



VPN Tracker 365

VPN Configuration Guide

Dell SonicWALL

© 2015 equinux AG and equinux USA, Inc. All rights reserved.

Under copyright law, this manual may not be copied, in whole or in part, without the written consent of equinux AG or equinux USA, Inc. Your rights to the software are governed by the accompanying software license agreement.

The equinux logo is a trademark of equinux AG and equinux 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.

equinux 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 equinux has been advised of the possibility of such damages.

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

Revised September 22, 2015

Created using Apple Pages.

www.equinux.com

Contents

Introduction.....4

- Prerequisites 4
- Using the Configuration Guide 4
- Scenario 5

My VPN Gateway Configuration.....6

Task 1 – SonicWALL Configuration7

Option A – Express Setup.....7

- Gather Configuration Information 7
- Set Up VPN Tracker 7

Option B – Complete Setup7

- Step 1 – WAN IP and LAN Network 7
- Step 2 – Enable VPN on your SonicWALL 8
- Step 3 – GroupVPN Settings 8
- Step 4 – Configure DHCP over VPN 11
- Step 5 – Check your DHCP Server Settings 12
- Step 6 – Add a VPN User 13
- Step 7 – Configuring VPN Access Lists 14

Task 2 – VPN Tracker Configuration15

- Step 1 – Add a Connection 15
- Step 2 – Configure the VPN Connection 16

Task 3 – Test the VPN Connection17

- Troubleshooting 18

Appendix20

Remote DNS Setup20

- Prerequisites 20
- Option A – Setup in VPN Tracker 20

- Option B – Setup on the SonicWALL 21
- Host to Everywhere 22
- Manual VPN Tracker Setup 24
- Prerequisites 24
- Step 1 – Add a Connection 24
- Step 2 – Configure the VPN Connection 24

Introduction

This configuration guide helps you configure VPN Tracker and your Dell SonicWALL VPN Gateway to establish a VPN connection between them.

Prerequisites

Your VPN Gateway

- ▶ This document applies to SonicWALLs running SonicOS 4.0 or newer. Documentation for older SonicOS versions may be available at <http://www.vpntracker.com/interop>.
- ▶ Make sure you have installed the newest SonicOS version available to ensure that you have all security updates.
- ▶ This guide is a supplement to the documentation included with your SonicWall device, it can't replace it. Please read it before starting.

Your Mac

- ▶ The configuration described in this guide requires VPN Tracker 365. Make sure you have installed all available updates. The latest VPN Tracker updates can be downloaded from <http://www.vpntracker.com>

Using the Configuration Guide

SonicWALL Configuration

Express Setup

If you are familiar with VPNs and SonicWALLs, and already have VPN configured on the SonicWALL, the Express Setup will guide you through setting up VPN Tracker as quickly as possible.

Complete Setup

If you do not yet have a working VPN setup on your SonicWALL, this is the place to start. We'll show you how to configure a VPN on your SonicWALL.



If you are setting up VPN on your SonicWALL for the first time, we strongly recommend you keep to setup proposed in this guide, and make modifications only after you have tested the basic setup.

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.

Appendix

The remainder of the guide covers advanced setups, such as Remote DNS and setting up VPN Tracker without SonicWALL Simple Client Provisioning.

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.

Scenario

In our example, we need to connect an employee's Mac to an office network. The diagram below illustrates this scenario.

This guide assumes that the Mac running VPN Tracker already has Internet connectivity. The office's SonicWALL (the "VPN gateway") is also already connected to the Internet and can be accessed through a static IP address (here: 203.0.113.1) or a DNS host name (here: vpn.example.com).

The VPN gateway's LAN interface is connected to the internal office network. In our example, the office network is 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.

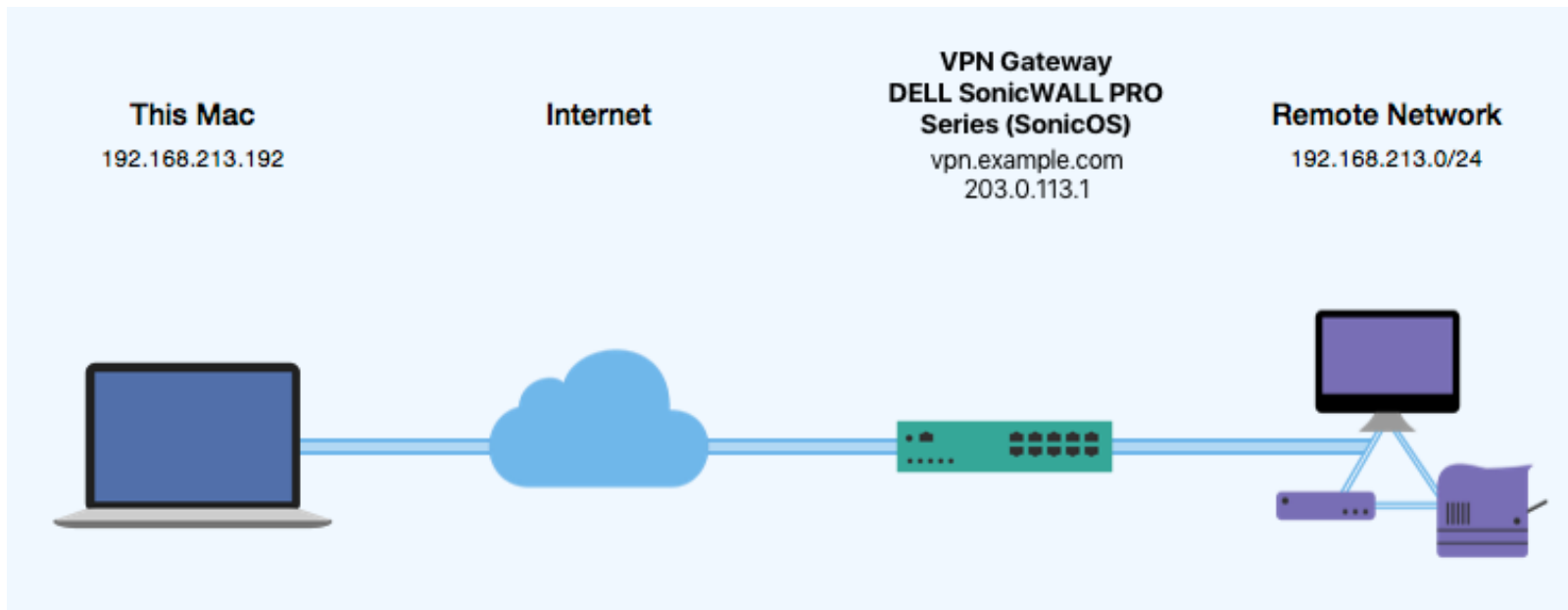
Terminology

A VPN connection is often called a **tunnel**. A VPN tunnel is established between two **endpoints**. Here one endpoint is VPN Tracker and the other endpoint is the VPN gateway. Each endpoint is the other endpoint's **peer**.

For each endpoint, the other endpoint's settings **remote**, while its own settings are **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 topology shown below is called **Host to Network**: A single computer, a **host**, establishes a VPN to an entire network "behind" the VPN gateway.

Another useful topology is called **Host to Everywhere**: A single computer sends its Internet traffic through the VPN, thereby protecting it from local attacks (e.g. in public Wi-Fi networks) and making it appear to originate from the VPN gateway's location.



