



VPN Tracker 365

VPN Configuration Guide

SonicWALL

PRO Series, SuperMassive Series, TZ Series, NSa Series, NSa E-Class, NSsp Series, NSv Series

© 2020 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 November 2020

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

Contents

[Introduction](#)

[My VPN Gateway Configuration Checklist](#)

[Task One - SonicWALL Configuration](#)

[Task Two - Configuration in VPN Tracker](#)

[Task Three - Testing the VPN connection](#)

[Manual Configuration](#)

[Remote DNS Setup \(Advanced\)](#)

Introduction

My VPN Gateway Configuration Checklist

Throughout this guide there will be certain pieces of information which are needed later on for configuring VPN Tracker. This information is marked with red numbers so it is easier for you to reference. Print out this checklist and use it to keep track of your device settings.

IP Addresses

1. SonicWALL WAN IP Address: _____
or Host Name _____
2. SonicWALL LAN Network: _____ / _____

Firewall Identifier

3. Unique Firewall Identifier: _____

Authentication

4. Pre-Shared Key: _____
5. XAUTH Username: _____
6. XAUTH Password: _____

Task One - SonicWALL Configuration

With Simple Client Provisioning, setting up your SonicWALL device is really straightforward and should only take you a couple of minutes:

Step One: Gather configuration information

You'll need this information to set up VPN Tracker, Use the Configuration Checklist on the previous page to keep a note of this for the VPN Tracker setup later on in the guide.

- Find your SonicWALL's Public (WAN) IP address or host name **(1)**. You will find this under "Network" > "Interfaces", or in the GlobalVPN Client on Windows.
- Configure the Pre-Shared Key **(4)** for your device. This is referred to as the "Shared Secret" on the SonicWALL. This is just an extra secure password which you configure especially for your SonicWALL device. You can set this up under "VPN" > "Group VPN" > "General" > "Shared Secret."

Tip: If "Use Default Key for Simple Client Provisioning" is enabled on the SonicWALL, no Pre-Shared Key is required.

- If your SonicWALL uses Extended Authentication (XAUTH), you'll need the username **(5)** and the password **(6)** of a user who is authorized to access the VPN.

Step Two: Insert this information to VPN Tracker

You can now use this information to skip ahead to Task Two and start the Simple Client Provisioning configuration for your SonicWALL device within VPN Tracker.

The screenshot displays the SonicWALL NSa 2650 web interface. The 'Interface Settings' window for 'Interface X1' is open, showing the 'General' tab. The IP Address field is highlighted with a red box and the text "You will find your WAN address here. 1". The interface also shows a table of network interfaces with their status, speed, and configuration options.

| Status | Enabled | Comment | Configure |
|--------------------|---------|---------------------------|-----------|
| 1 Gbps Full Duplex | ✓ | LiveDemo LAN (V110) | ⚙️ |
| 1 Gbps Full Duplex | ✓ | Primary WAN | ⚙️ |
| No link | ✗ | | ⚙️ |
| 1 Gbps Full Duplex | ✓ | WDS Provisioning | ⚙️ |
| 1 Gbps Full Duplex | ✓ | Firewall Uplink - ES1 | ⚙️ |
| 1 Gbps Full Duplex | ✓ | SonicWave Provisioning | ⚙️ |
| VLAN Sub-Interface | | WLAN IT Staff | ⚙️ ✕ |
| VLAN Sub-Interface | | WLAN Employees | ⚙️ ✕ |
| VLAN Sub-Interface | | WLAN Guests | ⚙️ ✕ |
| VLAN Sub-Interface | | WLAN WDS Link | ⚙️ ✕ |
| 1 Gbps Full Duplex | ✓ | WXA series appliance | ⚙️ |
| No link | ✗ | | ⚙️ |
| No link | ✗ | | ⚙️ |
| No link | ✗ | | ⚙️ |
| No link | ✓ | LiveDemo Servers (V100) | ⚙️ |
| 1 Gbps Full Duplex | ✓ | LiveDemo DMZ (DMZ Switch) | ⚙️ |
| No link | ✗ | | ⚙️ |
| No link | ✗ | | ⚙️ |
| No link | ✗ | | ⚙️ |
| No link | ✗ | | ⚙️ |

