VPN Tracker 365

VPN Configuration Guide

Amazon Web Services (AWS)
Virtual Private Cloud (VPC)

Configuration guide revision 2

Created using Apple Pages.

www.equinux.com

Contents

Introduction

Prerequisites

Your VPN Gateway

- You have an Amazon Web Services (AWS) account.
- You have configured a Virtual Private Cloud (VPC) at Amazon.

Your Mac

- Your Mac runs on Mac OS X 10.9 or later.
- You have the latest VPN Tracker 365 release installed. The latest VPN Tracker updates can always be obtained from http://www.vpntracker.com

Using the Configuration Guide

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.

Scenario

In our example, we want to give a couple of employees access to cloud servers and services hosted at Amazon inside a Virtual Private Cloud (VPC).

This guide is not about configuring access to the VPC using the standard VPN access that Amazon offers as this VPN access is a gateway to gateway VPN that requires both sides of the VPN to have a static IP address.

Instead we will setup a user based VPN where users with dynamic IP addresses directly connect to a an EC2 server that (also) acts as a VPN gateway and provides users with access to all the desired servers and services available within the private cloud.

This guide assumes that the Mac running VPN Tracker already has internet connectivity.

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.

Getting Additional 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.

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 three parts of this document and make modifications only after you have tested the basic setup.

Part 1 – Preparing Your VPC Setup

We will first prepare a virtual server (EC2) within your VPC that shall act as a VPN gateway. This guide assumes that you are already familiar with the Amazon Web Services. Please search the AWS help and contact Amazon's support if you need further help with AWS administration. Please note that we can't provide any support for Amazon services.

Step 1 – Choosing a Virtual Server

Unless you already have a suitable EC2 instance running in your Amazon VPC, you'll first need to create a new instance. It won't need a lot computation power or memory to act as a VPN gateway, but depending on the expected number of users and expected data throughput, it will need a sufficient amount of network performance.

You are free in the choice of an operating system as long as it is a Linux based operating system. For this guide, we assume you chose *Amazon Linux AMI*, but feel free to choose a different Linux system, as long as you are familiar with that system, know how to install software packages, control installed services and edit configuration files.

Step 2 – Assigning a Public IP Address

A VPN gateway needs to reachable from public Internet, so your EC2 instance needs a public IP address. Allocate one and assign it to the virtual server instance.

Remember that public IP address, it will become your **VPN gateway address** later on.

Step 3 – Modify the Security Group

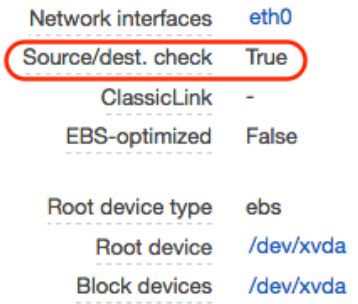
All virtual servers at Amazon are protected by a firewall. To allow a virtual server to act as a VPN gateway, you need to allow certain kinds of traffic to pass through that firewall. This is accomplished by adding three custom inbound rules to the security group of the virtual server. Two of them are required for negotiating VPN tunnels and tunneling the actual VPN traffic later on, one of them is required so that the server can actually act as a traffic forwarding gateway for all the other servers in your VPC:

- UDP port 500 from any source
- UDP port 4500 from any source
- Any traffic from the other VPC servers (10.0.0.0/16 in our example)

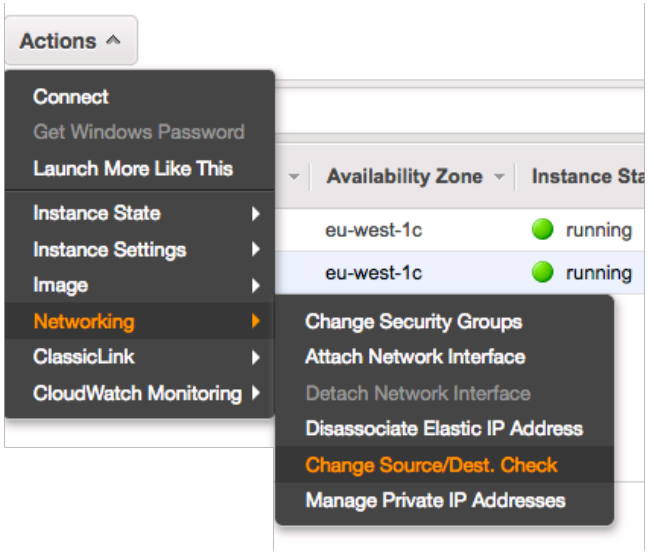
Type	Protocol	Port Range	Source	
All traffic	All	0 - 65535	Custom	10.0.0.0/16
SSH	TCP	22	Anywhere	0.0.0.0/0
Custom UDP Rule	UDP	4500	Anywhere	0.0.0.0/0
Custom UDP Rule	UDP	500	Anywhere	0.0.0.0/0