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

IP Addresses

- ❶ SonicWALL WAN IP Address: _____ or host name _____
- ❷ SonicWALL LAN Network: _____ / _____

Firewall Identifier

- ❸ Unique Firewall Identifier: _____

Authentication

- ❹ Pre-Shared Key: _____
- ❺ XAUTH Username: _____
- ❻ XAUTH Password: _____

Task 1 – SonicWALL Configuration

If you're familiar with SonicWALLs and already have a working VPN setup on your SonicWALL, you can skip the SonicWALL setup and use Option A. If your SonicWALL is not yet set up, use Option B. Regardless which option you choose, this guide assumes that your SonicWALL has Internet access and that a LAN network is configured.

Option A – Express Setup

Gather Configuration Information

You'll need the following information to set up VPN Tracker. Use the → *Configuration Checklist* on the previous page to keep track of it. You will not need any of the other information listed in the checklist.

Your SonicWALL's Public (WAN) IP address or host name ❶

Locate this information on your SonicWALL under **Network > Interfaces**, or in the GlobalVPN Client on Windows.

Pre-Shared Key ❷

The pre-shared key is called “**Shared Secret**” on the SonicWALL. The shared secret is configured on your SonicWALL under **VPN > Group-VPN > General > Shared Secret**.



If “Use Default Key for Simple Client Provisioning” is enabled on the SonicWALL (VPN > GroupVPN > Client), no pre-shared key is needed.

XAUTH Username ❸ and Password ❹

If your SonicWALL uses Extended Authentication (XAUTH), you need the username and password for a user who is authorized to access the VPN.

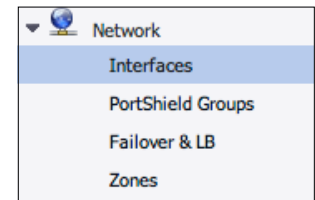
Set Up VPN Tracker

Skip ahead to → *Task 2 – VPN Tracker Configuration* to set up VPN Tracker with the information you've just gathered.

Option B – Complete Setup

Step 1 – WAN IP and LAN Network

- ▶ Connect to your SonicWall's web interface.
- ▶ Go to **Network > Interfaces**.
- ▶ Write down the **IP address of the external (WAN) interface** as ❶ and the **LAN Network** as ❷ on your → *Configuration Checklist*.



Interface Settings								
Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.13.1	255.255.255.0	Static	100 Mbps full-duplex	Default LAN	ⓘ
X1	WAN	Default LB Group	203.0.113.1	255.255.255.0	Static	100 Mbps full-duplex	Default WAN	ⓘ
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		ⓘ
W0	WLAN		172.16.31.1	255.255.255.0	Static	300 Mbps half-duplex	Default WLAN	ⓘ

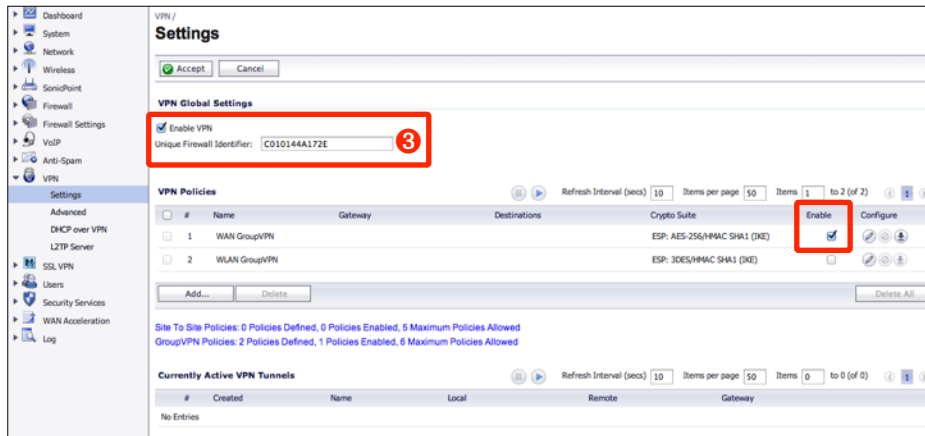
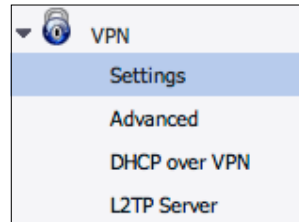


If your SonicWALL is reachable through a public host name (DynDNS or fixed host name) write that down instead as

❶.

Step 2 – Enable VPN on your SonicWALL

- ▶ Go to **VPN > Settings**.
- ▶ Check **”Enable VPN“** under “VPN Global Settings”.
- ▶ Check **“Enable”** for the WAN Group VPN policy.
- ▶ Write down your SonicWALL’s **Unique Firewall Identifier** ③ on your → *Configuration Checklist*.
- ▶ Click **”Accept”**

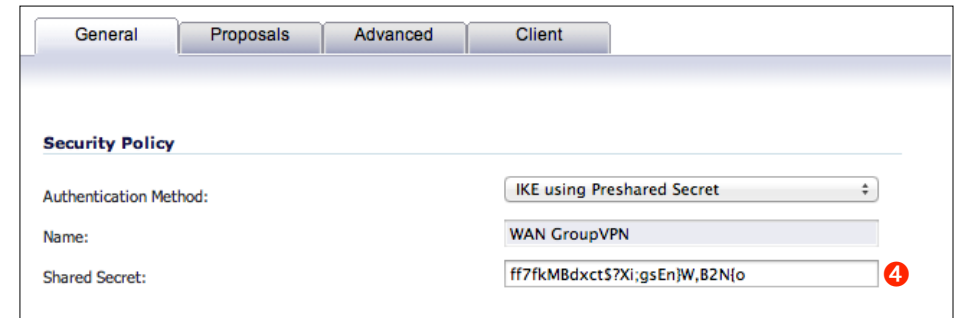


Step 3 – GroupVPN Settings

- ▶ Click the **”Configure”** icon for the GroupVPN policy
- ▶ We’ll be reviewing the settings on each tab. You typically won’t need to make a lot of changes, since VPN Tracker can be set up to match the settings already in place.



General



- ▶ **Authentication Method:** Select “IKE using Preshared Secret”.
- ▶ **Shared Secret:** This password protects your VPN. Choose a long, random password (ASCII characters only) and write it down as ④ on your → *Configuration Checklist*. In VPN Tracker, the shared secret is called **pre-shared key**.



The Unique Firewall Identifier is case-sensitive. Make sure to write it down exactly as it appears on your SonicWALL.



VPN Tracker also supports “IKE using 3rd Party Certificates”.

We recommend setting up the connection with “IKE using Preshared Secret” first. Once everything is working, switch to “IKE using 3rd Party Certificates” if desired.

- Perfect Forward Secrecy (PFS) enabled (with DH group 5 selected)

Proposals

The screenshot shows the 'Proposals' tab in the SonicOS configuration interface. It is divided into two sections: 'IKE (Phase 1) Proposal' and 'Ipsec (Phase 2) Proposal'. The 'General' tab is selected.