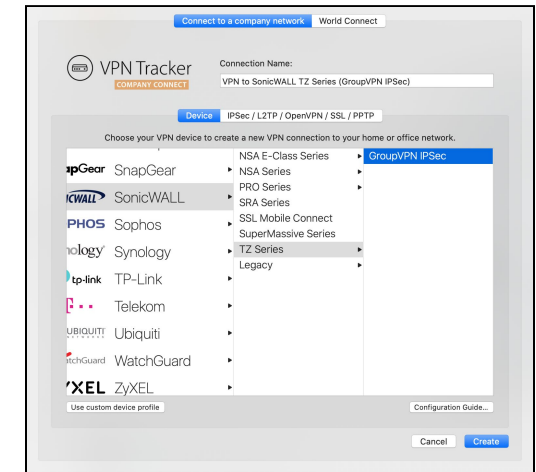
Task Two - Configuration in VPN Tracker

Simple Configuration using Simple Client Provisioning

With Simple Client Provisioning, all of your device's settings are automatically transmitted to VPN Tracker 365, which makes configuration very straightforward.

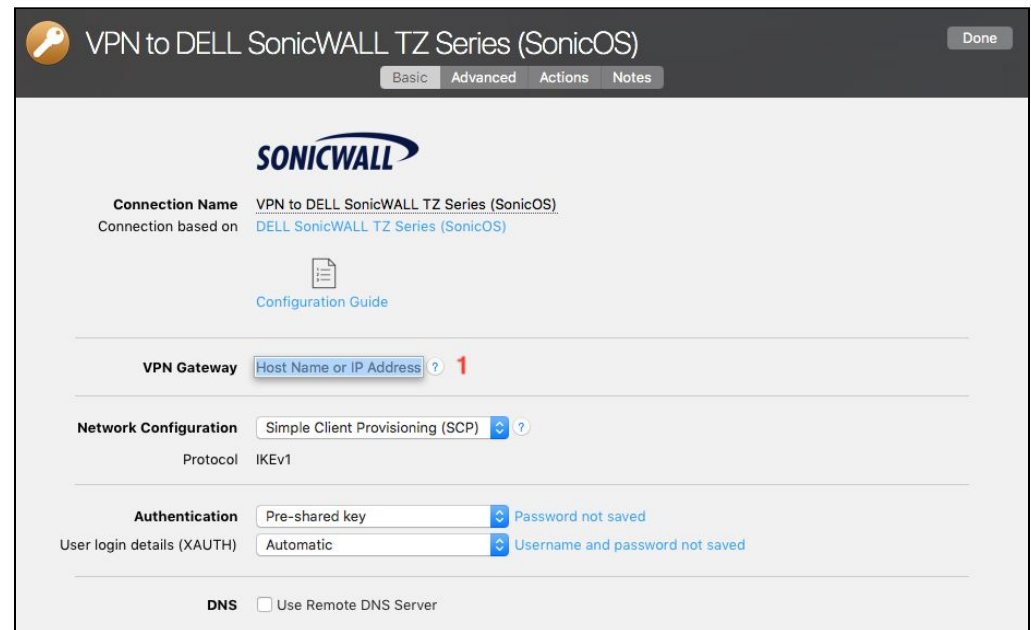
Step One: Add a connection

- Open VPN Tracker 365.
- Click on "Create a connection", or click on the + in the bottom left corner of the app window.
- Select **SonicWALL** from the list.
- Select your model (e.g. TZ Series)



Step Two: Configure the VPN connection

- Go to the "Basic" tab.
- **VPN Gateway:** Enter your device's IP address here **(1)**
- **Network Configuration:** Make sure "SonicWALL Simple Client Provisioning" is selected
- Click "Done"



Task Three - Testing the VPN connection

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

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

Connect to your VPN

- 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.

