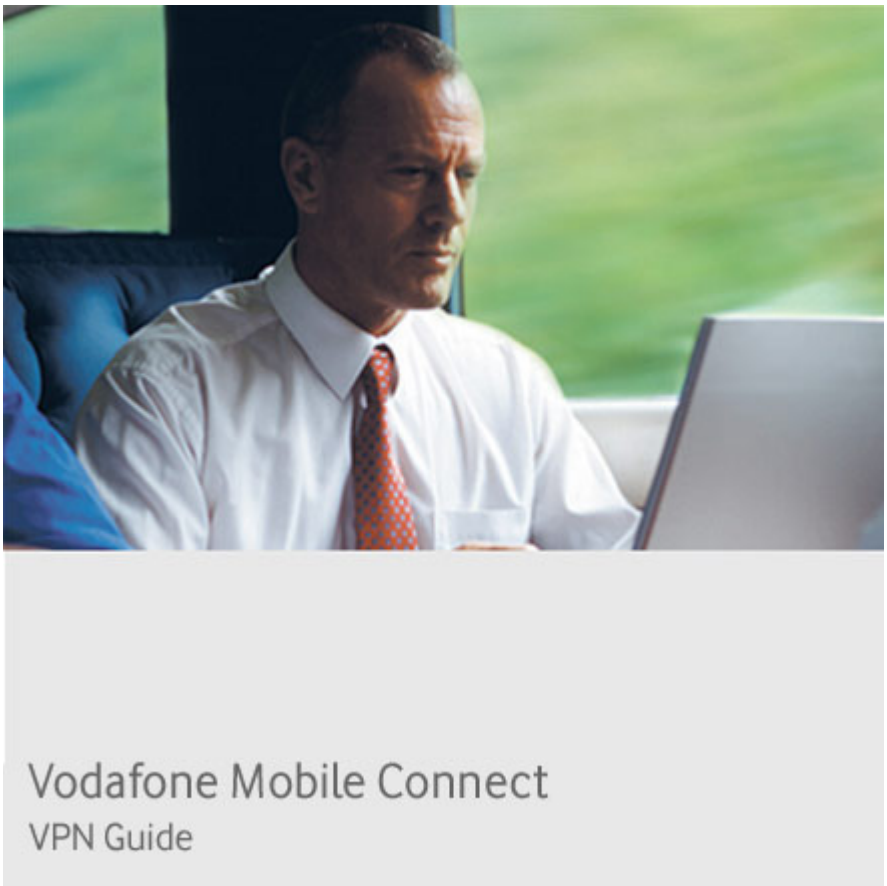
VPN End to End – SonicWall VPN Router

Appendix A: Configuration of the SonicWall TZ 170 W

Technical Notes for use with Vodafone Mobile Connect services

Date: **31 May 2007**

Revision No: **3.0**



© VODAFONE GROUP 2007

Scope

This document presents results of installation, configuration, and operations testing of VPN components with the Vodafone Mobile Connect service. The document is not intended to be a tutorial on VPN concepts nor does it supersede or replace the vendor's documentation. The reader is referred to the VPN vendor for definitive guidance on the proper and recommended use of their product. While Vodafone Group has taken care to ensure that the information contained herein is accurate, no responsibility can be accepted for errors, omissions, or inaccuracies.

Document History

Version	Date	Reason
1.0	October 2003	Initial release using GPRS network. Client documentation included in main document.
2.0	June 2006	Creation of separate document for client configuration. Update to new versions of VPN software and focus on 3G network performance.
3.0	May 2007	Minor changes & R9 review

File Reference

VPN_Netgear_FVS318_App A.doc

Document Authors

Peter Jaeger, TECON Terenci

Miroslaw Grzesica, TECON Terenci

Joerg Pfeffer, TECON Terenci

Document Distribution

Public via websites of Vodafone, its Affiliates, and its Partner Networks

© Vodafone Group 2007.

Other than as permitted by law, no part of this document may be reproduced, adapted, or distributed, in any form or by any means, without the prior written consent of Vodafone Group Plc.

Contents

1 Executive Summary 4

2 TZ 170 W appliance Installation and Configuration (Version 3.1.0) 5

2.1 Initial setup 5

2.2 Setup Wizard 5

2.3 Configuration of Routing 12

2.4 Configuration of VPN 13

2.5 Configuration of DHCP over VPN 18

2.6 Advanced Configuration 22

3 Logging 27

© VODAFONE GROUP 2007

1 Executive Summary

This Appendix is in addition to the overview document for SonicWall TZ 170 VPN system and describes the setup and update process in a detailed way with example screen shots taken from the initial processes:

- Initial setup of the router for basic operation
- Configuration of NAT-Traversal (generally required for use with mobile networks)
- Setup of user groups, timeouts, and other common parameters. In our tests, the Keepalive packet frequency did not change when the configuration settings were decreased.
- Device software upgrades, saving and restoring configuration files

Furthermore logging and additional functionality is described in the appropriate chapters.

The user is recommended to change the default settings for split-tunnelling and assignment of internal IP addresses.

Further information is available from the vendor documentation and website www.sonicwall.com.

© VODAFONE GROUP 2007

2 TZ 170 W appliance Installation and Configuration (Version 3.1.0)

The following description is intended for network administrators who are familiar with networking and IP concepts. The appliance has to be integrated into the internal company network. The appliance setup therefore has to comply with the configuration of the internal networking. This description is intended to allow a network administrator not yet familiar with the SonicWALL TZ 170 W appliance to configure a VPN with UMTS/GPRS usage.

2.1 Initial setup

After unpacking the device, connect a PC to one of the trusted network connections numbered 1 to 5 and the WAN network connection to the internet gateway. The PC must be configured to use DHCP to receive the IP address and network data from the network. Connect the power, either by connecting the power supply or Power over Ethernet (PoE) to Network connector “1-PoE”.

2.2 Setup Wizard

The initial configuration is aided by a setup wizard when using a web browser for the initial setup.

The TZ 170 W Security Manager requires a Java-enabled web browser, e.g.

- Microsoft Internet Explorer version 6.0 SP1 or higher (Windows) (SP2 required for Windows XP)
- Netscape Navigator version 7.2 or higher (Windows, Linux, or Solaris)
- Mozilla 1.73 or higher (Windows, Linux, or Solaris)
- Firefox 1.0 or 1.5 (Windows, Macintosh, or Linux)

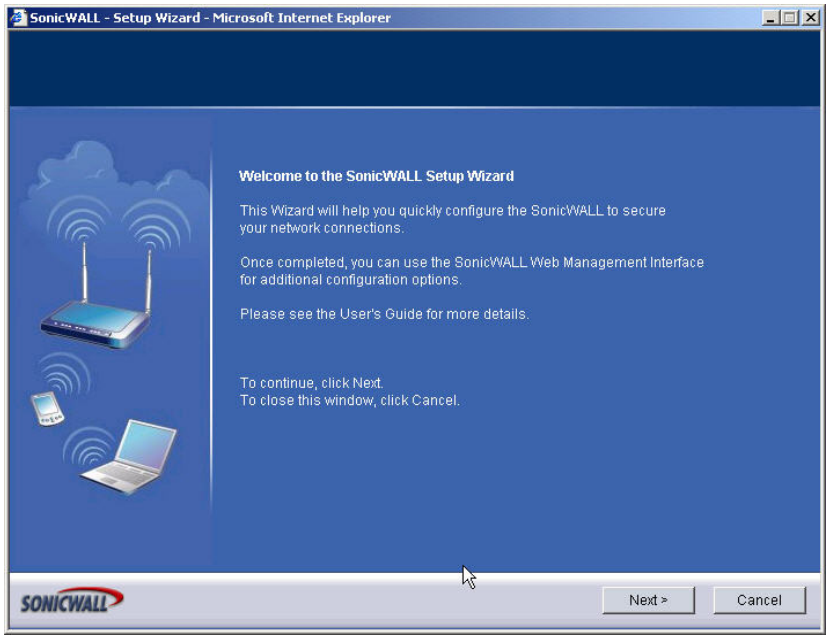
For best results, we recommend Internet Explorer. Whatever browser and version you use, install the latest patches and service packs for it.

Make sure you have Java script/Active scripting enabled in your browser.

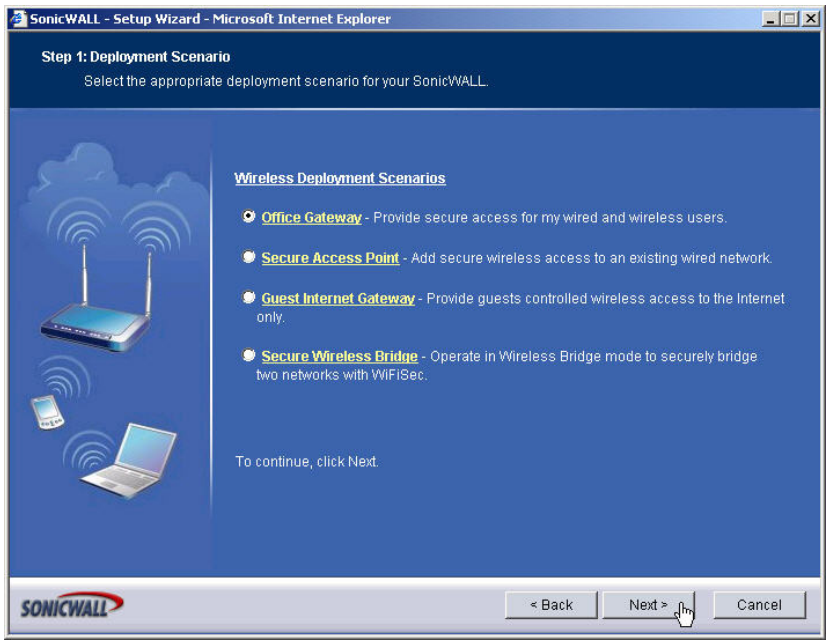
© VODAFONE GROUP 2007

When the browser is started, enter the URL http://192.168.168.168 and the “SonicWALL Setup Wizard” will be started.