IKE (Phase 1) Proposal

DH Group:	Group 2
Encryption:	3DES
Authentication:	SHA1
Life Time (seconds):	28800

Ipsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	3DES
Authentication:	SHA1
<input type="checkbox"/> Enable Perfect Forward Secrecy	
Life Time (seconds):	28800

- The settings shown in the screenshot above are the defaults used by SonicOS. They provide average security.
- For better security, use these settings
 - AES-256 encryption in both phases
 - DH group 5

Advanced

General Proposals **Advanced** Client

Advanced Settings

Enable Windows Networking (NetBIOS) Broadcast

Enable Multicast

Accept Multiple Proposals for Clients

Management via this SA: HTTPS SSH

Default Gateway: 0.0.0.0

Client Authentication

Require authentication of VPN clients by XAUTH

User group for XAUTH users: Trusted Users

Allow Unauthenticated VPN Client Access: --Select Local Network--

Advanced Settings

- ▶ **Enable Windows Networking (NetBIOS) Broadcast** and **Enable Multicast**: Not used for VPN Tracker. You may turn them on or leave them off.
- ▶ **Accept Multiple Proposals for Clients**: Needed for some L2TP clients. Should be off unless you also have L2TP clients connecting.
- ▶ **Management via this SA**: Enable to manage your SonicWALL via VPN.
- ▶ **Default Gateway**: Not used for VPN Tracker. Leave 0.0.0.0 if possible.

Client Authentication

- ▶ **Require authentication of VPN clients by XAUTH**: If checked, each user of the VPN needs to enter their individual username and password, in addition to the pre-shared key (shared secret). XAUTH

makes it easy to revoke VPN access for specific users and provides an additional layer of security.



Use XAUTH unless you have a specific reason not to. This guide will assume that XAUTH is being used.

User group for XAUTH users: The default group is Trusted Users, meaning all users in the group Trusted Users get to access the VPN. You can use a different group if you want to, e.g. one specifically for VPN users.

- ▶ **Allow Unauthenticated VPN Client Access**: If you are not using XAUTH, this setting determines the network(s) VPN clients are allowed to access. The typical choice is “LAN Subnets” (to permit VPN clients to access the SonicWALL’s LAN).

Client

General Proposals Advanced **Client**

User Name and Password Caching

Cache XAUTH User Name and Password on Client: Single Session

Client Connections

Virtual Adapter settings: DHCP Lease or Manual Configuration

Allow Connections to: Split Tunnels

Set Default Route as this Gateway

Client Initial Provisioning

Use Default Key for Simple Client Provisioning

- ▶ **Cache XAUTH User Name and Password on Client**: Using “Single Session” or “Always” is recommended to avoid prompts for XAUTH username and password and possible disconnects when rekeying the

VPN connection. This setting has no effect on VPN Tracker if SonicWALL Simple Client Provisioning is not used, or if XAUTH username and password are stored in keychain.

- ▶ **Virtual Adapter settings:** “DHCP Lease or Manual Configuration” or “DHCP Lease” is recommended. Use “None” only if other VPN users who are not using VPN Tracker rely on this setting.
- ▶ **Allow Connections:** This setting is not used for VPN Tracker at this time.
- ▶ **Set Default Route as this Gateway:** Leave unchecked.



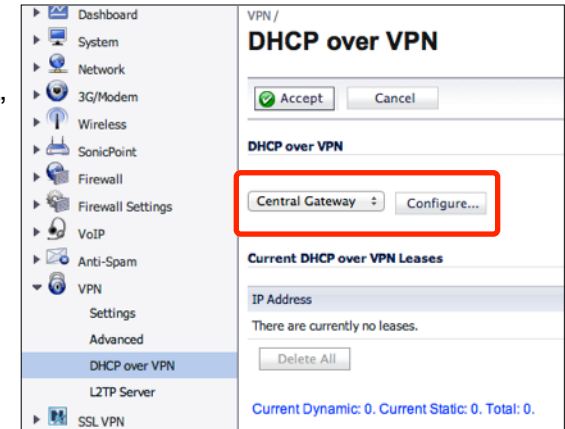
If you check this box, you'll set up a Host to Everywhere connection, tunneling all Internet traffic through the VPN. Such a setup requires additional configuration.

We therefore strongly recommend testing your setup with a Host to Network connection first. More information can be found in → *Host to Everywhere*.

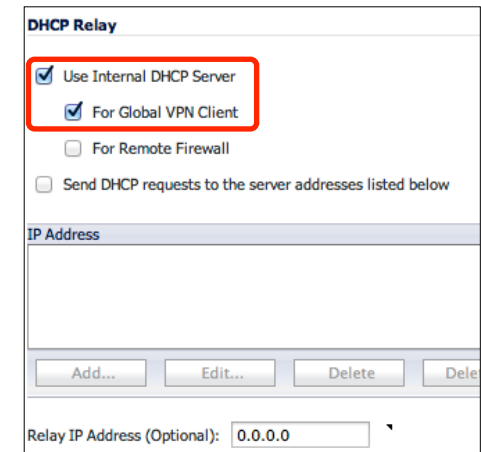
- ▶ **Use Default Key for Simple Client Provisioning:** If checked, users of VPN Tracker and of SonicWALL's GlobalVPN client do not need to know the pre-shared key (shared secret). For increased security, we recommend leaving this setting off.

Step 4 – Configure DHCP over VPN

- ▶ Go to **VPN > DHCP over VPN**.
- ▶ Select “**Central Gateway**” from the popup list.
- ▶ Click “**Configure...**”.

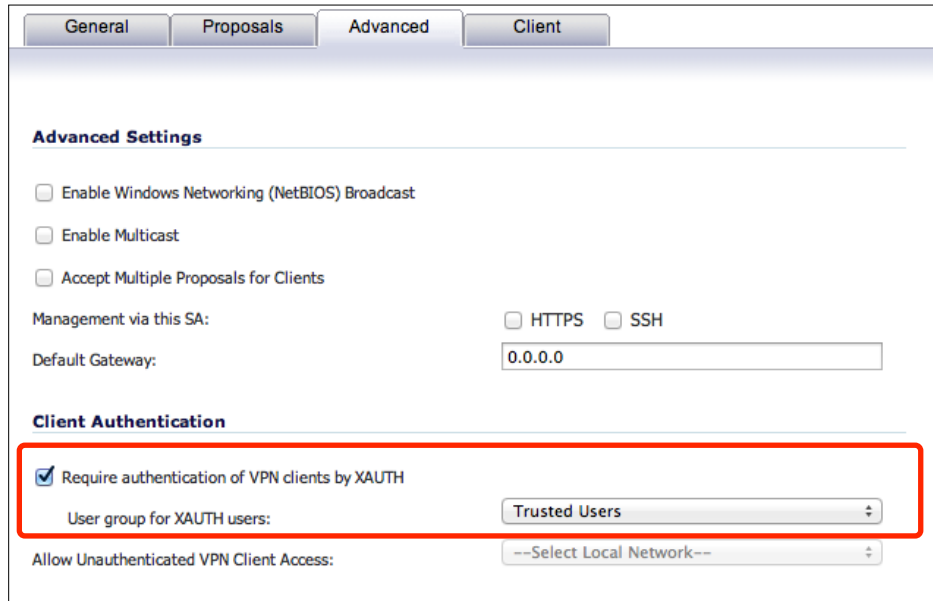


- ▶ Check “**Use Internal DHCP Server**”.
- ▶ Check “**For Global VPN Client**”.
- ▶ Click “**OK**”.

