Chapter 3

Deploying SonicWALL Firewalls

Solutions in this chapter:

- **Managing the SonicWALL Firewall**
- **Configuring the SonicWALL Firewall**
- **Configuring Your SonicWALL for the Network**
- **Configuring System Services**

- ☑ **Summary**
- ☑ **Solutions Fast Track**
- ☑ **Frequently Asked Questions**

Introduction

In this chapter we will look at the basics of deploying a SonicWALL firewall. The "basics" include a great deal of information. The SonicWALL firewall has a large number of configuration options. Before you can deploy a device, you must first understand how to manage it, so in the first section of this chapter we will look at the various methods of managing your SonicWALL firewall. Each option and best-known procedure is discussed. Strong system management is important, but no more so than preventing intruder attacks.

There are many management options available on the SonicWALL firewall. Of these options, there are two ways to manage the device directly. The first is using the command line interface (CLI). As mentioned previously, the CLI on SonicWALL appliances is limited in its capabilities. Some people prefer this method of device management for configuring interfaces and viewing interface statistics. Fully comprehending the command line interface allows you to better understand the SonicWALL firewall device.

The second firewall management option is the Web user interface (WebUI). This streamlined interface is user-friendly and intuitive, allowing anyone to jump in and manage your firewall with ease. Even command line junkies will use the WebUI to reference the configuration or to see a configuration more clearly.

Since a firewall is a core network component of the network, we will focus heavily on how to configure your device to interact with the network. This covers zone configuration and IP (Internet Protocol) address assignment. Properly configuring the network is crucial to the functionality of your network entity. Each type of zone and interface is documented to explain the different configuration options to you.

Finally, we will configure various system services. These services empower your firewall and stretch its possibilities.

Managing the SonicWALL Firewall

One of the most important aspects of securing your infrastructure with SonicWALL firewalls is knowing how to effectively manage them. In this section we will look at all of the various management options. Each option brings certain strengths and weaknesses to the table, so you should never rely on just one method. Instead, take advantage of the range of security options SonicWALL offers, and use multiple configurations.

All management access requires authentication, and it's critical that only authorized administrators are permitted to change your firewall's configuration. The last thing that you want to happen is to lose control of your firewall.

There may be times when you mistakenly erase parts of your configuration or lose your configuration altogether. We will review how to recover from these mistakes. Losing access to your device can be devastating. With so many different passwords to remember, you can easily forget how to gain access to your SonicWALL firewall. Even the most experienced administrators can find themselves in this situation.

Finally, we will look at how to update the operating system on your SonicWALL device. Staying current with software revisions is very important. It provides you with security-related fixes as well as new software enhancements. Each new release may also contain bug fixes or code changes that allow better interoperability with other devices. Some options may be more effective then others, depending on your needs. At the completion of this section you should be familiar with both the WebUI and CLI. Knowing this is a requirement for managing your SonicWALL firewall efficiently and correctly.

SonicWALL Management Options

Every SonicWALL management option centers around two forms of management: the WebUI and the CLI. SonicWALL also supports management via one other method. The SonicWALL Global Management System (GMS), an enterprise-class management interface, is designed to manage multiple SonicWALL appliances easily and efficiently through a single interface. The SonicWALL GMS will be discussed in more detail in Chapter 13 of this book.

Serial Console

SonicWALL security appliances offer a serial console for basic firewall setup and configuration. The *serial console* is a nine-pin female serial connection. This option gives you CLI access to the firewall. The serial console is used to initially connect to your device and to conduct *out-of-band management*. Out-of-band management is management that is not network-based, such as access via a modem or over Ethernet. When configuring over a serial port, you are not using any sort of network connectivity. In the case when you need to change IP addressing on the firewall and guarantee connectivity, using the serial console is an excellent option. With, and only with serial console can you view and interact with the booting process. This cannot be accomplished remotely because the OS has not started and it is unable to provide management services. Many devices from UNIX-type servers, as well as other embedded devices, use serial consoles to provide serial console management.

There are certain benefits to using a serial console that you do not get from using any other type of connection. The console provides secure, physical, and dedicated access to the SonicWALL appliance. Issues with network connectivity do not impact management using the serial console. Also, since your connection to the appliance is direct using a serial cable, your management is completely secured.

The command-line console provides an administrator the ability to manage interface setup and configuration, as well as to view statistical information regarding the appliance and its interfaces. The command line interface on a SonicWALL is only available when you are directly connected to the appliance using a serial cable. The CLI of the SonicWALL is not full-featured. Some management options cannot be set up using the CLI. For example, you cannot set up access rules using the CLI.

When connecting to a SonicWALL firewall for serial console management, use a null modem cable. When you purchase a SonicWALL, a null modem cable should be included in the packaging. Table 3.1 outlines the proper connection settings when connecting with a serial terminal and serial terminal emulation software.

Table 3.1 The Serial Terminal Settings

Setting	Value
Speed	115,200 (9,600 on TZ 170)
Character Size	8 Bit
Parity	None
Stop Bit	1
Flow Control	None

WebUI

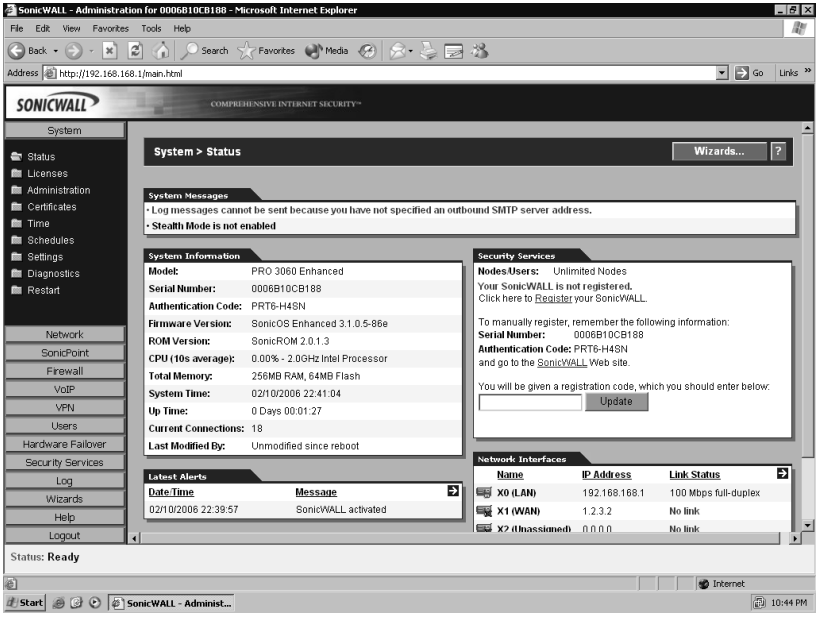
The integrated WebUI offers an easy-to-use interface to manage SonicWALL appliances and access SonicOS. Because of its simple point-and-click nature, it gives the end user a great jumpstart into the management of the SonicWALL firewall. Figure 3.1 depicts the Web interface of a SonicWALL appliance. The left side of the screen provides you with clickable menus and submenus to access each area of configuration options. By default, the WebUI is configured to work over the Hypertext Transfer Protocol (HTTP). It can, however, be configured to work over Hypertext Transfer Protocol Secure (HTTPS). This provides a mechanism to secure your Web management traffic. The Web interface is the preferred method for configuring the SonicWALL appliance. Throughout this book concepts and examples will utilize the Web interface for configuration.

Damage & Defense…

Web Interface Management

Although the SonicWALL appliance line supports management via the HTTP protocol, you should try to avoid using it as much as possible. Rather, use the HTTPS protocol, which utilizes a Secure Sockets Layer (SSL) connection for management. When you communicate with a SonicWALL over SSL, the traffic is encrypted, thus preventing attackers from sniffing traffic. You can tell that you are using SSL to manage a SonicWALL by looking at the address line in Internet Explorer—the URL will start with "https:"

Figure 3.1 The SonicWALL Web Interface



The SonicWALL GMS

The SonicWALL Global Management System is a separate tool that can be used to manage a SonicWALL firewall appliance. The SonicWALL GMS is an application that runs on either a Solaris server or a Windows XP Pro, 2000 (Pro or Server), or 2003

Server. It also requires the use of a database server—Oracle or MS SQL Server. The SonicWALL GMS requires a separate license, based on how many devices you want to manage. This product is used most effectively if you have several devices you need to manage at the same time. The GMS product is fully discussed in Chapter 13.

Administrative Users

Before you can perform any management functions, you must first authenticate to the SonicWALL appliance as an administrator. This holds true for management via the Web interface, serial console, or GMS. The SonicWALL default administrator account is the "admin" account. The admin account default password on all SonicWALL appliances is "password." You are allowed to change the name of the admin account to something more secure, up to 32 characters long. Note that the SonicWALL appliance does not see usernames as case-sensitive. The username "MillerT" and "millert" are the same name to the SonicWALL appliance. Only passwords are case-sensitive.

SonicWALL also allows you to create users that are known as *Limited Administrators*. Limited Administrators are allowed access to the following SonicWALL configuration pages:

- **General** Status, Network, and Time
- **Log** View Log, Log Settings, Log Reports
- **Tools** Diagnostics, except no permissions to Tech Support Report, Restart

Limited Administrators are only allowed management access to the SonicWALL from the LAN (local area network) zone, or via a VPN (virtual private network). Management from the WAN (wide area network) or any other zone is not permitted.

The Local File System and the Configuration File

Each SonicWALL firewall appliance has a similar design for its internal system components. Long-term storage on the device is stored in *flash memory*. Flash memory is a nonvolatile type of memory that retains information after the system is turned off. All of the component information that the SonicWALL appliance needs to store is stored in flash memory, including SonicOS log files, license keys, IPS (intrusion prevention system) databases, and virus definitions.

Each SonicWALL appliance also contains Random Access Memory (RAM). RAM is a volatile type of memory that is lost whenever the system is powered off or reset. When the SonicWALL device powers on, and after the power on self test (POST) is completed, the SonicOS image is loaded into RAM. After SonicOS is up and functional, it loads the saved configuration file from flash memory. The configuration that is stored in RAM is called the *running configuration*.