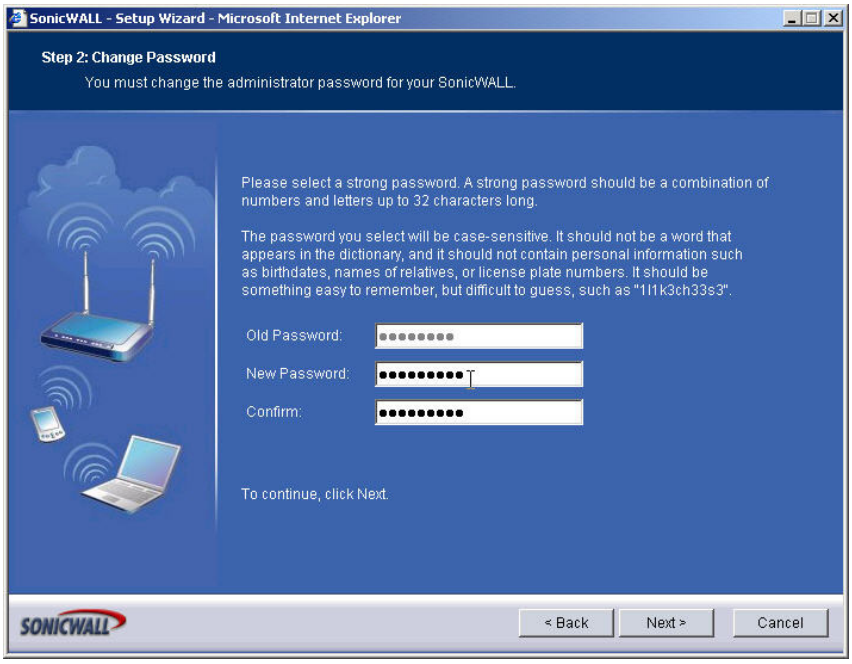
If no web page can be found with a new machine, check if the PC got an IP address via the network by using the command IPCONFIG in a command window. The IP address should be out of the range 192.168.168.0 to 192.168.168.254. To initiate the acquisition of a new IP address enter “IPCONFIG /RENEW” and check again. If that does not work, check the network connection to the SonicWALL device.



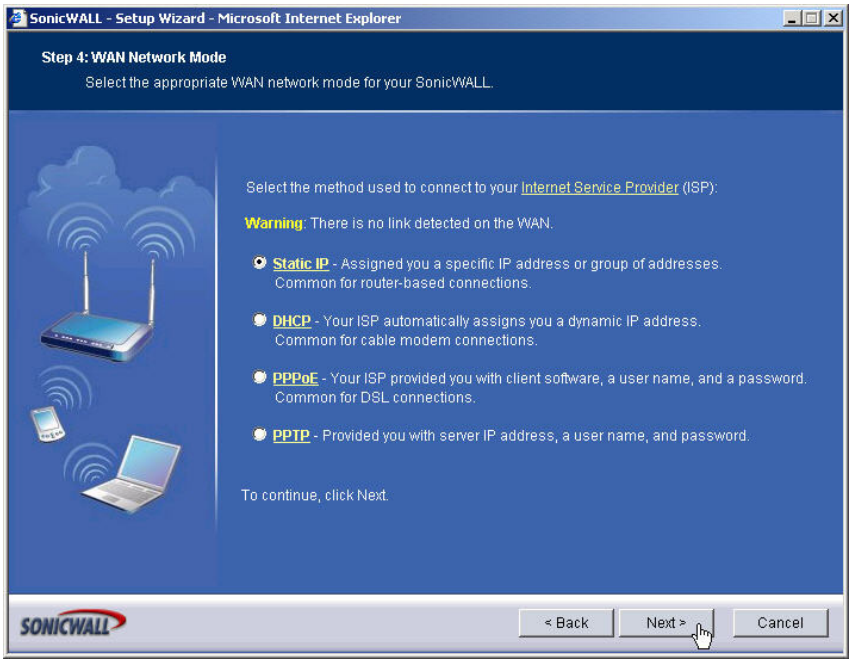
To use the device as a VPN gateway, select “Office Gateway”.



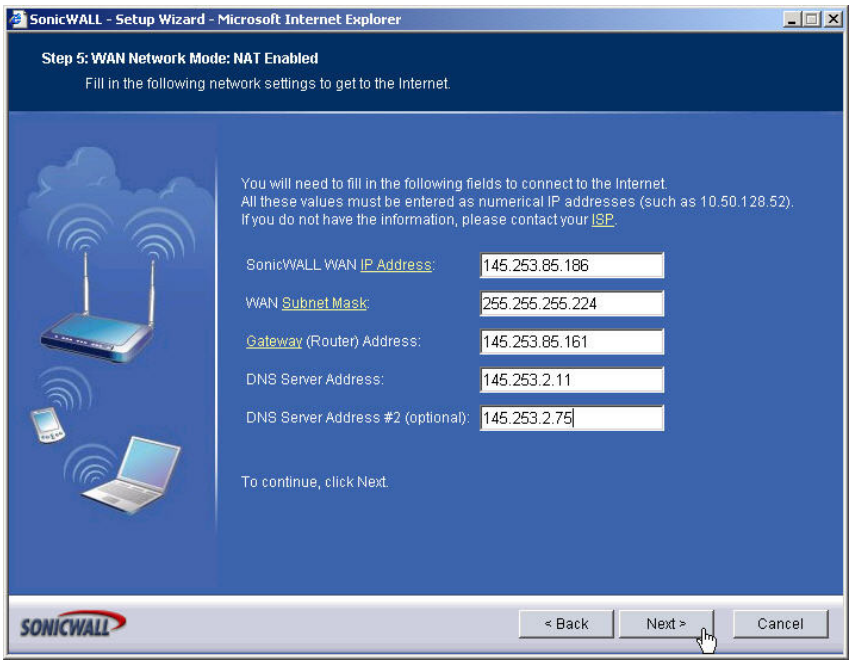
Enter a new administration password. The user name is fixed to “admin”.



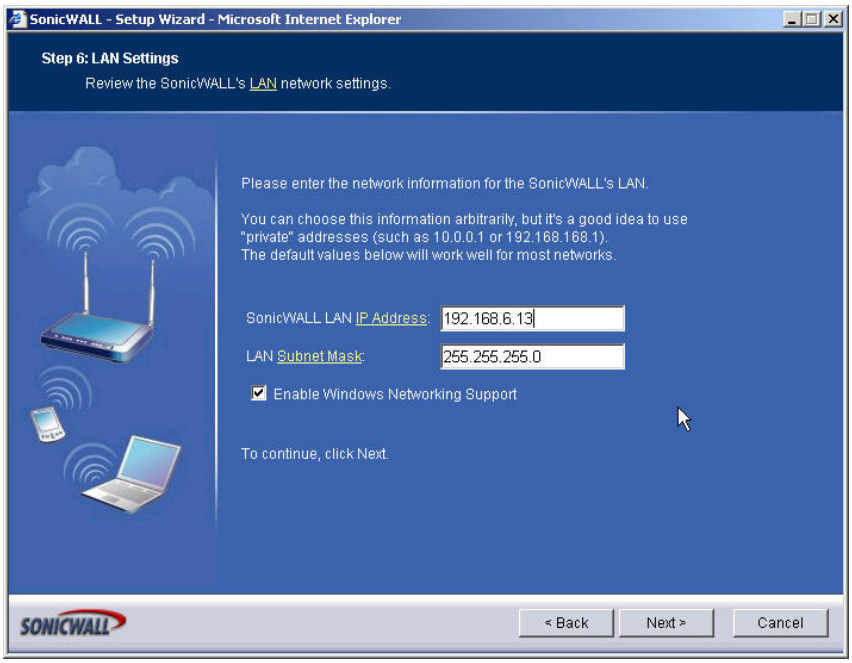
In Step 3, set up the time zone and click “NEXT >”. In Step 4, select how the appliance is connected to the internet. In our network, we use a static IP address. In other networks, the choice may be different. Please consult the ISP if unsure.



In Step 5, the network parameters of the WAN interface are set up. In case of a static IP address, the WAN IP address, subnet mask, default gateway and DNS servers are needed.

