VPN Tracker for Mac OS X

How-to:

Interoperability with

SonicWALL

Internet Security Appliances

Rev. 3.1

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a SonicWALL Internet Security Appliance.

The SonicWALL is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your SonicWALL. Please be sure to read those instructions and understand them before starting.

2. Prerequisites

First you have to make sure that your SonicWALL has VPN support built in. Please refer to your SonicWALL manual for details.

Furthermore you should use a recent SonicWALL fimware version. The latest firmware release for your SonicWALL appliance can be obtained from

https://www.mysonicwall.com/

For this document, 6.5.0.4 has been used.

When using Pre-shared key authentication you need one VPN Tracker Personal Edition license for each Mac connecting to the SonicWALL.

For certificate authentication you need a CA with private key, so one VPN Tracker Professional Edition is required in order to sign certificates. Only one VPN Tracker Professional Edition is required, other VPN users can use a Personal Edition. For further information please refer to chapter 3 in the VPN Tracker manual.

VPN Tracker is compatible with Mac OS X 10.2.x / 10.3.

3. Connecting a VPN Tracker host to a SonicWALL using Pre-shared Key Authentication

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.[1]

The SonicWALL is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the SonicWALL use 192.168.1.1 as their default gateway and should have a working Internet connection.

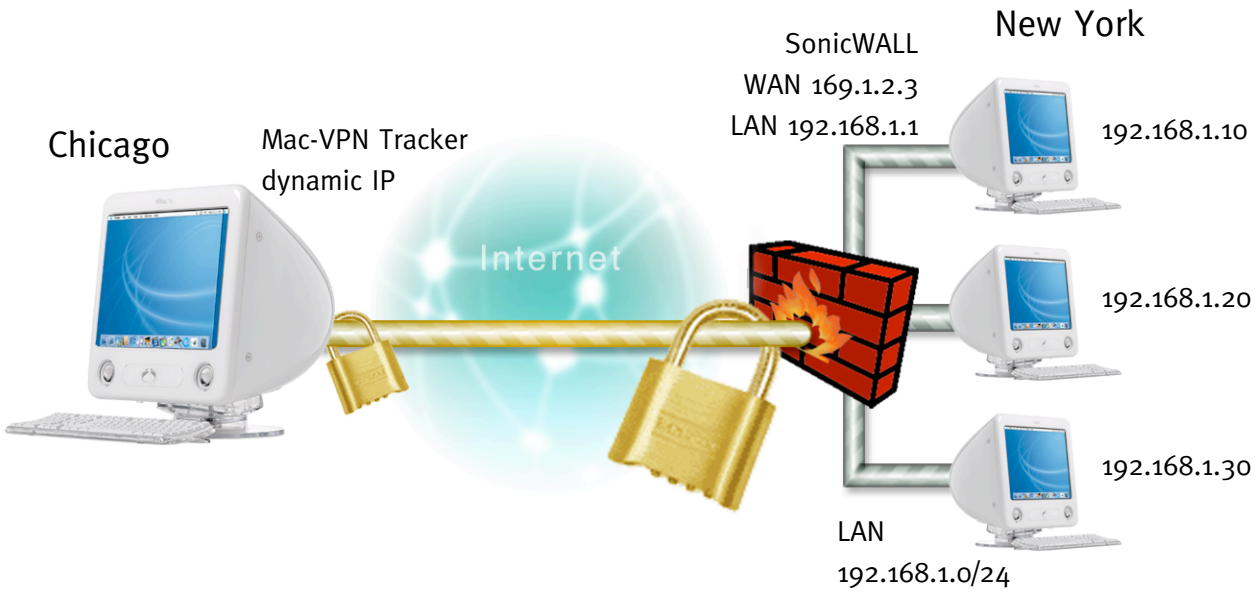


Figure 1: VPN Tracker – SonicWALL connection diagram

[1] Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports „IPSEC passthrough“. Please contact your router's manufacturer for details.

3.1 SonicWALL Configuration

The pre-defined VPN Tracker connection type has been created using the default settings for "Group-VPN". If you change any of the settings on the SonicWALL, you will eventually have to adjust the connection type in VPN Tracker.

Step 1 Change the Global VPN Settings:

- Enable VPN: **checked**
- Enable NAT Traversal: **unchecked**

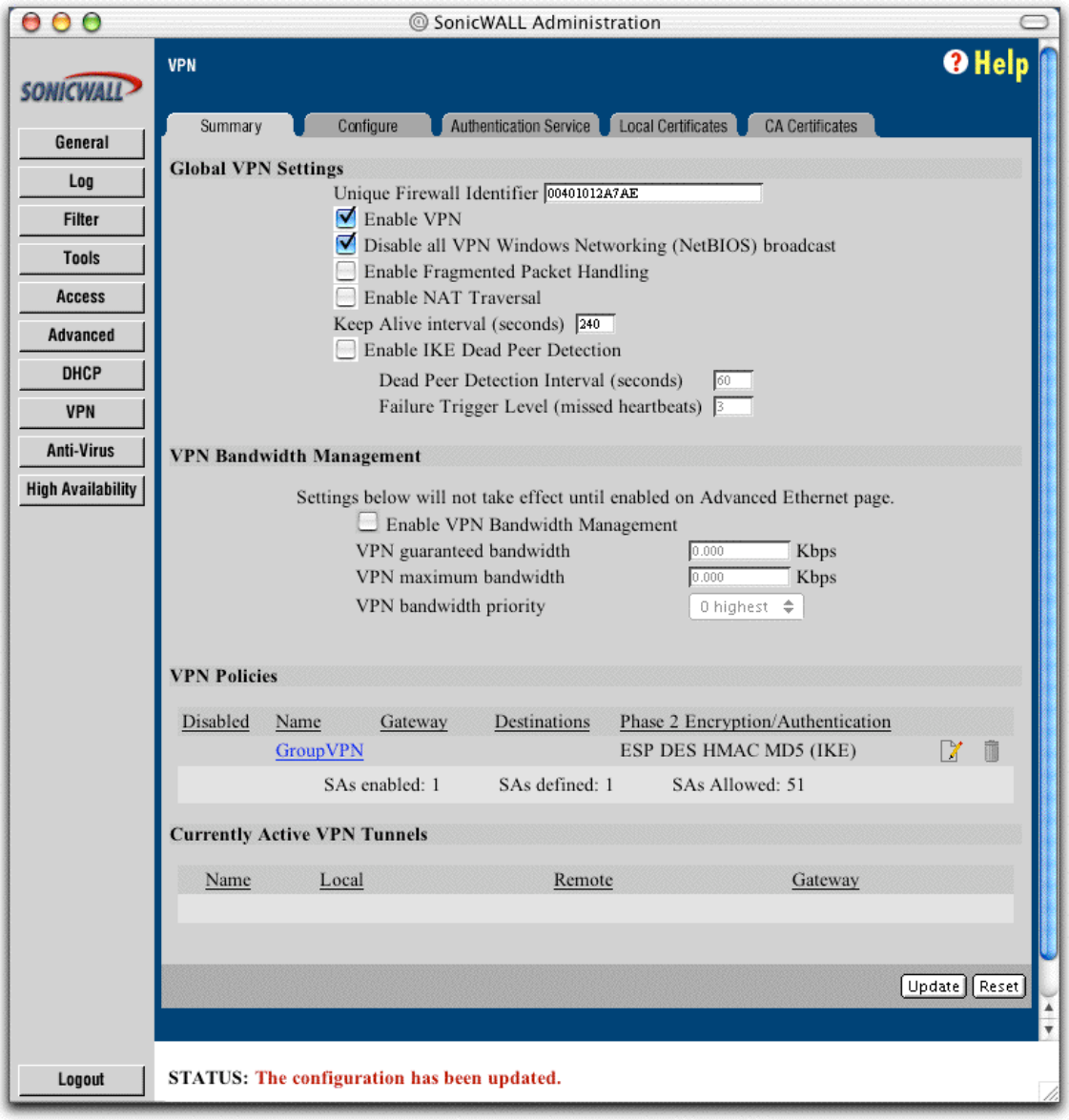


Figure 3: SonicWALL - Summary

Step 2 Change the GroupVPN Settings:

- Security Association: **GroupVPN**
- Phase 1 Encryption/Authentication: **3DES & SHA1**
- Phase 2 Encryption/Authentication: **"Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)"**
- Shared Secret: your Pre-share key