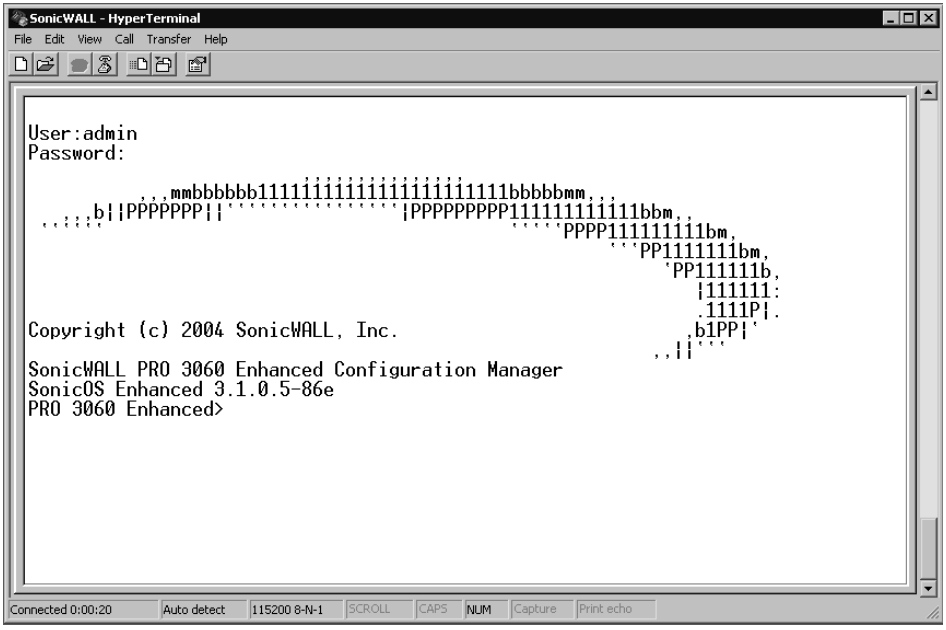
Using the Command-Line Interface

As mentioned earlier, the serial console can provide a stable and secure method to configure SonicWALL appliances. Although most administrators who only administer one or two SonicWALL firewalls never use the serial console for management, it is important to mention its features and capabilities.

To start using the SonicWALL serial console, connect a null modem cable to the port labeled "Console" on your SonicWALL appliance and attach the other end to a serial port on your computer. Start your preferred terminal emulation software, such as hyperterminal, and set the parameters for communications with the SonicWALL. For all SonicWALL appliances that support using the console other than the TZ 170, the settings are as follows: 115,200 baud, 8 data bits, no parity, 1 stop bit, and no flow control. For an appliance in the TZ 170 family use 9,600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Once the connection has been established with the SonicWALL appliance, press the **Return** key. You should see a prompt appear within your console session showing the device name, followed by a prompt for your username. Enter the administrator username and press **Enter**. You will then see a prompt for the password. Type in your **current administrator password**, press **Enter**, and if the login credentials were entered correctly, you will be granted access to the management console. If you've entered invalid credentials, you will receive an error message and will be allowed to retry logging in. Note that SonicWALL appliances do not use any kind of account lockout mechanism for login attempts from the CLI. When an attempted login on the CLI is unsuccessful, a warning entry is generated in the SonicWALL log acknowledging the attempt. Figure 3.2 shows a successful login to the SonicWALL serial console.

Figure 3.2 SonicWALL Console Login



Once you've successfully logged into the serial console, you can begin using configuration commands to modify your SonicWALL appliance's current settings.

The SonicWALL command-line interface is very user-friendly and easy to operate. It includes several control keys that can be used to make tasks within the CLI easier. Table 3.2 lists the control-key combinations for the SonicWALL CLI and their purpose.

Table 3.2 SonicWALL CLI Control Keys

Keys	Function
Tab	Completes the word currently being typed
?	Displays a listing of possible command completions
Left Arrow	Moves cursor to the previous character
Right Arrow	Moves cursor to the next character
Up Arrow	Displays previous command from command history
Down Arrow	Displays next command from command history
Ctrl+A	Places cursor at beginning of the command line
Ctrl+B	Move cursor to previous character

Continued

Table 3.2 continued SonicWALL CLI Control Keys

Keys	Function
Ctrl+C	Exits Quick Start Wizard
Ctrl+E	Moves cursor to end of the command line
Ctrl+F	Moves cursor to the next character
Ctrl+K	Erases all characters from the current cursor position to the end of the line
Ctrl+N	Displays the next command from command history
Ctrl+P	Displays the previous command from command history
Ctrl+W	Erases the previous word

The SonicWALL CLI supports several features common to other command-line interfaces. You can use the Tab key to complete the command currently being typed, as well as using the ? key to list all possible command completions. Commands can also be abbreviated, so long as the abbreviation is unique to the command word. Figures 3.3 and 3.4 show examples of using command features.

Figure 3.3 Using Tab to Complete Commands

```
PRO 3060 Enhanced> show int [TAB]
show interface
```

As you can see in Figure 3.3, when typing the command *show interface*, the user pressed the **Tab** key. When the Tab key was pressed, the SonicWALL CLI knew that there was one command word starting with "int"—the word "interface," and as a result, completed the command for the user. As mentioned before, the user could have simply completed the rest of the command as *show int x0* and the SonicWALL CLI would have also interpreted this properly, since the only possible command starting with "int" is *interface*.

Figure 3.4 Using "?" to Get Possible Command Completers

```
PRO 3060 Enhanced> show ?
alerts              log                 network             tech-support
arp                 log-categories      processes           timeout
buf-memzone         log-filters         route               tsr
cpu                 memory              security-services   web-management
device              memzone             sonicpoint          zone
gms                 messages            status              zones
if                  nat                 syslog
interface           netstat             system
```

In Figure 3.4 we knew that we wanted to use the *show* command to display information, but we were uncertain of the next command word to use. By typing **show ?** the SonicWALL CLI returns a list of all the possible sub-commands that can be used for *show*.

The SonicWALL command-line interface uses the command and sub-command model for configuration. This means that under a given command context, there can be other commands that are only available under that context. For example, suppose you want to configure the LAN interface manually to 10 megabits, you could use the following commands:

```
PRO 3060 Enhanced> configure
(config[PRO 3060 Enhanced])> int x0
(config[PRO 3060 Enhanced]-if[X0])> speed 10
(config[PRO 3060 Enhanced]-if[X0])> end
(config[PRO 3060 Enhanced])> end
PRO 3060 Enhanced>
```

A quick *show int x0* shows us the interface information for x0, the LAN interface. Note the linkAbility field and its value of 10Mbps full duplex.

```
PRO 3060 Enhanced> show int x0

General data:

  type                    ifLan
  zone                    LAN

  linkAbility             10Mbps full duplex
  fragmentPackets         off
```

```
  ignoreDontFragBit       off
  mtu                     1500
  proxyPcMacOnWan         off
  bwmEnabled              off
  bwmBandwidth            384

  name                    X0
  comment                 Default LAN

LAN data:

  ip                      192.168.168.1
  mask                    255.255.255.0
  transparent             0
```

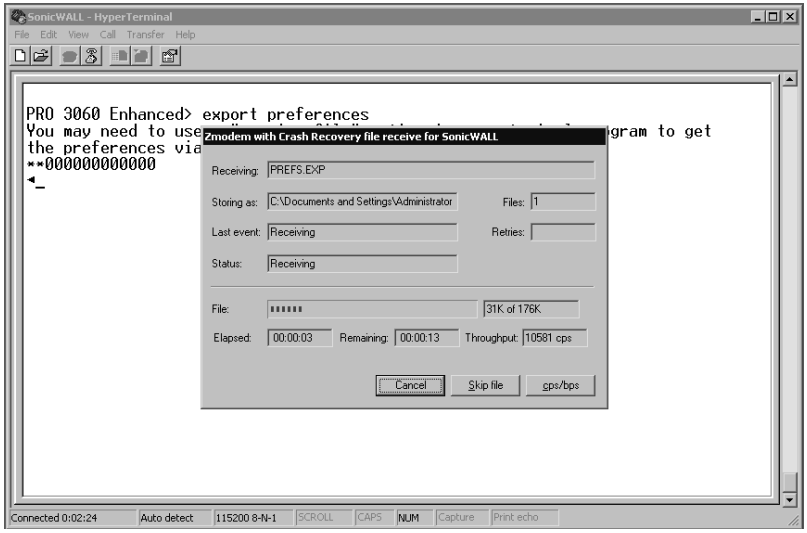
An excellent way to make use of the CLI is to back up the preferences file from your SonicWALL appliance. This can also be achieved from within the Web interface, but it can be quicker to do so via the CLI. SonicWALL appliances support the use of the ZModem protocol, and by default hyperterminal also supports receiving files using ZModem. To back up your preferences from the CLI, perform the following steps:

1. Connect to your SonicWALL appliance using a null modem cable and hyperterminal.
2. Authenticate to the SonicWALL with your administrator credentials.
3. Enter the command to export the preferences file via ZModem.

   ```
   PRO 3060 Enhanced> export preferences
   ```

4. The preferences file transfer using ZModem should begin. In just a short time, your preferences file will be backed up to the default location as set in hyperterminal. By default, the preferences file exported is named prefs.exp. Figure 3.5 shows an example of what the ZModem transfer looks like.

Figure 3.5 CLI Backup of the Preferences File



If an unforeseen event occurs and you lose the ability to manage your appliance through the Web interface, you can use the CLI and the command *restore* to restore your SonicWALL to its factory-default state. Afterward, however, you would need to reconfigure your appliance.

Managing the SonicWALL via the CLI can prove to be an efficient way to manage interface configuration. It can also be an excellent tool to look at statistics, alerts, and logs, as well as to back up your configuration.

Using the Web User Interface

The Web user interface is a simple tool to use for managing your SonicWALL firewall. It is very intuitive and allows even those with little firewall experience to easily control a SonicWALL appliance. As we continue through the book we will use the WebUI for our examples. You may see some examples for the CLI, but since the CLI does not provide you with full firewall management capabilities, the examples will be fewer. In Figure 3.1 , we looked at the main WebUI page following authentication. On the left side is the menu bar, where you can select the different configuration options. On the right-hand side of the screen is the current status of the device. The status display is divided into five different regions: System Messages, System Information, Security Services, Latest Alerts, and Network Interfaces.