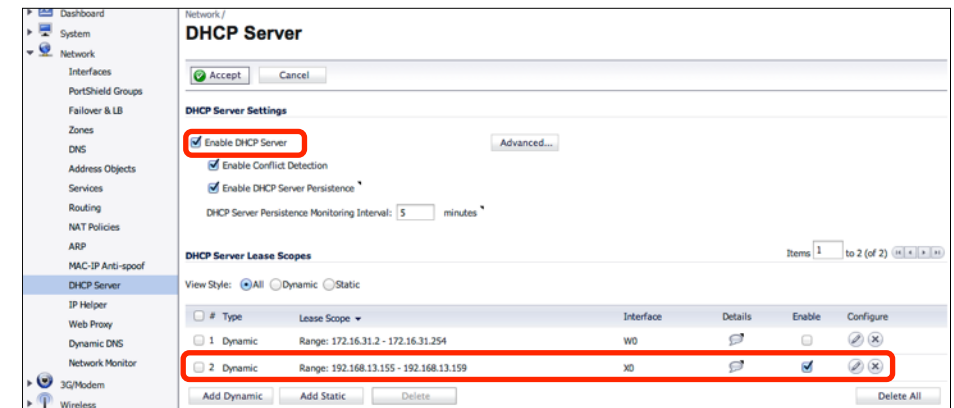


Step 5 – Check your DHCP Server Settings

- ▶ Go to **Network > DHCP Server**.
- ▶ Make sure the box “**Enable DHCP Server**” is checked.
- ▶ Check that a **dynamic range of IP addresses** is configured and enabled for the LAN interface.



The screenshot shows the 'Advanced' tab of the SonicWALL configuration interface. Under the 'Client Authentication' section, the checkbox 'Require authentication of VPN clients by XAUTH' is checked and highlighted with a red box. Below it, the 'User group for XAUTH users' dropdown menu is set to 'Trusted Users'. Other options include 'Enable Windows Networking (NetBIOS) Broadcast', 'Enable Multicast', and 'Accept Multiple Proposals for Clients'. The 'Default Gateway' is set to '0.0.0.0'.



The screenshot shows the 'DHCP Server' configuration page. The 'Enable DHCP Server' checkbox is checked and highlighted with a red box. Below it, the 'DHCP Server Lease Scopes' table is visible, with the second row highlighted in red. The table has columns for '#', 'Type', 'Lease Scope', 'Interface', 'Details', 'Enable', and 'Configure'.

#	Type	Lease Scope	Interface	Details	Enable	Configure
1	Dynamic	Range: 172.16.31.2 - 172.16.31.254	W0		<input type="checkbox"/>	
2	Dynamic	Range: 192.168.13.155 - 192.168.13.159	X0		<input checked="" type="checkbox"/>	



If your network infrastructure requires you to use an external DHCP server, you can configure the SonicWALL to relay DHCP requests to this server. Check the box “Send DHCP requests to the server addresses listed below” and enter the DHCP server’s address. In the following step, check your external DHCP server’s settings instead of the SonicWALL’s built-in DHCP server.

DHCP over VPN MAC Addresses

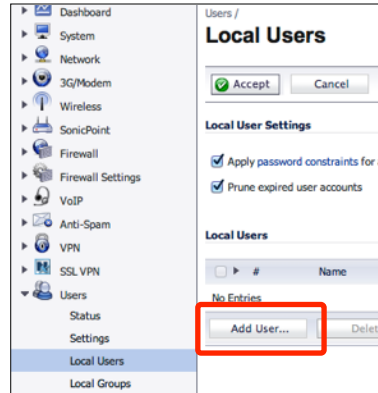
VPN Tracker uses a modified hardware address for DHCP over VPN to avoid conflicts with your Mac’s actual, factory-assigned hardware address. The modified hardware address is generated based on the Mac’s actual hardware address of the first network interface, e.g.

Original MAC address: 00:1b:63:B7:42:23

VPN Tracker MAC address: 02:1b:63:B7:42:23

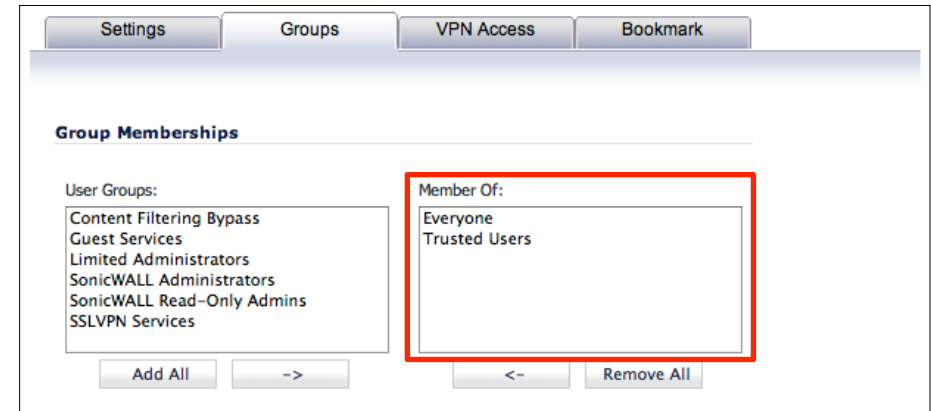
Step 6 – Add a VPN User

- ▶ Go to **Users > Local Users**
- ▶ Click “**Add User...**”

A screenshot of the 'User Settings' form in the SonicWall configuration interface. The form includes fields for 'Name' (containing 'alice'), 'Password', 'Confirm Password', 'E-mail address', 'Account Lifetime' (set to 'Never expires'), and 'Comment'. There are also checkboxes for 'User must change password' and 'Require one-time passwords'. The 'Name' and 'Password' fields are marked with red circles containing the numbers 5 and 6 respectively.

- ▶ **Name:** Enter a user name **5** and write it down on your → *Configuration Checklist*.
- ▶ **Password:** Enter a password **6**
- ▶ **Confirm Password:** Enter the same password again.

- ▶ Switch to the **Groups** tab.



- ▶ Make sure the new user is a member of the “**Trusted Users**” group (or whatever group you selected earlier under GroupVPN > Advanced > Client Authentication > User group for XAUTH users).
- ▶ Add the new user by clicking “**OK**”.

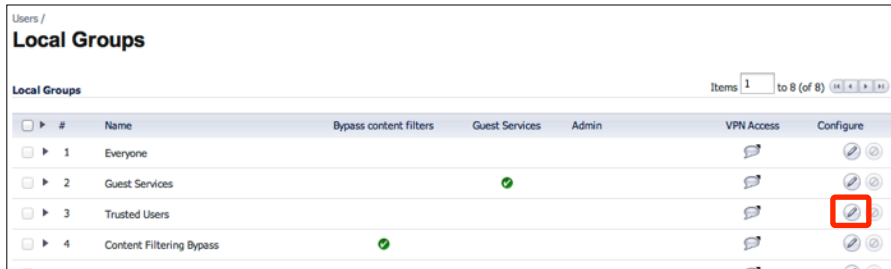


To add more users to your VPN connection later, repeat this step.

Step 7 – Configuring VPN Access Lists

The VPN Access list determines the networks that users can access through VPN. Access lists can be set up for each user individually or for the entire group. This is what we will be doing.

- ▶ Go to **Users > Local Groups**.



- ▶ Click the **“Configure”** button for the **“Trusted Users”** group.
- ▶ Switch to the **“VPN Access”** tab.
- ▶ Add the desired networks to the **“Access List”**. For most setups, **“LAN Subnets”** or **“Firewalled Subnets”** will be a good choice.



- ▶ Click **“OK”**.