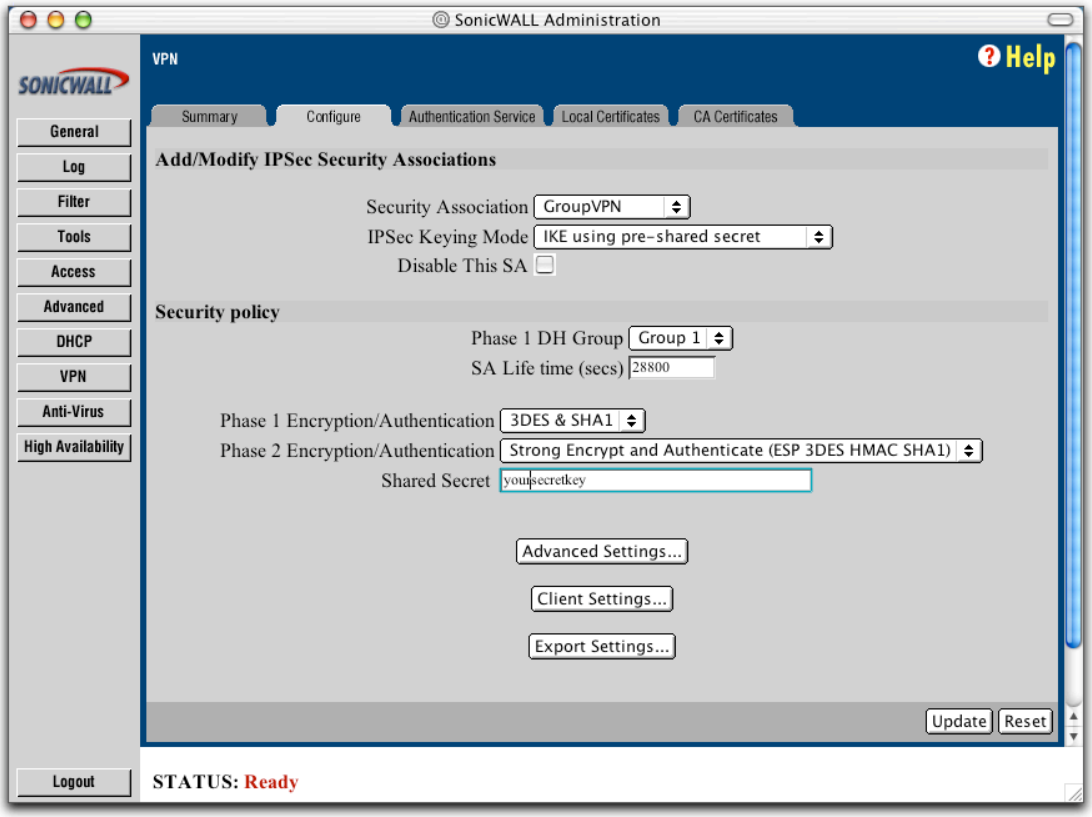


Figure 4: SonicWALL – Group VPN Configuration

Step 3 Change the Advanced settings:

- Default LAN Gateway: **0.0.0.0**

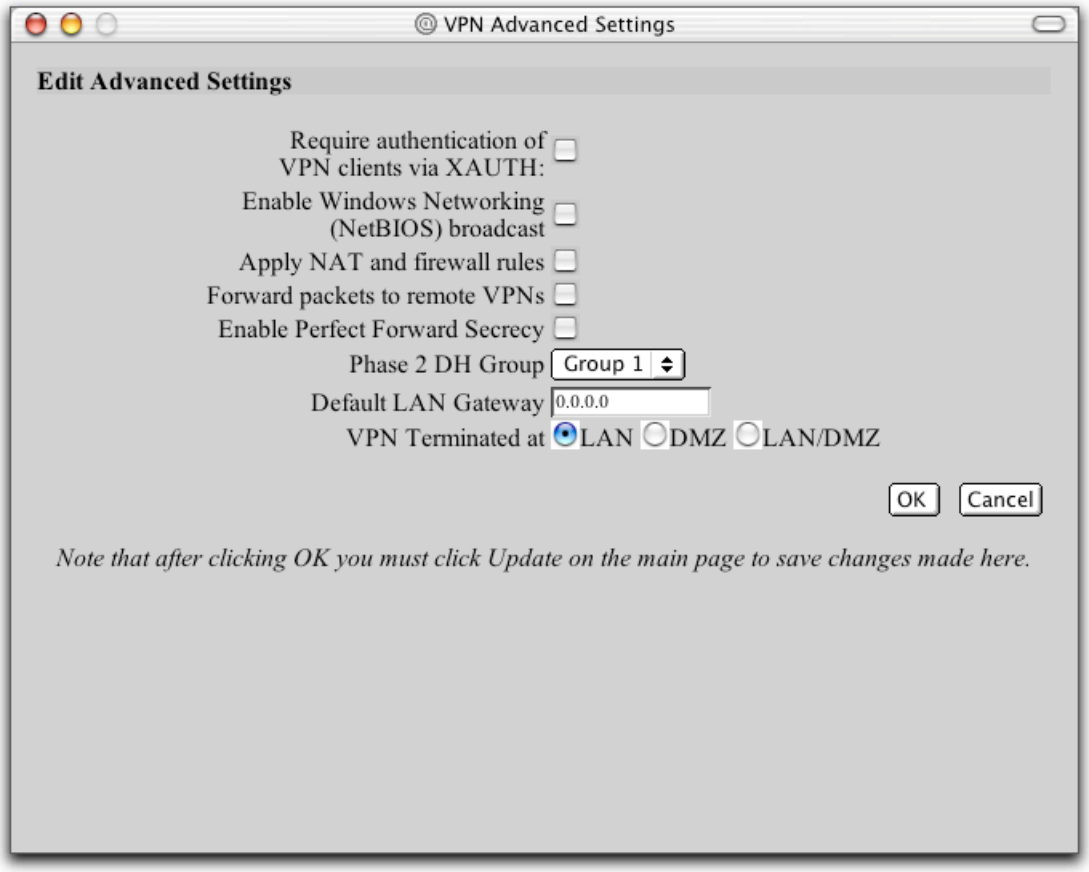


Figure 5: SonicWALL – Advanced Settings

Please note: In order to authenticate multiple clients with different credentials, please enable "Require Authentication of VPN Clients via XAUTH". In this case you'll also need to check "Extended Authentication (XAUTH)" in your VPN Tracker Authentication settings. Additionally you'll need to enable "Access from VPN client with XAUTH" for the specific user. Please refer to the SonicWALL manual for further assistance regarding user management.