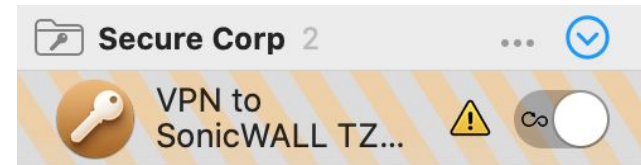
- Depending on your setup, You will be prompted to enter your pre-shared key **(4)** as well as your XAUTH username **(5)** and password **(6)**. To save time for the future, check the box "Store in Keychain" to save the password in your keychain so you are not asked for it again when connecting the next time.

Connected!

Connecting may take a couple of seconds. If the On/Off button turns blue that's great – you're connected! Now is a great time to take a look at the [VPN Tracker Manual](#). It shows you how to use your VPN and how to get the most out of it.

Troubleshooting

In case there's a problem connecting, a yellow warning triangle will show up. Click the yellow warning triangle to be taken to the log.



The log will explain exactly what the problem is. Follow the steps listed in the log.

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 model and the firmware version running on it.
- Screenshots of the VPN settings on your VPN gateway.

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.

Manual Configuration

This is only recommended for experienced users who don't have Simple Client Provisioning set up on their device.

Step One: 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 **(1)** and the LAN Network as **(2)** on your Configuration Checklist.

Tip: If your SonicWALL is reachable through a public host name (DynDNS or fixed host name), write this down as **(1)**.

SONICWALL NS_a 2650

Interface 'X0' Settings

Zone: LAN

Mode / IP Assignment: Static IP Mode

IP Address: **You will find your LAN address here 2** 255.255.255.0

Subnet Mask: 255.255.255.0

Default Gateway (Optional): 192.168.150.1

Comment: LiveDemo LAN (V110)

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Ready

OK CANCEL HELP

SONICWALL NS_a 2650

Interface 'X1' Settings

Zone: WAN

Mode / IP Assignment: Static

IP Address: **You will find your WAN address here. 1** 173.240.215.1

Subnet Mask: 255.255.255.0

Default Gateway: 173.240.215.1

DNS Server 1: 8.8.8.8

DNS Server 2: 8.8.4.4

DNS Server 3: 0.0.0.0

Comment: Primary WAN

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Ready

OK CANCEL HELP

| Status | Enabled | Comment | Configure |
|--------------------|-------------------------------------|---------------------------|-------------------------------------|
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | LiveDemo LAN (V110) | <input type="checkbox"/> |
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | Primary WAN | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | WDS Provisioning | <input type="checkbox"/> |
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | Firewall Uplink - ES1 | <input type="checkbox"/> |
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | SonicWave Provisioning | <input type="checkbox"/> |
| VLAN Sub-Interface | <input checked="" type="checkbox"/> | WLAN IT Staff | <input checked="" type="checkbox"/> |
| VLAN Sub-Interface | <input checked="" type="checkbox"/> | WLAN Employees | <input checked="" type="checkbox"/> |
| VLAN Sub-Interface | <input checked="" type="checkbox"/> | WLAN Guests | <input checked="" type="checkbox"/> |
| VLAN Sub-Interface | <input checked="" type="checkbox"/> | WLAN WDS Link | <input checked="" type="checkbox"/> |
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | WXA series appliance | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | LiveDemo Servers (V100) | <input type="checkbox"/> |
| 1 Gbps Full Duplex | <input checked="" type="checkbox"/> | LiveDemo DMZ (DMZ Switch) | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |
| No link | <input checked="" type="checkbox"/> | | <input type="checkbox"/> |

Step Two: Enable VPN on your SonicWALL

- Go to "Connectivity" > "VPN" > "Base Settings."
- Under "VPN Global Settings" check "Enable VPN."
- Write down your SonicWALL's Unique Firewall Identifier as **(3)** on your Configuration Checklist.

Tip: The Unique Firewall Identifier is case-sensitive. Please write this down exactly as it appears on your device.

Step Three: Set up GroupVPN

- Under "VPN Policies" check the box to enable the "WAN Group VPN" policy.
- Click on "Configure" to get started.

