Simply Better IT

Use Technology Better

Configuration of SonicWALL Tele3 SP Hardware Firewall

Introduction

Simply Better It is an IT consultancy operating out of the proprietor's home in New Mills. For its own use and to test out configurations prior to installations, it has its own Local Area Network with a connection to the Internet via a Demon Internet Broadband connection provided by BT Broadband over a standard telephone line provided by BT. The physical network infrastructure is outlined in the '*Network Infrastructure*' document, but briefly consists of an ADSL Broadband connection into the office, an ADSL modem feeding a Hardware Firewall into the office LAN. The Hardware Firewall feeds into a dedicated network card on a Small Business Server running Internet Security and Acceleration Server, and through this to a second network card feeding a Hub on the Local Area Network for office based PCs, printers and laptops.

This document details the process of configuring a '*SonicWALL Tele3 SP*' Hardware Firewall specifically, but should be useful in the configuration of any other Hardware Firewall used in its place.

This document should be used as a working document, updated as changes are made.

Configuring the Hardware Firewall

Hardware Item:	SonicWALL TELE3 SP
Model / Type:	APL10-01F
Serial Number:	00401937D39F
Assembly:	101-500038-00 REV B
ROM version:	6.3.7.0
Firmware Update:	6.6.0.6 (as at 31-05-05)
LAN/WAN Address:	00:40:19:37:D3:9F
Login Details:	Initially admin\password login set to be admin\notInH3re

WAN IP Address:	10.0.0.2
WAN Subnet Mask:	255.255.255.0
WAN Gateway:	10.0.0.1
DNS Server Addresses:	72.46.3.11, 72.46.6.35
LAN IP Address:	172.16.16.1
LAN Subnet Mask:	255.255.255.0

SonicWall Website Admin

Website:	http://www.mysonicwall.com
User Name:	**TryThis**
Password:	**ZBDHPJE**
Login prompt:	'?'
Answer:	?

Backup Dialup account

Phone Number: 0845 1234567
Username: trythis
Password: hf7524

Ensure that the SonicWALL Firewall is connected into the ADSL Modem/Router from the WAN port via a CAT 5 UTP Crossover cable, and into the Server WAN adapter via a CAT 5 UTP Crossover cable (though if connected into a switching hub from the LAN port, this will require a CAT 5 UTP Straight Through cable). The client PC used to configure the Firewall must also be patched into the hub.

Note: The following instructions should be used in conjunction with the SonicWall 'Getting Started' and 'Installation' Guides if you have any problems.

Item	Screen	Action
Start Firewall in Default or Reset Mode	Desktop	Power cycle the Firewall whilst pressing the reset switch for 5 seconds, or until the test light starts flashing, so that all settings are restored to factory defaults. Configure the client PC, connected to the same LAN switching hub, to have an IP address of **192.168.168.200** (restart the computer if prompted). Open an ***Internet Explorer*** browser session, clearing any proxy server settings (**Tools**, **Internet Options**, **Connections**, **LAN Settings**) and browse to **http://192.168.168.168**. Insert the CD labelled '*SonicWALL TELE3 SP Software & Documentation*', click on **Browse…**, select the **sw_t2e_6370** file from the *\Software\Firmware* directory on the CD Drive, and click on **Upload**. DO NOT INTERRUPT THE UPLOAD PROCESS, BUT ***REFRESH BROWSER*** or ***RELOAD*** http://192.168.168.168 IF PAGE NO LONGER SHOWS THE UPLOAD SCREEN.
Start configuration of hardware firewall	Browser session displaying *SonicWALL*	Login with *User Name:* of **admin**, *Password:* of **password**, select the **General** *menu option*,