3.2 VPN Tracker Configuration

Step 1 Add a new connection with the following options:

- Vendor: „SonicWALL“
- Model: your VPN device

Figure 5: VPN Tracker - Connection settings

Step 2 Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. **169.1.2.3**)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.255.0).

Figure 6: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.[2]

[2] For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the SonicWALL configuration.
- Enable XAUTH if the corresponding option is enabled on the SonicWALL.

Figure 7: VPN Tracker - Authentication settings

Step 4 Change your Identifier Settings:

- Local Identifier: Local endpoint IP address.
- Remote Identifier: Remote endpoint IP address.

Figure 8: VPN Tracker - Identifier settings

Step 5 Save the connection and Click „Start IPsec“ in the VPN Tracker main window.

You’re done. After 10-20 seconds the red status indicator for the connection should change to green, which means you’re securely connected to the SonicWALL. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the SonicWALL network from the dialed-in Mac in the “Terminal” utility:

```
ping 192.168.1.10
```

Troubleshooting

If the status indicator does not change to green please have a look at the log file on both sides. You can define the amount of information available in the log file in the VPN Tracker preferences. Below you can find a list of common error messages in the SonicWALL log file:

Log message: `IKE Responder: IKE proposal does not match (Phase 1)`
Solution: Check the Phase 1 algorithm and authentication settings.

Log message: `IKE Responder: ESP Perfect Forward Secrecy mismatch`
Solution: Check the Phase 2 Perfect Forward Secrecy settings.

Log message: `IKE Responder: Tunnel terminates inside firewall but proposed local network is not inside firewall`
Solution: Check the Remote Network settings in VPN Tracker.

4. Connecting a VPN Tracker Host to a SonicWALL Firewall using Certificates

For Certificate Authentication, you'll need a CA with private key, so one VPN Tracker Professional Edition is required if you don't yet have a signing CA. Only one VPN Tracker Professional Edition is required, other VPN users can use a Personal Edition. For further information please refer to chapter 3 in the VPN Tracker manual.

4.1 SonicWALL Configuration

Step 1 Check „Enable VPN" and disable „NAT Traversal" and click „Update" when you are finished.

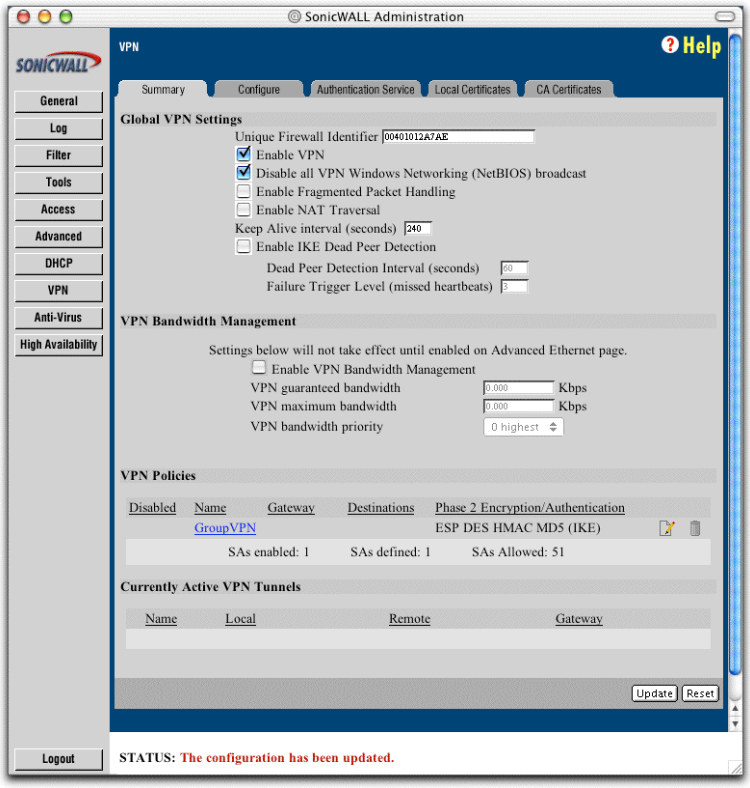


Figure 9: SonicWALL - Global VPN Settings

Step 2

Please go to [VPN -› Local Certificate] and generate a “Certificate Signing Request”. Enter a “Certificate name” and a “Common name” for the Certificate. You have to use a “Subject Alternative Name (Optional)”. Select “Domain Name” and enter an arbitrary name. This setting refers to the “Remote Identifier” in VPN Tracker.