VPN Global Settings

Enable VPN

Unique Firewall Identifier: **3**

View IP Version: IPv4 IPv6

VPN Policies

Refresh Interval (secs) Items per page Items to 3 (of 3)

| <input type="checkbox"/> | # | Name | Gateway | Destinations | Crypto Suite | Enable | Configure |
|--------------------------|---|-------------------|-------------|-------------------------------|----------------------------------|-------------------------------------|-----------|
| <input type="checkbox"/> | 1 | WAN GroupVPN | | | ESP: 3DES/HMAC SHA1 (IKE) | <input checked="" type="checkbox"/> | |
| <input type="checkbox"/> | 2 | WLAN GroupVPN | | | ESP: 3DES/HMAC SHA1 (IKE) | <input type="checkbox"/> | |
| <input type="checkbox"/> | 3 | SGMS-C0EAE4CEBB7C | 4.16.47.170 | 10.100.140.52 - 10.100.140.52 | ESP: AES-128/HMAC SHA256 (IKEv2) | <input checked="" type="checkbox"/> | |

ADD

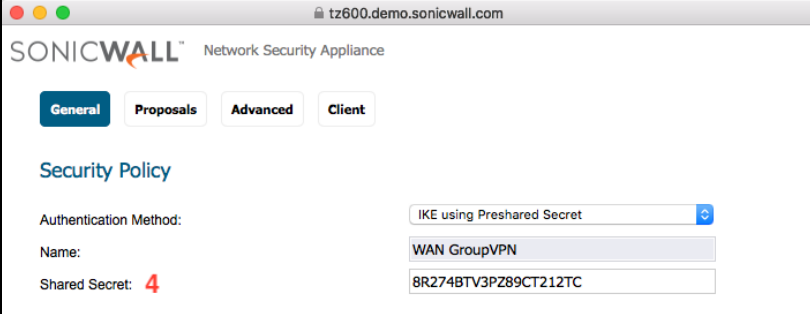
DELETE

DELETE ALL

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed
GroupVPN Policies: 3 Policies Defined, 0 Policies Enabled, 25 Maximum Policies Allowed

General Settings

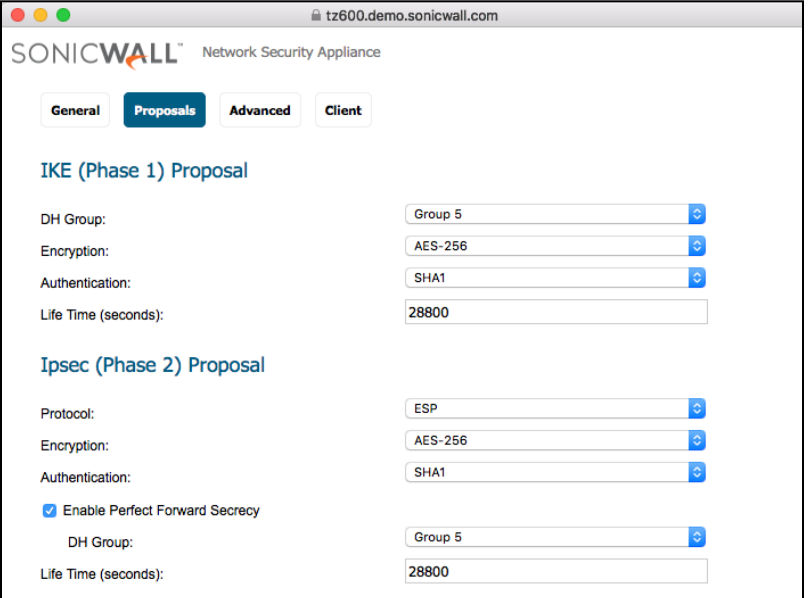
- Under "Authentication Method" select "IKE using Preshared Secret" This password protects your VPN. Choose a long, random password (ASCII characters only) and write it down as **(4)** on your Configuration Checklist. In VPN Tracker, the shared secret is called pre-shared key.



