Copyright Information

© 2002 SonicWALL, Inc. All rights reserved.

Under copyright laws, this manual or the software described within may not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions are subject to change without notice.

Part Number: 232-000185-00 Rev D
Software License Agreement for SonicWALL Global Management System

To review the SonicWALL Global Management System Software License Agreement, see the SonicWALL Global Management System Introduction Guide.
## Section I
Initial Configuration of SonicWALL GMS and SonicWALL Appliances

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>Configuring SonicWALL Appliances</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Configuring New SonicWALL Appliances</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Enabling Remote Management</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Migrating Existing SonicWALL Appliances</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Updating Firmware</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>Enabling Remote Management</td>
<td>29</td>
</tr>
<tr>
<td>3</td>
<td>Creating Groups and Adding SonicWALL Appliances</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Creating SonicWALL Fields and Views</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Creating Custom Fields</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>SonicWALL Fields</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Setting Up Views</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Changing Views</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Adding SonicWALL Appliances to SonicWALL GMS</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Importing SonicWALL Appliances</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Registering SonicWALL Appliances</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Moving SonicWALL Appliances Between Groups</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Inheriting Group Settings</td>
<td>42</td>
</tr>
<tr>
<td>4</td>
<td>SonicWALL GMS User Management</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Creating User Groups</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Configuring Screen Access</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Configuring Appliance Access</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Adding Users</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Configuring Screen Access</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Configuring Appliance Access</td>
<td>48</td>
</tr>
</tbody>
</table>

## Section II
SonicWALL Appliances

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Configuring and Maintaining SonicWALL Appliances</td>
<td>53</td>
</tr>
<tr>
<td>6</td>
<td>Configuring Network Settings</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Configuring Network Settings</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>Standard Mode</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>NAT-Enabled Mode</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>NAT with DHCP Client Mode</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>NAT With PPPoE Client</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>NAT With L2TP Client</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Configuring Time Settings</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Changing the SonicWALL Password</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Saving and Applying SonicWALL Settings</td>
<td>64</td>
</tr>
<tr>
<td>Chapter 7 Configuring Log Settings</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>Chapter 8 Configuring Website Blocking</td>
<td>69</td>
<td></td>
</tr>
<tr>
<td>Configuring General Website Blocking Options</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>Selecting the Content to Block</td>
<td>71</td>
<td></td>
</tr>
<tr>
<td>Controlling Access to Specific Domains</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>Deleting Domains from the Domain Lists</td>
<td>74</td>
<td></td>
</tr>
<tr>
<td>Blocking Access to Domains by Keywords</td>
<td>75</td>
<td></td>
</tr>
<tr>
<td>Blocking Web Features</td>
<td>76</td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>Websense and N2H2 Content Filtering</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td>N2H2</td>
<td>79</td>
<td></td>
</tr>
<tr>
<td>Websense</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>

| Chapter 9 Configuring Network Access Rules | 81 |
| Understanding the Network Access Rules Hierarchy | 82 |
| Defining Network Rules                     | 82 |
| Configuring General Access Settings        | 82 |
| Adding a Service                           | 83 |
| Creating Rules                             | 84 |
| Creating Users                             | 86 |
| Establishing an Authenticated Session       | 88 |
| Configuring Management Settings            | 88 |
| Configuring SNMP Settings                   | 89 |
| Configuring RADIUS                         | 90 |

| Chapter 10 Configuring Dynamic Host Configuration Protocol | 93 |
| Configuring DHCP                                         | 94 |
| Configuring DHCP Over VPN                                | 95 |

| Chapter 11 Configuring Advanced Settings and Options      | 97 |
| Configuring Proxy Settings                                | 98 |
| Configuration                                             | 98 |
| Configuring Intranet Settings                             | 99 |
| Configuration                                             | 99 |
| Configuring Routes                                        | 101 |
| Configuring DMZ (HomePort) Addresses                      | 102 |
| Configuration                                             | 102 |
| Configuring One-to-One Network Address Translation        | 103 |
| Configuration                                             | 103 |
| Configuring Ethernet Settings                             | 105 |

| Chapter 12 Configuring Virtual Private Networking         | 107 |
| Configuring VPN                                           | 108 |
| Enabling VPN                                              | 108 |
| Configuring Security Associations                          | 109 |
| Internet Key Exchange Using SonicWALL Certificates         | 109 |
| Internet Key Exchange Using Third-Party Certificates       | 114 |
| Internet Key Exchange Using Pre-Shared Secret             | 120 |
| Manual Keying                                             | 125 |
| Management of VPN Client users                            | 129 |
| Enabling VPN Client                                       | 129 |
| Downloading VPN Client Software                            | 130 |
| Basic Terms and Concepts                                  | 131 |
Chapter 13 Configuring Anti-Virus Settings
  Changing Anti-Virus Password 134
  Configuring Anti-Virus Settings 134
  Configuring Anti-Virus Email Filter Settings 136
  Creating License Sharing Groups 138
    Creating a License Sharing Group 138
    Adding a SonicWALL Appliance to an Existing Group 139
    Changing the Number of Licenses 140

Chapter 14 Configuring High Availability Settings

Chapter 15 Configuring PKI Options
  Working with PKI Administrator Certificates 143
  Working with PKI End User Certificates 144

Chapter 16 Configuring Modem Options
  Configuring the Modem Profile 145
  Configuring the Modem 146

Chapter 17 Maintaining SonicWALL Appliances
  Upgrading SonicWALL Appliances 149
  Restarting SonicWALL Appliances 150
  Synchronizing Now 151
  Requesting Diagnostics for SonicWALL 152
  Inheriting Group Settings 153
  Adding Contact Information 153

Chapter 18 Upgrading SonicWALL Appliances
  Adding Nodes to SonicWALL Appliances 155
    Purchasing Node Upgrades 155
    Licensing Node Upgrades 155
    Activating Node Upgrades 156
  Adding the Content Filter List to SonicWALL Appliances 157
    Purchasing Content Filtering Subscriptions 157
    Licensing Subscription Upgrades 157
    Activating Subscriptions for SonicWALL Appliances 158
  Adding Virtual Private Networking to SonicWALL Appliances 159
    Purchasing VPN Upgrades 159
    Licensing a VPN Upgrade 159
    Activating VPN Upgrades for SonicWALL Appliances 160
  Adding VPN Client Licenses to SonicWALL Appliances 161
    Purchasing VPN Client Licenses 161
    Licensing VPN Clients 161
    Activating VPN Clients 162
  Adding Anti-Virus Protection to SonicWALL Appliances 164
    Purchasing Anti-Virus Subscriptions 164
    Licensing Anti-Virus Upgrades 164
    Activating Anti-Virus Subscriptions 165
  Adding PKI Administrator Certificates 166
    Purchasing PKI Administrator Certificates 166
    Licensing PKI Administrator Certificate Upgrades 166
    Activating PKI Administrator Certificates 167
  Adding PKI End User Certificates 168
    Purchasing PKI End User Certificates 168
    Licensing a PKI End User Certificate Upgrade 168
    Activating PKI End User Certificates 169
Section III
Ravlin Devices

Chapter 19 Adding Ravlin Devices
Configuring Ravlin Devices
Configuring Devices for SonicWALL GMS Management
Creating Ravlin Fields and Views
Creating Custom Fields
Standard Fields
Setting Up Views
Changing Views
Adding Ravlin Devices to SonicWALL GMS

Chapter 20 Configuring Ravlins
Configuring Network Settings
Configuring IP Settings
Configuring Routes
Configuring PPPoE
Configuring Packet Handling Options
Configuring Miscellaneous Network Settings
Configuring Log Settings
Configuring SNMP Settings
Configuring Syslog Server Settings

Chapter 21 Configuring Virtual Private Networking
Configuring VPN
Configuring Key Management and Protocol Options
Policy Data Entry Creation Overview
Configuring One or More Security Associations
Enabling VPN
Configuring RADIUS
Adding Client Certificates
Basic Terms and Concepts

Chapter 22 Maintaining Ravlin Devices
Upgrading Ravlin Devices
Restarting Ravlin Devices
Clearing Security Associations
Clearing the ARP Caches

Section IV
SonicWALL GMS Configuration and Maintenance

Chapter 23 Configuring and Working with SonicWALL GMS
Changing the SonicWALL GMS Password
Configuring SonicWALL GMS Settings
Deleting the SonicWALL GMS Logs
Viewing the SonicWALL GMS Log
Working with SonicWALL GMS Tasks
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing SonicWALL GMS</td>
<td>225</td>
</tr>
<tr>
<td>Managing Sessions</td>
<td>225</td>
</tr>
<tr>
<td>Managing Agent Configurations</td>
<td>226</td>
</tr>
<tr>
<td>Upgrading SonicWALL GMS</td>
<td>228</td>
</tr>
<tr>
<td>Upgrading a Demo License to a Retail License</td>
<td>228</td>
</tr>
<tr>
<td>Upgrading the Node License</td>
<td>229</td>
</tr>
<tr>
<td>Activating SonicWALL GMS Support</td>
<td>229</td>
</tr>
<tr>
<td>Log into Mysonicwall.com</td>
<td>230</td>
</tr>
<tr>
<td>Performing a System Snapshot</td>
<td>232</td>
</tr>
<tr>
<td>Performing the Snapshot</td>
<td>232</td>
</tr>
<tr>
<td>Viewing the Snapshot or Diagnostics</td>
<td>233</td>
</tr>
</tbody>
</table>
Section I
Initial Configuration of SonicWALL GMS and SonicWALL Appliances
Introduction

This guide is designed to help you configure the SonicWALL Global Management System (SonicWALL GMS). If you have not used SonicWALL GMS before, you may want to familiarize yourself with some of the SonicWALL GMS concepts and features. For more information, see the SonicWALL Global Management System Introduction Guide.

Before configuring SonicWALL GMS, it must be properly installed. For more information, see the SonicWALL Global Management System Installation Guide.

This guide is divided into four sections: Introduction, SonicWALL Appliances, Ravlin Devices, and SonicWALL GMS Configuration and Maintenance. When you are ready to configure SonicWALL GMS, select from the following:

- **Section II: SonicWALL Appliances**
  - To create groups and add SonicWALL appliances to those groups, see Chapter 2, “Configuring SonicWALL Appliances.”
  - To configure SonicWALL appliances, see Chapter 3, “Configuring PKI Options.”
  - To configure VPN tunnels between SonicWALL appliances, see Chapter 12, “Configuring Virtual Private Networking.”