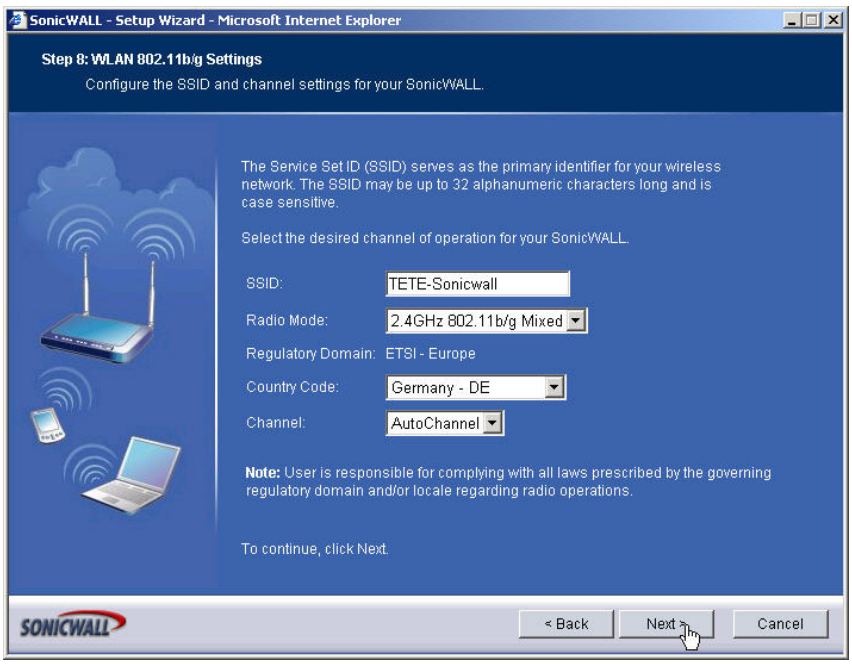


For the LAN, you can enter IP address and subnet mask in step 6. Keep in mind that routes cannot be entered here, so that after the changes are valid, the configuration must be continued from the directly connected network. The data entered here will not become valid immediately but will be activated after the wizard is completed.

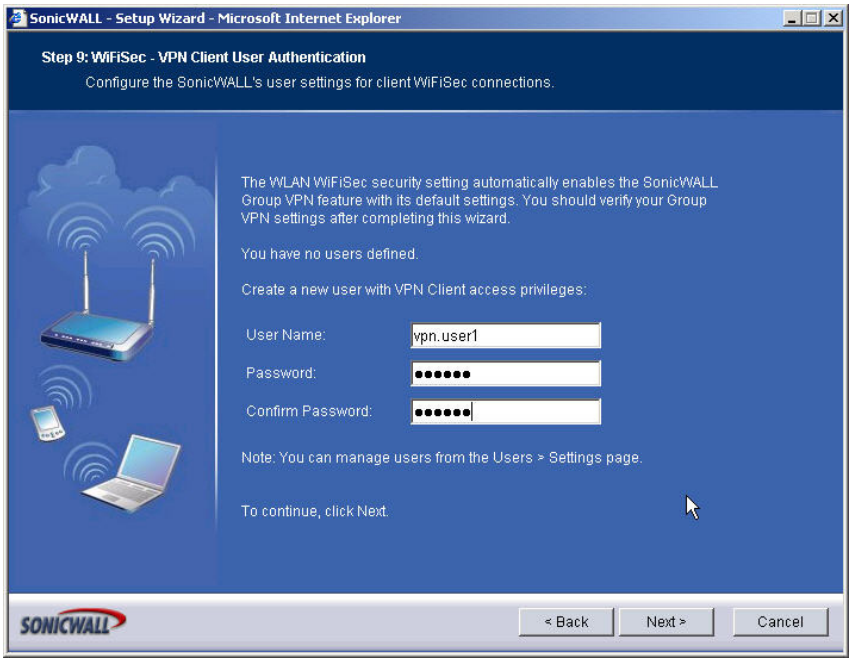


In Step 7, DHCP is disabled for the directly connected LAN because it is not needed in this setup. Uncheck “Enable DHCP Server on LAN” and then click “NEXT >”.

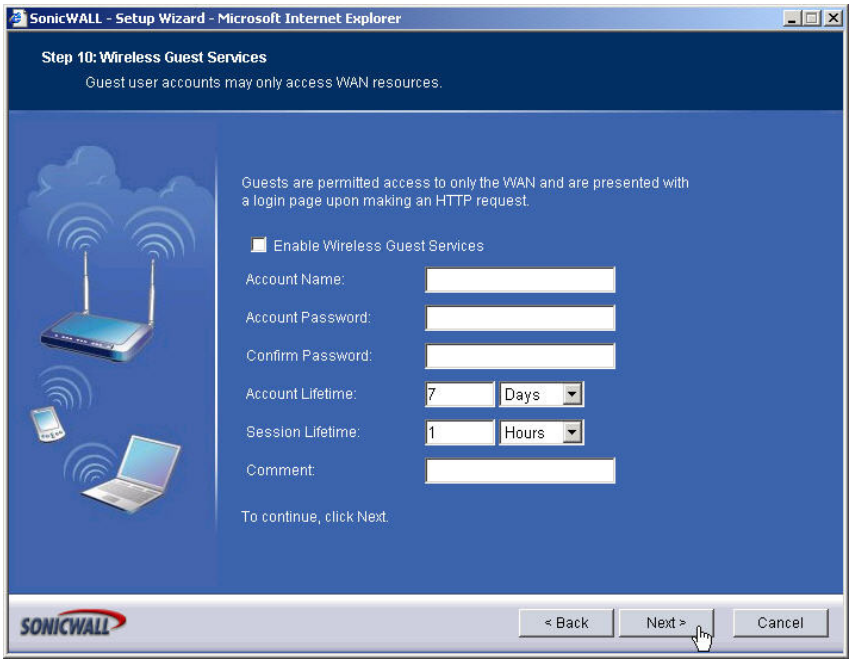
The next step is setting up the WLAN parameters. For the VPN tests, we do not use WLAN and therefore disable it later. Unfortunately, in Step 8, it is required to enter some data to continue. Click “NEXT >” to continue.



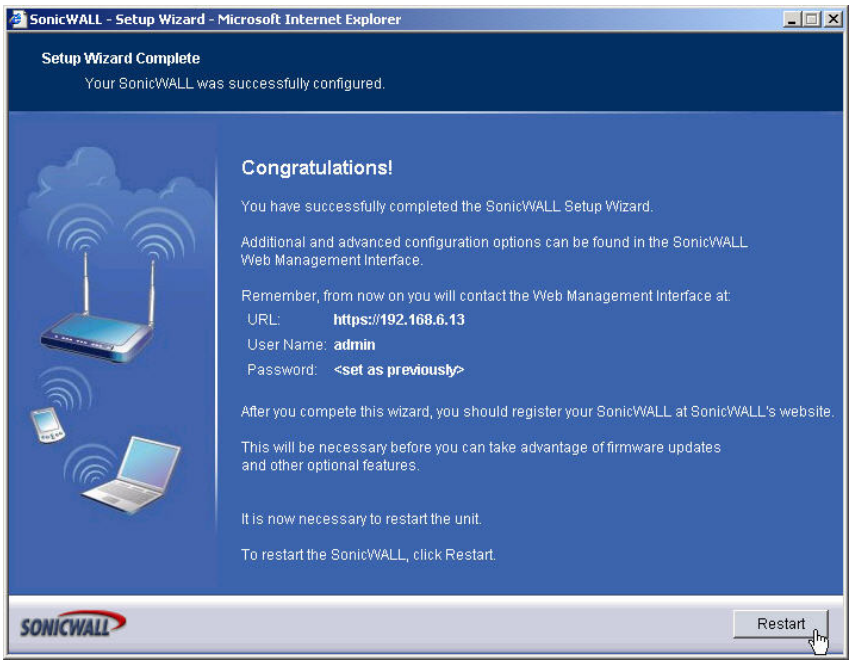
In Step 9, a VPN user can be defined for later use. Enter a user name and password and continue.



We do not use wireless guest services, so uncheck “Enable Wireless Guest Services” in Step 10 and continue.

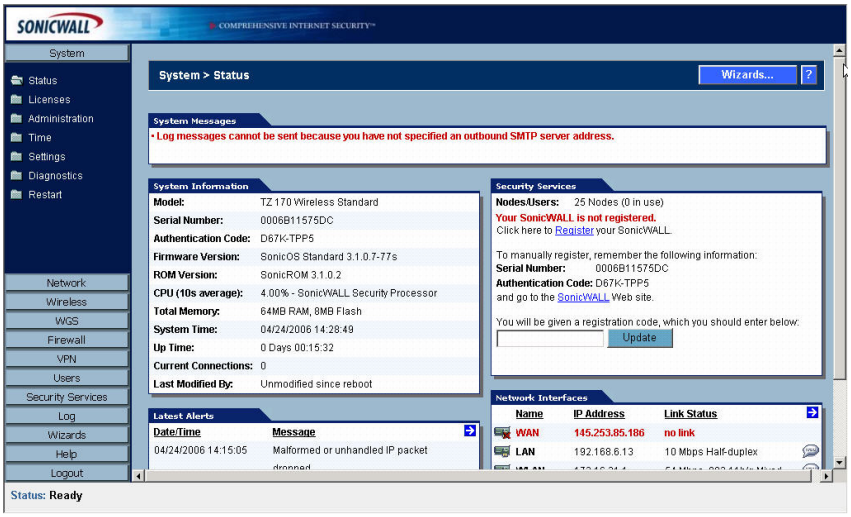


In Step 11, all parameters are displayed for review. Clicking “Apply” will update the configuration. After the configuration is updated, the user will be shown how to log in with the new configuration and is prompted to reboot the device.