The screenshot shows the SonicWall Network Security Appliance configuration page for a Security Policy. The browser address bar shows 'tz600.demo.sonicwall.com'. The page has four tabs: 'General', 'Proposals', 'Advanced', and 'Client'. The 'General' tab is selected. The 'Security Policy' section is visible. The 'Authentication Method' is set to 'IKE using Preshared Secret'. The 'Name' is 'WAN GroupVPN'. The 'Shared Secret' is '4', with a red '4' icon next to it. The shared secret field is highlighted in light blue.

Proposals

- For "DH Group", please choose "Group 5" from the dropdown list.
- For Encryption, we recommend "AES-256" in both phases for the best security.
- Check the box to enable Perfect Forward Secrecy and choose Group 5 again.



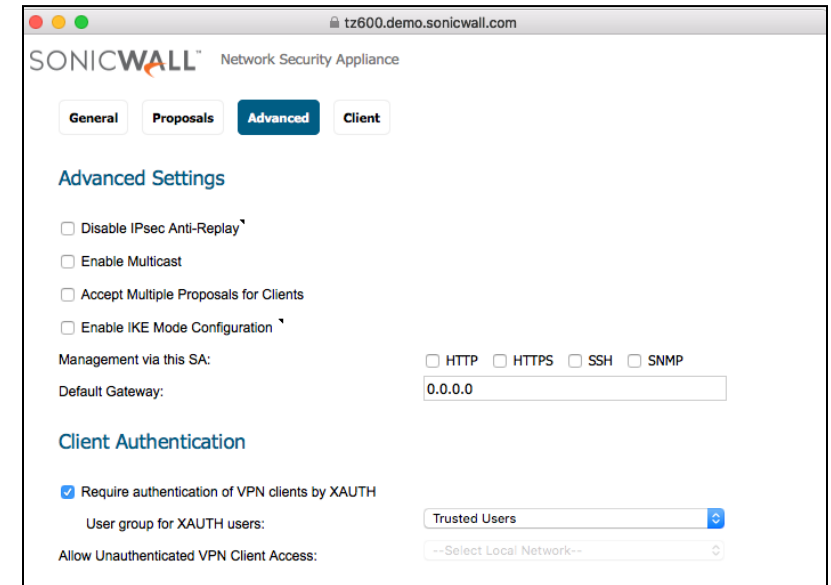
The screenshot shows the SonicWall Network Security Appliance configuration page for IKE and IPsec proposals. The browser address bar shows 'tz600.demo.sonicwall.com'. The page has four tabs: 'General', 'Proposals', 'Advanced', and 'Client'. The 'Proposals' tab is selected. The 'IKE (Phase 1) Proposal' section is visible. The 'DH Group' is 'Group 5', 'Encryption' is 'AES-256', 'Authentication' is 'SHA1', and 'Life Time (seconds)' is '28800'. The 'IPsec (Phase 2) Proposal' section is visible. The 'Protocol' is 'ESP', 'Encryption' is 'AES-256', 'Authentication' is 'SHA1', 'Enable Perfect Forward Secrecy' is checked, 'DH Group' is 'Group 5', and 'Life Time (seconds)' is '28800'.

Advanced

- If you have L2TP clients connecting to your device, check the box to enable “Accept Multiple Proposals for Clients.” Otherwise, you can leave this blank.
- For the “Client Authentication” section, check the box to “Require authentication of VPN clients by XAUTH.” This guide will assume that XAUTH is being used.
- You can now choose a user group for your XAUTH users. The default group here is “Trusted Users.” This means all users in this group have access to the VPN.