Step 4 – Disable Source/Destination Checking

By default, all EC2 servers have an additional firewall protection, named **Source/dest. check**. When enabled, a server cannot act as a packet forwarder for other servers and thus also not as a VPN gateway. Select your virtual server in the overview table and check the description to see if this option is enabled:



If it is enabled, disable it through the Actions menu (**Actions ▶ Networking ▶ Change Source/Dest. Check**):



Step 5 – Install ipsec-tools

Log in to your virtual server (e.g. using SSH) and install the ipsec-tools package. If you chose Amazon Linux AMI as your operating system, just execute the following command:

```
→ sudo yum install ipsec-tools
```

Step 6 – Activate the ipsec-tools Service

It is important to activate the background service of ipsec-tools, called "racoon", to make sure it is started automatically every time time the virtual server needs to be rebooted. On Amazon Linux AMI, this can be done by executing the following command:

```
→ sudo chkconfig racoon on
```

Step 7 – Enabling IP Forwarding

To make your virtual server act as a VPN gateway, it needs to forward IP packets. Without enabling forwarding, a server only accepts packets that are for itself, all other packets are discarded. To enable IP forwarding, edit the file /etc/sysctl.conf and make sure it contains the following line:

```
net.ipv4.ip_forward = 1
```

On Amazon Linux AMI, the line above is already present in the file but the setting is disabled. You can quickly change this by executing the following command:

```
→ sudo sed -i -E 's/(net.ipv4.ip_forward *= *)0/\11/'
      /etc/sysctl.conf
```

After changing the file, you need to make sure the settings take effect immediately. Just execute the following command to re-apply the settings:

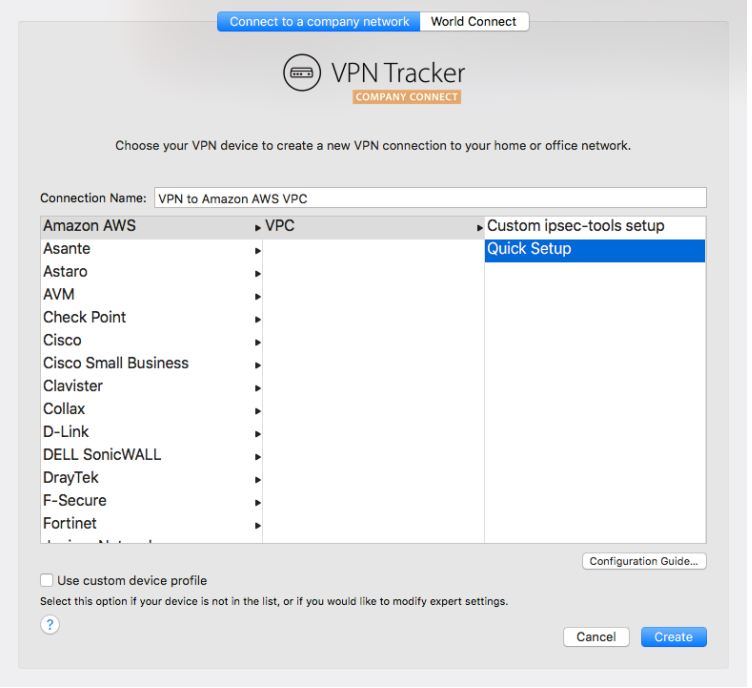
```
→ sudo sysctl -p /etc/sysctl.conf
```

Part 2 – Setting Up VPN Tracker

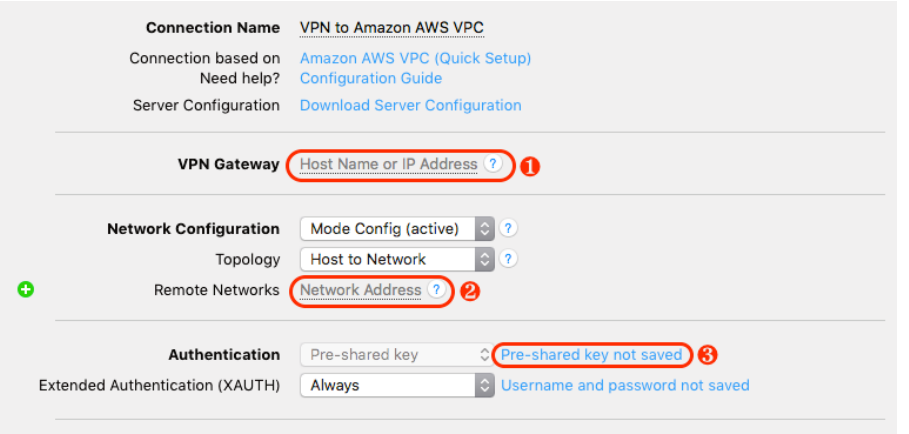
We will now configure a VPN connection within VPN Tracker on your Mac. This guide assumes that you are familiar with macOS and have VPN Tracker installed on your Mac. For any questions regarding VPN Tracker that are not covered by this guide, please have a look at the VPN Tracker manual.