Each of these boxes shows you the current events. The System Information box shows you several different bits of information, including the model number, serial number, firmware version, ROM version, CPU load, memory status, system time,

uptime, number of connections, authentication code, and when the SonicWALL configuration was last modified. The Security Services box shows your device registration status, number of nodes the device allows, and installed license information. The System Messages box shows general configuration information and warning messages. The Latest Alerts box shows you some of the latest alert messages that have been logged. This may include messages relating to packets dropped or blocked by firewall rules or the IPS service as well as login attempts. If you look at the box labeled Network Interfaces you will see all of the interfaces and their link statuses. This is handy for determining which interfaces are up or down. Some boxes in the upper right-hand corner have a small blue arrow icon. This icon contains a hyperlink, and by clicking on you are taken directly to the detail page for each one of those items.

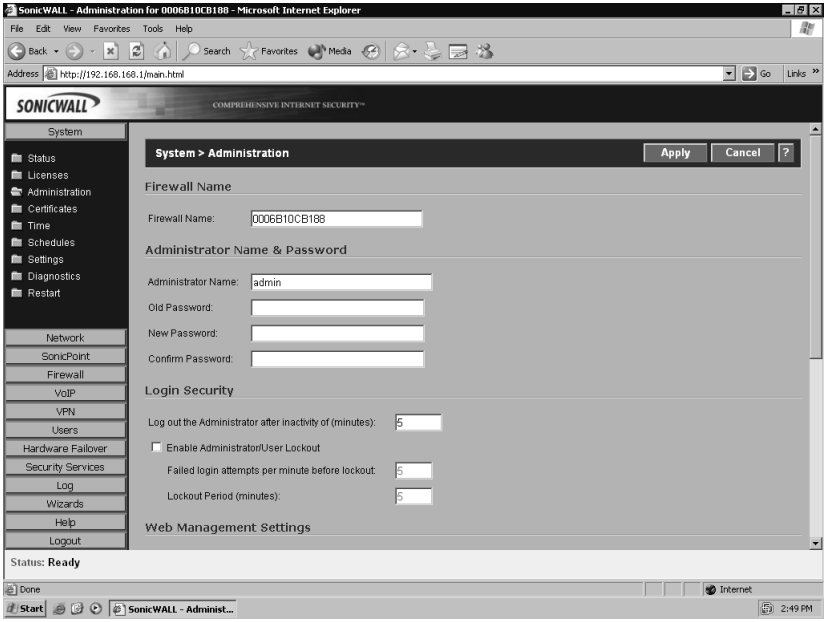
Securing the Management Interface

Now that you are beginning to understand the management of SonicWALL firewall appliances, it is time to secure the management access to your device. The last thing you want to do is leave the doors wide open for another individual to take over your device. There are some easy things that you can do to prevent this. First, as we mentioned earlier, you should change the root username and password. Everyone who owns a SonicWALL firewall is well aware of the default login and password to the device.

Use the following steps to change the root username and password via the WebUI:

1. Select **System** | **Administration**. A screen similar to Figure 3.6 will be displayed.
2. Type in the desired name for renaming the administration account. For our example we will use **Syngress**.
3. Enter the old password, and then enter the desired new password into the two corresponding blanks.
4. As an additional security option, you can also enable the administrator lockout feature on this same screen. To enable administrator lockout after failed login attempts, enable the **Enable Administrator/User Lockout** option. The default settings are to lock out a user or administrator if five invalid login attempts occur within one minute. The default time period for the lockout to last is five minutes.

Figure 3.6 WebUI Administration Screen



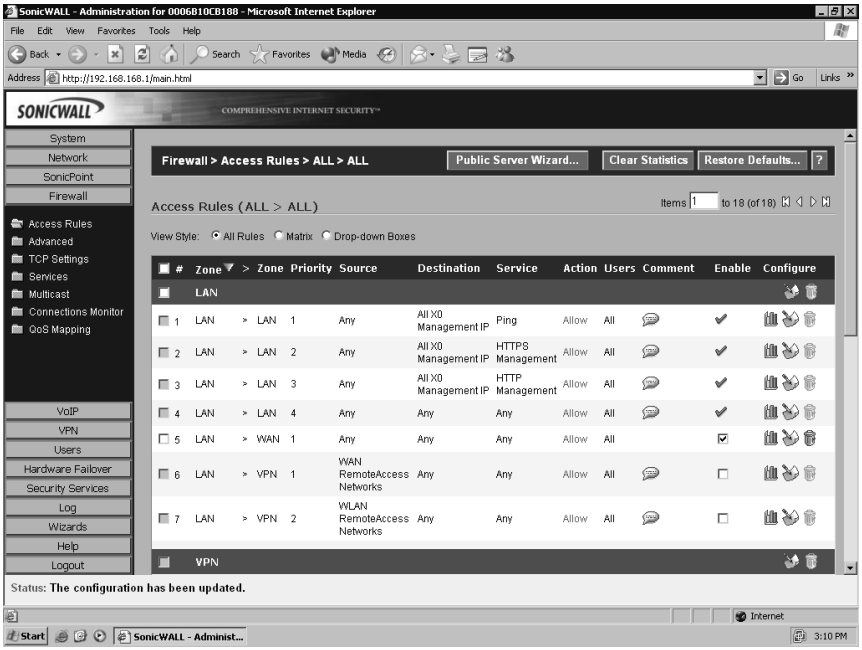
5. Click the **Apply** button on the top right side of the page. After the changes are completed, you will see the new administrator name in the Administrator Name field. Be sure you remember the updated administration information, as you will need this information in order to manage your SonicWALL.

Another option that you should configure is the idle timeout. By configure, I don't mean disable the feature. I have been to many locations where administrators would disable the idle timeout and you could simply connect to the console and have a privileged account ready and waiting for you. Anyone with a little know-how can cause trouble on your network this way. Be certain to set the idle timeout to something reasonable (the default is five minutes). If you find you are being logged out too often, then you can increase this number. However, to balance the scale between security and convenience, I would recommend at most 15 minutes.

The next step is to limit the systems that can access your firewall for management purposes. By restricting management to a specific short IP range or a single IP address, you can limit the chances and intruder may be able to gain access to your firewall. Once you enable this setting, it immediately takes effect, so if you are setting this up remotely, ensure that you add your own IP address and/or source network. Use the following steps to limit access to the management interface on your SonicWALL:

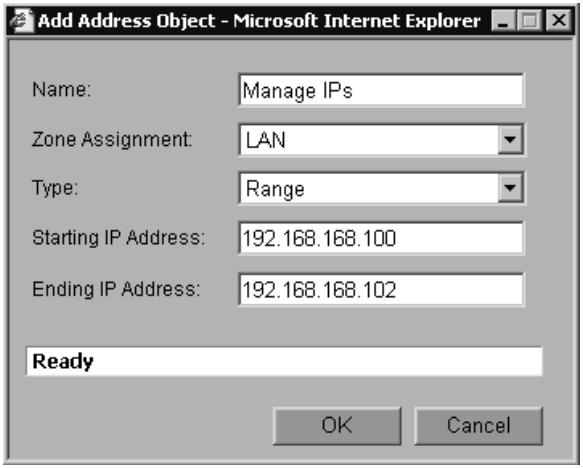
1. Select **Firewall** | **Access Rules**. A screen similar to Figure 3.7 will be displayed.

Figure 3.7 Access Rules Screen



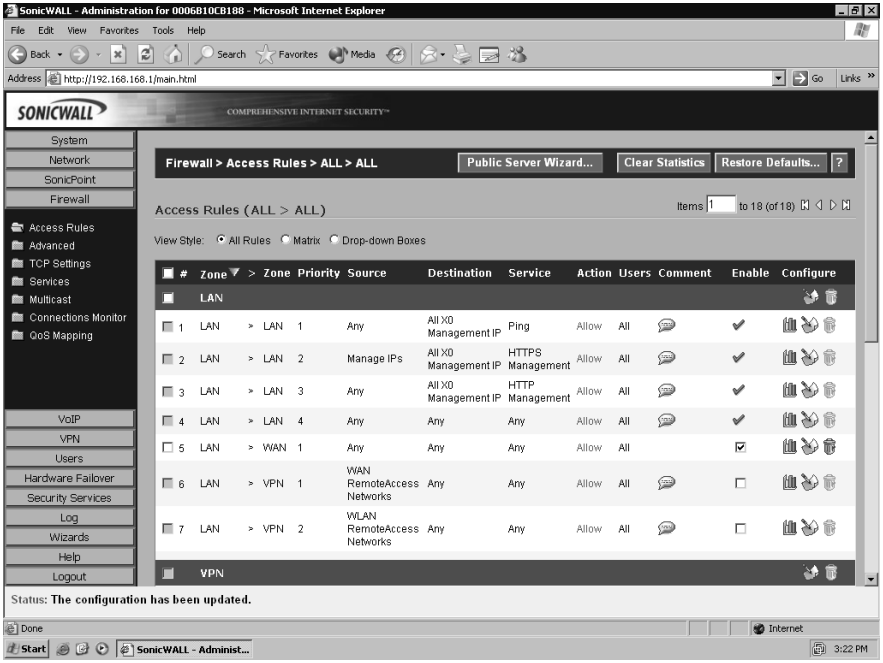
2. Locate the access rule with the service HTTPS Management. Click the **Configure** icon to the right of the rule. A window will open allowing you to modify the rule. Note that on the rules allowing management only the Source field can be modified.
3. Click the **arrow top**, open the drop-down menu, and then choose the option **Create New Network…** Another window will open allowing you to create an address object to apply to the rule. Enter the name for the **Address** object, and select the **Zone Assignment**, **Type**, and **IP address**. In our example, we call the object Manage IPs, and the zone is LAN. We are allowing a range of addresses for management. Figure 3.8 shows the object configuration.

Figure 3.8 Address Object configuration



4. Click **OK** to save the address object, and then on **OK** to save the changes to the access rule. Your completed rule will then look similar to Figure 3.9. Note that if you hover your mouse over the Source for the rule Manage IPs, a box will be displayed showing what the Manage IPs address object is.