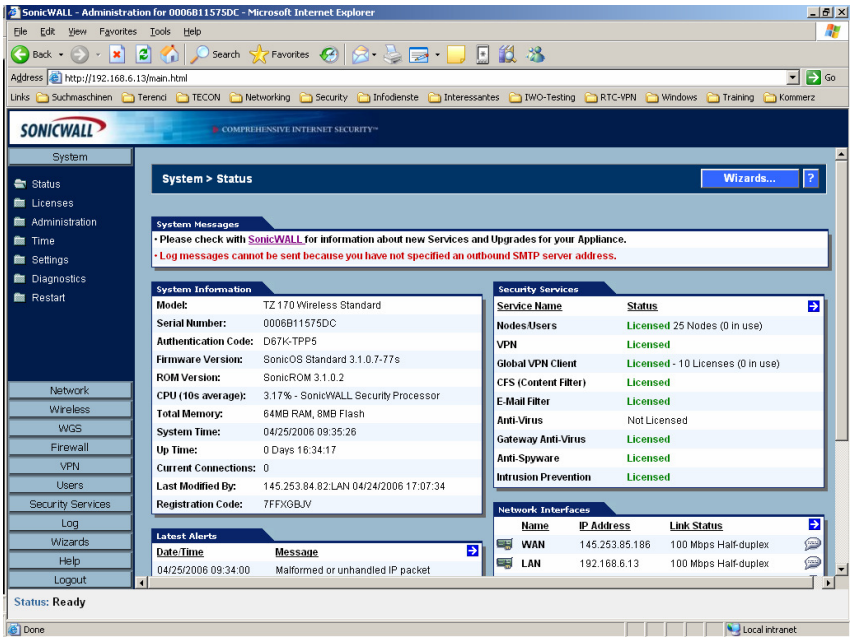


This concludes the setup wizard. After the reboot, the user is prompted for user and password to log in. After login, the machine should be registered. For this, access to the

internet is necessary. You can use the links given on the “System > Status” page, in the “Security Services” tab.



After registration, the state of the licenses will be shown.

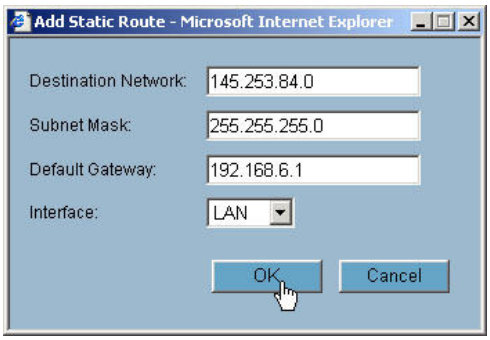


The system is now ready to be configured further.

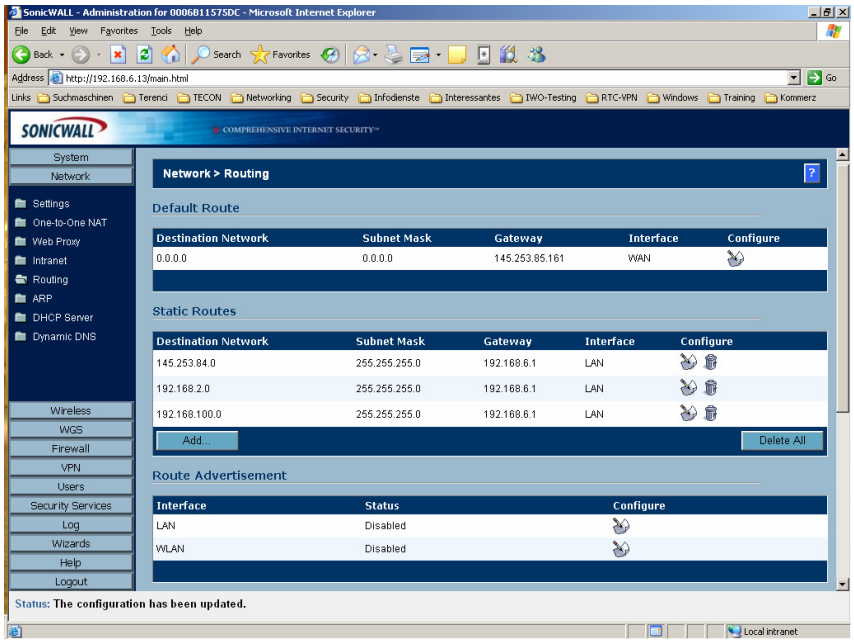
2.3 Configuration of Routing

Go to the “Network > Routing” screen. In the “Static Routes” tab, click “Add” to add a new static route.

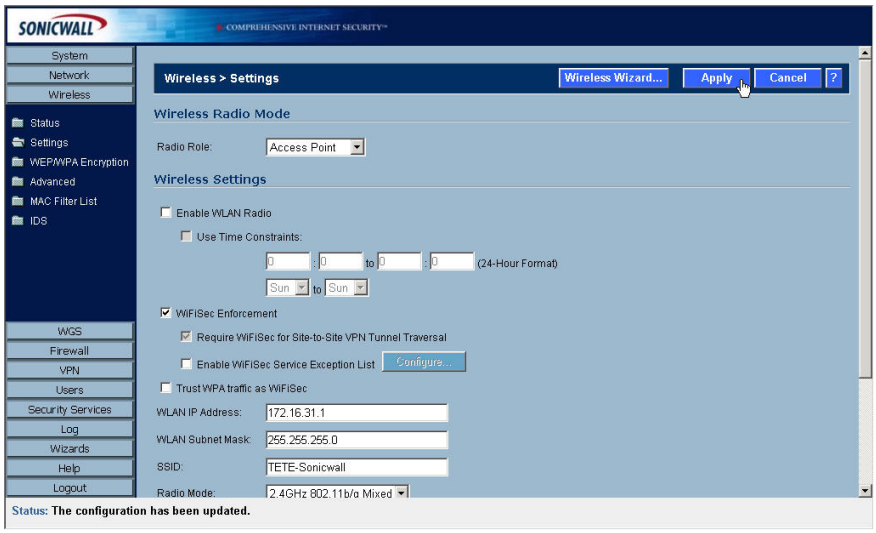
Enter the network, subnet mask and gateway data and click “OK” to add the route.



Make sure to configure the route to the internal network you wish to reach via the VPN.



To switch off WLAN, go to the “Wireless > Settings” screen. There, uncheck “Enable WLAN Radio”.



2.4 Configuration of VPN

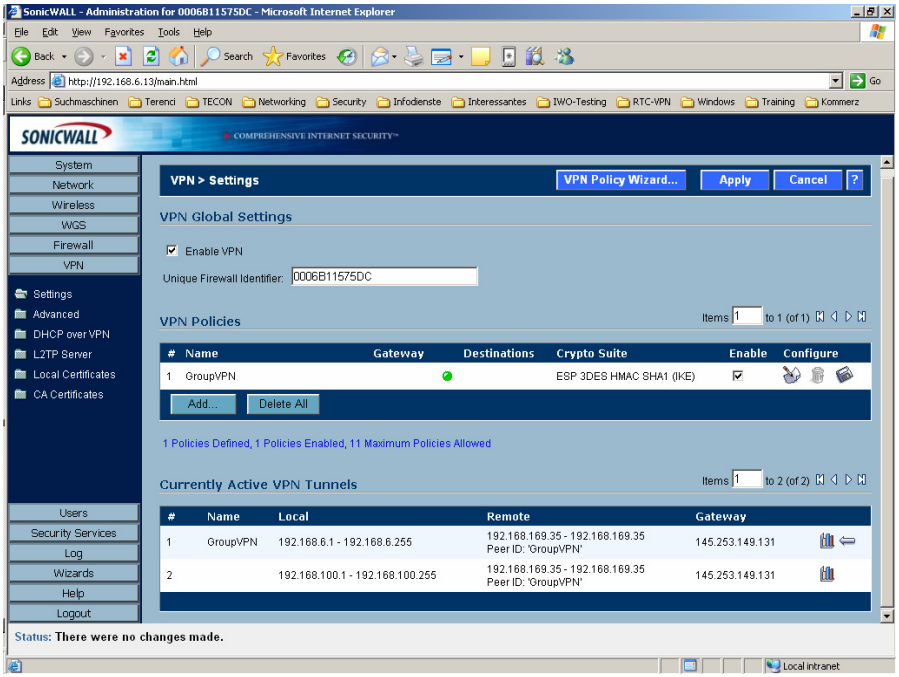
A basic set of VPN parameters and the first VPN user is already defined in the setup wizard. The VPN tunnel and authentication of this default VPN setup works, but the disadvantages of the default settings are the following:

- Access to the Internet is allowed while the VPN tunnel is active (Split Tunneling)

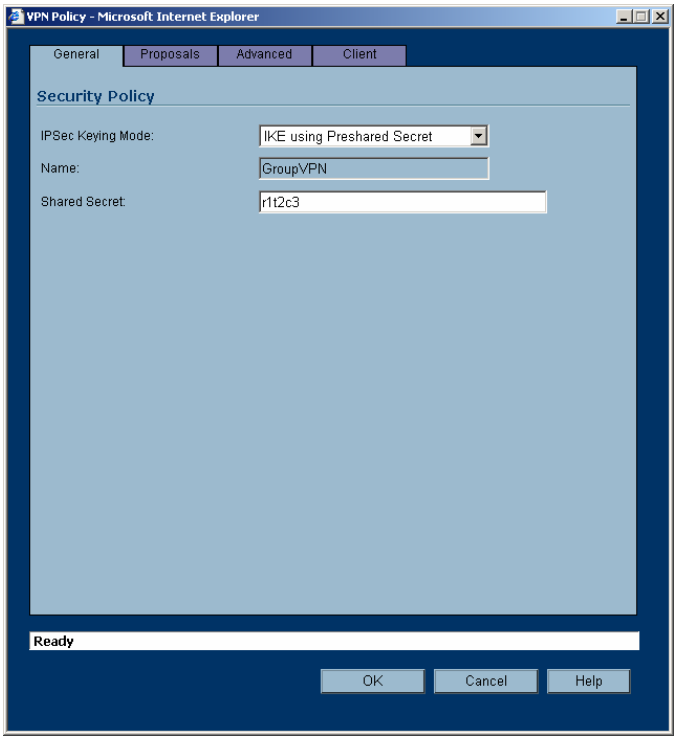
- There is no internal IP address assigned to VPN clients. This implies that the VPN gateway must be the default gateway of the corporate network for the VPN to work.