Client

- Under “User Name and Password Caching” select “Single Session” or “Always” to avoid prompts for your XAUTH username and password, as well as possible disconnects when rekeying the VPN connection.
- For “Virtual Adapter settings”, we recommend “DHCP Lease or Manual Configuration.” Only use “None” if there are other VPN users who are not using VPN Tracker who rely on this setting.
- The other settings can remain unchecked. They are not needed for the configuration with VPN Tracker.
- Click “OK” to move on to the next step.



tz600.demo.sonicwall.com

SONICWALL Network Security Appliance

General Proposals **Advanced** Client

Advanced Settings

- Disable IPsec Anti-Replay
- Enable Multicast
- Accept Multiple Proposals for Clients
- Enable IKE Mode Configuration

Management via this SA: HTTP HTTPS SSH SNMP

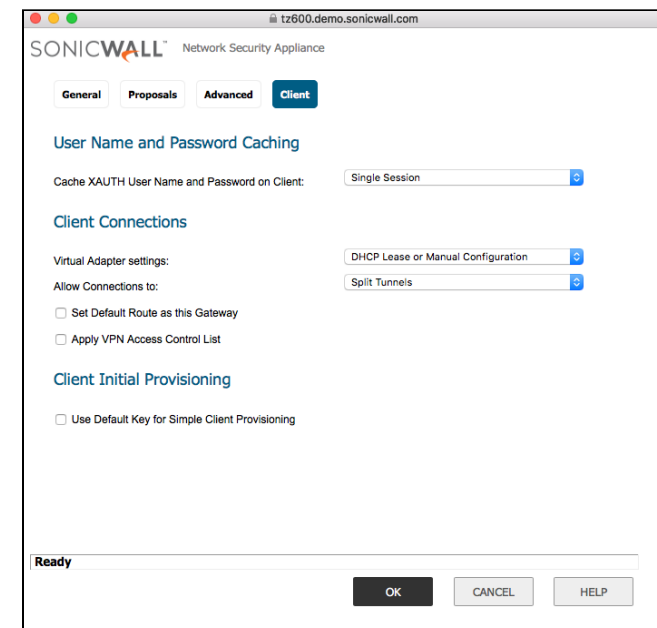
Default Gateway:

Client Authentication

- Require authentication of VPN clients by XAUTH

User group for XAUTH users:

Allow Unauthenticated VPN Client Access:



tz600.demo.sonicwall.com

SONICWALL Network Security Appliance

General Proposals Advanced **Client**

User Name and Password Caching

Cache XAUTH User Name and Password on Client:

Client Connections

Virtual Adapter settings:

Allow Connections to:

- Set Default Route as this Gateway
- Apply VPN Access Control List

Client Initial Provisioning

- Use Default Key for Simple Client Provisioning

Ready

OK CANCEL HELP

Step Four: Configure DHCP over VPN

- Go to "VPN" > "DHCP over VPN"
- Select "Central Gateway" from the list and click "Configure..."
- Check the box next to "Use Internal DHCP Server."
- Select "For Global VPN Client."

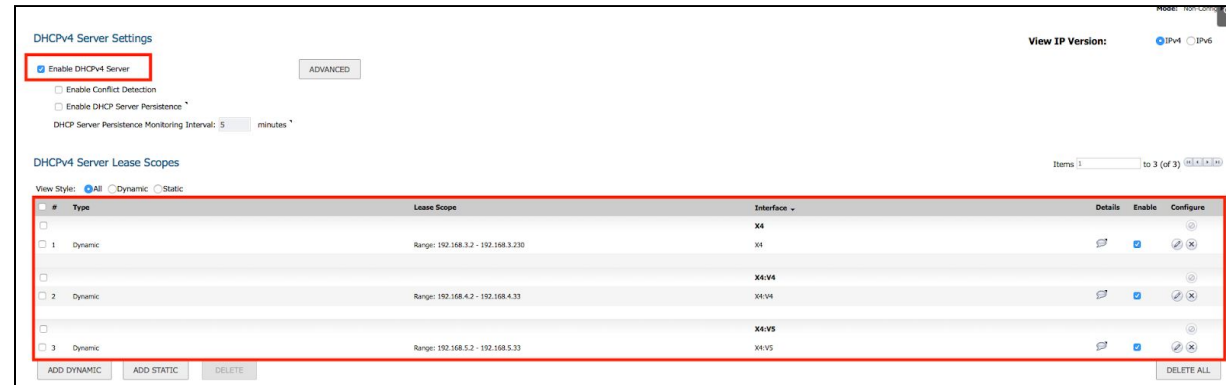
Tip: If your network infrastructure requires you to use an external DHCP server, you can configure the SonicWALL to relay DHCP requests to this server. Check the box "Send DHCP requests to the server addresses listed below" and enter the DHCP server's address. In the following step, check your external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

- Click "Ok."