Figure 3.9 Modified Management Rule



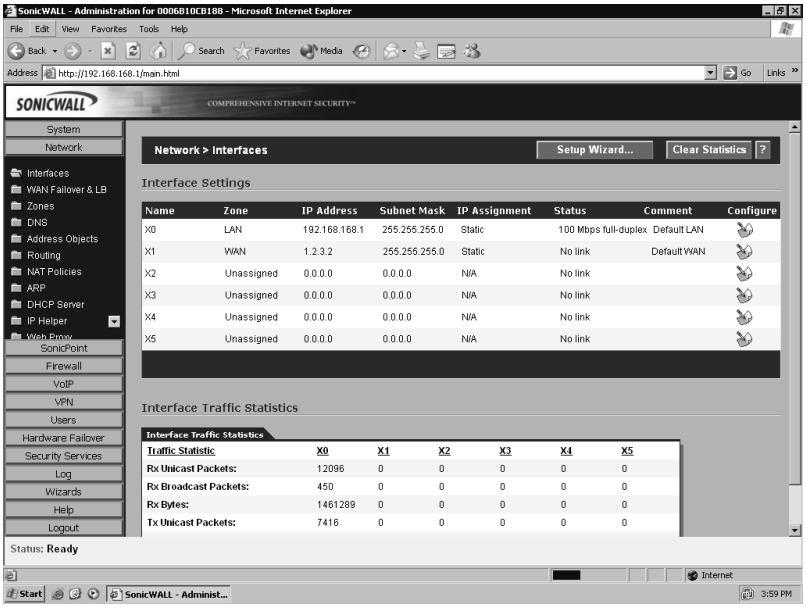
Now that we have the access restricted to specific hosts, there are yet several more options we can choose to enhance the security. The first task is to ensure that unnecessary management services are disabled. Management services are bound to individual interfaces. It is important to restrict them to the bare minimum. By default, SonicWALL does not allow management services from the WAN interface, or interfaces other than the LAN.

If you are taking over management of a SonicWALL previously managed by another person, it is highly recommend that you take a look at each interface to see which management options are enabled and disabled. If something is enabled that you will not be using, disable it. In this case, we are using a SonicWALL PRO 3060 with SonicOS Enhanced, and we will be modifying the WAN interface. We are going to disable the WebUI and WebUI using SSL as management options.

Use the following steps to disable unnecessary management services via the WebUI:

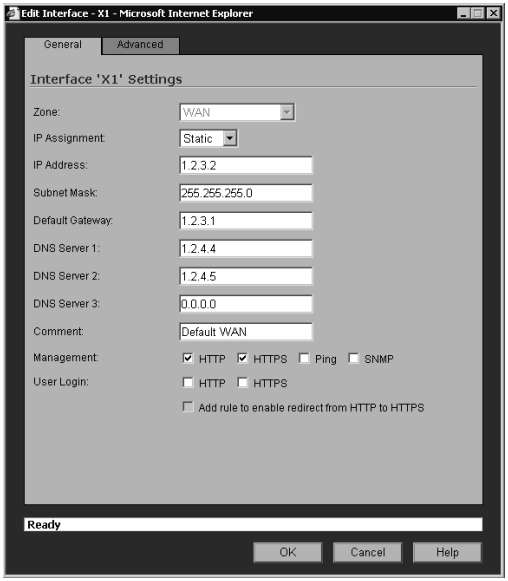
1. Select **Network** | **Interfaces**. A screen similar to Figure 3.10 will be displayed.

Figure 3.10 Network Interfaces Screen



2. Locate the WAN interface and click the **Configure** option to the far right. The configuration for the WAN interface will open in a window similar to the one shown in Figure 3.11.

Figure 3.11 WAN Interface Management Window



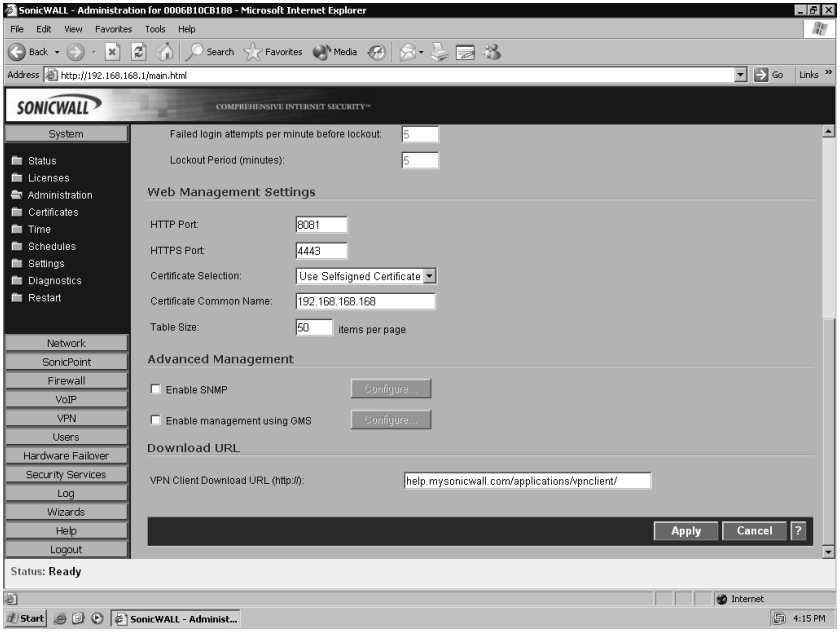
3. Disable the **HTTP** and **HTTPS** option and click **OK**. Now management via the WAN interface has been disabled.

You can follow the same steps for each interface on your SonicWALL to enable or disable management services.

Next, you can change the local port that your management services listen on. This can help prevent your services from being detected if someone was to do a scan looking for open services. Both HTTP and HTTPS management can be configured to listen on a different port. Use the following steps to change the ports via the WebUI:

1. Select **System** | **Administration**.
2. Scroll down and look under the heading **Web Management Settings**.
3. Modify the **HTTP Port:** and **HTTPS Port:** values to listen on the ports of your choice.
4. Click **Apply** to save your changes. Figure 3.12 shows the SonicWALL modified for HTTP Management on port 8081 and HTTPS management on port 4443.

Figure 3.12 Configuring the Management Ports



By default, SonicWALL appliances are configured to use a self-signed certificate for HTTPS management. SonicWALL firewalls also support the ability to import certificates.

The primary idea behind security is mitigating risks. By adding additional layers of protection such as those we've just discussed, you can reduce the chances you'll become a target for someone and also minimize the chances that security-related problems will arise. You may find that not all procedures fit within the guidelines for your organization's security. These guidelines are simply best practices, and although it is recommended that you use them, you can mix and match the configurations that work best in your environment to achieve the security level you desire.

Updating and Managing SonicOS

SonicWALL is committed to providing a secure and robust operating system for the SonicWALL firewall product line. From time to time SonicWALL publishes new versions of SonicOS. These may include security updates, feature enhancements, or both. It is very important that you keep the software on your firewall up to date. As a core component of your network security, your firewall has to be secure to perform its job properly. In fact, immediately after logging into a new SonicWALL, one

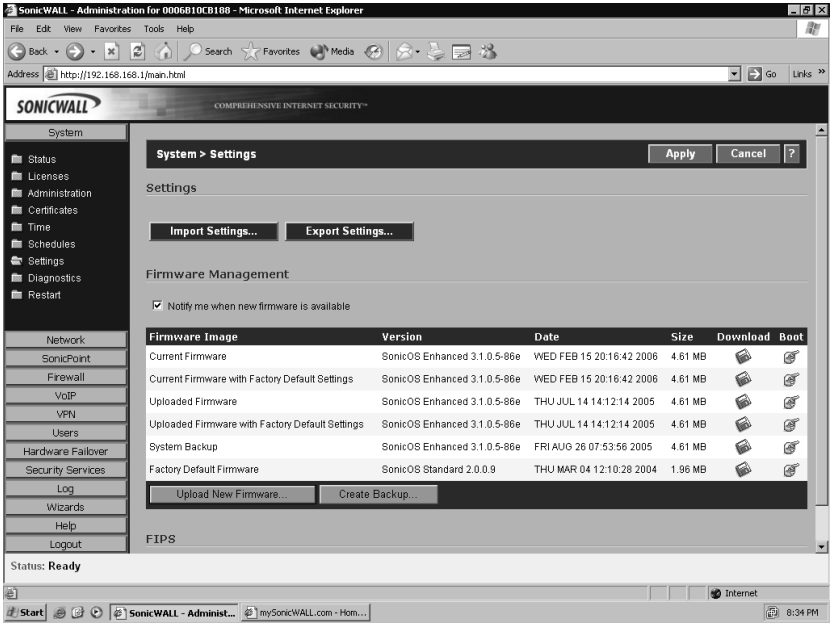
of the first things I do prior to configuration is to verify it is running the most current version of SonicOS, and if not, I update it. This helps to ensure a smooth deployment and reduces the risk that something could go wrong after spending time customizing the configuration.

To check to see if your appliance has a firmware update available, login to your account on www.mysonicwall.com. Note that SonicWALL only provides you with 90 days of complimentary firmware updates. After the initial 90-day period, you will need to obtain a support contract in order to download new firmware releases.

Your SonicWALL appliance can also check for firmware updates and notify you if an update is available. To enable automatic checking for firmware updates:

1. Select **System** | **Settings**.
2. Enable the **Notify me when new firmware is available** option. Figure 3.13 shows an example of this setting.

Figure 3.13 Automatic SonicOS Update Notification



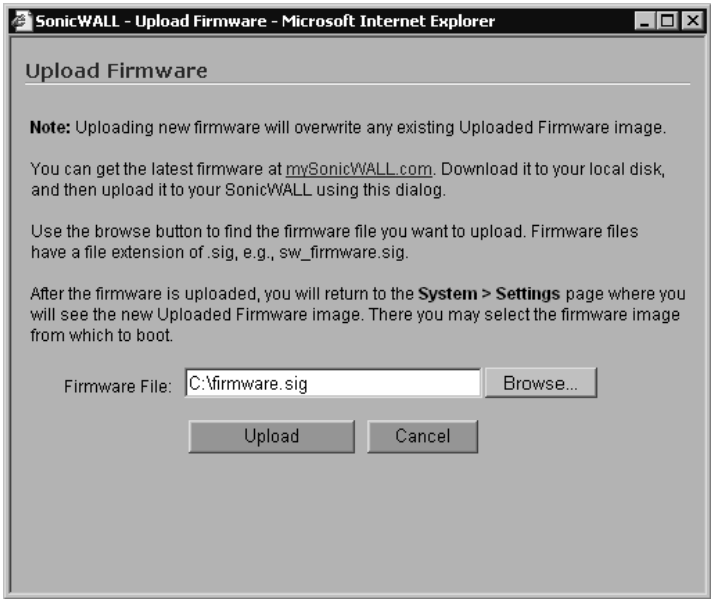
3. Click **Apply**.