Here, the additional configuration and the adding of new users and some adaptations to accommodate the 3G/2.5G environment are described.

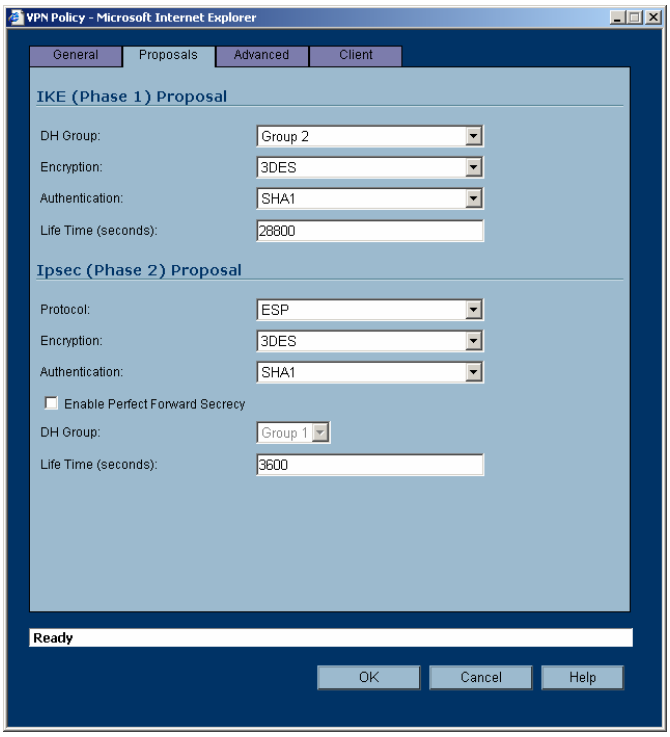
All VPN related setups for the Global VPN Client are entered in the “GroupVPN” policy. This policy is located on the screen “VPN > Settings”. In the “GroupVPN” line, click on the pen-and-paper icon below “Configure” to edit the policy.



A new window will open where the VPN parameters can be set up on four tabs. The “General” tab allows selecting the keying mode. For this example, “IKE using Preshared Secret” is selected. To improve security, certificates could also be selected. If “Preshared Secret” is used, change the Shred Secret to an individual one.



In the “Proposals” tab, optionally, you can change the Ipsec (Phase 2) Proposal Life Time to 3600 seconds (1 hour, compared to the default 8 hours) to improve security. Enabling Perfect Forward Secrecy further enhances security.

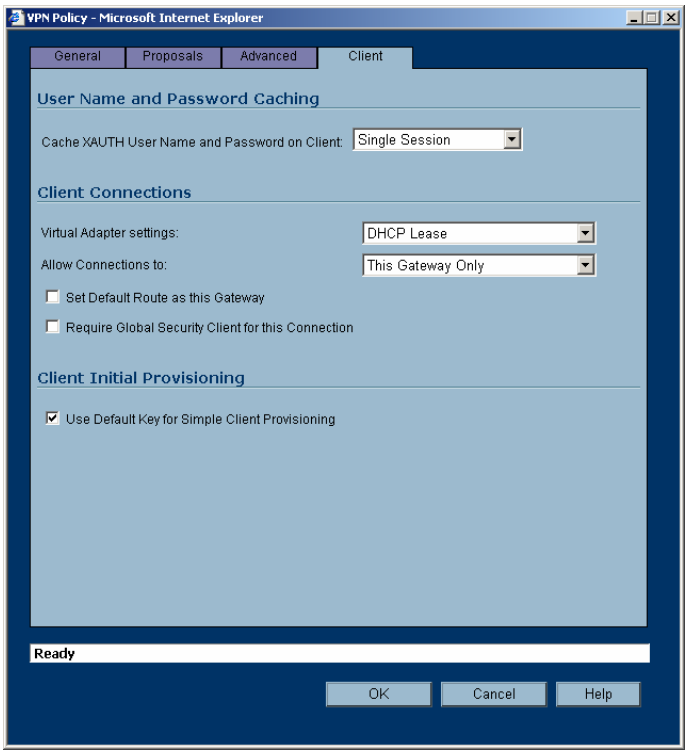


In the “Client” tab, set the “User Name and Password Caching” to “Single Session”. In the “Client Connections” part, Set the “Virtual Adapter Settings” to “DHCP Lease” to enable an internal IP address to be leased by a DHCP server.

Attention: Using the internal DHCP-Server for this purpose will only allow a pool of addresses taken from one of the directly connected networks.

© VODAFONE GROUP 2007

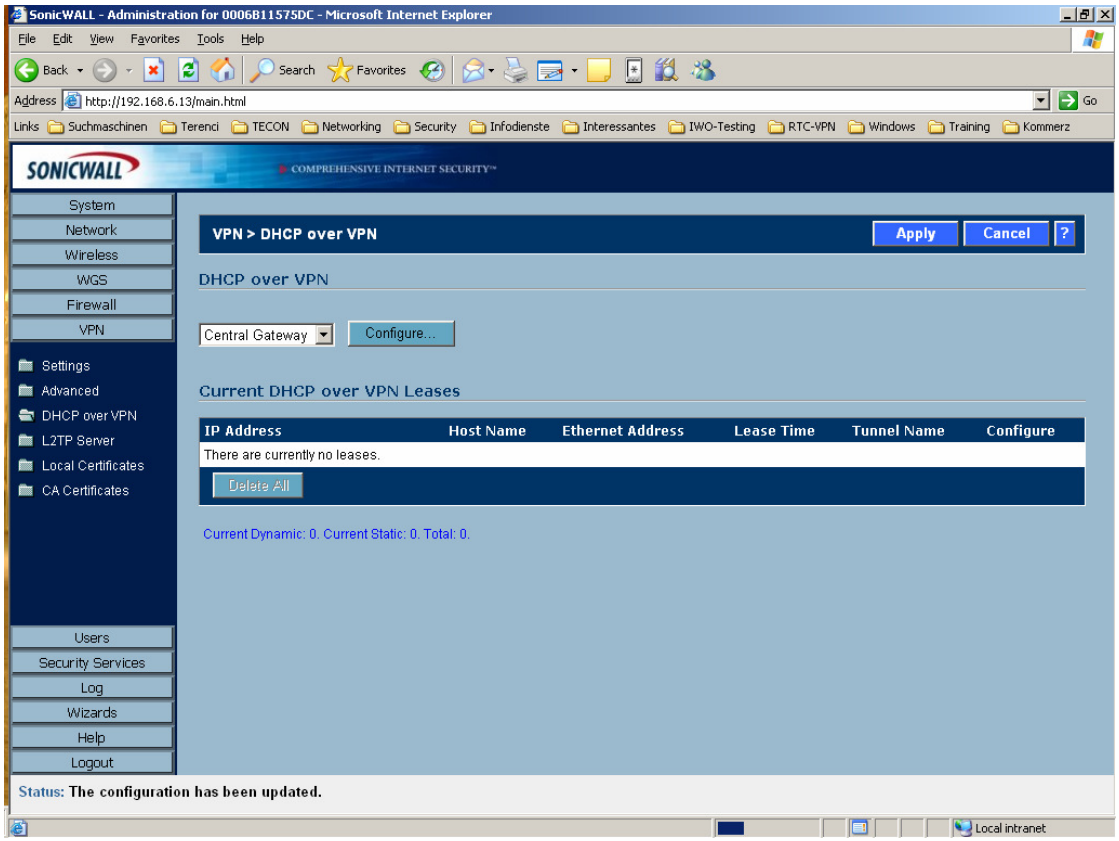
Changing the “Allow Connections to” entry from “Split Tunnels” to “This Gateway Only” will send all traffic from the VPN client to the SonicWALL device and therefore inhibit Split Tunnelling on the client.