Step 1 – Create a New Connection

- From the **File** menu, choose **New ▶ Company Connection…**
- Give your connection a name
- Select **Amazon AWS ▶ VPC ▶ Quick Setup**
- Choose **Create**



Step 2 – Configure Your Connection

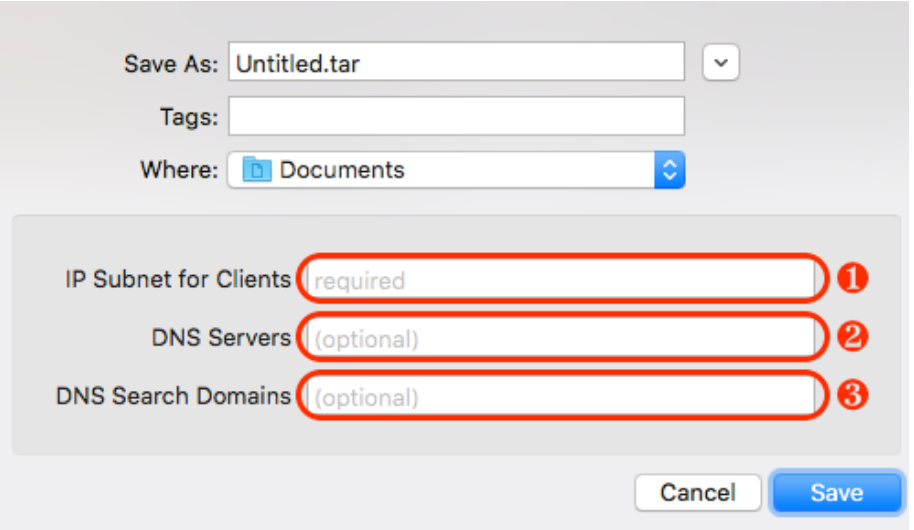


- Enter the **VPN Gateway** address, that is the elastic (public) IP you assigned to your virtual server acting as a VPN gateway. ❶
- Enter one or more **Remote Networks**. These are the networks that VPN users shall have access to once connect to the VPN. By default Amazon places VPC servers into the subnet range **10.0.0.0/24** (for publicly reachable servers) and the VPC network as a whole is **10.0.0.0/16**. ❷
- Enter a **Pre-Shared Key** (PSK) for the connection to use. You are totally free to choose any PSK you like but keep standard rules for secure passwords in mind, a PSK should be hard to guess! ❸

There are other connection settings available that you can alter if you know what you are doing. Note however that changing any settings other than those indicated in this guide is neither necessary nor recommended for beginners following this guide for the very first time.

Step 3 – Generate Server Configuration

- Click **Download Server Configuration**.



- Enter a file name of your choice. VPN Tracker will create a TAR archive with that name that contains the configuration you'll need to finish the VPN setup on your server.
- Enter the **IP Subnet for Clients**. This can be any private network of your choice. VPN clients will get IP addresses assigned from this subnet range. Assigning IP addresses to clients is important to avoid IP address conflicts between different VPN clients. Don't choose any subnet range of your VPC network, this isn't going to work. E.g. try **172.73.74.0/24**. ❶
- *Optionally:* Enter **DNS Servers**. If you like would VPN users to use custom DNS servers as soon as their VPN tunnel is up, e.g. to resolve private domains that would otherwise not resolve with standard DNS servers, enter them here. Multiple servers can be entered, separated by comma. ❷
- *Optionally:* Enter **DNS Search Domains**. If you want to limit the usage of the DNS Servers entered above to only certain domains or subdomains, enter these domains here. Multiple domains can be entered, separated by comma. ❸
- Click on **Save**.

Make sure the **IP Subnet for Clients** is not a subnet of your VPC network! VPN client addresses must not be part of that network, otherwise your VPC servers will think that VPN users are in fact local VPC hosts and will try to contact them directly (which won't work). Only if your VPC server can see from their address that they are external hosts, will their replies be forwarded to the Internet gateway of your VPC and this is crucial to make → *Part 3 Step 7* work!