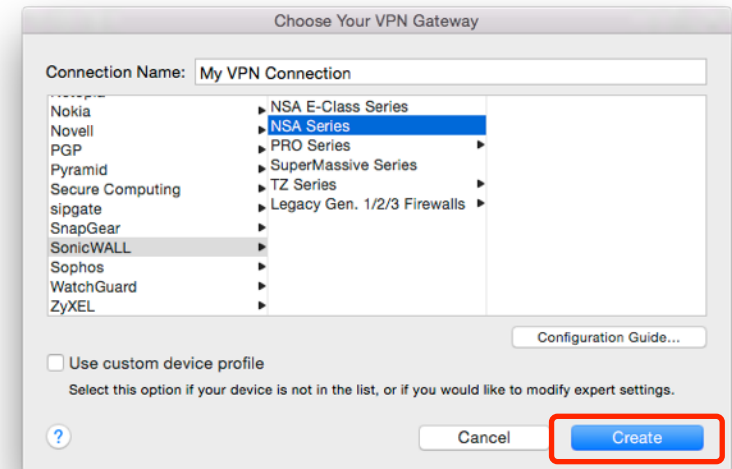
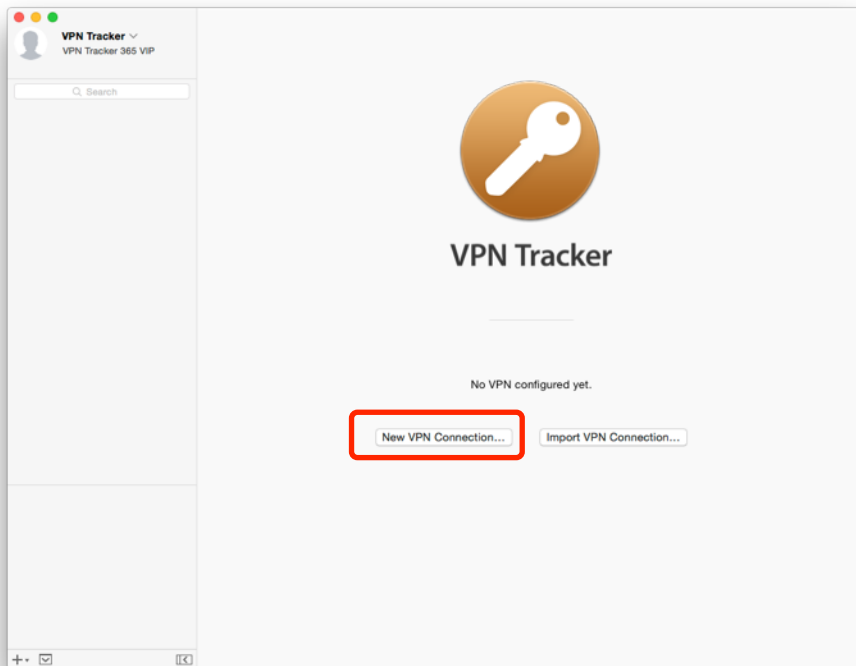


Refer to **“Network > Address Objects”** on your Sonic-WALL if you do not know which network or IP addresses a specific network object represents.

Task 2 – VPN Tracker Configuration

From Task 1, you should have a completed → *Configuration Checklist* containing your SonicWALL's settings. We will now create a matching configuration in VPN Tracker.

Step 1 – Add a Connection



- ▶ Select **“SonicWALL”** or **“DELL SonicWALL”** from the list.
- ▶ Select your SonicWALL model (e.g. NSA Series).
- ▶ Click **“Create”**.

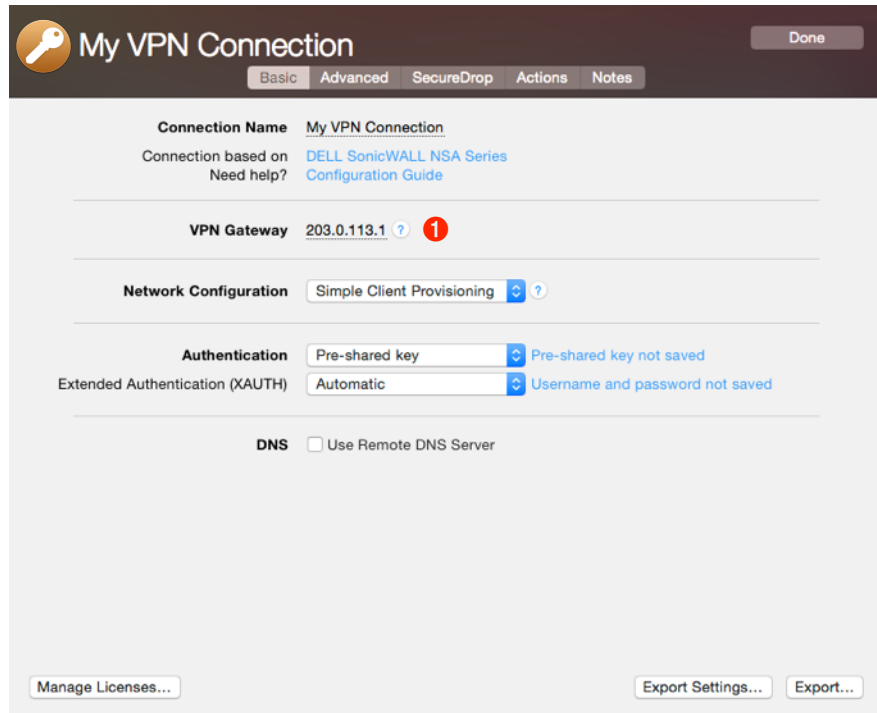


For some devices, multiple SonicOS versions are listed. Please select “SonicOS” if multiple versions are listed.

- ▶ Open VPN Tracker.
- ▶ Click **“New VPN Connection”** (or click the + button in the lower left corner).

Step 2 – Configure the VPN Connection

- ▶ Click “**Configure**” and switch to the “**Basic**” tab if it is not already displayed.
- ▶ **VPN Gateway**: Enter your SonicWALL’s public IP address or its host name **1** from your → *Configuration Checklist*.
- ▶ **Network Configuration**: Make sure “SonicWALL Simple Client Provisioning” is selected.
- ▶ Click “**Done**”



The screenshot displays the 'My VPN Connection' configuration page in the SonicWALL management interface. The page has a dark header with a key icon and the title 'My VPN Connection'. Below the header are tabs for 'Basic', 'Advanced', 'SecureDrop', 'Actions', and 'Notes'. The 'Basic' tab is active. The configuration is organized into sections:

- Connection Name**: My VPN Connection
- Connection based on**: DELL SonicWALL NSA Series
- Need help?**: Configuration Guide
- VPN Gateway**: 203.0.113.1 (with a red '1' icon and a help icon)
- Network Configuration**: Simple Client Provisioning (with a help icon)
- Authentication**: Pre-shared key (with a help icon and a note: Pre-shared key not saved)
- Extended Authentication (XAUTH)**: Automatic (with a help icon and a note: Username and password not saved)
- DNS**: Use Remote DNS Server

At the bottom of the page, there are three buttons: 'Manage Licenses...', 'Export Settings...', and 'Export...'.

Task 3 – Test the VPN Connection

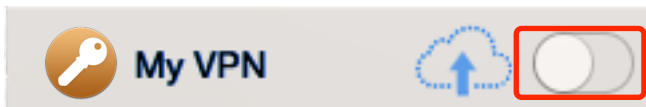
It's time to go out!

You will not be able to test and use your VPN connection from within the SonicWALL's network. In order to test your connection, you will need to connect from a different location.

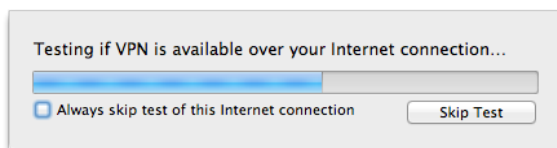
For example, if you are setting up a VPN connection to your office, try it out at home. If you are setting up a VPN connection to your home network, try it from an Internet cafe, or go visit a friend.