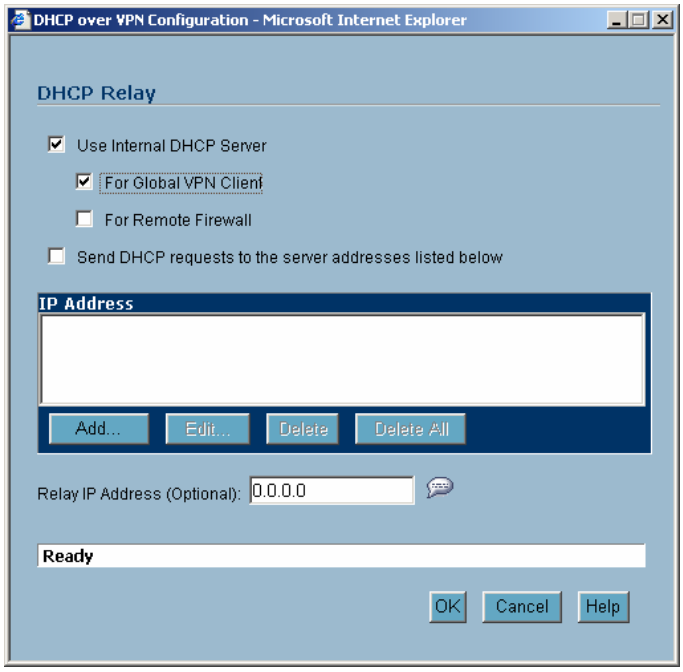
Click OK to accept the changes in the GroupVPN policy.

2.5 Configuration of DHCP over VPN

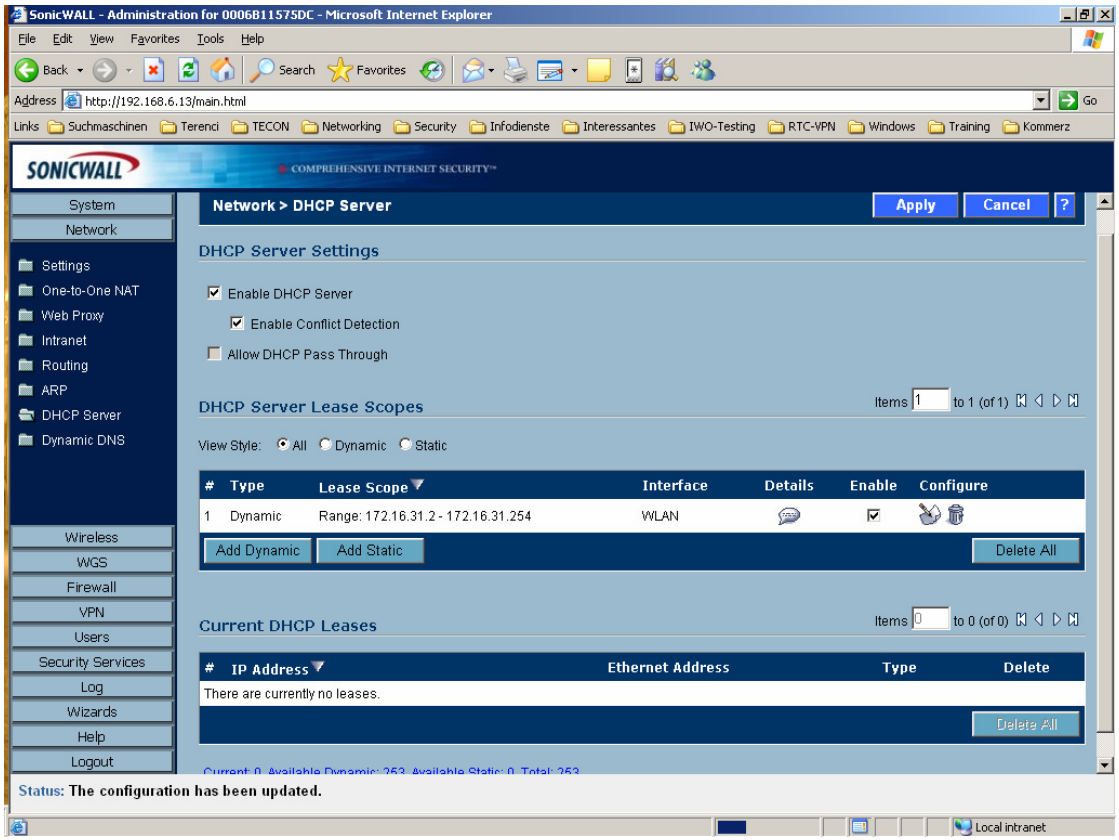
When “DHCP Lease” is activated in the GroupVPN policy, DHCP over VPN must be configured for the VPN to work. Go to the screen “VPN > DHCP over VPN”.



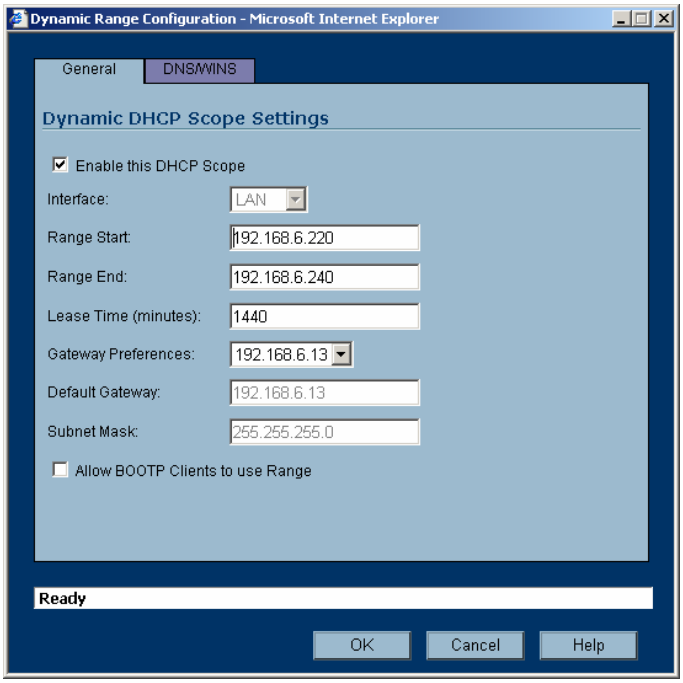
Click configure for the “Central Gateway”. Check “Use Internal DHCP Server” and “For Global VPN Client” and click OK to confirm the changes.



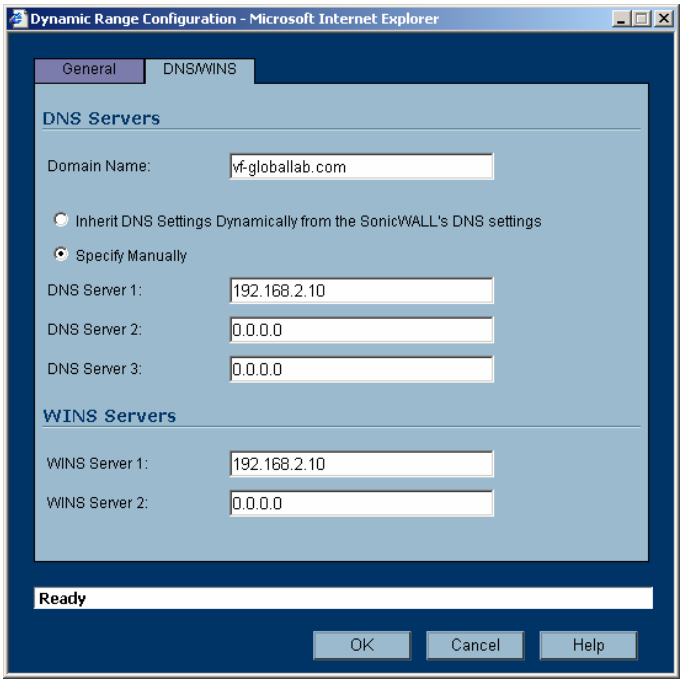
The DHCP setup of the internal DHCP server is done on the screen “Network > DHCP Server”. Disable unused ranges by unchecking the “Enable” fields of existing DHCP Server Lease Scopes. Add a new range with the “Add Dynamic” button.



Add a scope for the LAN interface. Please keep in mind that the internal DHCP server can only manage a range of the directly connected network. In the “General” tab, enter a range start and end IP address and lease time. Select the LAN interface IP address of the SonicWALL as “Gateway Preference”.