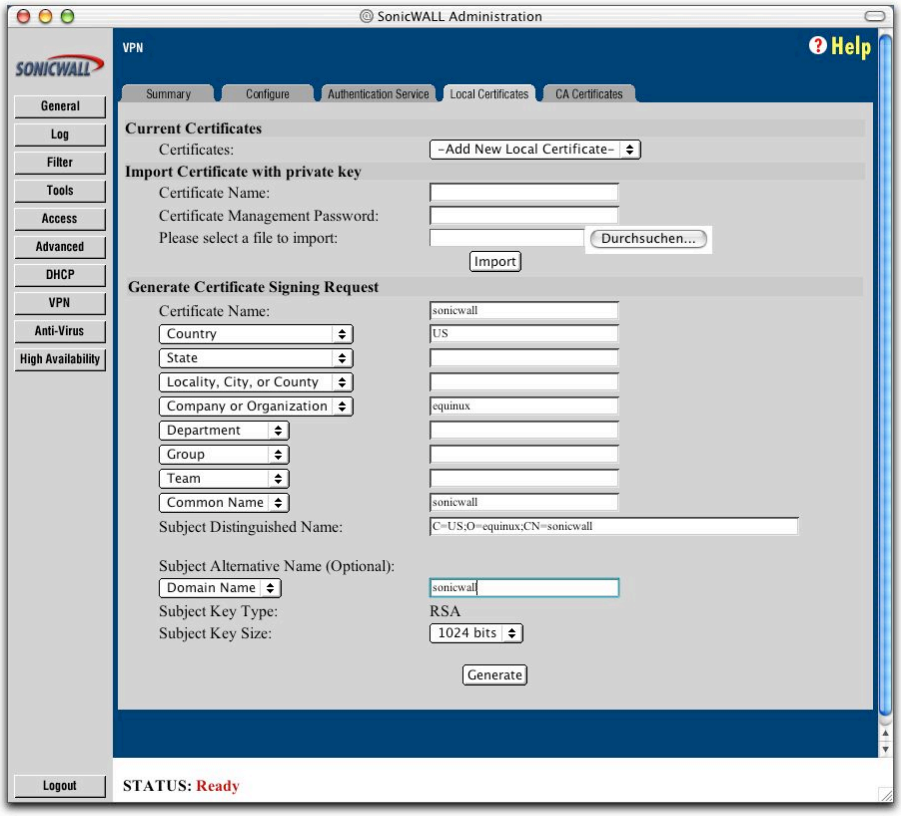


Figure 10: SonicWall - Certificate Signing Request

Step 3

Export the certificate request to a file, import the Request in the “Request” tab in VPN Tracker. Finally “Sign” the request with a CA. The “Alternative Name” field is pre-defined with the value you entered in the Certificate Signing request. It should be the same as the “Alternate Subject Name”, defined before.

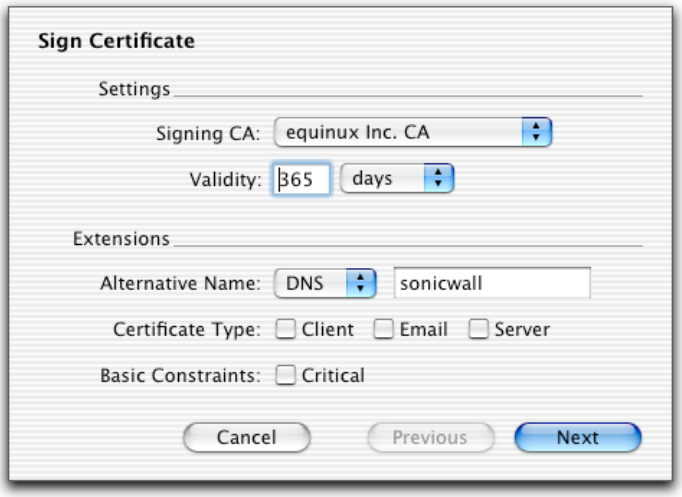


Figure 11: VPN Tracker - Sign Certificate

Step 4

Export the signed certificate in the PEM- format and Import the Certificate in the SonicWALL.

Please note: The “Alternative subject name” of the certificate must be set and the Subject name Type must be “Domain Name”.

After step 4 the configuration should look like this:

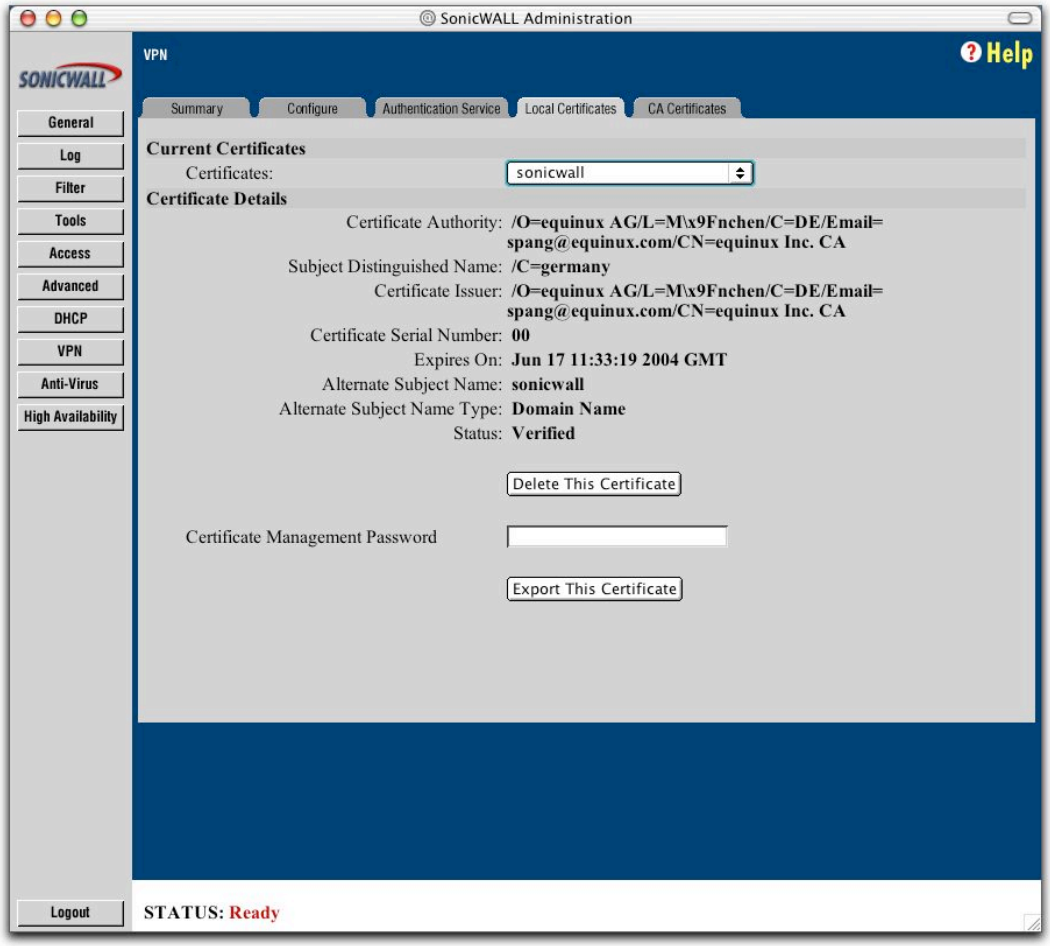


Figure 12: SonicWALL - Import the signed Certificate

Step 5

On the Sonicwall go to [VPN -› CA Certificates] and import the CA, which you used for signing, into the Sonicwall. The CA file must be exported in the DER- format.