Connect to your VPN

- ▶ Make sure that your Internet connection is working – open your Internet browser and check that you can open <http://www.equinux.com>
- ▶ Open VPN Tracker.
- ▶ Click the On/Off slider for your connection.

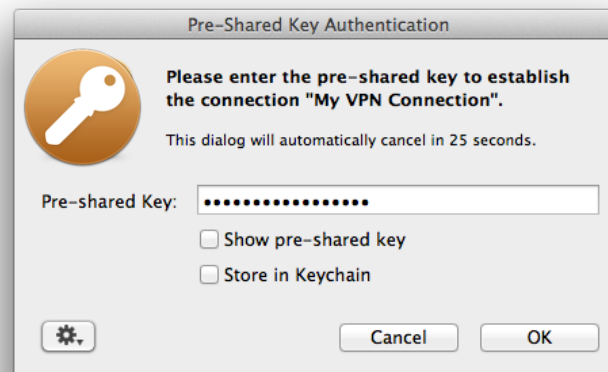


- ▶ If you are using VPN Tracker for the first time with your current Internet connection, it will test your connection. Wait for the test to complete.



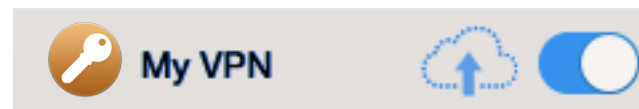
- ▶ Depending on your setup, you will be prompted to enter your pre-shared key 4 and Extended Authentication (XAUTH) user name 5

and password 6. 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 newly established VPN and how to get the most out of it.

VPN on – Internet off?

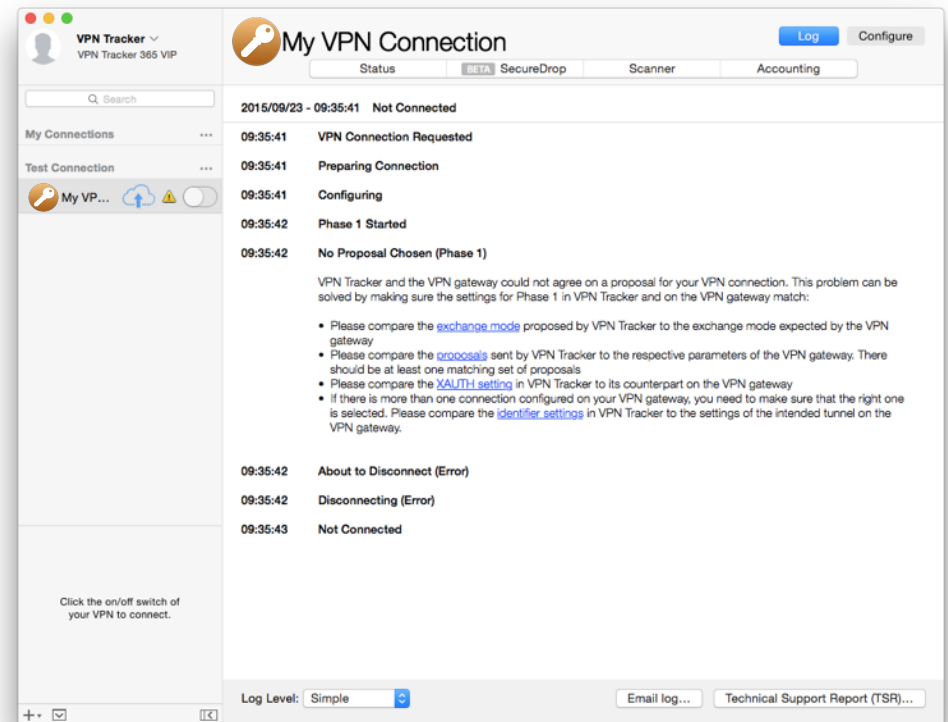
If your Internet connection seems to be offline whenever you connect the VPN, your SonicWALL might be configured to send all your Internet traffic through the VPN, but you're probably missing the right remote DNS setup to make it work. Please refer to the chapters about "Remote DNS" and "Host to Everywhere" connections for information how to configure remote DNS.

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.



The screenshot shows the 'My VPN Connection' window in the VPN Tracker application. The window title is 'My VPN Connection' and it includes a 'Log' button and a 'Configure' button. The main content area displays a log of events for the connection attempt on 2015/09/23 at 09:35:41. The status is 'Not Connected'. The log entries are:

- 09:35:41 VPN Connection Requested
- 09:35:41 Preparing Connection
- 09:35:41 Configuring
- 09:35:42 Phase 1 Started
- 09:35:42 No Proposal Chosen (Phase 1)

Below the log entries, there is a detailed error message: "VPN Tracker and the VPN gateway could not agree on a proposal for your VPN connection. This problem can be solved by making sure the settings for Phase 1 in VPN Tracker and on the VPN gateway match:"

- Please compare the [exchange mode](#) proposed by VPN Tracker to the exchange mode expected by the VPN gateway
- Please compare the [proposals](#) sent by VPN Tracker to the respective parameters of the VPN gateway. There should be at least one matching set of proposals
- Please compare the [AUTH setting](#) in VPN Tracker to its counterpart on the VPN gateway
- If there is more than one connection configured on your VPN gateway, you need to make sure that the right one is selected. Please compare the [identifier settings](#) in VPN Tracker to the settings of the intended tunnel on the VPN gateway.

Further log entries show:

- 09:35:42 About to Disconnect (Error)
- 09:35:42 Disconnecting (Error)
- 09:35:43 Not Connected

At the bottom of the window, there is a 'Log Level' dropdown set to 'Simple', and buttons for 'Email log...' and 'Technical Support Report (TSR)...'. A small instruction at the bottom left says: "Click the on/off switch of your VPN to connect."



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.

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 information can be found at

<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).
- ▶ SonicWALL model and the SonicOS version running on it.
- ▶ Screenshots of the GroupVPN settings on your SonicWALL.



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.

Appendix

Remote DNS Setup

VPN Tracker can use DNS servers on the remote network of the VPN to look up host names of resources on the remote network of the VPN.

Prerequisites

If you or your organization operate a DNS server on your SonicWALL's network, VPN Tracker can use it to look up the host names of internal resources (e.g. for turning intranet.ny.example.com into the IP address 192.168.13.94).

Remote DNS is entirely optional for Host to Network connections. You can always use IP addresses instead of host names, that's just less convenient.

DNS Server

To set up remote DNS, you need to know the IP address(es) of the DNS server(s) that you want to use.

My DNS Server: _____

Domain

VPN Tracker can use the remote DNS server for all DNS lookups (All Domains) or just for some domains (Search Domains). If you want VPN Tracker to use the remote DNS servers only for some domains (e.g. everything ending in "ny.example.com"), write down these domains here:

Search Domains: _____

Option A – Setup in VPN Tracker

Remote DNS can be set up in VPN Tracker without making any changes to your SonicWALL.

- ▶ Click "**Configure**" and go to the "**Basic**" tab in VPN Tracker.
- ▶ Check the box "**Use Remote DNS Server**".
- ▶ Uncheck the box "**Receive DNS Settings from VPN Gateway**".
- ▶ **DNS Servers:** Enter your DNS server. To enter additional DNS servers, press the green plus button.
- ▶ **Search Domains:** Enter the domains that you want this DNS server to be used for. Can be left empty to use the remote DNS server for all DNS lookups.
- ▶ **Use DNS Server for:** Choose "**Search Domains**" to only use the DNS server for the domains listed above. Choose "**All Domains**" to always use this DNS server when the VPN is connected.
- ▶ **Use for reverse lookup of IP addresses in remote networks:** Should be checked unless your DNS server is incapable of reverse lookups.