- **Section III: Ravlin Devices**
  - To create groups and add Ravlin devices to those groups, see Chapter 19, “Adding Ravlin Devices.”
  - To configure Ravlin devices, see Chapter 20, “Configuring Ravlins.”
  - To configure VPN tunnels between Ravlin devices, see Chapter 21, “Configuring Virtual Private Networking.”

- **Section IV: SonicWALL GMS Configuration and Maintenance**
  - To create and modify custom views, see Chapter 4, “SonicWALL GMS User Management.”
  - To perform maintenance tasks such as upgrading firmware, see Chapter 17, “Maintaining SonicWALL Appliances.”
  - To configure SonicWALL GMS settings, see Chapter 23, “Configuring and Working with SonicWALL GMS.”
  - To add upgrades or subscription services to SonicWALL appliances, see Chapter 18, “Upgrading SonicWALL Appliances.”
Configuring SonicWALL Appliances

Before managing SonicWALL appliances from SonicWALL Global Management System (SonicWALL GMS), you must configure them for SonicWALL GMS management and add them to SonicWALL GMS user interface. This chapter describes how to set up new or currently configured SonicWALL appliances for SonicWALL GMS management. Select from the following:

- To prepare new SonicWALL appliances for SonicWALL GMS, see “Configuring New SonicWALL Appliances” on page 16.
- To configure existing SonicWALL appliances for management by SonicWALL GMS, see “Migrating Existing SonicWALL Appliances” on page 29.
Configuring New SonicWALL Appliances

This section describes how to configure new SonicWALL appliances SonicWALL GMS management. For information on adding existing SonicWALL appliances, see “Migrating Existing SonicWALL Appliances” on page 29.

Enabling Remote Management

*Note: Ensure the SonicWALL appliance is running firmware version 6.1.1.0 or later.*

To configure a new SonicWALL appliance for remote management, follow these steps:

*Note: For information on migrating existing SonicWALL appliances, see “Migrating Existing SonicWALL Appliances” on page 29.*

1. Start the SonicWALL installation Wizard. The Welcome screen appears (Figure 1).

   **Figure 1: Installation Welcome Screen**

   ![Image](image1.png)

   **Welcome to SonicWALL Internet Security Appliance Wizard**

   This Wizard will help you quickly configure the SonicWALL to secure your Internet connection. Once completed, you can use the SonicWALL Web Management Interface for additional configuration options. Please see the User's Guide for more details.

   To bypass this Wizard, click “Cancel”.

2. Click **Next**. The Set Password screen appears (Figure 2).

   **Figure 2: Set Password Screen**

   ![Image](image2.png)

   **Set Your Password**

   First, you will need to choose a good administrator password in order to protect the security of your SonicWALL. Note that this password will be encrypted when sent over your network.

   Your password should be a combination of letters, numbers, and punctuation. You should not use a password which can easily be guessed by others (such as the name of your spouse, or your birthday). Note also that your password is case sensitive.

   ![Password Input Fields](password_fields.png)

   If you plan to manage your SonicWALL remotely using the SonicWALL Global Management System, check the following checkbox.

   ![Checkbox](checkbox.png)

   **Use Global Management System**

   ![Next/Cancel Buttons](buttons.png)
3. Enter the password for the SonicWALL appliance, select the **Use Global Management System** check box, and click **Next**.

*Note:* In order for SonicWALL GMS to manage a SonicWALL appliance, it must have the password. For more information, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

The Set Global Management System Information screen appears (Figure 3).

**Figure 3: Set Global Management System Information Screen**

4. Enter the IP address of the SonicWALL GMS server in the **Host Name or IP Address** field.

5. Enter a 16-character encryption key in the **Encryption Key** field. The key must be exactly 16 characters long and composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

6. Enter a 32-character authentication key in the **Authentication Key** field. The key must be exactly 32 characters long and composed of hexadecimal characters. For example, a valid key would be “1234567890abcdef1234567890abcdef.”

7. If a NAT device is between the SonicWALL appliance and SonicWALL GMS, select the **Interposed NAT Device** check box and enter the IP address of the SGMS gateway in the **NAT Device IP Address** field.

8. When you are finished configuring this page, click **Next**. The Time Zone screen appears (Figure 4).
9. Select the time zone.

10. Make sure you have all required network information and click Next. The Connecting to the Internet screen appears (Figure 5).

Figure 5: Connecting to the Internet Screen

11. Select how the device will connect to the Internet:

- If the device uses a single IP address provided by the Internet Service Provider (ISP), select **Assigned you a single static IP address** and click Next. Continue to “Single IP Address” on page 19.
- If the device uses two or more IP addresses provided by the ISP, select **Assigned you two or more IP addresses** and click Next. Continue to “Two or More IP Addresses” on page 21.
- If the device will use point-to-point protocol over Ethernet (PPPoE), select **Provided you with desktop software, a username, and password** and click Next. Continue to “PPPoE” on page 24.
- If the device will automatically be assigned a dynamic IP address, select **Automatically assigns you a dynamic IP address** and click Next. Continue to “DHCP” on page 26.
Single IP Address

If the ISP provided a single IP address, follow these steps:

1. From the Use Network Address Translation screen, click Next.

Figure 6: Use Network Address Translation Screen

The Getting to the Internet screen appears (Figure 7).

Figure 7: Getting to the Internet Screen

2. Enter the WAN IP address of the SonicWALL appliance.
3. Enter the WAN subnet mask of the SonicWALL appliance.
4. Enter the IP address of the gateway or router that provides Internet access to the SonicWALL appliance.
5. Enter the IP addresses of the DNS servers (maximum of three IP addresses). SonicWALL appliances require the IP address of at least one DNS server to function properly.
6. When you are finished configuring this page, click Next. The LAN Information screen appears (Figure 8).
7. Enter an IP address for the SonicWALL LAN interface in the SonicWALL LAN IP Address field. This address is also used for configuration and monitoring. Although you can enter any IP address, we highly recommend using a private IP address. The following IP address ranges are reserved for private IP networks and are not routed on the Internet:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Note: If your network uses IP addresses that are not registered to your organization and are not within the private IP address ranges, the servers on the Internet to which those IP addresses belong will not be accessible from your network. For example, if an IP address on your network is 185.5.20.105 and it is not registered to your organization, the server that uses that IP address on the Internet will not be accessible from your network.

8. Enter the subnet to which the LAN IP address belongs in the LAN Subnet Mask field.

9. When you are finished configuring this page, click Next. The DHCP Server screen appears (Figure 9).

Figure 9: DHCP Server Screen
10. If the SonicWALL appliance will act as the Dynamic Host Configuration Protocol (DHCP) server on the network, select the **Enable DHCP Server** check box and enter the beginning and end of the address range.

11. When you are finished configuring this page, click **Next**. The Restart screen appears (Figure 10).

**Figure 10: Restart Screen**

12. To restart the SonicWALL appliance, click **Restart**. The SonicWALL device is configured and ready to be managed by SonicWALL GMS. To add the unit to SonicWALL GMS, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

**Two or More IP Addresses**

If the ISP provided two or more IP address, follow these steps:

1. From the Network Address Translation screen, select whether the device will provide NAT for the network.

**Figure 11: Use Network Address Translation Screen**
NAT provides anonymity to machines on the LAN by connecting the entire network to the Internet using a single IP address. This provides security to the internal machines by hiding them from the outside world and conserves IP addresses.

When using NAT, we recommend using internal network IP addresses from a special range. The following IP address ranges are reserved for private IP networks and are not routed on the Internet:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

**Note:** If your network uses IP addresses that are not registered to your organization and are not within the private IP address ranges, the servers on the Internet to which those IP addresses belong will not be accessible from your network. For example, if an IP address on your network is 185.5.20.105 and it is not registered to your organization, the server that uses that IP address on the Internet will not be accessible from your network.

After selecting whether the SonicWALL device will use NAT, click **Next**. The Getting to the Internet screen appears (Figure 12).

**Figure 12: Getting to the Internet Screen**

2. Enter the WAN IP address of the SonicWALL appliance.
3. Enter the WAN subnet mask of the SonicWALL appliance.
4. Enter the IP address of the gateway or router that provides Internet access to the SonicWALL appliance.
5. Enter the IP addresses of the DNS servers (maximum of three IP addresses). SonicWALL appliances require the IP address of at least one DNS server to function properly.
6. When you are finished configuring this page, click **Next**. The LAN Information screen appears (Figure 13).
7. Enter an IP address for the SonicWALL LAN interface in the **SonicWALL LAN IP Address** field. Although you can enter any IP address, we highly recommend using a private IP address.

   *Note: This address is also used for configuration and monitoring.*

8. Enter the appropriate subnet in the **LAN Subnet Mask** field.

9. When you are finished configuring this page, click **Next**. The DHCP Server screen appears (Figure 14).

   **Figure 14: DHCP Server Screen**

10. If the SonicWALL appliance will act as the DHCP server on the network, select the **Enable DHCP Server** check box and enter the beginning and end of the address range.

11. When you are finished configuring this page, click **Next**. The Restart screen appears (Figure 15).
12. To restart the SonicWALL appliance, click **Restart**. The SonicWALL device is configured and ready to be managed by SonicWALL GMS. To add the unit to SonicWALL GMS, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

**PPPoE**

If the device connects to the Internet using Point-to-Point over Ethernet (PPPoE), follow these steps:

1. From the PPPoE screen, enter the account user name and password.

2. Click **Next**. The LAN Information screen appears (Figure 17).
3. Enter an IP address for the SonicWALL LAN interface in the **SonicWALL LAN IP Address** field. Although you can enter any IP address, we highly recommend using a private IP address.

   **Note:** This address is also used for configuration and monitoring.

4. Enter the appropriate subnet in the **LAN Subnet Mask** field.

5. When you are finished configuring this page, click **Next**. The DHCP Server screen appears (Figure 18).

   **Figure 18: DHCP Server Screen**

   - **Optional - SonicWALL’s DHCP Server**

     SonicWALL contains a Dynamic Host Configuration Protocol (DHCP) server to automatically configure the IP settings for the PC’s and other network devices on your LAN. If you wish to use SonicWALL’s DHCP Server, check the "Enable DHCP Server" checkbox below and enter a range of IP addresses to assign to the network devices on your LAN.