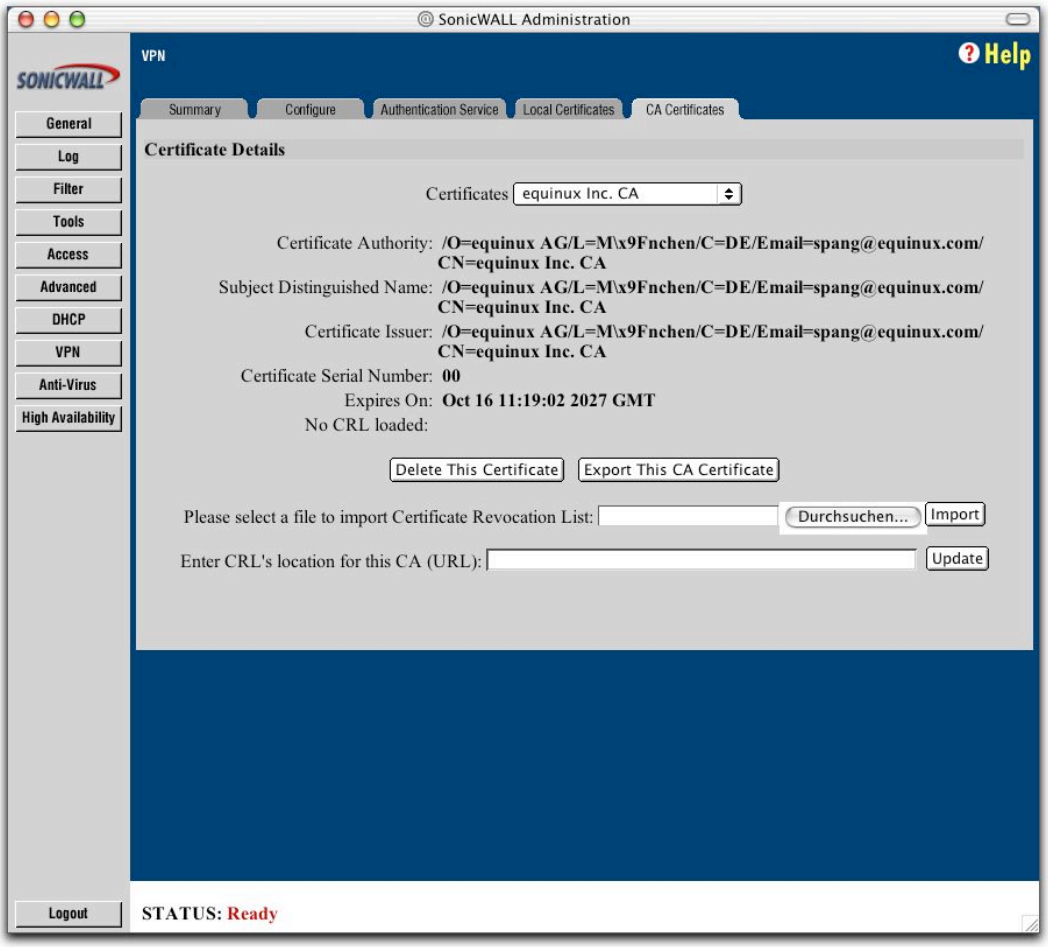
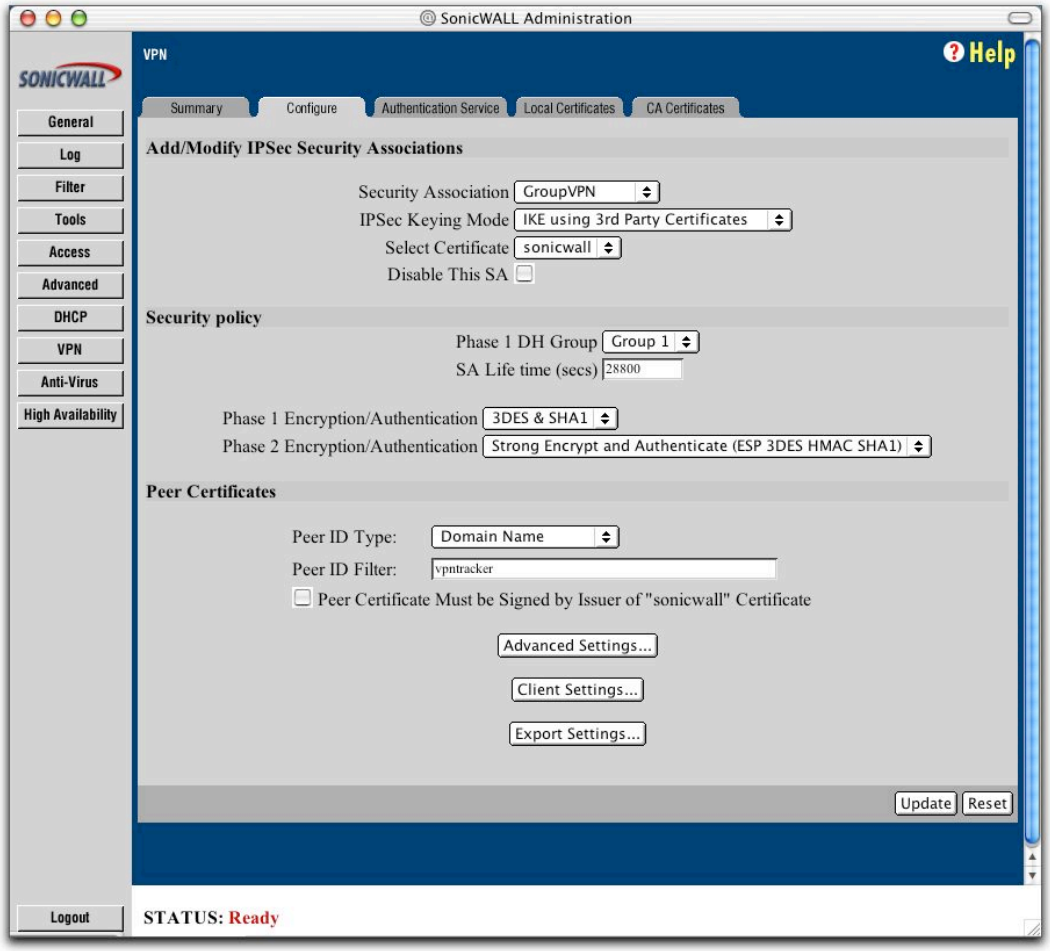


Figure 13: SonicWALL - Import your CA

Step 6

Please go to [VPN -› Configure] and configure the predefined Security Association „GroupVPN”:

- IPSec Keying Mode: IKE using 3rd Party Certificates
- Select Certificate: select your previously imported Certificate
- Peer ID Type: **Domain Name**
- Peer ID Filter: Domain Name of the client certificate (e.g. **vpntracker**)



[3] For this step, VPN Tracker Professional Edition is required.

4.2 VPN Tracker Configuration

Step 1 Create a new "Own certificate" for VPN Tracker.