The screenshot shows the DNS configuration section in VPN Tracker. It includes the following elements:

- DNS** section with a checked checkbox for "Use Remote DNS Server" and an unchecked checkbox for "Receive DNS Settings from VPN Gateway".
- DNS Servers** field containing "192.168.13.11" with a help icon.
- Search Domains** field containing "my.example.com" and "london.example.com" with a help icon.
- Use DNS Server for** dropdown menu set to "Search Domains".
- A checked checkbox for "Use for reverse lookup of IP addresses in remote networks" with a help icon.

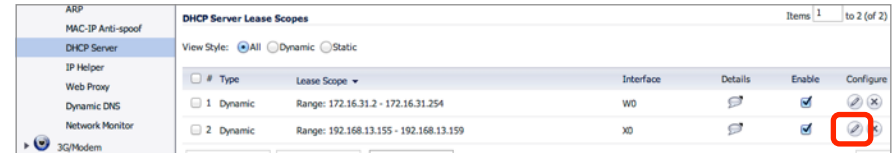


Requests to a remote DNS server do **not** necessarily go through the VPN. Which traffic is sent through the VPN is determined solely by the VPN's remote network(s) and topology.

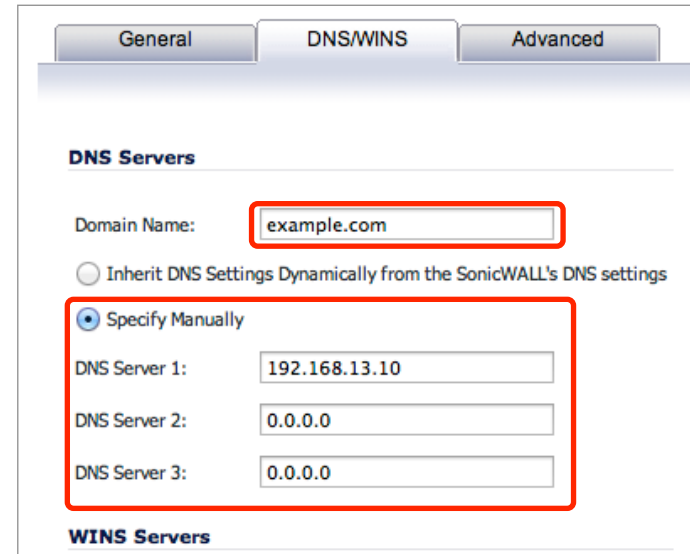
If the remote DNS server is located on the remote network(s) of the VPN (or if a Host to Everywhere connection is used), requests to the remote DNS server will go through the VPN.

Option B – Setup on the SonicWALL

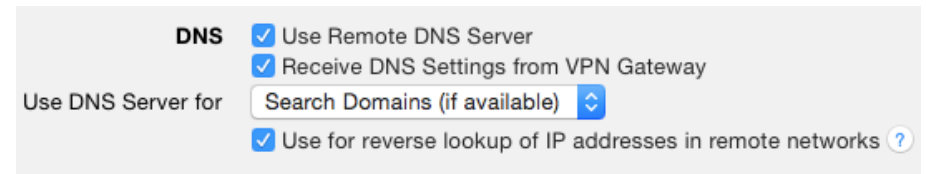
You can have the SonicWALL distribute your DNS settings when using DHCP over VPN. On your SonicWALL, go to “**Network > DHCP Server**” and edit the dynamic lease scope that is used for the VPN.



Enter your DNS server IP address(es) and a search domain (optional).



Use these settings in VPN Tracker to receive your DNS settings from the SonicWALL:



Host to Everywhere

To send all Internet traffic through the VPN, you'll need a connection that uses a "Host to Everywhere" topology.

Switch to Host to Everywhere

Prerequisites

Follow the first part of this guide until you have a working VPN to connect to your SonicWALL's LAN.

SonicWALL

To switch to Host to Everywhere, check the box "Set default route as this gateway" on the SonicWALL (VPN > WAN GroupVPN > Client).

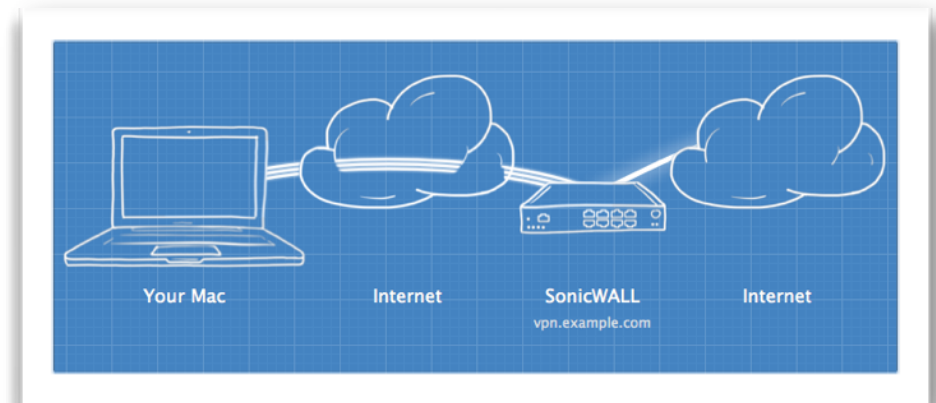
The screenshot shows the SonicWALL VPN Client configuration interface. The 'Client' tab is active. Under the 'Client Connections' section, the checkbox 'Set Default Route as this Gateway' is checked and highlighted with a red box. Below it, the checkbox 'Apply VPN Access Control List' is unchecked. Other settings include 'Virtual Adapter settings' set to 'DHCP Lease or Manual Configuration' and 'Allow Connections to' set to 'Split Tunnels'. The 'User Name and Password Caching' section shows 'Cache XAUTH User Name and Password on Client' set to 'Single Session'. The 'Client Initial Provisioning' section has 'Use Default Key for Simple Client Provisioning' unchecked.

VPN Tracker

Reconnect the VPN to fetch the new configuration from the SonicWALL. In case you are using a → *Manual VPN Tracker Setup* switch the

"Topology" (Basic > Network Configuration) to "Host to Everywhere".

If you check the Status tab in VPN Tracker, it should now display "Internet" to the right of your VPN gateway, instead of the remote network.



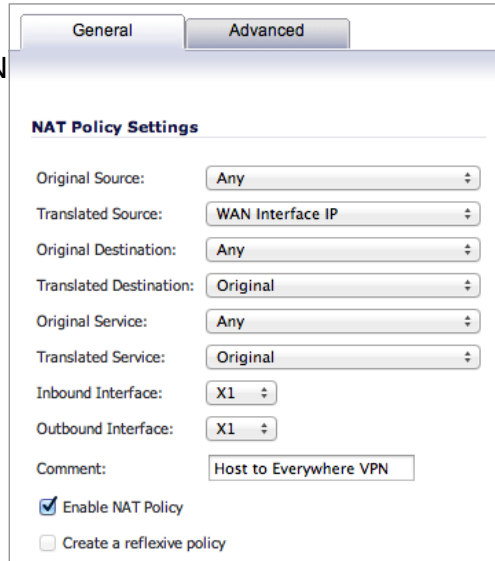
It is very likely that at this point, your Mac will seem to be cut off from the Internet any time you connect the VPN. This is normal and expected. You'll need to make two more configuration changes to ensure that traffic is sent out correctly by your SonicWALL and to ensure that your Mac is able to access a DNS server.

