Contents

Introduction..............................................................................................................4
  Prerequisites 4
  Using the Configuration Guide 4
  Scenario 5

My VPN Gateway Configuration.................................................................6

Task 1 – SonicWALL Configuration .......................................................7
  Option A – Express Setup.................................................................7
    Gather Configuration Information 7
    Set Up VPN Tracker 7
  Option B – Complete Setup.............................................................7
    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 11
    Step 6 – Add a VPN User 12
    Step 7 – Configuring VPN Access Lists 13

Task 2 – VPN Tracker Configuration.................................................14
  Step 1 – Add a Connection 14
  Step 2 – Configure the VPN Connection 14

Task 3 – Test the VPN Connection.....................................................15
  Troubleshooting 16

Appendix .........................................................................................................17

Remote DNS Setup....................................................................................17
  Prerequisites 17
  Option A – Setup in VPN Tracker 17

Option B – Setup on the SonicWALL ..................................................18

Host to Everywhere..................................................................................19

Manual VPN Tracker Setup.....................................................................21
  Prerequisites 21
  Step 1 – Add a Connection 21
  Step 2 – Configure the VPN Connection 21

Host to Everywhere..................................................................................19

Manual VPN Tracker Setup.....................................................................21
  Prerequisites 21
  Step 1 – Add a Connection 21
  Step 2 – Configure the VPN Connection 21
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 and bugfixes.
- This guide is a supplement to the documentation included with your SonicWall device, it can’t replace it. Please it before starting.

Your Mac
- VPN Tracker runs on Mac OS X 10.8 and 10.7
- The configuration described in this guide requires VPN Tracker 7. Make sure you have all available updates installed. The latest VPN Tracker updates can be obtained 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 are **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 it later. 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**

1. SonicWALL WAN IP Address: ______.______.______.______ or host name ____________________________

2. SonicWALL LAN Network: ______.______.______.______ / ______.______.______.______

**Firewall Identifier**

3. Unique Firewall Identifier: ____________________________

**VPN Connection**

4. Pre-Shared Key: ____________________________

**User Authentication (XAUTH)**

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

Pre-Shared Key ➍
The pre-shared key is called “Shared Secret” on the SonicWALL. The shared secret is configured on your SonicWALL under VPN > GroupVPN > 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 ➎ and Password ➏
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 ➊ and the LAN Network as ➋ on your → Configuration Checklist.

If your SonicWALL is reachable through a public host name (DynDNS or fixed host name) write that down instead as ➊.
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** on your → *Configuration Checklist*.
- Click “Accept”.

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

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 on your → *Configuration Checklist*. In VPN Tracker, the shared secret is called **pre-shared key**.

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

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

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

Advanced

- 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

![Client Configuration](image)

- **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”.

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

For experts: VPN Tracker sets the second least significant bit of the most significant byte of the MAC address to 1, thereby turning it into a self-assigned MAC address.

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.
Step 6 – Add a VPN User

- Go to Users > Local Users
- Click “Add User…”

- Name: Enter a user name and write it down on your Configuration Checklist.
- Password: Enter a password
- 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.

![Local Groups](image)

‣ 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.

![VPN Client Access Networks](image)

‣ Click “OK.”

Refer to “Network > Address Objects” on your SonicWALL 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

› 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

› 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 from your → Configuration Checklist.
› Network Configuration: Make sure “SonicWALL Simple Client Provisioning” is selected.
› Click “Done”
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 ✅ and Extended Authentication (XAUTH) user name ✅ and password ✅. 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:

![My VPN Connection](image)

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.

![Log](image)

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](http://www.vpntracker.com/support) contains detailed troubleshooting advice.

**Frequently Asked Questions (FAQs)**

Answers to frequently asked questions can be found at [http://www.vpntracker.com/support](http://www.vpntracker.com/support)

**Technical Support**

If you’re stuck, the technical support team at equinux is here to help. Contact information can be found at [http://www.vpntracker.com/support](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.
- 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.

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).

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.  

- **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](http://opendns.com) 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:
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

- 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 ➊ 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.

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

**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.