     The address range must be in the same subnet as the SonicWALL Web management address (currently set to 192.168.168.1). The range below should work on your network.

     If you don’t want to use the DHCP server, uncheck the "Enable DHCP Server" checkbox and click "Next".

     ```
     Enable DHCP Server [ ]
     Beginning of LAN client address range: 192.168.168.2
     End of LAN client address range: 192.168.168.254
     ```

6. If the SonicWALL appliance will act as the DHCP server on the network, select the **Enable DHCP Server** check box and enter the beginning and end of the address range.

7. When you are finished configuring this page, click **Next**. The Restart screen appears (Figure 19).
8. To restart the SonicWALL appliance, click **Restart**. The SonicWALL device is configured and ready to be managed by SonicWALL GMS. To add the unit to SonicWALL GMS, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

### DHCP

If the device is dynamically assigned an IP address, follow these steps:

1. From the Obtain an IP Address Automatically Screen, click **Next**.

**Figure 20: Obtain an IP Address Automatically Screen**

If your ISP has not provided you with any static IP addresses, then they probably told you that you will obtain an IP address automatically. SonicWALL can do this using its DHCP client.

If this sounds correct to you, then click “Next”. Otherwise, click “Back” to choose another option. If you’re not sure, please contact your ISP for clarification.

**Note:** If you select this option, the Wizard will enable Network Address Translation (NAT) to share the IP address among the PC’s and other network devices on your Local Area Network (LAN).

If you want to continue and use NAT, click “Next”. Otherwise, click “Back” to select another option.

The LAN Information screen appears (Figure 21).
2. Enter an IP address for the SonicWALL LAN interface in the **SonicWALL LAN IP Address** field. Although you can enter any IP address, we highly recommend using a private IP address.

   *Note: This address is also used for configuration and monitoring.*

3. Enter the appropriate subnet in the **LAN Subnet Mask** field.

4. When you are finished configuring this page, click **Next**. The DHCP Server screen appears (Figure 22).

   **Figure 22: DHCP Server Screen**

5. If the SonicWALL appliance will act as the DHCP server on the network, select the **Enable DHCP Server** check box and enter the beginning and end of the address range.

6. When you are finished configuring this page, click **Next**. The Restart screen appears (Figure 23).
7. To restart the SonicWALL appliance, click **Restart**. The SonicWALL device is configured and ready to be managed by SonicWALL GMS. To add the unit to SonicWALL GMS, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

8. To add the SonicWALL appliance to SonicWALL GMS UI using the import option, save the SonicWALL appliance's configuration (prefs) file.
Migrating Existing SonicWALL Appliances

Before an existing SonicWALL appliance can be administered from the SonicWALL GMS user interface (UI), the following must occur:

- The firmware must be updated to a version that is compatible with SonicWALL GMS. For more information, see “Updating Firmware,” below.
- Remote management must be enabled on the SonicWALL appliance. For more information, see “Enabling Remote Management” on page 29.

After you have completed these steps, add the SonicWALL appliance to the SonicWALL GMS UI as outlined in “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

Updating Firmware

SonicWALL appliances that are managed by SonicWALL GMS must be running firmware version 6.1.1.0 or later. For information on updating firmware, refer to the SonicWALL appliance’s documentation.

Enabling Remote Management

To configure the SonicWALL appliance to be remotely managed by SonicWALL GMS, follow these steps:

1. Log into the SonicWALL appliance.
2. Click Access.
3. Select the Management tab. The Management page appears (Figure 24).

4. Select by SonicWALL Global Management System from the Managed list box.
5. Enter the IP address of the SonicWALL GMS server in the **SGMS Host Name IP Address** field. Select the **SGMS behind NAT Device** check box and enter the IP address of the SGMS gateway in the **NAT Device IP Address** field.

6. Enter a 16-character encryption key in the **Encryption Key** field. The key must be exactly 16 characters long and composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

7. Enter a 32-character authentication key in the **Authentication Key** field. The key must be exactly 32 characters long and composed of hexadecimal characters. For example, a valid key would be “1234567890abcdef1234567890abcdef.”

8. When you are finished, click **Update**. The SonicWALL appliance is now configured for management by SonicWALL GMS. To clear the settings and start over, click **Reset**. To add the unit to SonicWALL GMS, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

9. To add the SonicWALL appliance to SonicWALL GMS UI using the import option, save the SonicWALL appliance's configuration (prefs) file.
Creating Groups and Adding SonicWALL Appliances

After you configure the SonicWALL appliances for SonicWALL GMS management, you can create SonicWALL fields that will be used to organize SonicWALL appliances. For more information, see “Creating SonicWALL Fields and Views” on page 31.

After you determine how you will organize SonicWALL GMS, you can use the following methods to add SonicWALL appliances to the SonicWALL GMS UI:

- To add SonicWALL appliances one at a time through the SonicWALL GMS UI, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.
- To add the SonicWALL appliances using the import option, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.
- To add multiple SonicWALL appliances using the SonicWALL GMS Command Line Interface, see the SonicWALL GMS Command Line Interface User Guide.

After you have added the SonicWALL appliances, you must register them. See “Registering SonicWALL Appliances” on page 40.

Note: If you need to move SonicWALL appliances to different groups, see “Moving SonicWALL Appliances Between Groups” on page 41.

Creating SonicWALL Fields and Views

The SonicWALL GMS uses an innovative method for organizing SonicWALL appliances. SonicWALL appliances are not forced into specific, limited, rigid hierarchies. Simply create a set of fields that define criteria (e.g., country, city, state) which separate SonicWALL appliances. Then, create and use views to display and sort appliances on the fly.

To organize SonicWALL appliances, follow these steps:

- Create custom fields that will be useful to your organization. See “Creating Custom Fields” on page 31.
- Review the standard SonicWALL fields. See “SonicWALL Fields” on page 33.
- Create views that will make your job easier. See “Setting Up Views” on page 33.

Creating Custom Fields

When first configuring SonicWALL GMS, you will create custom fields that will be entered for each SonicWALL appliance. SonicWALL GMS supports up to ten custom fields.

Note: Although SonicWALL GMS supports up to ten custom fields, only seven fields can be used to sort SonicWALL appliances at any given time.

The following are examples of custom fields that you can use:

- Geographic—useful for organizing SonicWALL appliances geographically. Especially useful when used in combination with other grouping methods. Geographic fields may include:
  - Country
  - Time Zone
  - Region
  - State
  - City
- Customer-based—useful for organizations that are providing managed security services for multiple customers. Customer-based fields may include:
  - Company
  - Division
  - Department
- Configuration-based—useful when SonicWALL appliances will have very different configurations. (e.g., Filtering, No Filtering, Pornography Filtering, Violence Filtering, or VPN).
- User-type—different service offerings can be made available to different user types. For example, engineering, sales, and customer service users can have very different configuration requirements. Or, if offered as a service to end users, you can allow or disallow network address translation (NAT) depending on the number of IP addresses that you want to make available.

SonicWALL GMS is pre-configured with four custom fields: Country, Company, Department, and State. These fields can be modified or deleted. To add fields, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the Console tab.
3. Expand the Management tree and click Custom Groups (Figure 26).

**Figure 26: Adding a Group**

4. Right-click Custom Groupings in the right pane.
5. Select Add Group from the pop-up menu.
6. Enter the name of the first field.
7. Select the newly created field and select Add Group from the pop-up menu.
8. Enter the name of the new field.
9. Repeat Steps 6 through 8 for each field that you want to create. You can create up to ten fields.

*Note: Although the fields appear to be in a hierarchical form, this has no effect on how the fields will appear within a view. To define views, see “Setting Up Views” on page 33.*

To modify or delete fields, right-click any of the existing fields and select Modify or Delete from the pop-up menu.
SonicWALL Fields

SonicWALL GMS includes standard fields that can be used to sort SonicWALL appliances based on their model, their firmware version, and other criteria. SonicWALL GMS fields include the following:

- AV Status—places the SonicWALL appliances into two groups: appliances that have anti-virus (AV) subscriptions and appliances that do not.
- CFL Status—places the SonicWALL appliances into two groups: appliances that have content filter list (CFL) subscriptions and appliances that do not.
- Firmware—creates a group for each Firmware version and places each SonicWALL appliance into its corresponding group.
- Model—creates a group for each SonicWALL model and places each SonicWALL appliance into its corresponding group.
- Nodes—creates a group for each node range and places each SonicWALL appliance into its corresponding group.
- PKI Status—places the SonicWALL appliances into two groups: appliances that have Public Key Infrastructure (PKI) certificates and appliances that do not.
- Registered—places the SonicWALL appliances into two groups: appliances that are registered and appliances that are not.
- VPN Present—places the SonicWALL appliances into two groups: appliances that have VPN and appliances that do not.
- Warranty Status—places the SonicWALL appliances into two groups: appliances that have current warranties and appliances that do not.

Setting Up Views

After creating custom fields and reviewing SonicWALL GMS fields, SonicWALL GMS administrators can set up views to perform different functions.

*Note: Each view can show a maximum of seven fields.*

Some views can include the following:

- Standard Geographic Views
  When the number of SonicWALL appliances managed by SonicWALL GMS becomes large, you can divide the appliances geographically among SonicWALL administrators.
  For example, if one administrator will be responsible for each time zone in the United States, you can choose the following grouping methods:
  - Administrator 1: Country: USA, Time Zone: Pacific, State, City.
  - Administrator 2: Country: USA, Time Zone: Mountain, State, City.
  - Administrator 3: Country: USA, Time Zone: Central, State, City.
  - Administrator 4: Country: USA, Time Zone: Eastern, State, City.

- Firmware Views
  To ensure that all SonicWALL appliances are using the current firmware, you can create a view to check and update firmware versions and batch process firmware upgrades when network activity is low.
  For example, if you want to update all SonicWALL appliances to the latest firmware at 2:00 A.M., you can use the following grouping method:
  - Firmware Version, Time Zone
  If you want to update SonicWALL appliances only for companies that have agreed to the upgrade and you want the upgrades to take place at 2:00 A.M., you can use the following grouping method:
  - Company, Firmware Version, Time Zone

- Registration Views
  To ensure that all SonicWALL appliances are registered, you can create a registration view and check it periodically. To create a registration view, you can use the following grouping method:
  - Registration Status, any other grouping fields

- Upgrade View
You can create views that contain information on which upgrades customers do not have and forward this information to the Sales Department.

