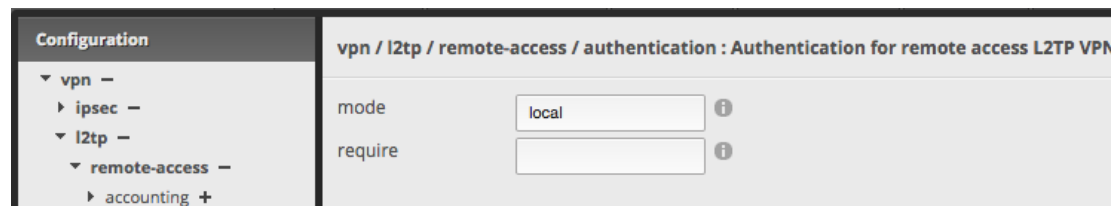
Step Three: Setting up remote-access

- Open up the branch “vpn > l2tp > remote-access”.
- Choose a description of your choice.
- Set an idle timeout between 30 and 86400 second.
- If the port configured in [Step Two](#) obtains its IP address via DHCP, enter the port name at “dhcp-interface” as shown in the screenshot.
 - ◆ If the port has a static IP address, leave “dhcp-interface” empty and enter the static IP address into the field “outside-address” instead.
 - ◆ If the port obtains its IP address via PPPoE, leave “dhcp-interface” empty and enter “0.0.0.0” into the field “outside-address”.



Step Four: Setting up authentication

- Open up the branch “vpn > l2tp > remote-access > authentication”.
- Type “local” into the field labeled “mode”.

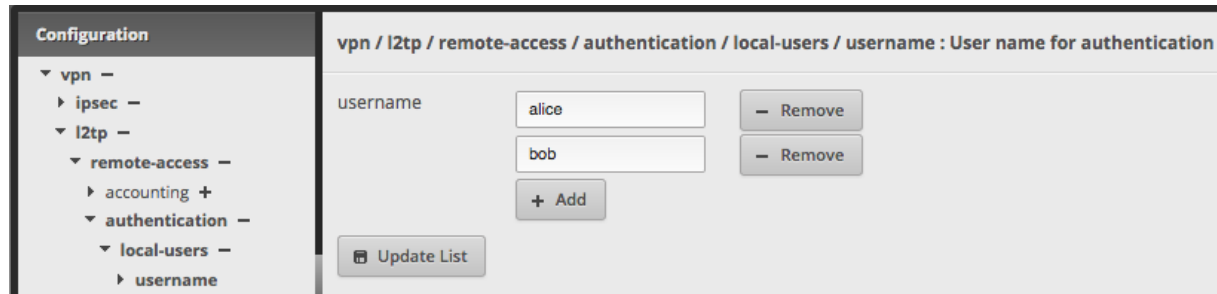


Step Five: Setting up the VPN users

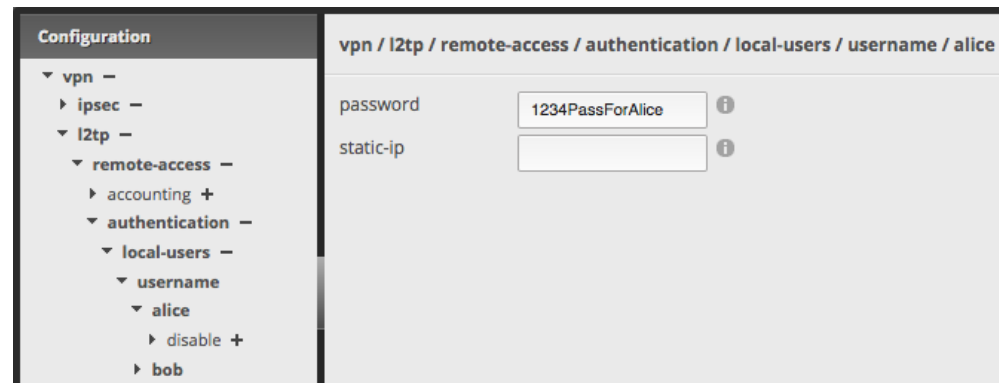
- Open up the branch “vpn > l2tp > remote-access > authentication > local-users > username”.
- Enter the name of at least one VPN user or add as many VPN users as you wish.
- Once done, press “Update List” to add the user entries to the tree.

Note:

You can always return there to add more users at a later time, so it's not necessary to add all of them at once.



- After pressing “Update List”, your added users will appear in the tree as additional branches under “username”.
- For every user created, repeat the following steps:
 - ◆ Select the user.
 - ◆ Enter a password.
 - ◆ Optionally you can assign a static IP address to this user, in case it is important to identify specific users by specific IP addresses.