Go to the VPN Tracker certificate manager (⌘ + "E") and create and sign a new certificate. You have to use an "Alternative Name". Choose DNS from the drop-down box and enter the alternative name. This name must be the same as the "Peer ID Filter" field in your SonicWALL VPN settings.

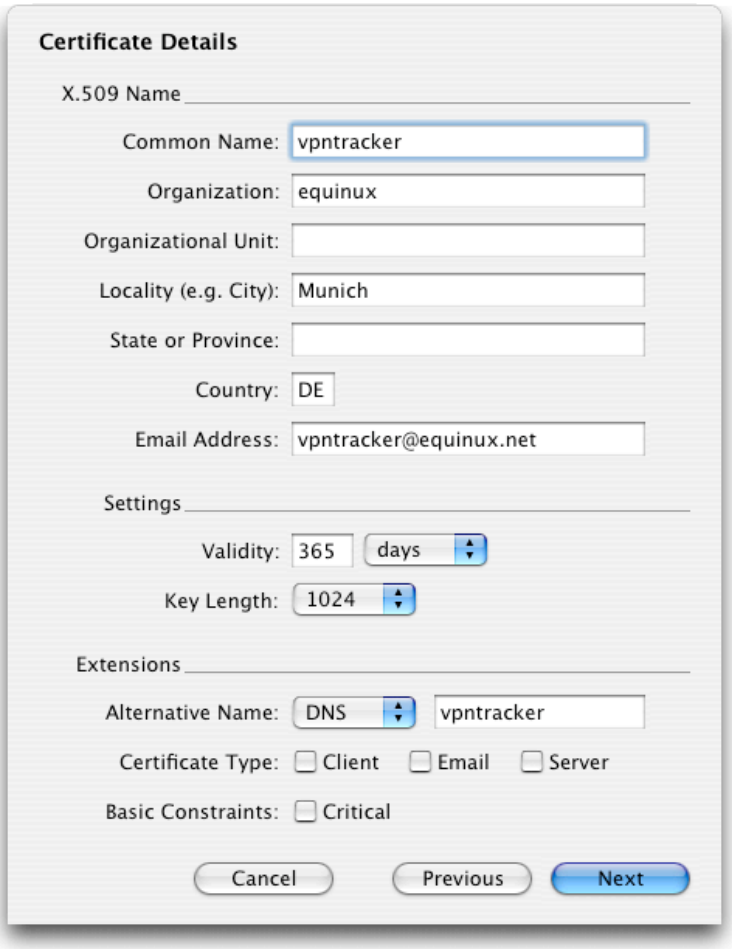


Figure 15: VPN Tracker - Own certificate

[4] For this step, VPN Tracker Professional Edition is required.

Step 2-3 Please refer to section 3.2 step 1-2.

Step 4 Change your Authentication Settings:

- Own Certificate: a self-signed certificate, created by VPN Tracker
- Remote Certificate: **Verify with CA's**

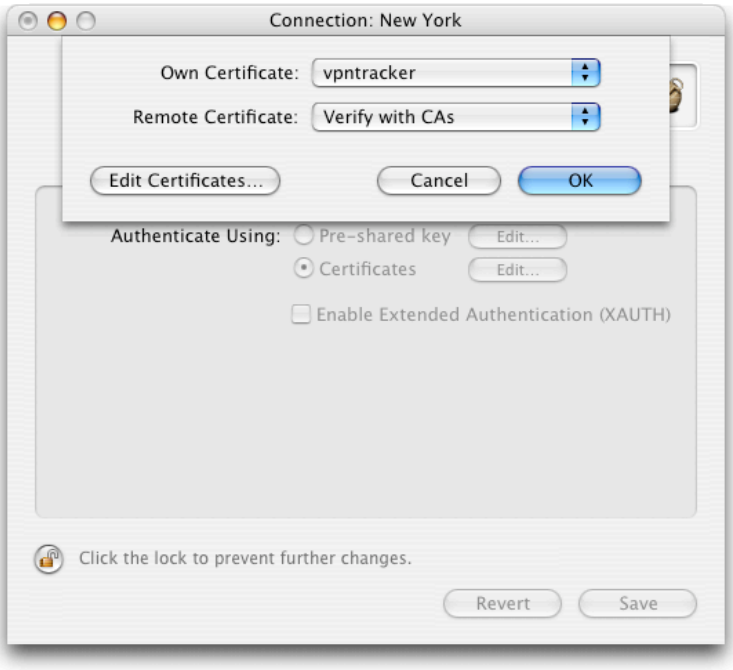


Figure 17: VPN Tracker - Authentication Settings

Step 5 Change your Identifier Settings:

- Local Identifier: Domain Name of the self-signed certificate (e.g. **vpntracker**)
- Remote Identifier: Domain Name of the SonicWALL certificate (e.g. **sonicwall**)

Figure 18: VPN Tracker - Identifier Settings

Step 6 Please refer to section 3.2 step 5.