For example, you can choose the following grouping methods:

- Content Filter List, Company, Division, Department
- Anti-Virus, Company, Division, Department
- Warranty Status, Company, Division, Department
Creating Views

To create a view, follow these steps:

1. Start and log into SonicWALL GMS.
2. Right-click anywhere in the left pane of the SonicWALL GMS window and select **Edit/Modify/Delete View** from the pop-up menu. The Edit/Modify/Delete View page appears (Figure 27).

**Figure 27: Edit View Page**

3. Enter the name of the new view in the **View Name** field. Save the view by clicking **Add View**.
4. To add a view category, click **Add Level**. These categories will be used to sort SonicWALL appliances in your view. The categories are a combination of custom fields and SonicWALL GMS fields. To change a field, type the name of the field in the **Group Category** field or select one by clicking the **Group Category** field. For a list of SonicWALL GMS fields and their meanings, see “SonicWALL Fields” on page 33.
5. You can add up to seven categories. Repeat Step 4 for each category that you would like to add.
6. To delete a view category, select the level and click **Delete Level**.
7. When you are finished configuring this view, click **Modify View**.
8. To add another view, repeat Steps 3 through 7.
9. When you are finished, click **Done**.

Changing Views

To change views from within the SonicWALL GMS UI, follow these steps:

1. Start and log into SonicWALL GMS.
2. Right-click anywhere in the left pane of the SonicWALL GMS window and select Change View from the pop-up menu. The Change View dialog box appears (Figure 28).

**Figure 28: Change View Dialog Box**

3. Select a view and click **OK**. The new view is displayed.
Adding SonicWALL Appliances to SonicWALL GMS

SonicWALL GMS communicates with SonicWALL appliances through VPN tunnels. SonicWALL GMS can communicate with SonicWALL appliances using individual management VPN tunnels or through site-to-site VPN tunnels that already exist between the SonicWALL appliances and the SGMS gateway.

To add a SonicWALL appliance to the SonicWALL GMS UI using the management VPN tunnel, follow these steps:

1. Start and log into SonicWALL GMS. The Status page appears (Figure 29).

   **Figure 29: Adding a SonicWALL Appliance**

   ![Adding a SonicWALL Appliance](image)

   2. Right-click in the left pane of the SonicWALL GMS UI and select **Add Unit** from the pop-up menu. The Add Unit dialog box appears (Figure 30).

   **Figure 30: Add Unit Dialog Box**

   ![Add Unit Dialog Box](image)

   3. Enter a descriptive name for the SonicWALL appliance in the **SonicWALL Name** field.
Note: Do not enter the single quote character (’) in the SonicWALL Name field.

4. Enter the password used to access the SonicWALL appliance in the SonicWALL Password field.

5. Select from the following:
   - If the WAN IP address of the SonicWALL appliance is static, enter it in the IP Address field.
   - If the WAN IP address of the SonicWALL appliance changes dynamically, leave the field blank.

SonicWALL GMS uses the IP address of the SonicWALL appliance to create a management SA. If a static IP address is used, it always uses the same address. If a dynamic IP address is used, SonicWALL GMS will receive notifications of IP address changes through the syslog data stream and update its database and the SGMS Gateway accordingly.

6. Enter the serial number of the SonicWALL appliance in the Serial Number field.

7. Enter a 16-character encryption key in the SA Encryption Key field. The key must be exactly 16 characters long and composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”
   
   Note: This key must match the encryption key of the SonicWALL appliance.

8. Enter a 32-character authentication key in the SA Authentication Key field. The key must be exactly 32 characters long and composed of hexadecimal characters. For example, a valid key would be “1234567890abcdef1234567890abcdef.”
   
   Note: This key must match the authentication key of the SonicWALL appliance.

9. If the SonicWALL appliance uses the Anti-Virus feature, enter the Anti-Virus password. Otherwise, leave the field blank.

10. Select the IP address of the SonicWALL GMS agent server that will manage the SonicWALL appliance from the Scheduler IP Address list box:
    - If SonicWALL GMS is configured in a two-tier distributed environment, you must select the SonicWALL GMS Agent whose IP address matches the IP address that you specified when configuring the SonicWALL appliance for SonicWALL GMS management.
    - If SonicWALL GMS is in a single-server environment, the IP address of the SonicWALL GMS agent server already appears in the field.

11. If SonicWALL GMS is configured in a two-tier distributed environment, enter the IP address of the backup SonicWALL GMS server in the Standby Scheduler IP field. The backup server will automatically manage the SonicWALL appliance in the event of a primary failure. Any Agent can be configured as the backup.
    
    Note: If SonicWALL GMS is in a single server environment, leave this field blank.

12. If you are trying to add a SonicWALL appliance over a site-to-site VPN tunnel that already exists between the SGMS gateway and the SonicWALL appliance, deselect the Establish a Management VPN Tunnel check box.

13. Click Properties. The Unit Properties dialog box appears (Figure 31).

   Figure 31: Unit Properties Dialog Box

   ![Properties Dialog Box]

14. This dialog box displays fields to which the SonicWALL appliance belongs. To change any of the values, enter a new value. When you are finished, click OK. You are returned to the Add Unit dialog box.

15. Click OK. The new SonicWALL appliance appears in the SonicWALL GMS UI. It will have a yellow icon that indicates it has not yet been successfully acquired.

The SonicWALL GMS will then attempt to establish a management VPN tunnel or use the existing site-to-site VPN tunnel to access the appliance, read its configuration, and acquire it for management. This will take a few minutes.
After the SonicWALL appliance is successfully acquired, its icon will turn blue, its configuration settings will be displayed at the unit level, and its settings will be saved to the database. A text version of this configuration file is also saved in `<sgms_directory>/etc/Prefs`.

**Note:** In two-tier distributed environment, both the primary and secondary SonicWALL GMS Agents must be configured to use management VPN tunnel or site-to-site VPN tunnel.

### Importing SonicWALL Appliances

To add a SonicWALL appliance to the SonicWALL GMS UI using the import option, follow these steps:

1. Start and log into SonicWALL GMS. The Status page appears (Figure 32).

   **Figure 32: Adding a SonicWALL Appliance**

2. Right-click in the left pane of the SonicWALL GMS UI and select Add Unit from the pop-up menu. The Add Unit dialog box appears (Figure 33).

   **Figure 33: Add Unit Dialog Box**

3. Enter a descriptive name for the SonicWALL appliance in the SonicWALL Name field.
4. Enter the password to access the SonicWALL appliance in the SonicWALL Password field.

5. Click **Import**. The Import dialog box appears (Figure 34).

**Figure 34: Import Dialog Box**

Note: Do not enter the single quote character (’) in the SonicWALL Name field.

![Import Dialog Box](image)

Note: If the above Import Dialog Box does not appear, you need to edit the java.policy file on your system. See “Using the Import Feature from Applet” on page 237.

6. Find and select the saved prefs file of the SonicWALL appliance. Click **Import**. You are returned to the Add Unit dialog box.

7. Click **Properties**. The Unit Properties dialog box appears (Figure 38).

**Figure 35: Unit Properties Dialog Box**

![Unit Properties Dialog Box](image)

8. This dialog box displays fields to which the SonicWALL appliance belongs. To change any of the values, enter a new value. When you are finished, click **OK**. You are returned to the Add Unit dialog box.

9. Click **OK**. The new SonicWALL appliance appears in the SonicWALL GMS UI. It will have a yellow icon that indicates it has not yet been successfully acquired.

The SonicWALL GMS will then attempt to establish a management VPN tunnel to the appliance, read its configuration, and acquire it for management. This will take a few minutes.

After the SonicWALL appliance is successfully acquired, its icon will turn blue, its configuration settings will be displayed at the unit level, and its settings will be saved to the database. A text version of this configuration file is also saved in `<sgms_directory>/etc/Prefs`. 
Registering SonicWALL Appliances

After successfully adding one or more SonicWALL appliances to the SonicWALL GMS UI, the next step is to register them. Registration is required for firmware upgrades, technical support, and more.

To register one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Register/Upgrades tree and click **Register SonicWALLs**. The Register SonicWALLs page appears (Figure 36).

**Figure 36: Register SonicWALLs Page**

4. Click **Register**. SonicWALL GMS creates a task for each SonicWALL appliance registration.

By default, SonicWALL GMS executes the tasks immediately. However, they can also be scheduled for another time and will remain in the schedule queue until they are executed. To view the status of these tasks, click the **Console** tab. Then, expand the Tasks tree and click **Scheduled Tasks**.

During the task execution, SonicWALL GMS registers each selected SonicWALL appliance using the information that you used to register with the SonicWALL registration site. After registration is complete, the task will be removed from the Scheduled Tasks page and the status of the task execution will be logged. To view these logs, click the **Console** tab. Then, expand the Log tree and click **View Log**.
Moving SonicWALL Appliances Between Groups

To move SonicWALL appliances between groups, simply change the properties of their custom fields. To change these properties, follow these steps.

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance or group in the left pane of the SonicWALL GMS UI (Figure 37).

   Figure 37: Moving a SonicWALL Appliance

3. Right-click the appliance or group and select Properties from the pop-up menu. The Unit Properties dialog box appears (Figure 38).

   Figure 38: Unit Properties Dialog Box

4. Make any changes to the categories to which the SonicWALL appliance or group of appliances belongs. For information on creating categories, see “Creating SonicWALL Fields and Views” on page 31.
5. Click OK. The SonicWALL appliance(s) are moved to the new group.
Inheriting Group Settings

If you move SonicWALL appliances between groups, the SonicWALL appliances can inherit the settings from the new group.

To move one or more SonicWALL appliances inheriting the group settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the SonicWALL appliance.
3. Expand the General tree and click **Tools**. The Tools page appears (Figure 39).

**Figure 39: Tools Page**

![Tools Page](image)

4. Click **Inherit Settings from Group**.
   
   You are prompted to continue.