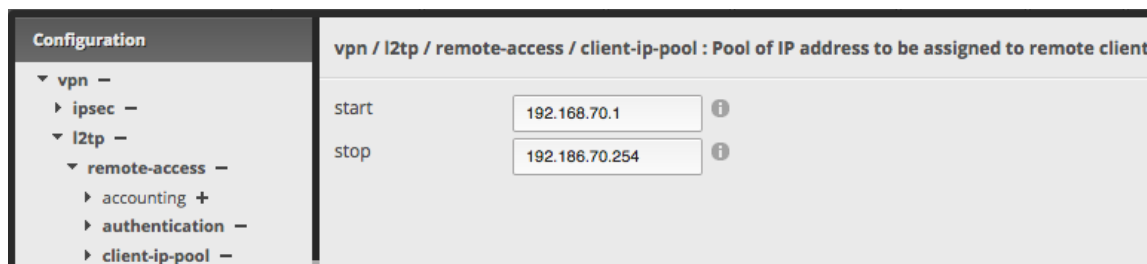


Step Six: Setting up a client IP pool

- Open up the branch “vpn > l2tp > remote-access > client-ip-pool”.
- Enter a the first address of the client IP pool at “start”.
- Enter the end of the client IP pool at “stop”.

Note:

Users without a static IP address in [Step Five](#) will obtain a random IP address from this pool every time they connect.



The screenshot shows the configuration page for the client IP pool. The left sidebar is titled "Configuration" and has a tree view with the following items: "vpn" (expanded), "ipsec", "l2tp" (expanded), "remote-access" (expanded), "accounting", "authentication", and "client-ip-pool" (selected). The main content area is titled "vpn / l2tp / remote-access / client-ip-pool : Pool of IP address to be assigned to remote clients". It contains two input fields: "start" with the value "192.168.70.1" and "stop" with the value "192.186.70.254". Each input field has an information icon to its right.

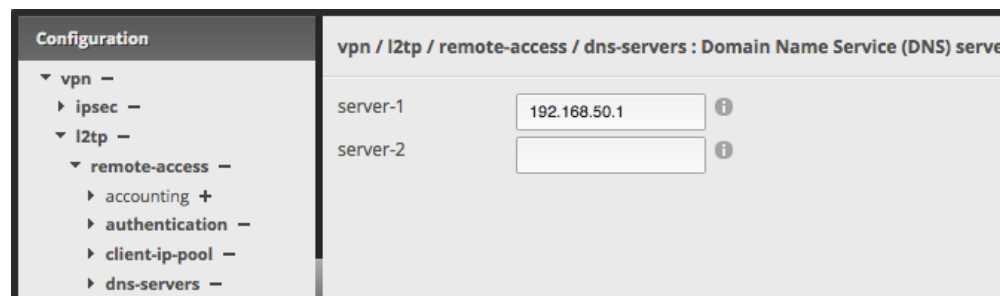
IMPORTANT:

It is allowed that the address pool overlaps with the address range of your LAN network but it must not overlap with the DHCP range of any network!

Step Six: Setting up DNS servers

Setting up DNS servers is optional. It is only required if VPN clients need to use specific DNS servers once connected to the VPN, e.g. to be able to resolve private DNS names from within the LAN.

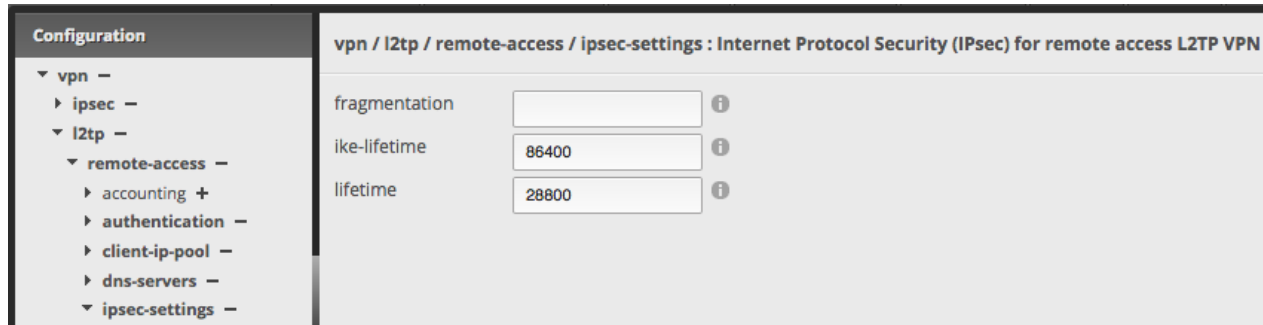
- Open up the branch “vpn > l2tp > remote-access > dns-servers”.
- Enter one or two DNS servers.