When a firmware update is available, it can be applied through the Web interface. It is important, however, that you read any accompanying technotes for the release of firmware you intend to use. Often these notes will acknowledge changes made to the new firmware, including default behavior changes and any possible

caveats in the new version. It is also important before updating your firmware that you back up your preferences file. Use the following procedure to back up and update your SonicWALL appliance's version of SonicOS:

1. Log in to your SonicWALL appliance. Click **System** | **Settings**.
2. Create a backup of your current firmware by clicking **Create Backup…** at the bottom of the screen. You will receive a warning message to verify that you want to overwrite your current backup if one exists.
3. Click **OK** to proceed with the backup. After a couple of seconds, notice the changes to the System Backup in the firmware listings. The version number should match the current running version. Also note the date the backup was created and ensure that it is correct.
4. Click **Upload New Firmware** A window like the one shown in Figure 3.14 will open.

Figure 3.14 Upload New Firmware Window



5. Browse to the path of the new firmware and select the file. Click **Upload** to start the upload process. The upload processes time to run depends on your network bandwidth. Once the upload is complete view the System | Settings window again. Note that the line labeled New Firmware should now show the version of SonicOS you just uploaded as well as today's date and time.

6. To reboot the SonicWALL with the newly uploaded version of SonicOS, Click the **Boot** icon to the right of the new firmware. You may be prompted to make a backup of your settings and old firmware prior to rebooting. Click **OK** to confirm and initiate the reboot sequence with the new firmware.

After the restart has completed and the SonicWALL appliance is running the new version of SonicOS, the browser window will refresh and take you back to the login page. You can now log back in to the SonicWALL Web interface and continue management of your appliance.

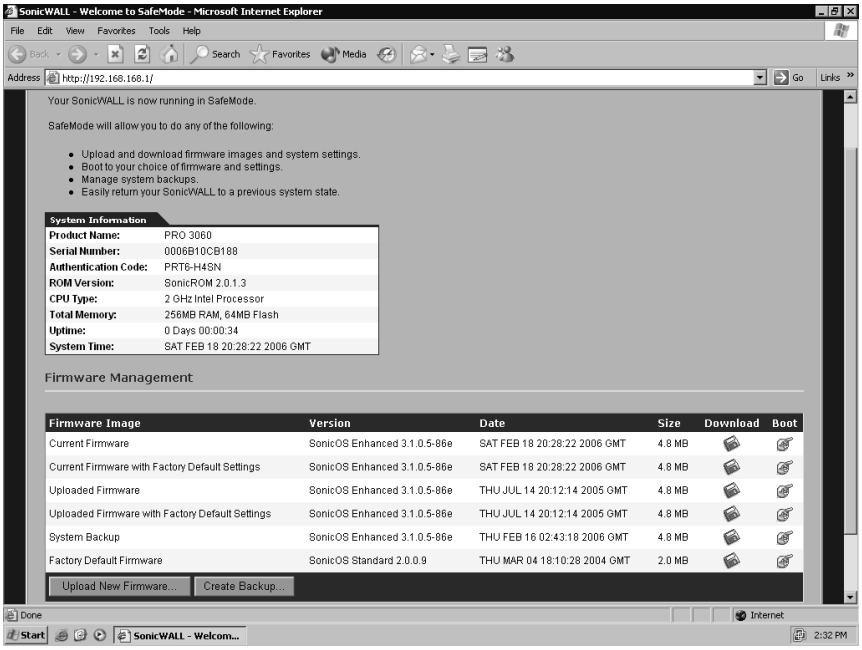
System Recovery

There comes a time in every administrator's life that it happens. You are modifying a system configuration, and somehow, during the modification you make a bad keystroke, mouse click, or worse, something locks up. It could even be as simple as a power outage, leaving you locked out of your device, or leaving the device unmanageable. It's time to perform a system recovery.

If you're having problems with accessing the Web interface, SonicWALL has provided a feature called *safe mode*. Safe mode can also be used in event the firmware on your appliance has become corrupted. Safe mode allows you to use one of several boot options including booting the current firmware with your preferences, booting the current firmware with factory default preferences, or uploading new firmware to the SonicWALL appliance. SonicWALL safe mode is available on all SonicWALL models except the SonicWALL TZW.

Accessing safe mode requires physical access to the appliance. To access safe mode, locate the hardware reset button on your SonicWALL appliance. The button is usually located in a recessed hole near the console port on the SonicWALL. Using a paperclip or similar tool, press and hold the reset button for five to seven seconds and let go. Allow the SonicWALL appliance time to reboot, and then open a Web browser. Enter the SonicWALL appliance's currently configured IP address, or enter the factory default IP address 192.168.168.168. Your browser should load the safe mode interface. Figure 3.15 shows a SonicWALL appliance booted in safe mode.

Figure 3.15 SonicWALL Safe Mode



Occasionally, you may find that even after pressing the reset button you still cannot get the Web interface to load. If this occurs, you can use the SonicWALL CLI to restore your appliance to the factory default settings. Figure 3.16 shows using the CLI to restore a SonicWALL to the factory default settings.

Figure 3.16 Restoring Factory Settings via the CLI

```
User:Syngress
Password:
SonicWALL PRO 3060 Enhanced Configuration Manager
SonicOS Enhanced 3.1.0.5-86e
PRO 3060 Enhanced> restore
Are you sure you want to restore the device to factory defaults? (Y/N):y
restoring to factory defaults.
Are you sure you want to restart? (Y/N):y
Restarting the firewall
```

Zones, Interfaces, and VLANs

Before we get into the configuration of interfaces, access rules, and objects, we will first take a look at the zones and interfaces. By establishing what each zone and interface entails, it makes for understanding the configuration later. We will also review SonicWALL's support for VLANs. VLAN support is only available on the SonicWALL PRO 4060 and PRO 5060 model appliances.

Zones

As we've previously mentioned, zones logically group one or more interfaces together to make configuration and management simpler and more efficient. Out of the box, SonicWALL appliances come with several pre-defined zones. Each zone also has a security type defined. The security type specifies the level of trust given to that zone. The SonicWALL predefined zones cannot be modified from their factory configuration. The default zones are WAN, LAN, DMZ, VPN, WLAN (wireless LAN), and Multicast. Each zone is defined below:

WAN The WAN zone can consist of up to two physical interfaces. This allows for the support of load balancing and WAN failover. By default, the WAN zone contains one interface. If you intend to use either of these services, you'll need to add a second interface to the zone. The WAN zone has the security type "untrusted," which means that without rules, no traffic from this zone is allowed to reach any other zone.

LAN The LAN zone may consist of as many as five physical interfaces. Each interface is configured for a network subnet, with all interfaces being manageable as the LAN zone. The LAN zone has the security type "trusted," which allows any traffic from this zone to reach any other zone with restriction.

DMZ The DMZ is designed to contain any servers and devices that will be publicly accessible or have an Internet-facing port, such as an MTA (message transfer agent) or Web server. The DMZ can consist of up to four physical interfaces. The DMZ falls into the security zone "public." The security type public really just says the zone has less trust than the LAN, but more than the WAN. By default, traffic from the DMZ can exit to the WAN, but cannot exit to the LAN.

VPN The VPN zone contains no physical interfaces. It is a virtual zone, used to provide secure remote network access. The VPN zone has a security type of "encrypted." All traffic flowing to and from the VPN zone is encrypted.

WLAN The WLAN zone is used to provide support for using *SonicPoints* on your network. SonicPoints are SonicWALL's wireless network product used for providing wireless network connectivity. On a TZ 170 Wireless or TZ 170 Wireless SP, the integrated SonicPoint falls into the WLAN zone. The WLAN zone falls into the security type "wireless," which is just a security zone where the wireless traffic is considered to reside.

Multicast The multicast zone provides support for IP multicasting. IP multicasting is a method for sending packets arriving from a single source to multiple destinations.

Even though you can assign multiple physical interfaces to a single zone to make management simpler, it is still important to remember that you can manage and apply access rules to each interface independently of its zone.

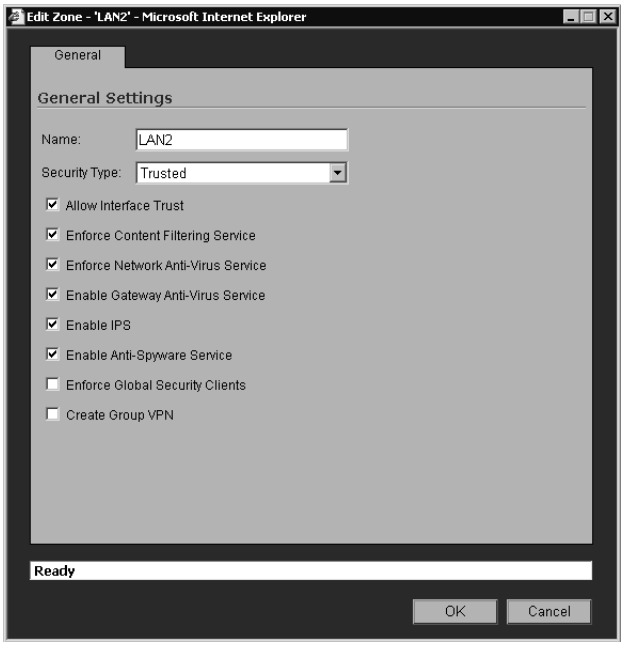
Another benefit of using the SonicWALL zones is that you can apply most of the SonicWALL security services to a specific security zone. For example, you can enable the SonicWALL intrusion prevention service across the entire LAN zone, and at the same time you could have this service disabled on the VPN zone.

If necessary, you can also create custom-defined zones on your SonicWALL appliance, applying the security type "trusted," "public," or "wireless," as well as the SonicWALL security service features to the traffic to your liking.

To add a custom zone:

1. Select **Network** | **Zones**.
2. Click **Add**. An add zone window will open.
3. Name the new zone and select the options for the services you want to enforce for the new zone.
4. Click **OK** to create the new zone. Figure 3.17 shows the addition of a zone.