Add a NAT Policy

To ensure that your SonicWALL performs Network Address Translation (NAT) for your Mac's traffic when sending it out onto the Internet, you'll need to add a new NAT policy on your SonicWALL.

Add a new NAT policy on your SonicWALL under **Network > NAT Policies**¹.

- ▶ **Original Source:** Any
- ▶ **Translated Source:** Your WAN interface's IP address, e.g. WAN Interface IP, or WAN Primary IP, or X1 Interface IP.
- ▶ **Original Destination:** Any
- ▶ **Translated Destination:** Original
- ▶ **Original Service:** Any
- ▶ **Translated Service:** Original
- ▶ **Inbound Interface:** X1
- ▶ **Outbound Interface:** X1
- ▶ **Enable NAT Policy:** Check
- ▶ **Create a reflexive policy:** Don't check
- ▶ Click "OK" to save the new policy. It'll take effect immediately.



Incorrect NAT policies on your SonicWALL can lock you out from the SonicWALL. Only modify NAT policies if you have physical access to the SonicWALL, a backup at hand, and know how to reset the device and/or boot into safe mode.

Remote DNS for Host to Everywhere

When sending all Internet traffic through the VPN, using remote DNS is usually required for two reasons:

1. Sending all Internet traffic through the VPN may cut you off from your ISP's DNS servers. It may seem as if your Mac loses its Internet connection every time you connect the VPN.
2. When sending all Internet traffic through the VPN, but using a DNS server on the local network, DNS traffic is vulnerable to eavesdropping and attacks from the local network.

Remote DNS for Host to Everywhere connections is set up exactly the same way as remote DNS for internal resources. If you already have a working remote DNS (or plan to), you won't need to set up anything specifically for Host to Everywhere. Just make sure you've got a working → *Remote DNS Setup* and VPN Tracker will automatically use the remote DNS server for all DNS lookups.

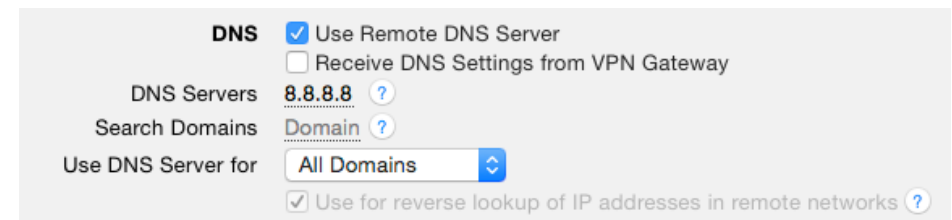
What if I don't have a remote DNS Server?

If you don't operate your own DNS server, you can set up remote DNS using public DNS servers, e.g.

- ▶ Google DNS: 8.8.8.8
- ▶ OpenDNS: See the [OpenDNS website](#) for IP addresses.

When using a public remote DNS server with a Host to Everywhere VPN, VPN Tracker will send DNS requests through the (encrypted) VPN, and the VPN gateway will send them back out (unencrypted) on the Internet to the public DNS server.

The following setup uses Google's public DNS server to ensure that your Mac can reach a DNS server when you're connected to your Everywhere VPN:



¹Refer to the [SonicWALL Knowledge Base](#) for more details.

Manual VPN Tracker Setup

With SonicWALL Simple Client Provisioning, all settings are transmitted automatically to VPN Tracker. If for some reason you cannot use SonicWALL Simple Client Provisioning, this chapter will show how to do a manual setup.

Prerequisites

Please follow the complete setup in → *Task 1 – SonicWALL Configuration*. You'll need all the information on the → *Configuration Checklist* to do a manual setup. In addition, you may need the information on the → *Proposals* tab of the SonicWALL's GroupVPN policy.

Step 1 – Add a Connection

- ▶ Open VPN Tracker.
- ▶ Click “**Add Connection**” (or click the + button in the lower left corner).
- ▶ Select “**SonicWALL**” from the list.
- ▶ Select your SonicWALL model (e.g. NSA Series).
- ▶ Click “**Create**”.



For some devices, multiple SonicOS versions are listed. Please select “SonicOS” if multiple versions are listed.

Step 2 – Configure the VPN Connection

Basic Tab

The screenshot shows the 'My VPN Connection' configuration page. The 'Basic' tab is selected. The 'VPN Gateway' is set to 203.0.113.1. The 'Network Configuration' section is set to 'DHCP over VPN' with a topology of 'Host to Network' and remote networks of '192.168.13.0 / 24'. The 'Authentication' section is set to 'Pre-shared key' and 'Automatic'. The 'Identifiers' section is set to 'Fully Qualified Domain Name (FQDN)' for both Local and Remote, with values 'GroupVPN' and 'C010144A172E' respectively. The 'DNS' section has the option 'Use Remote DNS Server' unchecked.

- ▶ Click “**Configure**” and switch to the “**Basic**” tab if it is not already displayed.
- ▶ **VPN Gateway**: Enter your SonicWALL's public IP address or its host name ① from your → *Configuration Checklist*.
- ▶ **Network Configuration**: Select “**DHCP over VPN**” if your SonicWALL is set up for DHCP over VPN (→ *Virtual Adapter Setting* is “**DHCP**”).

Lease” or “DHCP or Manual Configuration”). Select “Manual” if your SonicWALL is not set up for DHCP over VPN (→ *Virtual Adapter Setting* is “None”).

- ▶ **Topology:** Select “Host to Network” if → *Set Default Route as this Gateway* is unchecked on your SonicWALL. Select “Host to Everywhere” if it is checked. Additional configuration is required for Host to Everywhere, see → *Host to Everywhere* for details.
- ▶ **Local Address** (non-DHCP over VPN only): Leave empty.
- ▶ **Remote Networks** (Host to Network only): Enter the remote network(s) you would like to access through the VPN. This is typically the SonicWALL’s LAN network ②. Access to the network(s) must be permitted in the XAUTH user’s → *VPN Access List*.
- ▶ **Authentication:** Leave the defaults. VPN Tracker will automatically determine whether to use XAUTH or not.
- ▶ **Local Identifier:** Leave the default (Fully Qualified Domain Name (FQDN) / GroupVPN).
- ▶ **Remote Identifier:** Fully Qualified Domain Name (FQDN). Enter the SonicWALL’s Unique Firewall Identifier ③.

Advanced Tab

The settings on the Advanced tab match the SonicWALL’s defaults. You need to make changes to the Phase 1 and Phase 2 settings only if you changed the SonicWALL’s defaults or if your SonicWALL uses different default values. Refer to the → *Proposals* tab on your SonicWALL for the correct settings.

My VPN Conn Done

Basic Advanced SecureDrop Actions Notes

Phase 1

Exchange mode Aggressive Mode

Lifetime 28800 seconds

Encryption algorithm

- AES-256
- AES-192
- AES-128
- 3DES

Hash algorithm

- SHA1
- MD5

Diffie-Hellman Group 2 (1024 bit)

Phase 2

Lifetime 28800 seconds

Encryption algorithm

- DES
- 3DES
- AES-128
- AES-192

Authentication algorithm

- HMAC MD5
- HMAC SHA1

Perfect Forward Secrecy (PFS) Off