The screenshot shows the configuration page for DNS servers. The left sidebar is titled "Configuration" and has a tree view with the following items: "vpn" (expanded), "ipsec", "l2tp" (expanded), "remote-access" (expanded), "accounting", "authentication", "client-ip-pool", and "dns-servers" (selected). The main content area is titled "vpn / l2tp / remote-access / dns-servers : Domain Name Service (DNS) server". It contains two input fields: "server-1" with the value "192.168.50.1" and "server-2" which is empty. Each input field has an information icon to its right.

Step Seven: Setting up IPsec settings

- Open up the branch “vpn > l2tp > remote-access > ipsec-settings”.
- Enter an IKE lifetime in seconds into the field “ike-lifetime”. We recommend 86400 (24 hours).
- Enter an IPsec lifetime into the field “lifetime”. We recommend 28800 (8 hours).

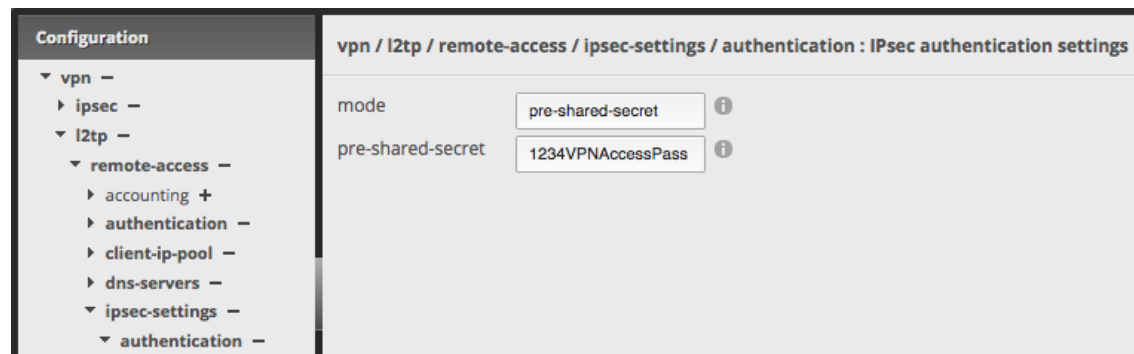


Step Eight: Setting up IPsec authentication

- Open up the branch “vpn > l2tp > remote-access > ipsec-settings > authentication”.
- Type “pre-shared-secret” into the field “mode”.
- Enter a Pre-Shared-Key into the field “pre-shared-secret”.

Note:

All VPN users will require to know this secret password to be able to connect to the VPN, yet they will also have to know a valid user login from [Step Five](#).



Step Nine: Applying the configuration

- Press the “Preview” button that is found at the bottom of every settings page to see a list of all settings you have changed.
- Press “Apply” to save and activate these settings.

Note:

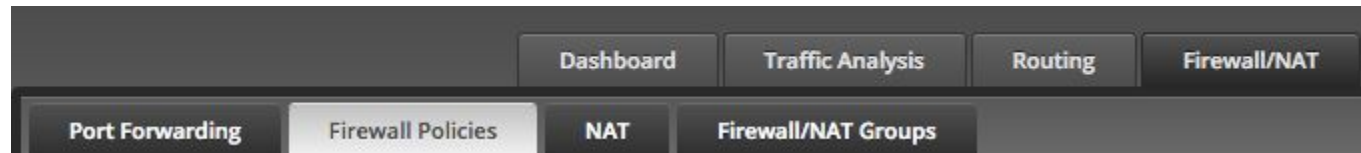
The device will first try to activate and then save the settings. If the settings cannot be activated in, e.g. in case of a settings mistake, they also won't be saved to avoid that broken settings are persistently stored. If you leave the config UI without the settings being stored, all the settings you've just changed will be lost, even without the device rebooting. If applying failed with an error, please go back and proofread the settings. In case you found and fixed a mistake, just repeat this step.

Task Two - Setting up the firewall

By default the firewall drops all incoming data packets that don't seem to be replies to previously sent outgoing data packets. In case you have completely disabled the firewall, you can skip Task Two, otherwise you need to poke a view holes into the firewall to let VPN related traffic from clients pass through.

Step One: Open the firewall policies

- Select the tab "Firewall/NAT".
- Select the sub-tab "Firewall Policies".