5. To inherit the settings from the new group, click **OK**. To cancel without applying the group settings, click **Cancel**.
   
   One or more tasks are scheduled and the SonicWALL appliance(s) will receive the group settings.

**Note:** For the Access/Services and Access/Rules pages, by default, inheriting group settings overwrites the values at the unit level with the group values. If you wish for SonicWALL GMS to append the group settings to the values at the unit level, you need to enable the Append Group Settings option on the General/SGMS Settings page on the Console Panel.

**Note:** See Appendix C for the list of group values that get inherited at the unit level.
Overview

To operate in complex environments, the SonicWALL Global Management System (SonicWALL GMS) is designed to support multiple users, each with his or her own set of permissions and access rights. To add a new user, follow these steps:

- Select the group to which the new user will belong. If an appropriate group does not exist, you can create one. See “Creating User Groups” on page 44.
- Add the user and configure general settings. See “Adding Users” on page 46.
- Configure the screens to which the new user has access if they are different from the group settings. See “Configuring Screen Access” on page 47.
- Configure the SonicWALL appliances and Ravlin devices to which the new user has access if they are different from the group settings. See “Configuring Appliance Access” on page 48.

**Note:** If you do not want to restrict access to SonicWALL appliances or SonicWALL GMS functions, but want to divide SonicWALL GMS responsibility among multiple users, you can use views. Views use specific criteria to display groups of SonicWALL appliances or Ravlin devices. Depending on the type of task they are trying to perform, users can switch between these views as often as necessary. For more information, see “Setting Up Views” on page 33.
Creating User Groups

A user group is a group of SonicWALL GMS users who perform similar tasks and have similar permissions. SonicWALL GMS provides three preconfigured groups:

- Administrators—full view and update privileges.
- Operators—view privileges only.
- End Users—no privileges.

To create a new group, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the Console tab.
3. Expand the Management tree and click Users. The General Page of the User screen appears (Figure 40).

Figure 40: Adding a User Group: General Page

4. Right-click All Users and select Add User Types from the pop-up menu. A new user group appears.
5. Enter the name of the new user group.
6. Enter any comments regarding the new user group in the Comments field.
7. Select a default view for the new user group from the Default View pull-down menu. This view will be displayed for members of the user group when they first log in to SonicWALL GMS.
8. Click Update. The new user group is added. By default, the new group has no privileges. To configure screen access settings, see “Configuring Screen Access” on page 44.

Configuring Screen Access

The Screen Permissions page contains a hierarchical list of all screens that appear within SonicWALL GMS. From this screen, you can control access to sections or individual screens.

To configure screen access settings for a user group, follow these steps:
1. Open the Users configuration screen.
2. Select the new user group.
3. Click the **Screen Permissions** tab (Figure 41).

![Figure 41: Adding a User Group: Screen Permissions Page](image)

4. Select a panel, section, or screen.

5. Select from the following:
   - To allow unrestricted access to the object, select View and Update and click **Update**. The object will be preceded by a ![access_icon].
   - To allow view only access, select View Only and click **Update**. The object will be preceded by a ![view_icon].
   - To prevent any access to the object, select None and click **Update**. The object will be preceded by a ![block_icon].

   **Note:** By default, a new user group has no privileges.

6. To clear all screen settings and start over, click **Reset**.

   **Note:** You can allow access rights to multiple panels, sections, or screens.

### Configuring Appliance Access

The Appliance Permissions page contains a hierarchical list of all SonicWALL appliances and Ravlin devices that appear within SonicWALL GMS. From this screen, you can control access to SonicWALL groups or individual SonicWALL appliances and Ravlin devices.

To configure appliance access settings for a group, follow these steps:

1. Open the Users configuration screen.
2. Select the user group.
3. Click the **Unit Permissions** tab (Figure 45).
Figure 42: Adding a User Group: Unit Permissions Page

4. Select a View from the Views pull-down menu.
5. To provide the group with access to a SonicWALL group or appliance, select a SonicWALL group or appliance in the left pane of the window and click Add. The group or appliance appears in the right pane.
6. Repeat Step 5 for each group or appliance to add.
7. To prevent the group from accessing a SonicWALL group or appliance, select the group or appliance in the right pane of the window and click Remove. The group or appliance moves to the left pane.
8. Repeat Step 7 for each group or appliance to remove.

Adding Users

This section describes how to create a new user. Although the user will inherit all group settings, individual user settings will override the group settings.

To add a new user, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the Console tab.
3. Expand the Management tree and click Users. The General Page of the User configuration screen appears (Figure 43).
4. Right-click a user group and select Add User from the pop-up menu. The Add User window appears.

5. Enter a username and click OK; enter a password and click OK. The new user appears beneath the group to which it is assigned.

   **Note:** The username and password are case-sensitive. Do not enter the single quote character (') in the User ID field.

6. Select the new user.

7. Enter the full name of the user in the Name field.

8. Enter contact information for the user in the Phone, Fax, Pager, and Email fields.

9. Select the default view for the user from the Default View list box.

10. Enter any comments regarding the new user in the Comments field.

11. Click Update. The new user is added.

   If the user will inherit the user permissions from the group user settings, you are finished.

   If the user settings will be different than the group user settings, see “Configuring Screen Access,” below and “Configuring Appliance Access” on page 48.

   **Note:** To temporarily disable a user account, select the Account Disabled check box and click Update.

---

**Configuring Screen Access**

The Screen Permissions page contains a hierarchical list of all screens that appear within SonicWALL GMS. From this screen, you can control access to screens or all screens within a section.

To configure screen access settings for a user, follow these steps:

1. Open the User configuration screen.

2. Select a user.

3. Click the Screen Permissions tab (Figure 44).
4. Select a panel, section, or screen.

5. Select from the following:
   - To allow unrestricted access to the object, select View and Update and click Update. The object will be preceded by a .
   - To allow view only access, select View Only and click Update. The object will be preceded by a .
   - To prevent any access to the object, select None and click Update. The object will be preceded by a .

6. To clear all screen settings and start over, click Reset.

   **Note:** You can allow access rights to multiple panels, sections, or screens.

### Configuring Appliance Access

The Appliance Permissions page contains a hierarchical list of all SonicWALL appliances and Ravlin devices that appear within SonicWALL GMS. From this screen, you can control access to SonicWALL and Ravlin groups or individual SonicWALL appliances and Ravlin devices.

To configure appliance access settings for a user, follow these steps:

1. Open the Users configuration screen.

2. Select a user.

3. Click the **Unit Permissions** tab (Figure 45).
4. Select a View from the Views pull-down menu.

5. To provide the user with access to a SonicWALL group or appliance, select a SonicWALL group or appliance in the left pane of the window and click Add. The group or appliance appears in the right pane.

6. Repeat Step 5 for each group or appliance to add.

7. To prevent the user from accessing a SonicWALL group or appliance, select the group or appliance in the right pane of the window and click Remove. The group or appliance is deleted from the right pane.

8. Repeat Step 7 for each group or appliance to remove.
Section II
SonicWALL Appliances
The SonicWALL Global Management System (SonicWALL GMS) user interface (UI) is similar to the standard SonicWALL appliance UI. However, SonicWALL GMS offers the ability to push configuration settings to a single SonicWALL appliance, a group of SonicWALL appliances, or all SonicWALL appliances being managed by the SonicWALL GMS.

For example, to change the time for all SonicWALL appliances within a group, select the group, expand the General tree, and click Time. The Time page appears (Figure 46).

Figure 46: Time Page

When you have finished making changes, click Update. The changes become tasks and are applied to all SonicWALL units within the group.

Note: For detailed information on making changes to the Time page and other pages in the Policies Panel, refer to the other chapters of this section.

To view the status of these tasks, click the Console tab. Then expand the SonicWALL GMS Tasks tree and click Scheduled Tasks. The Scheduled Tasks page appears (Figure 47).
The task appears in the Scheduled Tasks page. After a task is successfully applied to a SonicWALL appliance, the task is removed from the page.

**Note:** The status of task execution is logged on the View Log page. For more information, see Chapter 7, “Configuring Log Settings.”

SonicWALL GMS provides a scheduling engine. Once a configuration policy is defined for a SonicWALL appliance or a group of SonicWALL appliances, SonicWALL GMS schedules a task for this policy for each SonicWALL appliance.

By default, SonicWALL GMS queues and executes tasks immediately. To configure SonicWALL GMS to execute tasks when network activity is low, you can schedule them for a specific window of operation. To do this, configure the default task execution schedule. For more information, see “Managing Agent Configurations” on page 226.

If you configure tasks to execute at a specific time, but need to execute one or more tasks now, you can execute the tasks immediately from the Scheduled Tasks page. You can also reschedule the tasks for a specific time outside of the scheduled window of operation. For more information, see “Working with SonicWALL GMS Tasks” on page 224.
Configuring Network Settings

When configuring new or existing SonicWALL appliances, it is important to make sure that the network and general settings are correct.

This chapter describes how to use the SonicWALL Global Management System (SonicWALL GMS) to configure general SonicWALL settings. Select from the following:

- **Network Settings**—describes how to configure the network settings of the SonicWALL appliance(s). See “Configuring Network Settings” on page 56.
- **Time**—describes how to change the time and time options for one or more SonicWALL appliances. See “Configuring Time Settings” on page 62.
- **SonicWALL Password**—describes how to change passwords for one or more SonicWALL appliances. See “Changing the SonicWALL Password” on page 63.
Configuring Network Settings

Note: In order for changes on this page to take effect, the SonicWALL appliance will automatically restart. We recommend scheduling the tasks to run when network activity is low.

The Network settings page is used to configure the network addressing mode, LAN (WorkPort) settings, WAN settings, DMZ (HomePort) settings, and the DNS server address(es).

Note: The Network settings page cannot be used at the Global and Group levels, except for configuring the DNS server address(es).

Before configuring any settings, it is important to determine the network addressing mode. These options include:

- **Standard**—see “Standard Mode,” below.
- **NAT Enabled**—see “NAT-Enabled Mode” on page 57.
- **NAT with Dynamic Host Configuration Protocol (DHCP) Client**—see “NAT with DHCP Client Mode” on page 58.
- **NAT with PPP over Ethernet (PPPoE) Client**—see “NAT With PPPoE Client” on page 59.
- **NAT with L2TP Client**—see “NAT With L2TP Client” on page 60.