Figure 3.17 Adding a Zone to the SonicWALL



Interfaces

SonicWALL firewall appliances may contain several physical interfaces, including Ethernet, modem, or fiber, depending on the model you have. Interfaces go hand in hand with zones, because most zones rely on interfaces to be assigned to them for traffic to flow in and out. There are some exceptions, such as the VPN zone, which relies on a virtual interface rather than an actual physical interface.

On all SonicWALL appliances, the first two interfaces, x0 and x1, are permanently assigned to the LAN and WAN zones respectively. The TZ 170 may also have two special interfaces; one for the modem, and one for the wireless LAN. All remaining interfaces can be configured and bound to any zone type, depending on the model SonicWALL you have.

Some SonicWALL appliances have special interfaces. The SonicWALL Pro 1260 has a single LAN interface, but this interface includes all 24 numbered ports of the integrated switch, as well as the uplink port on the front of the firewall. The TZ 170 has a single LAN interface that includes all five of the ports in its integrated switch. These physical ports cannot be separated from the LAN interface and used in other zones.

The SonicWALL PRO 3060, PRO 4060, and PRO 5060 contain four user-definable interfaces, interfaces x2 through x5. The SonicWALL PRO 2040 contains two user-definable interfaces, x2 and x3. The SonicWALL PRO 1260 and TZ 170 contain a single user-definable interface—the interface labeled as OPT.

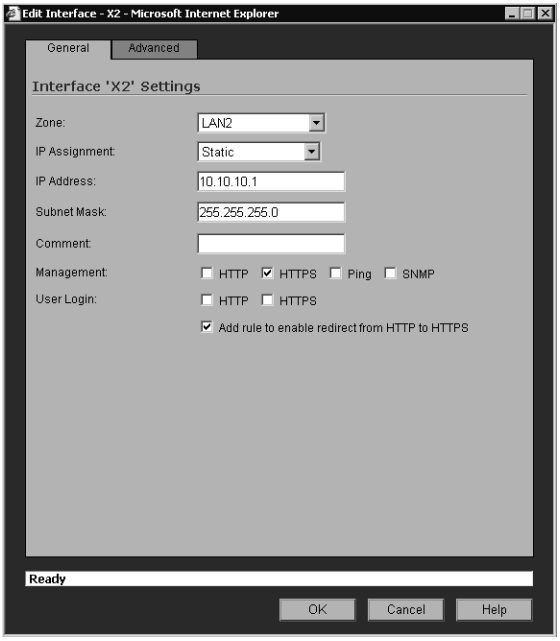
Binding an Interface to a Zone

Now that we've created our new zone, we need to bind an interface to the zone. Suppose that we want to assign interface x2 to the zone. We want this interface to be assigned the IP address 10.10.10.1. This network is a full class C network. We also want to allow management via HTTPS on this interface.

From the Web interface:

1. Select **Network** | **Interfaces**. Locate the x2 interface and click the **Configure** icon to the right. The Edit Interface window will open.
2. Choose the desired zone for the interface. In this case we are using LAN2. Upon making a selection, you will see additional interface configuration is required.
3. Enter the IP address **10.10.10.1** and verify the netmask is correct. Since we know that the network is a class C network, we know the netmask 255.255.255.0 is correct.
4. Enable HTTPS management on this interface. Note that by default, the option **Add rule to enable redirect from HTTP to HTTPS** is enabled.
5. Click **OK** to complete the addition of interface x2 to the LAN2 zone. Figure 3.18 shows the proper configuration of the interface.

Figure 3.18 Binding an Interface to a Zone



VLANs

The SonicWALL PRO 4060 and PRO 5060 also support the use of virtual interfaces, or VLANs. A virtual interface is a sub-interface of a physical interface. Virtual interfaces allow you to have more than one network on a single wire and physical connection. The virtual interfaces can provide services just as the regular interface can, including assignment to zones, the ability to act as a DHCP (Dynamic Host Control Protocol) server, and can provide NAT (Network Address Translation) and enforce access rules. SonicOS does not participate in any VLAN trunking protocols, and requires each VLAN to be configured and assigned appropriate security characteristics.

Trunk links are supported by adding the VLAN ID as a sub-interface on your SonicWALL and configuring it just as you would a physical interface. Any VLANs not explicitly defined will be disregarded by the SonicWALL. This allows the same interface to support traffic that is native traffic and to act as a normal interface would.

Advanced Features

SonicOS also provides several advanced features configurable for each interface. These features include such settings as manually setting link speed, bandwidth management, and creating a default NAT policy.

SonicOS Enhanced supports bandwidth management, allowing you to specify the amount of traffic that can flow across a link. SonicOS Enhanced can manage bandwidth both inbound and outbound. Inbound management is provided by using an ACK delay algorithm to control traffic flow. Outbound management uses class-based queuing (CBQ), which provides guaranteed and maximum bandwidth, to control the flow of traffic. CBQ works by queuing each packet into different priority queues, based on its priority. The packets are then delivered and transmitted by the quality of service scheduler based on the flow and available bandwidth on the link.

Configuring the SonicWALL Firewall

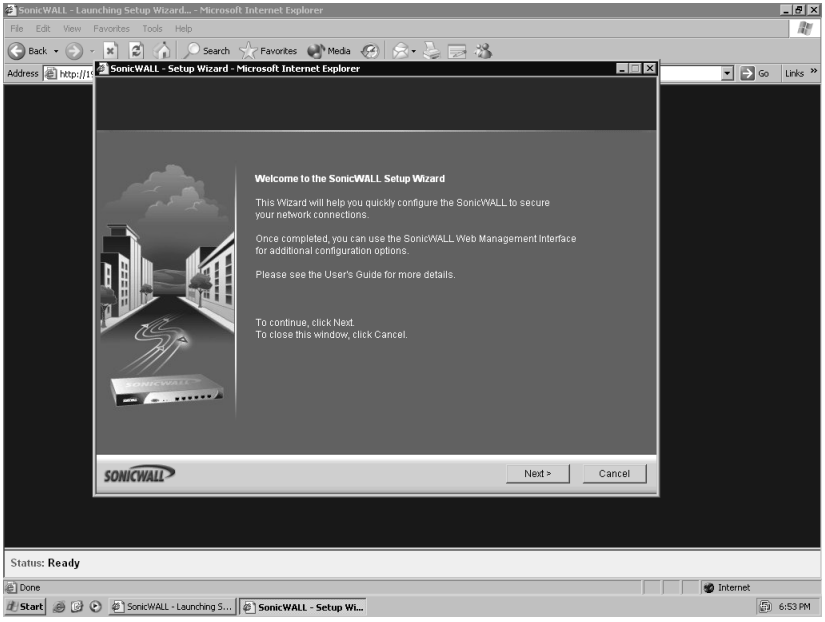
In this section we will look at configuring basic requirements to make your SonicWALL appliance functional on your network. In order to start configuring your SonicWALL, you will need some basic information about your network architecture. You will need information on the configuration of your connection to the Internet, which will be the WAN interface on the SonicWALL. This will include information such as the type of connection you are using, IP address or address range, netmask, gateway, and DNS (domain name system) servers. You will also need information about your local area network, which will be used to configure the LAN interface on the SonicWALL. This will include information such as your local IP address range and netmask.

There are two different methods for configuring a SonicWALL appliance for the first time. First, the SonicWALL appliance can be configured using the configuration wizard. Using the configuration wizard allows you to configure a SonicWALL with a basic configuration in about 10 minutes. Once you've completed the wizard, you should have network connectivity and traffic should be able to pass through the SonicWALL.

An alternative method for configuration is to cancel the setup wizard and log directly in to the Web interface. You can then manually configure all the necessary options to get the SonicWALL ready for your network. To get started using the configuration wizard:

1. Using an Ethernet cable, connect the SonicWALL to your computer and verify you have a network link light. If you do not have a link light, replace the Ethernet cable with a crossover cable.
2. Set your computer's IP address to something in the 192.168.168.0/24 range. I usually use the IP address 192.168.168.100.
3. Power the SonicWALL appliance on. Wait until the "Test" light goes off. Point your Web browser to http://192.168.168.168. This is the factory-assigned IP address of the SonicWALL appliance. Your Web browser will load the SonicWALL setup wizard, shown in Figure 3.19 Click **Next** to continue setting up your SonicWALL appliance.

Figure 3.19 SonicWALL Setup Wizard

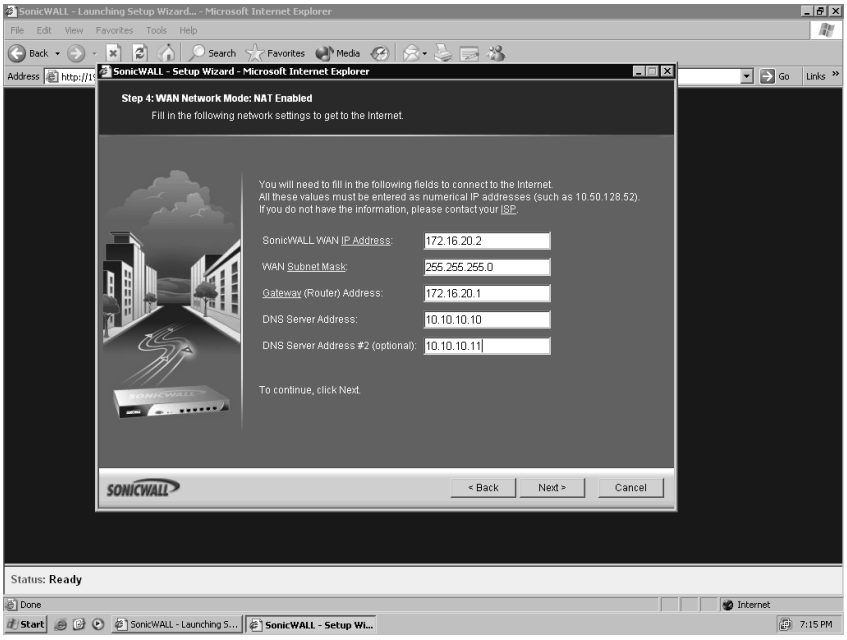


4. The first requirement is to change the default password. Input your desired password into the fields. The ideal password is something that is made up of letters, symbols, and numbers, and would be difficult for someone to guess. Be sure that you remember this password, as you will need it every time you want to make changes to your SonicWALL appliance! Once you've chosen your password, click **Next** to proceed.
5. Select the correct **Time Zone** for your location from the drop-down list. If desired, enable the **Daylight Savings Time** option. Since SonicWALL

appliances by default use NTP (Network Time Protocol) to keep time, it is not necessary to set the clock. Click **Next** to proceed.