	login	click on the **Password** *tab*, enter the *Old Password:* as **password**, *New Password:* and *Confirm Password:* as **notInH3re**. Click on the **Update** button, **Tools**, **Restart SonicWALL** and **Yes** to restart the firewall.
Configure IP Addressing information	Browser session displaying *SonicWALL Installation Wizard*	Login as *User Name:* of **admin** and *new Password:* of **notInH3re**, click on the **General** *menu*, then the ***Network*** *tab*. In the *Network Addressing Mode* section, select the drop-down option of **NAT Enabled**, in the *LAN Settings* section, change the *SonicWALL LAN IP Address* to **172.16.16.1**, *LAN Subnet Mask:* as **255.255.0.0**, click on the ***Update*** button, and the ***Restart*** button. Reset the PC's *IP Address:* to **172.16.16.200**, *Subnet Mask:* **255.255.0.0**, browse to http://172.16.16.1, login with new password. Click on the **General** *menu*, then the ***Network*** *tab*. In the ***WAN Settings:*** section enter the *WAN Gateway (Router) Address:* as **10.0.0.1**; the SonicWALL WAN IP (NAT Public) Address: as **10.0.0.2**; In the DNS Settings section, enter the *DNS Server Address 1:* as **72.46.3.11**; the *DNS Server Address 2:* as **72.46.6.35**, click on the **Update**, **Restart**, **OK** buttons and login with new password.
Check configuration and register firewall	Desktop	In the *General* section, on the *Status* tab, enter the registration code of **X438HJ55** (originally **15729037** sourced from http://www.mysonicwall.com site), and click on the **Update** button, then **Tools**, **Restart SonicWALL** and **Yes**.
Update Firmware on firewall	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen, click on the **Upload Firmware Now** button (*Tools, Firmware)*. Ensure that the '*Notify me when new firmware is available*' option is **selected**, and click on **Upload Firmware Now**. A '*Stop'* dialogue box appears asking you if you have saved your preferences. Click on **No**, then **Export** and **Save**. Browse to the **c:\ drive** in the '*Save In*' dialogue box and **OK** to progress. When the *Download complete*, dialogue box appears, click **Close**. Again click on the **Upload Firmware Now** button (*Tools, Firmware*), and this time click on the **Cancel** button. Click on the **SonicWALL Internet Site** link and follow the site instructions for downloading latest version of *Firmware* (at the time of writing, this was version *6.6.0.2*). Save the *Firmware Update file* (at the time of writing this was *sw_t2e_6602.bin*) to the **C:\ drive**. When the *Download* is complete, click on **Close** and close the SonicWall Internet web page. The remaining window should be in the *SonicWALL administration* screen (which may have logged you off if not accessed for more than 5 minutes). Click on the **Upload Firmware**

		Now button (*Tools, Firmware*), **Cancel**, and then the **Upload Firmware** button. ***Browse*** to **C:\sw_t2e_6602.bin** and click on **Upload**. THE UPDATE MAY TAKE A FEW MINUTES, BUT SHOULD RESTART THE FIREWALL ITSELF. Refresh the screen if required, or go to http://172.16.16.1 and refresh.
Set login inactivity timeout options on Firewall	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen (General, Administrator), select the **Enable user lockout on login failure:** option in the *Administrator* tab of the *General* section, and click on the **Update, Tools, Restart SonicWALL** and **YES**.
Configuring of firewall activation logging	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen, select the *Log Settings* tab from the *Log* menu. For *Mail Server:* enter **mail.demon.co.uk**, *Send log to:* enter **newmon@dunit.co.uk**, and *Send alerts to:* enter **newmon@dunit.co.uk**. Change the *Firewall Name:* to **SBIT_Firewall**, ensure ***all Categories*** are selected, click on the **Update** button, **Tools, Restart SonicWALL** and **Yes**.
Configure Web Traffic filtering	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen, select the *Configure* tab from the *Filter* menu, select the **Known Fraudulent Certificates** option, and amend the *Message to display when a site is blocked* entry to '**Web Site Blocked by Firewall – contact newmon@dunit.co.uk about getting access.** Click on **Update**, **Tools**, **Restart SonicWALL** and **Yes**.
Configure Access rights to Firewall	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen, select the *Services* tab from the *Access* menu, ***deselect*** the **File Transfer (FTP)** and **News (NNTP)** options, ***select*** the **Enable SIP Transformations**, **Enable Stealth Mode** and **Randomize IP ID** options, click on **Update**, **Tools**, **Restart SonicWALL** and **Yes**. **Login** to *SonicWALL administration* screen, select the *Management* tab from the *Access* menu, ***deselect*** the **HTTP** option and change the *IP Address* in the **HTTPS** option to be **172.16.16.1**, click on **Update**, **Yes**, **Tools**, **Restart SonicWALL** and **Yes**.
Configure Backup Modem dialup	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen (https://172.16.16.1 from now), from the *Modem* menu, and select the ***Profiles*** tab. Enter the *Name:* as **Demon Internet**, *Primary Phone Number:* as **0845 1234567**, *User:* as **Demon139@Demon**, *Password:* as **d2BAi4RH**, *Confirm:* as **jhadsf56**, select the **Dial on Data** option, click on the **Update** button, **Tools**, **Restart SonicWALL** and **Yes**. **Login** to *SonicWALL administration* screen (https://172.16.16.1 from now), select the *Configure* tab from the *Modem* menu, select **Demon Internet** from the drop down list for *Primary Profile*, **United Kingdom** from the drop down list for *Initialize Modem for use in* option, ***select*** the **Enable WAN Failover** option, click on the **Update** button, **Tools**, **Restart SonicWALL** and **Yes**.

Testing of Firewall Settings	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen, remove the WAN connection and access http://www.bbc.co.uk. This should result in a modem (WAN failure) dial-out.
Save the configuration setting	Authentication screen in Browser session	**Login** to *SonicWALL administration* screen, click on **Tools**, **Preferences**, **Export**, **Export** and **Save** to **c:\sonicwall.exp**. Later, copy this file to the IT_Admin area on the server.