Standard Mode

When you select Standard Mode, Network Address Translation (NAT) is disabled. All nodes on the LAN or WorkPort that will access or be accessed from the Internet must use valid, Internet-accessible IP addresses.

To configure a SonicWALL appliance for standard network addressing, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click **Network**.
4. Select **Standard** from the Network Addressing Mode area. The Network page appears (Figure 48).

**Figure 48: Network Page: Standard Mode**
5. Configure the following LAN (WorkPort) Settings:
   - **SonicWALL LAN (WorkPort) IP Address**—IP address assigned to the SonicWALL LAN or WorkPort interface. This address is also used for configuration and monitoring.
   - **LAN (WorkPort) Subnet Mask**—Determines the subnet to which the LAN or WorkPort IP address belongs.

6. To add an additional subnet, enter the IP address and subnet in the **Network Gateway** and **Subnet Mask** fields.

7. Configure the following WAN Settings:
   - **WAN Gateway (Router) Address**—Address of the router that provides Internet access to SonicWALL appliances.
   - **SonicWALL WAN IP Address**—This value is automatically set to the SonicWALL LAN (WorkPort) IP Address.
   - **WAN/DMZ (HomePort) Subnet Mask**—This value is automatically set to the LAN (WorkPort) Subnet Mask.

8. Enter the IP addresses of the DNS servers in the Other Settings area (maximum of three IP addresses). SonicWALL appliances require the IP address of at least one DNS server to function properly.

9. When you are finished, click **Update**. The settings are changed for the selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### NAT-Enabled Mode

NAT provides anonymity to machines on the LAN or WorkPort by connecting the entire network to the Internet using a single IP address. This provides security to the internal machines by hiding them from the outside world and conserves IP addresses.

When using NAT, we recommend using internal network IP addresses from a special range. The following IP address ranges are reserved for private IP networks and are not routed on the Internet:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

**Note:** If your network uses IP addresses that are not registered to your organization and are not within the private IP address ranges, the servers on the Internet to which those IP addresses belong will not be accessible from your network. For example, if an IP address on your network is 185.5.20.105 and it is not registered to your organization, the server that uses that IP address on the Internet will not be accessible from your network.

If you choose to use NAT, but need to make some machines available to the outside world, use One-to-One NAT. One-to-One NAT maps external IP addresses to private IP addresses. For more information, see “Configuring One-to-One Network Address Translation” on page 103.

To configure a SonicWALL appliance for NAT, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click **Network**.
4. Select NAT Enabled from the Network Addressing Mode area. The Network page appears (Figure 49).
5. Configure the following LAN (WorkPort) Settings:
   - **SonicWALL LAN (WorkPort) IP Address**—IP address assigned to the SonicWALL LAN or WorkPort interface. This address is also used for configuration and monitoring.
   - **LAN (WorkPort) Subnet Mask**—Determines the subnet to which the LAN or WorkPort IP address belongs.

6. To add an additional subnet, enter the IP address and subnet in the **Network Gateway** and **Subnet Mask** fields.

7. Configure the following WAN Settings:
   - **WAN Gateway (Router) Address**—Address of the router that attaches the LAN or WorkPort to the Internet.
   - **SonicWALL WAN IP (NAT Public) Address**—Public IP address used to access the Internet. All activity on the Internet will appear to originate from this address. This IP address must be valid and is generally supplied by your Internet Service Provider (ISP).
   - **WAN/DMZ (HomePort) Subnet Mask**—Determines the subnet to which the public IP address belongs. This is generally supplied by your ISP.

8. Enter the IP addresses of the DNS servers in the Other Settings section (maximum of three IP addresses). SonicWALL appliances require the IP address of at least one DNS server to function properly.

9. When you are finished, click **Update**. The settings are changed for the selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### NAT with DHCP Client Mode

When you select the NAT with DHCP Client mode, the SonicWALL appliance uses DHCP to obtain a dynamic IP address from the ISP and NAT. For more information on NAT, see “NAT-Enabled Mode” on page 57. For more information on configuring DHCP, see Chapter 10, “Configuring Dynamic Host Configuration Protocol.”

To configure a SonicWALL appliance for NAT with a DHCP client, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click **Network**. The Network page appears (Figure 50).

**Figure 50: Network Page: NAT with DHCP Client Mode**

4. Select **NAT with DHCP Client** from the Network Addressing Mode area.

5. Configure the following LAN (WorkPort) Settings:
   - **SonicWALL LAN (WorkPort) IP Address**—IP address assigned to the SonicWALL LAN (WorkPort) interface. This address is also used for configuration and monitoring.
   - **LAN (WorkPort) Subnet Mask**—Determines the subnet to which the LAN or WorkPort IP address belongs.
   - To add an additional subnet, enter the IP address and subnet in the **Network Gateway** and **Subnet Mask** fields.
   - The WAN settings and the DNS server IP addresses are automatically provided by the DHCP server of the service provider. You do not need to configure any parameters in the WAN Settings area.
   - In the Other Settings area, enter the name of the DHCP server in the **Host Name** field.

6. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### NAT With PPPoE Client

When you select the NAT with PPPoE Client mode, the SonicWALL appliance uses PPP over Ethernet (PPPoE) to connect to the Internet. PPPoE is required by some ISPs to authenticate users over broadband Internet access devices (e.g., DSL, cable modems, wireless).

**Note:** When this mode is selected, the **SonicWALL LAN (WorkPort) IP Address** is used as the gateway address for computers on the LAN or WorkPort.

To configure a SonicWALL appliance for NAT with PPPoE, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click **Network**.
4. Select NAT with PPPoE Client from the Network Addressing Mode area. The Network page appears (Figure 51).

Figure 51: Network Page: NAT With PPPoE Client Mode

5. Configure the following LAN (WorkPort) Settings:
   - **SonicWALL LAN (WorkPort) IP Address**—IP address assigned to the SonicWALL LAN or WorkPort interface. This address is also used for configuration and monitoring.
   - **LAN (WorkPort) Subnet Mask**—Determines the subnet to which the LAN or WorkPort IP address belongs.

6. To add an additional subnet, enter the IP address and subnet in the **Network Gateway** and **Subnet Mask** fields.

7. Configure the following ISP Settings:
   - **User Name**—username provided by the ISP.
   - **Password**—password used to authenticate the username with the ISP. This field is case-sensitive.

8. To specify how long the SonicWALL appliance waits before disconnecting from the Internet, enter the amount of time in the inactivity field.

9. Select from the following:
   - To configure the SonicWALL appliance(s) to dynamically obtain an IP address, select **Obtain an IP Address automatically**.
   - To configure the SonicWALL appliance(s) to use a fixed IP address, select **Use the following IP Address** and enter the IP address.

10. When you are finished, click **Update**. The settings are changed for the selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

**NAT With L2TP Client**

When you select the NAT with L2TP Client mode, the SonicWALL appliance uses Layer Two Tunneling Protocol (L2TP) to connect to the Internet.

*Note: When this mode is selected, the SonicWALL LAN (WorkPort) IP Address is used as the gateway address for computers on the LAN or WorkPort.*
To configure a SonicWALL appliance for NAT with PPPoE, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click **Network.**
4. Select NAT with L2TP Client from the Network Addressing Mode area. The Network page appears (Figure 52).

**Figure 52: Network Page: NAT With L2TP Client Mode**

5. Configure the following LAN (WorkPort) Settings:
   - **SonicWALL LAN (WorkPort) IP Address**—IP address assigned to the SonicWALL LAN or WorkPort interface. This address is also used for configuration and monitoring.
   - **LAN (WorkPort) Subnet Mask**—Determines the subnet to which the LAN or WorkPort IP address belongs.

6. To add an additional subnet, enter the IP address and subnet in the **Network Gateway** and **Subnet Mask** fields.

7. Select from the following WAN settings:
   - To configure the SonicWALL appliance to dynamically obtain an IP address, select **Obtain an IP address using DHCP**.
   - To configure the SonicWALL appliance to use fixed settings, select **Use the specified IP address** and enter the following:
     - **SonicWALL WAN IP (NAT Public) Address**—Public IP address used to access the Internet. All activity on the Internet will appear to originate from this address. This IP address must be valid and is generally supplied by your Internet Service Provider (ISP).
     - **WAN Gateway (Router) Address**—Address of the router that attaches the LAN (WorkPort) to the Internet.
     - **WAN/DMZ (HomePort) Subnet Mask**—Determines the subnet to which the public IP address belongs. This is generally supplied by your ISP.

8. Enter the IP address of the DNS server in the **DNS Server 1** field.
9. Configure the following ISP L2TP Settings:
   - **L2TP Host Name**—this information is provided by your ISP.
   - **L2TP Server IP Address**—this information is provided by your ISP.
   - **User Name**—username provided by the ISP.
   - **Password**—password used to authenticate the username with the ISP. This field is case-sensitive.

10. To specify how long the SonicWALL appliance(s) wait before disconnecting from the Internet, select the **Disconnect after** check box and enter the amount of time.

11. When you are finished, click **Update**. The settings are changed for the selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

## Configuring Time Settings

To change time settings on one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the General tree and click **Time**. The Time page appears (Figure 53).

   **Figure 53: Time Page**

4. Select the Time Zone of the appliance(s) from the **Time Zone** field.

5. To configure the SonicWALL(s) to automatically adjust their clocks for Daylight Savings Time, select the **Automatically Adjust Clock for Daylight Savings Changes** check box.

6. To configure the SonicWALL(s) to use Universal Time Coordinated (UTC) or Greenwich Mean Time (GMT) instead of local time, select the **Display UTC in Logs Instead of Local Time** check box.

7. To configure the SonicWALL(s) to display the time in the international time format, select the **Display Time in International Format** check box.

8. Select from the following:
   - To manually configure the time and date, make sure the **Use NTP to set time automatically** check box is deselected. The SonicWALL appliance(s) will automatically use the time settings of the SonicWALL GMS agent.
   - To configure the SonicWALL(s) to automatically set the local time using Network Time Protocol (NTP), select the **Use NTP to set time automatically** check box.
9. When you are finished, click **Update**. A task gets scheduled to apply the new settings for each selected appliance.