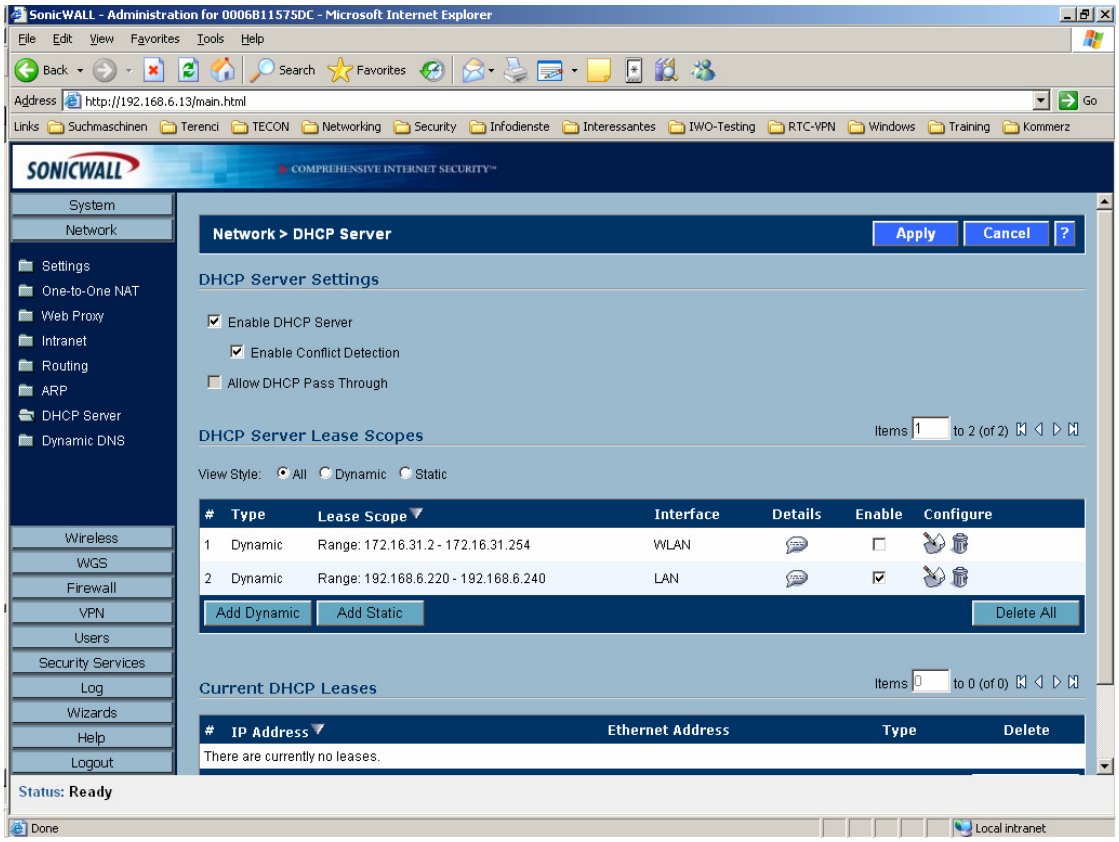


In the “DNS/WINS” tab, enter the desired DNS and WINS servers.



© VODAFONE GROUP 2007

Click OK to confirm the changes.



2.6 Advanced Configuration

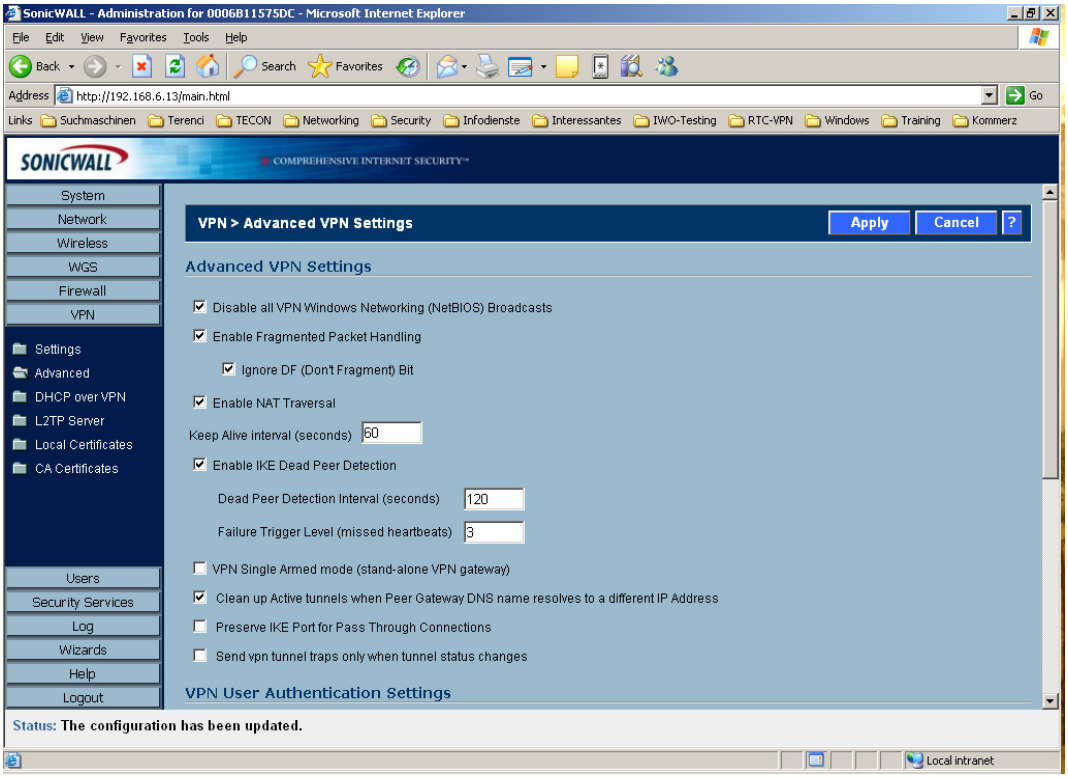
2.6.1 Keepalive Intervals

The default keepalive settings used for the VPN are not suited well for the use with a 3G or GPRS network. They are either too long to keep the connection entries in NAT devices stable or so short that they cause a high management traffic.

On the SonicWALL appliance, go to the “VPN > Advanced VPN Settings” screen.

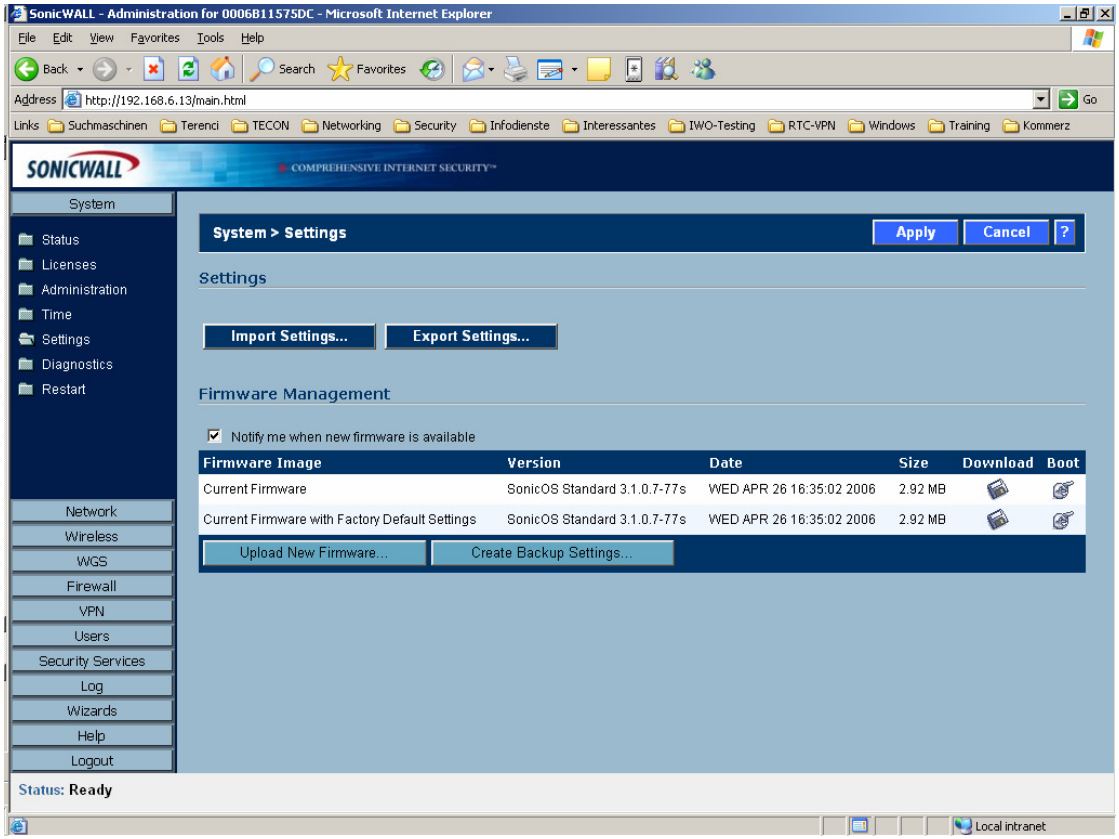
Change the “Keep Alive Interval (seconds)” to a value in the range of 30 to 60 seconds to decrease administrative traffic. **Unfortunately, a change of this value has no effect in the tested software-version / setup and the interval will remain at 10 seconds.**

Increase the “Dead Peer Detection Interval (seconds)” to 60 seconds. Since there are also Keepalive packets, this is sufficient.

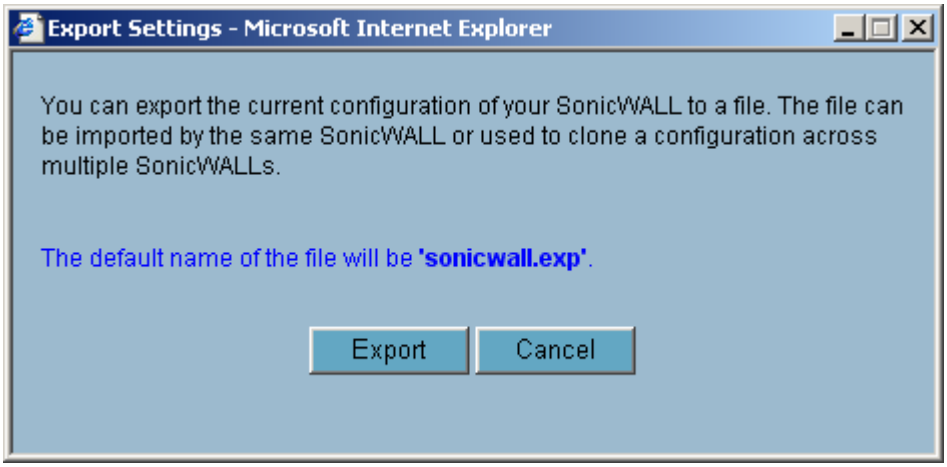


2.6.2 Backup of the SonicWALL TZ 170 W Configuration File

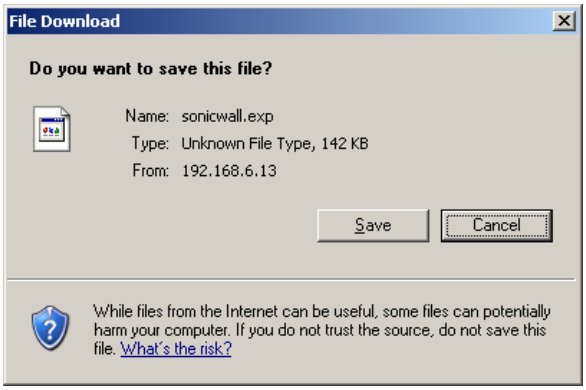
Backup and restore of the SonicWALL configuration is done in the “System > Settings” screen.