6. The next screen configures the WAN interface for network connectivity. Here you are presented with four options. SonicWALL supports setting the WAN interface to a static IP address, to perform a PPPoE (Point-to-Point Protocol over Ethernet) login, to utilize DHCP to obtain its WAN configuration, or to use PPTP (Point-to-Point Tunneling Protocol). Figure 3.20 shows an example of configuring the SonicWALL to use statically set WAN addressing information. Once you've chosen the option for your needs, click **Next** to proceed.

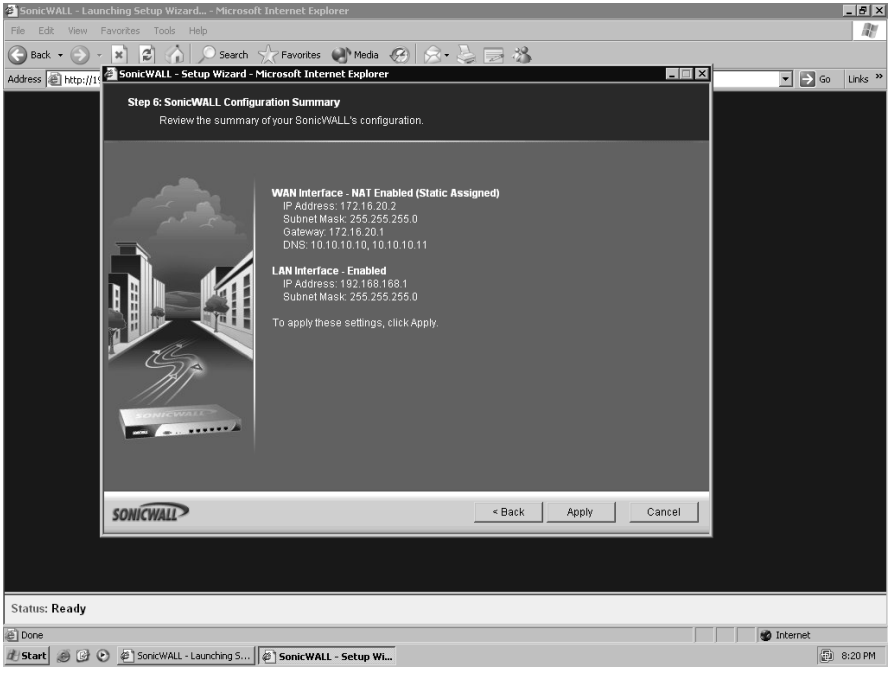
Figure 3.20 WAN Interface Configuration



7. Depending on your choice from step six, proceed with the configuration. Since we are configuring a static IP scenario, we will enter the IP address, netmask, default gateway, and DNS server information. Configuration for the other methods will be discussed later in this chapter. Click **Next** to continue to the LAN configuration page.
8. The SonicWALL will now ask you for its LAN interface address and netmask. Input the desired network information and click **Next** to continue.

9. The final quickstart screen will appear, similar to the one in Figure 3.21. This screen allows you to review the configuration as you have entered into the SonicWALL. Check all values to ensure they are set as you want them. If anything is incorrect, click the **Back** button to go back and make any necessary changes. Once you've verified the configuration, click **Apply**. The SonicWALL Quickstart wizard will apply the configuration to your SonicWALL for you and then acknowledge completion. Click **Close** to end the Quickstart wizard and be redirected to the SonicWALL login page.

Figure 3.21 Final Configuration Review



Congratulations! You've just completed the initial configuration of your SonicWALL appliance for your network. You can now log into the Web interface to work with other features that your SonicWALL has to offer.

Other Methods for Configuring the WAN Interface

Statically assigning network information to your SonicWALL appliance is only one method for configuring the WAN interface. SonicWALL appliances support addi-

tional methods for configuring the WAN interface. This includes configuration by DHCP, PPPoE, PPTP, and L2TP (Layer 2 Tunneling Protocol).

Configuring the DHCP Client

SonicWALL supports acting as a DHCP client to configure the WAN interface. In this mode, the SonicWALL sends a DHCP request out from the WAN interface, expecting to receive network configuration information including an IP address, netmask, default gateway, and DNS servers back from a DHCP server. This method is sometimes used when connecting the SonicWALL to a router that provides DHCP addresses, or a cable modem. To configure the SonicWALL for DHCP:

1. Click the **Network | Interfaces** tab. Locate the WAN interface and click the **Configure** icon.
2. Change **IP Assignment** to **DHCP**.
3. Click **OK** to complete the configuration.

Configuring PPPoE for the WAN interface

Most DSL (digital subscriber line) service providers require the use of PPPoE. PPPoE connects to the Ethernet network using a username and password. Once the device is authenticated, it is assigned an IP address. This requires additional configuration to the WAN interface. To configure the WAN interface for PPPoE:

1. Click the **Network | Interfaces** tab. Locate the WAN interface and click the **Configure** icon.
2. Change **IP Assignment** to **PPPoE**. The window will update with fields specific to PPPoE.
3. Enter your username and password in the **User Name** and **User Password** fields as provided to you by your DSL provider.
4. Click **OK** to complete the configuration.

You can also configure the PPPoE connection to terminate after a specified number of minutes of inactivity, although I don't know why one would want to use this feature. Just enable the **Inactivity Disconnect (minutes)** option and input the desired timeout. The default value is ten minutes.

Configuring PPTP

SonicWALL also supports using PPTP to obtain its WAN configuration. PPTP is seldom used for configuring the WAN, but is included. It is used to obtain network information from older versions of Microsoft Windows. To configure PPTP:

1. Click the **Network | Interfaces** tab. Locate the WAN interface and click the **Configure** icon.
2. Change **IP Assignment** to **PPTP**. The window will update with fields specific to PPTP.
3. Enter your username and password in the **User Name** and **User Password** fields. Enter the IP address of the PPTP server in the **PPTP Server IP Address** field.
4. Click **OK** to complete the configuration.

Configuring L2TP

SonicWALL supports L2TP as a method of WAN configuration. L2TP uses an encrypted IPSec connection to connect to the specified server, either Windows 2000 or Windows XP. Only the traffic passing between the server and the SonicWALL is encrypted. All traffic to other destinations is passed in the clear.

1. Click the **Network | Interfaces** tab. Locate the WAN interface and click the **Configure** icon.
2. Change **IP Assignment** to **L2TP**. The window will update with fields specific to L2TP.
3. Enter your username and password in the **User Name** and **User Password** fields. Enter the IP address of the L2TP server in the **L2TP Server IP Address** field. If the IP address is manually assigned, enter the values as required. If the IP is acquired through DHCP, change the **L2TP IP Assignment** to **DHCP**.
4. Click **OK** to complete the configuration.

Interface Speed Modes

By default, all of the ports on your SonicWALL firewall are auto-sensing. This means they negotiate the Ethernet settings such as speed and duplex automatically with the device they are connected to. This is great most of the time, but in an ideal world you may want to hard code these settings to ensure that you are getting the proper

performance out of your network. Occasionally you may also see an instance where link speed or duplex mode will not properly negotiate, resulting in no link or traffic not flowing. Interface speed can be configured through both the serial console and the Web interface.

To set an interface's speed mode manually through the Web interface:

1. Select **Network | Interfaces**. Select the interface you want to hard code the interface speed for and click the **Configure** icon
2. Click on the **Advanced** tab.
3. Change the value of the field **Link Speed** to the setting you wish to use.
4. Click **OK** to save the settings.

Setting an interface's speed mode using the serial console looks something like this:

```
PRO 3060 Enhanced> configure
(config[PRO 3060 Enhanced])> int x0
(config[PRO 3060 Enhanced]-if[X0])> speed 100
(config[PRO 3060 Enhanced]-if[X0])> end
(config[PRO 3060 Enhanced])> end
PRO 3060 Enhanced>
```

Configuring System Services

On your SonicWALL firewall there are some other notable things to configure. We will first look at configuring the local clock on the device. Configuring the time is very important for being able to correlate information in the logs to a specific time.

SonicWALL firewalls contain a built in DHCP server. Typically, you can have a server on each interface. This allows you to manage your internal IP addressing in a single location. All SonicWALL firewalls are able to query DNS servers. This allows them to resolve hostnames to IP addresses just as normal systems do. It is important to have working DNS servers configured on your firewall so that URL filtering and other services that utilize hostnames can work properly.

There is a great deal of information generated by your firewall in the form of logs. Because all SonicWALL firewalls have very limited space for storing the logs, you may want to be able to send this logging information to a remote system. We will look at how to configure and use remote log repositories. Finally, we will examine how to unlock certain features of your firewall device with license keys and also how to update these keys.

Setting the Time

Every SonicWALL device contains an internal clock. This clock continually runs while the device is turned on. You can manually adjust the clock from within the WebUI on the System | Time page. The SonicWALL uses the clock for time-stamping logs, as well as for managing rules that are on a schedule. As previously mentioned, all SonicWALL firewalls are factory-configured to use an internal list of NTP servers to set and keep the time. The firewall periodically queries the time-servers to ensure that it has the proper time. You can also add your own preferred NTP server or servers for the SonicWALL to use for timekeeping purposes. The update interval for NTP is also configurable. The default NTP update interval is 60 minutes.

DHCP Server

SonicWALL appliances support the ability to act as a DHCP server for your network. This allows your firewall to manage and control IP address allocation to client devices on the network. The number of DHCP scopes and addresses that can be assigned varies depending on the model of SonicWALL appliance you are using. The DHCP server can give out IP addresses from a specified pool or from a reserved list based on MAC (media access control) addresses. An additional feature that SonicWALL supports is DHCP conflict detection. If the SonicWALL detects that there is another DHCP server handing out addresses on the network, it can automatically cease DHCP functionality. This can prevent IP address conflicts on your local network.

IP Helper

SonicWALL appliances provide functionality to act as an IP helper. Rather than the SonicWALL acting as a DHCP server on the local subnet and allocating addresses to client devices, the SonicWALL just listens for DHCP requests. When it receives a DHCP request, it forwards the request to a specified DHCP server on another subnet, which in turn, allocates an address for the client. The address is then passed back to the client device from the SonicWALL. This allows for centralized management of DHCP scopes from a single DHCP server, even when the DHCP server resides on a remote network.