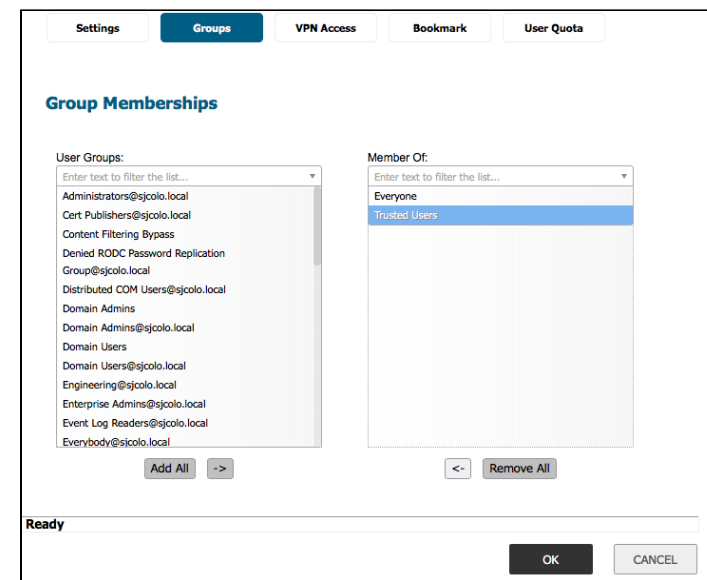
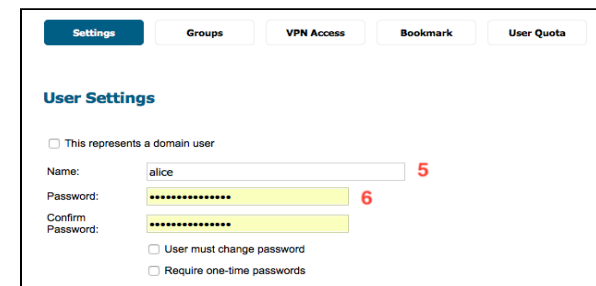
Step Five: Check your DHCP Server Settings

- Go to “System Setup” > “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 Six: Add a VPN User

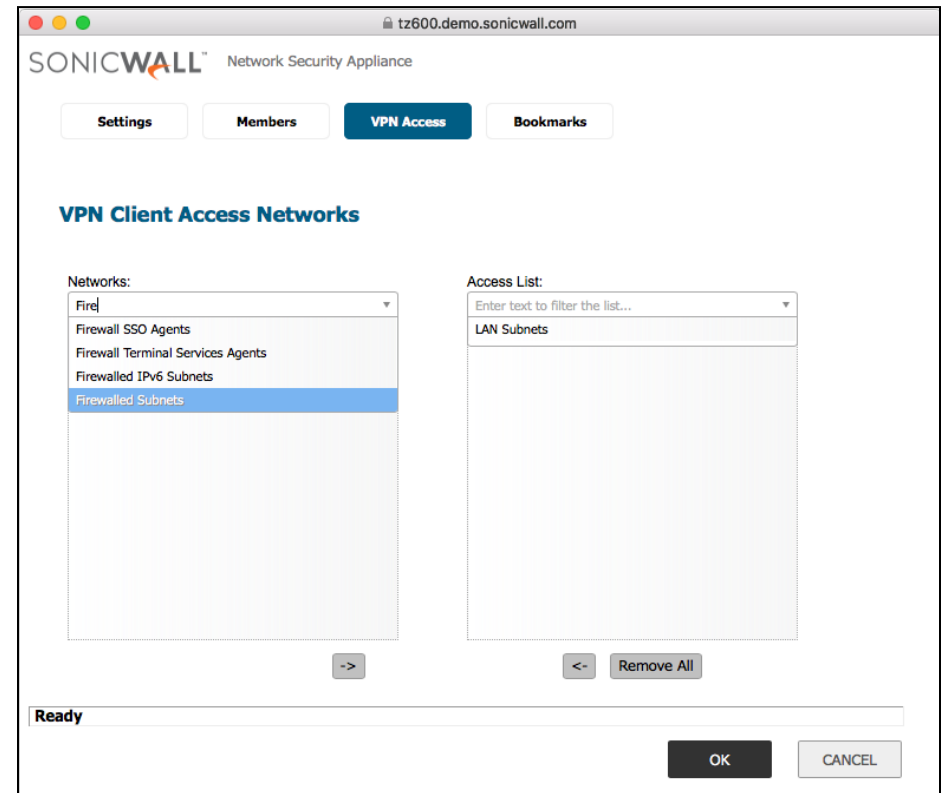
- Go to “Users” > “Local Users & Groups”
- Click on the “Local Users” tab and select “Add User”
- Next to “Name”, write down a username. This is your XAUTH username (5) on your Configuration Checklist.
- Now enter a password. This is your XAUTH password (6) on your Configuration Checklist.
- Navigate to the “Groups” tab.
- Add your user to the group you selected previously under Group VPN > Advanced > Client Authentication > User group for XAUTH users (i.e. **Trusted Users**)
- Click “OK” to add the new user.