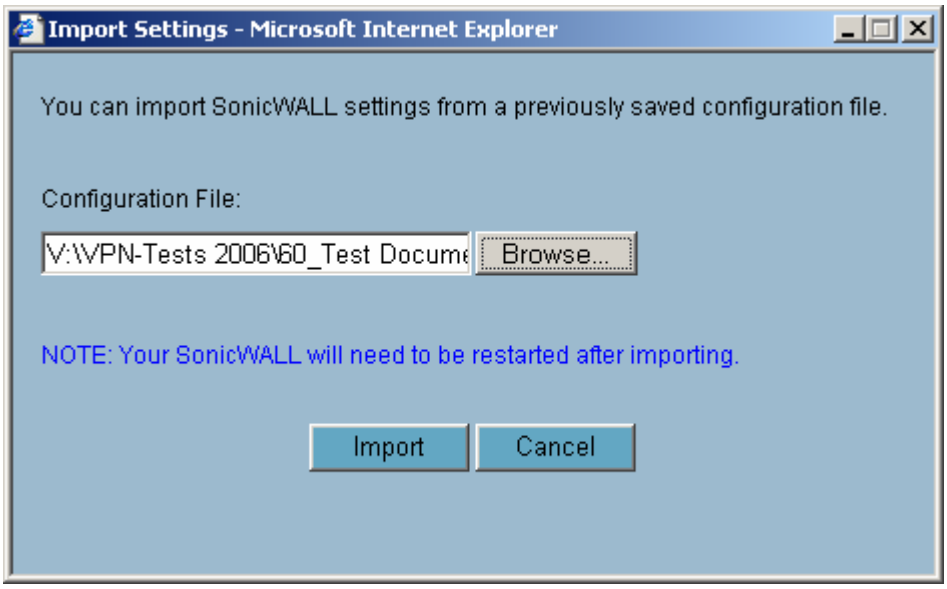
Click “Export Settings…” to download a configuration file to the management PC.



When clicking “Export” the file is saved to the local PC.

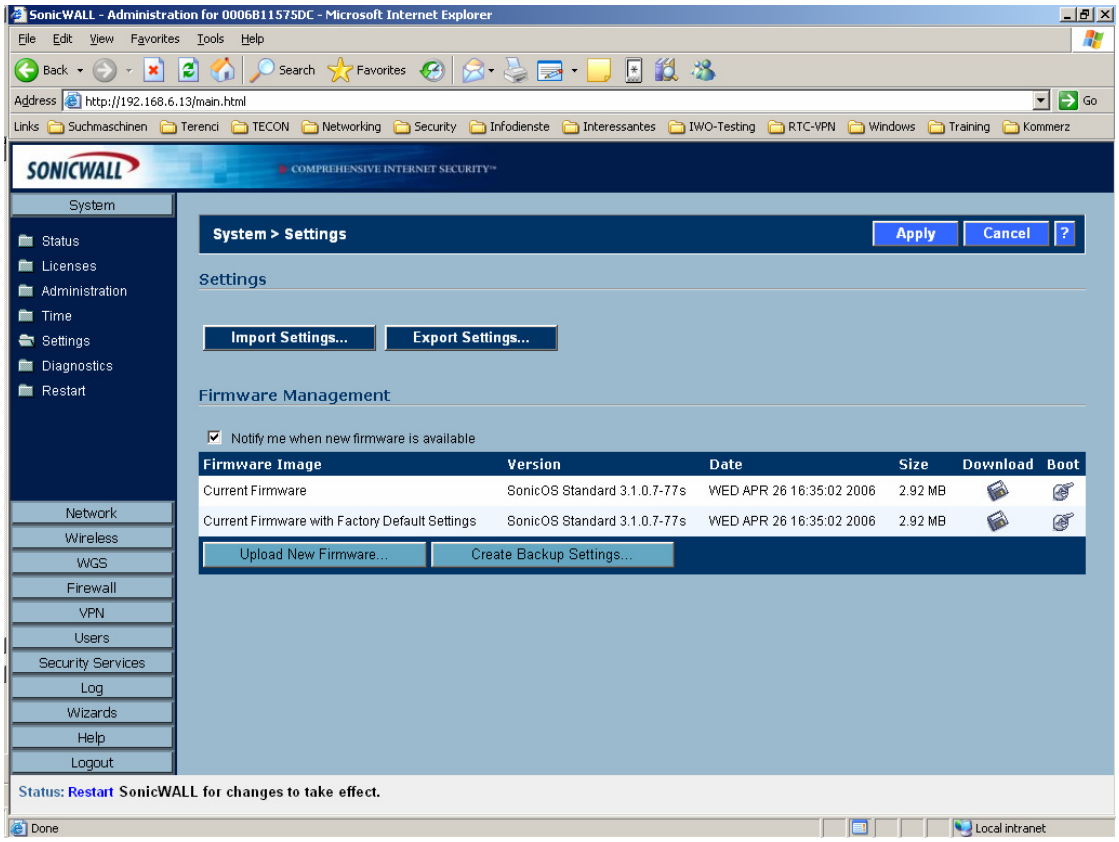


A configuration restore is possible from the same screen by clicking “Import Settings…”.



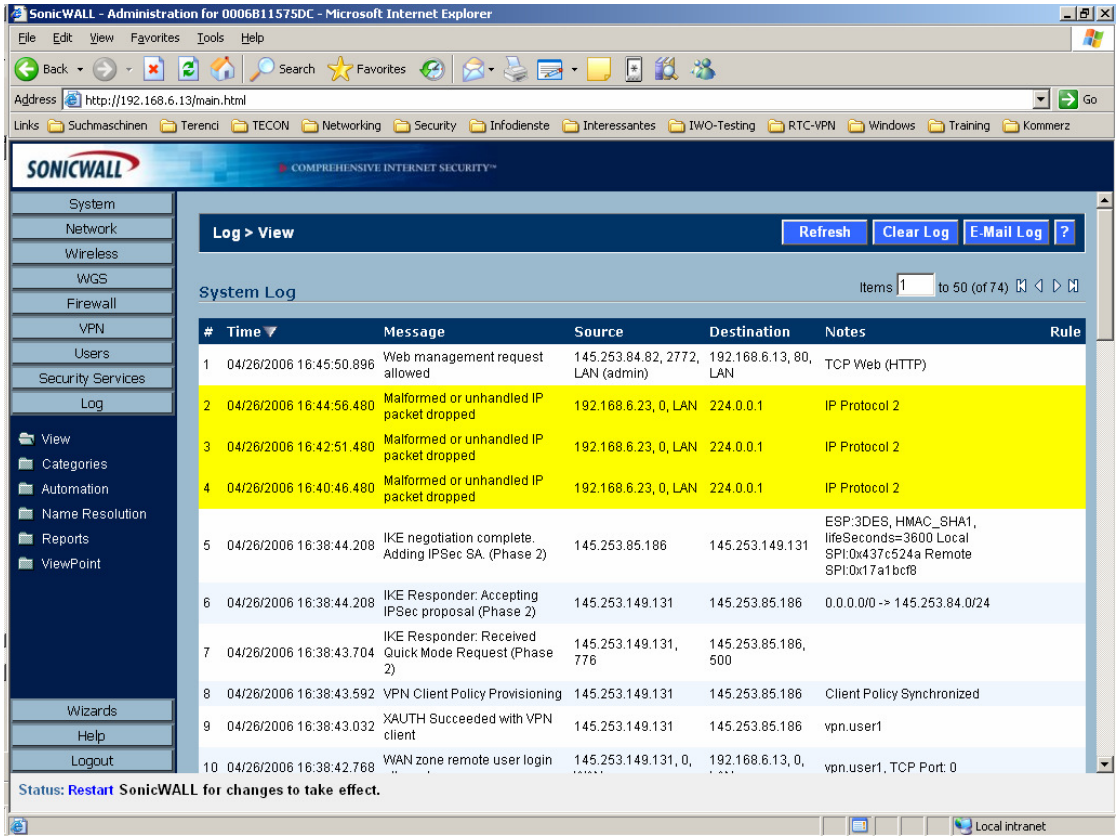
Click “Browse” to locate the configuration file and click “Import” to upload it to the device.

A restart is necessary to activate the new configuration.



3 Logging

Several logging options are available in the logging screens below “Log”.



For VPN purposes, the log configuration should be adapted on the screen “Log > Categories”. Depending on the necessary information, enable “VPN TCP stats”, “Denied LAN IP” and/or Network Debug.

**** End of Document ****