DNS

Configuring the SonicWALL appliances for client DNS is a simple process. The Network | DNS page allows you to configure DNS settings manually. SonicWALL supports the ability to inherit DNS from the WAN zone. When this option is enabled, the DNS servers assigned to the WAN zone are the servers that the SonicWALL will use for DNS. If you prefer, or if you need to use a different DNS server or servers, choose the **Specify DNS Servers Manually** option, and input the desired values.

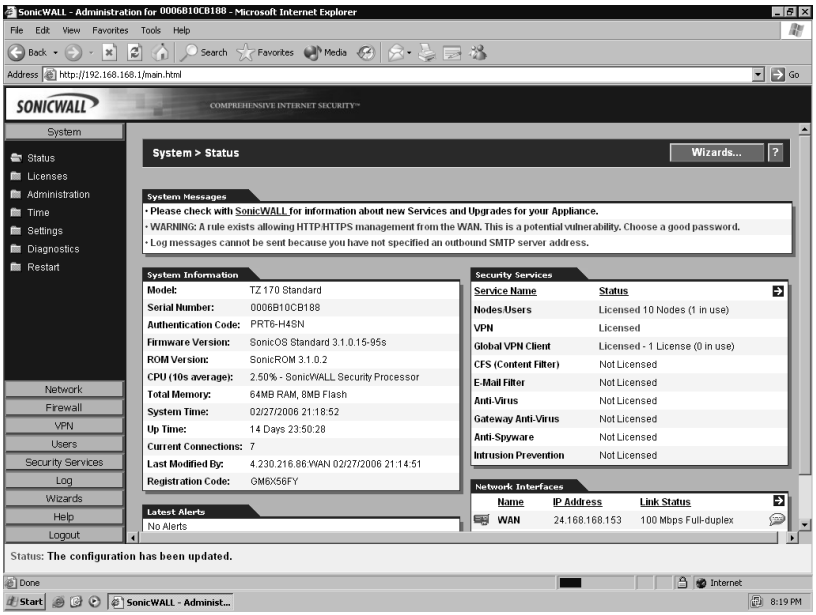
Licenses

Most SonicWALL security service features require proper licensing be configured on the appliance. This may include the number of allowed nodes, antivirus and anti-spyware filtering, content filtering, and VPN tunnel availability. All SonicWALL security licenses are centrally managed from the System | Licenses page.

For example, on the lower-end SonicWALL models such as the TZ 170, you can purchase the appliance with support for as few as 10 nodes. SonicWALL defines a node as a computer or device connected to your local area network that has an IP address. When this computer or device attempts to access the Internet through the SonicWALL, a node license is said to be in use. If you have only 10 node licenses available, when all 10 licenses are consumed by devices, the next device that attempts to access the Internet will be denied access, and an event will be logged to the SonicWALL system log. In the event that this happens, you have two possible solutions: you can exclude a node or nodes from connecting to the network, or you can purchase a node upgrade license for your SonicWALL appliance. Once the upgrade has been purchased, you simply install the upgrade license on your SonicWALL to activate the new functionality, in this case, additional node support. Figure 3.22 shows the System Licensing page on a SonicWALL appliance.

Licensing for your SonicWALL appliance is managed through your mysonicwall.com account. When you first set up your SonicWALL appliance, you create a mysonicwall.com account and enter your device serial number and authentication code to obtain the registration code for the appliance. After you enter this code into your SonicWALL, the appliance is registered. At this point you can install additional security service features for your SonicWALL.

Figure 3.22 SonicWALL Security Services Licensing



The Security Services Summary shows an overview of the currently activated security services, as well as the available features that are not currently active. The Status column indicates if a service has been activated (Licensed), can be activated (Not Licensed), or if the subscription to the service has expired (Expired). This chart also notes the node count supported by your SonicWALL appliance. The column labeled Expiration shows the expiration date of licensed services.

Once a day your SonicWALL firewall "phones home" to your mysonicwall.com account and updates your license information. You can also manually synchronize the licenses by clicking **To synchronize licenses with mySonicWALL.com click here**.

SonicWALL also offers free trial subscriptions of some of their security services, including the Content Filter Service and Network Antivirus. To activate any of the trial features, or to activate any other features, click the link to activate the service. You will be presented with the mysonicwall.com login page. You can then login to your account and complete the trial setup, or optionally purchase a security service subscription.

Sometimes you may need to deploy a SonicWALL firewall in a closed environment (an environment that cannot get access to the Internet). For this, SonicWALL offers the manual upgrade. The manual upgrade allows you to install license keys for

security services when connecting to mysonicwall.com is not possible. To perform a manual upgrade, do the following:

1. Log in to the mysonicwall.com site.
2. Click the **registered appliance** for which you want to obtain security license keys.
3. Click the link **View License Keyset**. You will be presented with a text box that contains the license keyset. Copy the license keyset to your clipboard, and paste it into a text document.
4. If possible, paste the license keyset into the SonicWALL **Manual Upgrade** area on the System | Licenses page. If you cannot paste the license directly into the SonicWALL, print the license keyset and manually key the information into the SonicWALL.
5. Click **Submit** or **Apply** to update your SonicWALL.

After performing a manual upgrade, you will not see any registration or license information on the System | Licenses page. Also, you may see a "SonicWALL Registration Update Needed" warning message. If this occurs, you can simply ignore this message.

Syslog

By default, the SonicWALL stores event log information in its onboard memory on a "first in, first out" basis. Older events are the first to be overwritten. If you intend to keep your logs for a period of time or require the ability to audit or do reporting on your logs, it is recommended that you use a syslog server to perform logging.

The SonicWALL syslog captures and reports all log activity and includes source and destination addresses, number of bytes transferred, and IP service. Syslog support does require that you have a syslog server running on your network, and that the syslog daemon is running on UDP port 514. You can use a log analyzer such as SonicWALL's Viewpoint software, or WebTrend's Firewall Suite to analyze and graph the logged data. The SonicWALL appliances can support up to three syslog servers at a time.

Summary

Before you begin using your firewall, you must understand how to manage it.

There are two core types of management, the WebUI and the CLI. If you are using the serial console, you are using the CLI. The SonicWALL CLI is not full-featured, but can be a valuable tool to perform some management functions. The WebUI is easier to use, and provides you with full management capabilities. However, you will see that some advanced troubleshooting techniques can easily be carried out from the command-line interface. These techniques are invaluable for more advanced configurations. We also mentioned a third type of management called the Global Security Manager. The Global Security Manager product is an external source of management, and is covered in detail in Chapter 9.

This chapter also discussed configuring your SonicWALL firewall to run on the network. Zones have become a core part of the SonicWALL security infrastructure, and will remain so in the future. Each interface must be bound to a zone. In the next chapter we will focus on basic policy creation and policy theory. In that chapter you will see the application of security zones. In this chapter, we looked at all of the various types of interfaces that the firewall supports. The physical interface will be used on each type of SonicWALL device to interact with the network. The firewall can operate in two modes, Layer 3 and Layer 2. In this chapter we focused on the Layer 3 configuration of the device. In Chapter 8 we will focus completely on the Layer 2 mode, called *transparent mode*.

In the last section of the chapter we looked at configuring various system components. Ensuring that the time is properly adjusted on your device is critical. Time is the central reference point used to correlate all events on your firewall. If someone was to break in to your network and your logs were off by several hours or days, this could hinder your investigation of the break-in. Configuring your logs to be sent to a separate location is also important if you intend to keep your logs long term. The syslog server and WebTrends server are both great options to choose if you plan to keep your logs for a long time.

Solutions Fast Track

Managing the SonicWALL Firewall

- ☑ There are two methods that can be used to directly manage a SonicWALL appliance—the Web interface and the serial console.
- ☑ The SonicWALL serial console does not provide for rules management, but is a great tool for interface configuration or backing up your preferences.
- ☑ As often as possible, use HTTPS Management (SSL) over HTTP since the management traffic is encrypted and will be secured from possible sniffing.
- ☑ The SonicWALL Global Management System is a tool used to make management of several SonicWALL appliances unified and simple.

Configuring the SonicWALL Firewall

- ☑ Prior to making any configuration changes, always back up your current preferences file!
- ☑ Limited administrators can only manage a few select areas of the firewall, and can only do so from the LAN zone via a VPN.
- ☑ SonicWALL safe mode can assist you in gaining access to a firewall that you've been locked out of or have experienced problems accessing via the Web interface.
- ☑ SonicWALL security services such as anti-spyware and intrusion prevention service can be activated on a per-interface basis.

Configuring Your SonicWALL for the Network

- ☑ The SonicWALL WAN interface can be configured using several methods, including static IP assignment, DHCP, PPPoE, PPTP, and L2TP.

Configuring System Services

- ☑ It is important to ensure that your time zone is configured properly on your SonicWALL so that scheduled rules are in effect at the correct time, and the system log timestamps are accurate.

- ☑ If you need the ability to store your logs long-term for auditing or reporting, it is best that you configure the SonicWALL to send log messages to a syslog server.
- ☑ SonicWALL automatically inherits the WAN interface's DNS server settings, but you can manually specify DNS servers if there is need.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: What are the advantages of using SonicOS Enhanced instead of SonicOS Standard?

A: SonicOS Enhanced provides many additional features that are not available in SonicOS Standard. Some of these include security zones, rule scheduling, and support for hardware failover. In most corporate or small business environments today, these features can be crucial to maximizing resource availability and minimizing downtime. Many of the features in SonicOS Enhanced also aid in simplifying firewall and access rule management.

Q: Why does SonicWALL use zones on interfaces? I have used this type of configuration on other devices and I did not find it to be very effective.

A: Zones are designed to segment areas of the network from each other. On a SonicWALL firewall, using security zones during policy creation allows or disallows traffic from one zone to another. This simplifies policy creation by specifying which zone traffic can leave from and go to. Furthermore, it removes the chance that you accidentally configure access from one system to another. This can easily happen if you use a firewall that does not support zones.

Q: You cover securing the management interface extensively. Are all of those options really required?

A: Because the firewall is such a critical part of your network, you need to ensure its own security as well. Each option may be used in your network, or perhaps a combination of all of the options makes the most sense in your environment. By understanding all of the options, you will have the ability to pick and choose among all of them.