Step Seven: 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.
- Go to the "VPN Access" tab.
- Add the desired networks to the "Access List." For most setups, "LAN Subnets" or "Firewall Subnets" will be a good choice.
- Click "Ok."



Manual Configuration in VPN Tracker 365

Use this configuration if your device does not support Simple Client Provisioning...

- Go to the “Basic” tab.
- Next to “VPN Gateway”, enter your device’s IP address **(1)**
- For “Network Configuration”, select “DHCP over VPN”
- For “Topology”, select “Host to Network.”
- If you selected “DHCP over VPN” you can leave the box next to “Local Address” empty.
- Next to “Remote Networks” you can enter the remote network(s) you want to access via the VPN connection. This is typically the SonicWALL’s LAN network **(2)**.

Tip: Access to the network(s) must be permitted in the XAUTH user’s VPN Access List.

- Under “Authentication” enter your Pre-Shared Key/Shared Secret **(4)**.
- Then, enter your XAUTH username **(5)** and password **(6)**.
- By “Remote Identifier”, enter the SonicWALL’s Unique Firewall Identifier **(3)**.

The screenshot displays the configuration page for a VPN connection to a Dell SonicWALL TZ Series device. The page is titled "VPN to DELL SonicWALL TZ Series (SonicOS)" and has a "Done" button in the top right corner. Below the title are tabs for "Basic", "Advanced", "Actions", and "Notes". The SonicWALL logo is prominently displayed in the center. The configuration is organized into several sections:

- Connection Name:** VPN to DELL SonicWALL TZ Series (SonicOS). Connection based on: DELL SonicWALL TZ Series (SonicOS). A "Configuration Guide" link is provided.
- VPN Gateway:** Host Name or IP Address **1**
- Network Configuration:** DHCP over VPN. Protocol: IKEv1. Topology: Host to Network.
- Remote Networks:** Network Address **2**
- Authentication:** Pre-shared key **4**. Password not saved. User login details (XAUTH): Automatic. Username and password not saved **5 & 6**.
- Identifiers:** Local: Fully Qualified Domain Name (FQDN) **GroupVPN**. Remote: Fully Qualified Domain Name (FQDN) **Unique Firewall Identifier** **3**.
- DNS:** Use Remote DNS Server.

Remote DNS Setup (Advanced)

This point is **optional**. 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.

Requirements

If you or your organization operate a DNS server on your Sophos device'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. You can get this from your administrator.

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: _____

Setup in VPN Tracker

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

- Click on your VPN connection
- Click **"Configure"** and go to the **"Basic"** tab
- Check the box **"Use Remote DNS Server"**
- Now fill in your information from above for **"DNS Servers"** and **"Search Domains"** to configure for your network.