Step Two: Choosing an appropriate Ruleset

- Locate the Ruleset "WAN_LOCAL".
- From the "Action" button to the right, select "Edit Ruleset".

Name	Interfaces
WAN_IN	eth0/in
WAN_LOCAL	eth0/local

IMPORTANT:

If you deleted the Ruleset "WAN_LOCAL" or replaced it by a new Ruleset, you might have to first create a Ruleset or add the following rules to a different Ruleset. The required rules need to be added to a Ruleset that is attached to the WAN interface with direction "local". If your WAN interface is named eth0, the Ruleset table should list "eth0/local". The default Ruleset named "WAN_LOCAL" serves this purpose. Do not add the rules to a Ruleset bound to direction "in", as this only affects traffic whose destination lies within any LAN network but not traffic that terminates at the router itself, as is the case for all VPN traffic.

Step Three: Creating an IKE rule

- Press "Add New Rule".
- Enter "IKE" as "Description".
- Select "Accept" as "Action".
- Select "UDP" as "Protocol".
- Select the tab "Destination".
- Enter "500" at "Port".
- Press the button "Save".

Step Four: Creating a NAT-T rule

- Press "Add New Rule".
- Enter "NAT-T" as "Description".
- Select "Accept" as "Action".
- Select "UDP" as "Protocol".
- Select the tab "Destination".
- Enter "4500" at "Port".
- Press the button "Save".

Step Five: Creating an ESP rule

- Press "Add New Rule".
- Enter "ESP" as "Description".
- Select "Accept" as "Action".
- Select "Choose a protocol by name" as "Protocol".
- Select "ESP" from the drop-down.
- Press the button "Save".

Step Six: Creating an L2TP rule

- Press "Add New Rule".
- Enter "L2TP" as "Description".
- Select "Accept" as "Action".
- Select "UDP" as "Protocol".
- Switch to tab "Advanced".
- Select "Match inbound IPSec packets" at the section "IPSec".
- Select the tab "Destination".
- Enter "1701" at "Port".
- Press the button "Save".

Step Seven: Verifying the new rules

After following the steps three to six, the rule table should list the following new rules:

IKE	port 500	udp	accept
NAT-T	port 4500	udp	accept
ESP		esp	accept
L2TP	port 1701	udp	accept

The edit dialog can simply be closed as the newly created rules have already been stored and are already active.

Task Three - Setting up VPN Tracker

Step One: Add a connection

- Open VPN Tracker 365.
- Click on "Create a connection", or click on the + in the bottom left corner of the app window.
- Select "Ubiquiti > EdgeRouter"
- Click "Create."

Step Two: Configure the VPN connection for your device

- Click on "Configure" and go to the "Basic" tab.
- Enter the public (WAN) IP address or DNS name of your EdgeRouter in the field "VPN Gateway".
- By default only traffic to the IP pool network from [Step Six of Task One](#) will be routed over the VPN connection, so by default VPN clients can only talk to other connected VPN clients but not reach anything else on the remote side. You have two options here:
 - ◆ You can either list all the remote networks that you require access to under "Additional Remote Networks" (e.g. 192.168.50.0 / 24)
 - ◆ You can change the "Topology" from "Host to Network" to "Host to Everywhere" to make the VPN tunnel your new default route, in which case all non-local network traffic is sent over the VPN tunnel, including traffic to public IP addresses.

Note:

If the Internet shall stay reachable for VPN clients in a "Host to Everywhere" setup, the router needs to be configured to also forward and possibly also NAT the traffic from VPN users to the Internet. VPN clients will then access the Internet as if they were in the LAN behind the router, thus their public IP address may not be visible to Internet services and their traffic can be filtered by firewall filter rules. The router setup for this scenario is beyond the scope of this guide, though.

Task Four - Testing the VPN connection

In order to test your connection, you will need to connect from a different Internet connection than the one the gateway is using. For example, if you are setting up a VPN connection to your office, try it out at home, from an Internet cafe, or use your mobile phone as your own personal hotspot.

Connect to your VPN

- Check first of all that your internet connection is working as it should be. Use this link as a test: <http://www.equinux.com>
- Start the VPN Tracker 365 app.
- Click on the On/Off slider to turn on your connection.

IMPORTANT:

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.

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.

TIP: 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.

VPN Tracker Manual

The [VPN Tracker Manual](http://www.vpntracker.com/support) contains detailed troubleshooting advice. Answers to frequently asked questions (FAQs) 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).
- Device vendor, model, and firmware version installed.
- Screenshots of the VPN settings on your VPN gateway as shown by this guide.

IMPORTANT: 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.