Part 3 – Finalizing Your VPN Gateway Setup

Step 1 – Copy the Server Configuration

Copy the TAR archive that VPN Tracker has created for you to your virtual EC2 server, e.g. using SCP by running the following command on your Mac in a terminal window (instead of Untitled.tar, use the filename you have chosen in → *Part 2 Step 3* instead of the IP address 203.0.113.33, use the IP address of your gateway server):

```
→ scp ~/Documents/Untitled.tar ec2-user@203.0.113.33:/tmp/
```

Step 2 – Unarchive the Server Configuration

Log in to your virtual server (e.g. using SSH) and extract TAR archive. Here's an example how you could do it:

```
→ cd /tmp
→ tar xf Untitled.tar
→ rm Untitled.tar
```

You will find two new files in your current folder:

```
vpntracker.racoon.conf
psk.txt
```

Step 3 – Install the racoon Configuration

Move the racoon config file to the folder /etc/racoon and include it from within the racoon.conf file. For example:

```
→ sudo mv vpntracker.racoon.conf /etc/racoon/
→ echo 'include "vpntracker.racoon.conf";' |
      sudo tee -a /etc/racoon/racoon.conf
```

Step 4 – Install the Pre-Shared Key

Add the pre-shared key entry found in the file psk.txt to the already existing psk.txt in /etc/racoon, then **delete it for security reasons**:

```
→ cat psk.txt | sudo tee -a /etc/racoon/psk.txt
→ rm psk.txt
```

Step 5 – Restart the racoon Daemon

To make sure racoon picks up the new configuration, you have to restart it (or start it):

```
→ sudo service racoon restart
```

Step 6 – Create a Local User

A user based VPN also requires user authentication. For the simple setup described in this guide, we'll just create a local user directly on the virtual server and assign them passwords. Here's an example how you could do it (instead of "vpnuser", use the actual username you wish to set up):

```
→ sudo useradd vpnuser
→ sudo passwd vpnuser
```

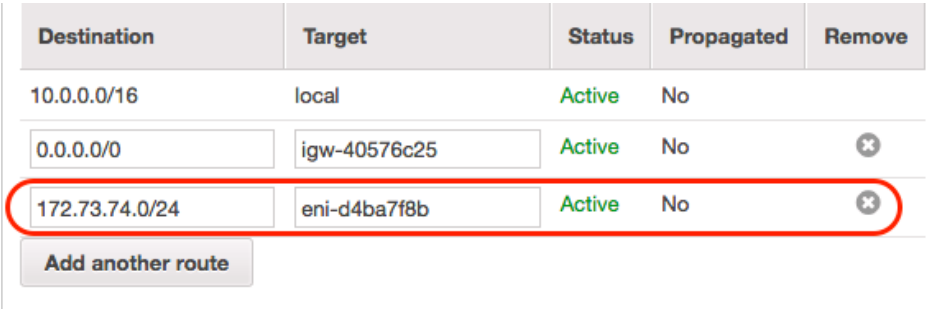
Just repeat Step 6 multiple times to setup multiple user accounts. You should create one account per VPN user. In case you ever want to lock out a user from your VPN, just delete that user account again. Of course, more advanced user setups are possible. E.g. you can add all VPN users to a user group and then limit VPN access to users of that group. It is also possible to hint racoon towards an external user database, e.g. a LDAP server or a Radius server, so that your VPN is connected to your existing central user management.

Step 7 – Setup VPN Routing

In our final step, you have to teach the Internet gateway (which is implicitly created for you when you create a VPC and connects your whole VPC to the Internet and acts as a central router and firewall for all your VPC servers), how to reach the VPN users. This is crucial as all your VPC servers (other than the one you use as VPN gateway) don't know about the existence of your VPN and won't be able to get any network replies to your VPN users.

We want the VPC Internet gateway to forward all packets intended for VPN users to the virtual server from → *Part 1 Step 1* that acts as a VPN gateway (this is the only server that knows about the VPN and how to correctly forward packets to VPN users).

Go to the VPC dashboard and select **Route Tables**. You need to add a custom route to every routing table of every subnet that shall be reachable for VPN users. The **Destination** is the IP Subnet for Clients you chose in → *Part 2 Step 3* and the **Target** is the ID of your virtual server from → *Part 1 Step 1* ("i-..."), in that case Amazon will choose an interface for you, or even better, the ID of one of its interfaces (e.g. "eni-…"):



You're ready to test the VPN Connection

Start your connection

- Slide the On/Off slider for the connection you have just configured to On
- Check whether your new VPN server is working as expected