10. If you don’t want to use the SonicWALL appliance’s internal NTP list, you can add your own NTP list. To add an NTP server, enter the IP address of an NTP server in the **Add NTP Server** field.

   A task gets scheduled to add the NTP server to each selected SonicWALL appliance.

   **Note:** To add additional NTP servers, click **Add** and enter another NTP server.

11. To clear all screen settings and start over, click **Reset**.

---

### Changing the SonicWALL Password

To change the password of a SonicWALL appliance, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click **Password**. The Password page appears (Figure 54).

   **Figure 54: Password Page**

   ![Password Page](image)

4. Enter a password for the SonicWALL appliance.
5. Confirm the password by reentering it.
6. Enter the SonicWALL GMS password.
7. When you are finished, click **Update**. A task gets spooled and once it is executed successfully, the password is changed for the selected SonicWALL appliance.

   **Note:** If you selected the global icon or a group, you will need to enter the SonicWALL GMS password. Each SonicWALL appliance will receive a unique randomly generated password. This unique password is encrypted and recorded in the SonicWALL GMS database.

   **Note:** The unique encrypted password is also written into a file in `<sgms_directory>/etc/Prefs`. File name format is `<serialnumber>.pwd`; each file contains the old and the new password for the SonicWALL appliance. The file gets overwritten every time the password for the SonicWALL appliance is changed. The encryption is base64.
Note: If you need to change the unique encrypted password for a SonicWALL appliance, perform steps 2 through 7.

Saving and Applying SonicWALL Settings

SonicWALL GMS enables you to save SonicWALL appliance settings to the SonicWALL GMS database or a file which can be used for restoration purposes. To save or apply SonicWALL appliance settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance
3. Expand the General tree and click Settings. The Settings page appears (Figure 55).

Figure 55: Settings Page

4. To save the settings of a SonicWALL appliance to the SonicWALL GMS database, enter a name for the settings in the Name field and click Store settings read from unit. Then, if you want to save these settings to a local file, click Save the settings to a local file. You can save multiple version of settings for each SonicWALL appliance to the SonicWALL GMS database and to different local files.

5. To apply settings to the SonicWALL appliance directly from SonicWALL GMS database, select the saved settings and click Restore the settings to the unit.

6. To restore settings from a file to the SonicWALL appliance, enter the path to the file and click Store settings from local file.

7. To delete settings from the SonicWALL GMS database, select the saved settings and click Delete the settings.
Configuring Log Settings

This chapter describes how to use the SonicWALL Global Management System (SonicWALL GMS) to configure where the SonicWALL appliance(s) send their logs, how often the logs are sent, and what information is included.

To configure log settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Log tree and click Log Settings. The Log Settings page appears (Figure 56).

*Figure 56: Log Settings Page*

4. Enter the IP address of the mail server in the Mail Server IP Address field.
5. Enter the name of the SonicWALL appliance in the Firewall Name field. The firewall name appears in the subject of email sent by the SonicWALL appliance. By default, the firewall name is the same as the SonicWALL appliance serial number.

*Note:* The name of the SonicWALL appliance cannot be configured at the group or global level.

6. Select a syslog format:
   - **Default**—standard SonicWALL syslog format.
   - **WebTrends**—reporting software that analyzed traffic activity, protocol usage, security problems, resource usage, bandwidth consumption, and more. For more information, visit [http://www.webtrends.com](http://www.webtrends.com).
7. The Syslog Event Rate prevents repetitive events from being logged to the syslog. If duplicate events occur during the specified period, they will be logged as a single event that specifies the number of times that the event occurred.

To specify how often SonicWALL GMS logs repetitive events, enter the period in the **Syslog Event Rate** field (default: 60 seconds). The minimum is 0 seconds and the maximum is 86,400 seconds (24 hours). If you specify 0, all events are logged.

**Note:** If you are using ViewPoint reporting, make sure the Syslog Event Rate is set to 0. Otherwise, ViewPoint reports will not be accurate.

8. Specify how often the SonicWALL appliance(s) send heartbeats to SonicWALL GMS in the **Heartbeat Rate** field (default: 60 seconds). If SonicWALL GMS does not receive a heartbeat message within three intervals, SonicWALL GMS will consider the SonicWALL appliances offline or unavailable and its icon will turn red.

**Note:** It is highly recommended to leave the Heartbeat Rate at the default setting of 60 seconds. Values close to zero will generate a large number of status messages. The maximum value is 86400 seconds (24 hours).

9. Enter the complete email address (for example, administrator@company.com) where the log will be sent in the **Email Log to** field. If this field is left blank, the log will not be sent.

**Note:** This address will also be used as the return address.

10. Some events, such as an attack, may require immediate attention. Enter the complete email address or email pager address in the **Email Alerts to** field. If this field is left blank, alerts will not be sent.

**Note:** This address will also be used as the return address.

11. Select when the log file will be sent from the **Send Log** list box. Options include daily, weekly, or when log is full. If the log will be sent daily, select the time that the log will be sent (24 hour format). If the log will be sent weekly, select the time and day of the week.

12. In some cases, the log buffer may fill up. This may occur if there is a problem with the mail server and the log cannot be successfully emailed. By default, SonicWALL appliances will overwrite the log and discard its contents. To prevent any further traffic from traveling through without being logged, select **Shutdown SonicWALL**.

13. Select information to log:

- **System Maintenance**—logs messages showing general system maintenance activity, such as administrator logins, automatic loading of Content Filter Lists, activation, and restarting SonicWALL PRO (default: enabled).
- **System Errors**—logs messages showing problems with DNS, Email, and automatic Content Filter List loading (default: enabled).
- **Blocked Web Sites**—logs messages showing Web sites, newsgroups, or other services blocked by the Content Filter List, by keyword, or for any other reason (default: enabled).
- **Blocked Java, ActiveX, and Cookies**—logs messages showing Java, ActiveX, and Cookies that are blocked by SonicWALL PRO (default: enabled).
- **User Activity**—logs messages showing any successful or unsuccessful user logins (default: enabled).
- **VPN TCP Stats**—logs messages showing errors that occur while the VPN tunnel is active (default: enabled).
- **Attacks**—logs messages showing SYN Floods, Ping of Death, IP Spoofing, and attempts to manage SonicWALL PRO from the Internet (default: enabled).
- **Dropped TCP**—logs messages showing blocked incoming Transmission Control Protocol (TCP) connections (default: enabled).
- **Dropped UDP**—logs messages showing blocked incoming User Datagram Protocol (UDP) packets (default: enabled).
- **Dropped ICMP**—logs messages showing blocked incoming Internet Control Message Protocol (ICMP) packets (default: enabled).
- **Network Debug**—logs messages showing Ethernet broadcasts, Address Resolution Protocol (ARP) resolution problems, ICMP redirection problems, and NAT resolution problems (default: disabled).
- **Denied LAN (WorkPort) IP**—logs messages showing blocked LAN IP connections (default: disabled).
- **Attacks**—logs an entry categorized as an Attack as an alert message (default: enabled).
- **System Errors**—logs an entry categorized as a System Error as an alert message (default: enabled).
- **Blocked Web Sites**—logs a Blocked Web Site entry as an alert message (default: enabled).

**Note:** If you are using SonicWALL GMS ViewPoint, make sure that it can generate all reports for each SonicWALL appliance by selecting all log category check boxes.
14. To immediately send the log to the specified email address now, click **Email Log Now**.

15. To delete the contents of the log, click **Clear Log Now**.

16. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
This chapter describes how to use SonicWALL Global Management System (SonicWALL GMS) to configure one or more SonicWALL appliances’ website blocking options. This functionality can be used to deny access to material supplied by the active content filtering subscription, specific domains, domains by keyword, and web features such as ActiveX, Java, and cookies.

To configure website blocking features, select from the following:

- **General Options**—configure when SonicWALL blocks access to the selected content and whether access is blocked or only logged. See “Configuring General Website Blocking Options” on page 70.
- **Content Subscription Material**—select which material will be blocked when you sign up for an active content filtering subscription. See “Selecting the Content to Block” on page 71.
  
  **Note:** SonicWALL appliances are entitled to a one-month content filter trial subscription. To enable the trial subscription, see “Adding the Content Filter List to SonicWALL Appliances” on page 157.
- **Domain Blocking**—block access to specific domains. See “Controlling Access to Specific Domains” on page 73.
- **Domains Keyword Blocking**—block access to domains by keyword. See “Blocking Access to Domains by Keywords” on page 75.
- **Feature Blocking**—block access to web features such as ActiveX, Java, and cookies. See “Blocking Web Features” on page 76.
Configuring General Website Blocking Options

The General page is used to configure whether access to restricted content, sites, and features is blocked or logged, when users can access blocked material (if ever), and the message that will be displayed when users attempt to access blocked material.

In addition to the SonicWALL content filtering service, SonicWALL now supports two other content filtering packages: N2H2 and Websense Enterprise. To configure filtering options for N2H2 or Websense, view the documentation that came with the software package.

To configure general blocking options, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click General. The Website Blocking General page appears (Figure 57).

   Figure 57: Website Blocking General Page

4. Select the content filtering package that you will use:
   - SonicWALL—standard content filtering package. To configure SonicWALL content filtering, see “Selecting the Content to Block” on page 71.
   - N2H2—To use N2H2, you must have the N2H2 software package running on a server in your network. For more information, visit www.n2h2.com.
   - Websense—To use Websense, you must have the Websense Enterprise software package running on a server in your network. For more information, visit www.websense.com.

   Note: If you select N2H2 or Websense, make sure to configure their filtering options. For more information, see “Websense and N2H2 Content Filtering” on page 79.

5. To apply content filtering to and web feature restrictions to the LAN port (WorkPort), select LAN/WorkPort.
6. To apply content filtering to and web feature restrictions to the DMZ port (HomePort), select DMZ/HomePort.
7. Select one of the following:
   - Always Block—Always blocks access to all restricted content, sites, and features.
   - Block From—Blocks access to restricted content, sites, and features between the selected hours.
8. Select one of the following:
   - **Log and Block Access**—Blocks access to restricted content, sites, and features and logs access attempts.
   - **Log Only**—Does not block access to restricted content, sites, and features, but logs access. This enables organizations to monitor appropriate usage without restricting access.

9. Enter the message that will be displayed when users attempt to access restricted content, sites, and features. For example, “This material is restricted. Get back to work.”

10. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

11. Continue to the next section, “Selecting the Content to Block.”

---

**Selecting the Content to Block**

The Filter List page defines categories of website content that will be blocked and when the SonicWALL appliance(s) will download the content filter list.

*Note: This page does not affect N2H2 or Websense content filtering. For information on configuring filtering options for these software packages, refer to their documentation.*

To configure the filter list, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click **Filter List**. The Website Blocking Filter List page appears (Figure 58).

**Figure 58: Website Blocking Filter List Page**

4. Select the content to block:
   - **Violence/Profanity**—Includes pictures or text exposing extreme cruelty, or physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. Obscene words, phrases, and profanity are defined as text that uses, but is not limited to, George Carlin’s seven censored words more often than once every 50 messages (Newsgroups) or once a page (Web sites).
• **Partial Nudity**—Pictures exposing the female breast or full exposure of either male or female buttocks, except when exposing genitalia. Excludes all swimsuits, including thongs.

• **Full Nudity**—Pictures exposing any or all portions of the human genitalia. Excludes sites containing nudity or partial nudity of a wholesome nature. For example, web sites hosted by publications such as National Geographic or Smithsonian Magazine and museums such as the Guggenheim, the Louvre, or the Museum of Modern Art are not blocked.

• **Sexual Acts (graphics or text)**—Pictures or text exposing anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior, including masturbation, copulation, pedophilia, and intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. This also includes phone sex ads, dating services, adult personals, CD-ROMs, and videos.

• **Gross Depictions (graphics or text)**—Pictures or descriptive text of anyone or anything that are crudely vulgar or grossly deficient in civility or behavior, or that show scatological impropriety. For example, maiming, bloody figures, or indecent depiction of bodily functions.

• **Intolerance (graphics or text)**—Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Includes any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

• **Satanic/Cult (graphics or text)**—Pictures or text advocating devil worship, an affinity for evil or wickedness, or the advocacy to join a cult. A cult is defined as a closed society headed by a single individual where loyalty is demanded and leaving is punishable.

• **Drugs/Drug Culture (graphics or text)**—Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual’s state of mind, such as glue sniffing. Excludes currently illegal drugs legally prescribed for medicinal purposes (e.g., drugs used to treat glaucoma or cancer).

• **Militant/Extremist (graphics or text)**—Pictures or text advocating extremely aggressive and combative behaviors, or unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes “how to” information on weapons making, ammunition making, or the making or use of pyrotechnic materials. Also includes the use of weapons for unlawful reasons.

• **Sex Education (graphics or text)**—Pictures or text advocating the proper use of contraceptives. This topic includes condom use, the correct way to wear a condom and how to put a condom in place. Also included are sites relating to discussion about the use of the Pill, IUDs, and other types of contraceptives. In addition to the above, this includes discussion sites on discussing diseases with a partner, pregnancy, and respecting boundaries. Excluded from this category are commercial sites selling sexual paraphernalia.

• **Questionable/Illegal Gambling (graphics or text)**—Pictures or text advocating materials or activities of a dubious nature which that be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone’s phone lines without permission), and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports, and financial betting, including non-monetary dares.

• **Alcohol & Tobacco (graphics or text)**—Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

5. To configure the SonicWALL appliance(s) to download the content list weekly, select the **Automatically Download List Every** check box and select the day of the week and time when the download will occur.

   If you select this option, configure the SonicWALL appliance(s) to download the list at a time when network activity is low.

   **Note:** This option requires a subscription to the Content Filter List updates.

6. To download a new content filter list now, click the **Download Filter List Now** button.

7. Select from the following filter list expiration options:

   • To block access to all web sites except trusted domains thirty days after the filter list expires, select **Block traffic to all websites except for trusted domains.**

   • To allow access to all web sites thirty days after the filter list expires, select **Allow traffic access to all websites.**

8. When you are finished, click **Update.** The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset.**

9. Continue to the next section, “Controlling Access to Specific Domains.”
Controlling Access to Specific Domains

The Customization page is used to block or allow access to specific domain names. This enables an organization to block access to domains that are not in the content filter list, allow access to domains in the content filter list, or only allow access to specific domains.

Trusted domains are domains that users can access, regardless of whether they appear in the content filter list. Trusted domains are particularly useful for dedicated systems that are only allowed to access specific websites. Up to 256 entries are supported in the Trusted Domains list.

Forbidden domains are domains that users will not be allowed to access. This is useful when a website disrupts a corporate or educational environment. To find out which websites are most frequently accessed, refer to the Top Web Site Hits section of the log report. Up to 256 entries are supported in the Trusted Domains list.

To configure list customization options, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click Customization. The Customization page appears (Figure 59).

4. Enable list customization by selecting the Enable Filter List Customization check box.
5. To add a trusted domain, enter a domain name in the Trusted Domains field and click Add. Repeat this step for each trusted domain you would like to add.
   
   Note: Enter the domain name only. For example, “yahoo.com.” Do not include “http://.” Entering “yahoo.com” will also allow access to www.yahoo.com, my.yahoo.com, sports.yahoo.com, and so on.

6. To add a forbidden domain, enter a domain name in the Forbidden Domains field and click Add. Repeat this step for each forbidden domain you would like to add.
   
   Note: Enter the domain name only. For example, “bad-site.com.” Do not include “http://.” Entering “bad-site.com” will also block access to www.bad-site.com, really.bad-site.com, amazingly.bad-site.com, and so on.

7. To block access to all websites except for the listed trusted domains, select the Disable all web traffic except for Trusted Domains check box.
8. To allow Java, ActiveX controls, and cookies from domains in the Trusted Domains list, select the Don’t Block Java/ActiveX/Cookies to Trusted Domains check box.

9. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.

10. Continue to the next section, “Blocking Access to Domains by Keywords.”

Deleting Domains from the Domain Lists

To delete one or more domains from the Trusted Domain or Forbidden Domain lists, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click Customization.
4. Select an item to delete and click its check box below the trash can icon. Repeat this step for each domain that you want to remove from the domain lists.
5. When you are finished, click Update. The selected items are deleted.
Blocking Access to Domains by Keywords

The URL Keywords page is used to block access to domain names by keyword. This provides a second line of defense against objectionable material. For example, if the keyword “xxx” was included in the list, the site “www.new-site.com/xxx.html” would be blocked.

Note: Be careful when using this feature. For example, blocking the word “breast” can prevent access to both pornographic or objectionable sites and those on breast cancer.

To configure domain blocking by keyword, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click URL Keywords. The URL Keywords page appears (Figure 60).

Figure 60: URL Keywords Page

4. Enable keyword blocking by selecting the Enable Keyword Blocking check box.
5. Click Update. A task is scheduled that will apply the new setting to each selected SonicWALL appliance.
6. To add a keyword, enter the keyword and click Add. A task is scheduled to add the keyword to each selected SonicWALL appliance. Repeat this step for each keyword you would like to add.
7. To remove a keyword, select its check box below the trash can icon. Repeat this step for each domain that you want to remove from the domain lists.
8. Continue to the next section, “Blocking Web Features.”
9. To clear all screen settings and start over, click Reset.
Blocking Web Features

The Web Features page is used to block ActiveX Controls, Java, cookies, web proxy, and known fraudulent certificates. To block these features, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click Web Features. The Web Features page appears (Figure 61).

Figure 61: Web Features Page

4. Select objects to block:
   - **ActiveX**—blocks ActiveX controls. ActiveX is a programming language used to imbed small programs in web pages. It is generally considered insecure because it is possible for malicious programmers to write controls that can delete files, compromise security, or cause other damage.
   - **Java**—blocks Java applets. Java applets are downloadable web applications that are used on many websites. Selecting this option will block all Java applets, regardless of their function.
   - **Cookies**—prevents websites from placing information on user hard drives. Cookies are used by Web servers to track Web usage and remember user identity. Cookies can compromise users' privacy by tracking Web activities.
     
     *Note*: Blocking cookies on the public Internet creates a large number of accessibility problems. Most sites make extensive use of cookies to generate web pages and blocking cookies will make most e-commerce applications unusable.
   - **Access to HTTP Proxy Servers**—blocks users from accessing web proxy servers on the Internet to circumvent content filtering by pointing their computers to the proxy servers.
   - **Known Fraudulent Certificates**—blocks access to web content that originated from a known fraudulent certificate. Digital certificates help verify that web content originated from an authorized party.

5. To configure the SonicWALL appliance(s) to not block these web features from trusted domains, select the **Don’t Block Java/ActiveX/Cookies to Trusted Domains** check box. To add or remove domains from the trusted domains list, see “Controlling Access to Specific Domains” on page 73.

6. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

7. Continue to the next section, “Consent.”
Consent

The consent feature allows organizations to specify computers that are always filtered and computers that are filtered by user request. This feature is popular in libraries, Internet cafes, and other public Internet systems.

The following is an example of a consent web page (Figure 62).

**Figure 62: Sample Consent Page**

To configure the consent feature, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click Consent. The Consent page appears (Figure 63).
4. Select the **Require Consent** check box.

5. Enter the maximum time a user can access the Internet in the **Maximum Web Usage** field.

6. Specify the maximum amount of time (in minutes) a connection may remain idle before the user is logged out and must agree to the consent agreement again in the **User Idle Timeout** field.

7. When the consent feature is enabled, users must choose whether they want filtering. Configure the following:
   - Enter the URL of the web page from which users choose to enable filtering. This page appears when users first attempt to access the Internet and must contain a link for choosing unfiltered access and a link for choosing filtered access. The link for unfiltered access is `IPaddress/iAccept.html`. The link for filtered access is `IPaddress/iAcceptFilter.html`. `IPaddress` is the LAN (WorkPort) IP address of the SonicWALL appliance.
   - Enter the URL of the page that appears when users choose to access the Internet without content filtering in the **Consent Accepted URL (Filtering Off)** field. This page must be accessible on the LAN (WorkPort).
   - Enter the URL of the page that appears when users access the Internet with content filtering enabled in the **Consent Accepted URL (Filtering On)** field. This page must be accessible on the LAN (WorkPort).

8. When a user opens a web browser on a computer with mandatory content filtering they will be shown a consent page. You will need to create this Web page. It usually contains an Acceptable Use Policy and a notification that violations will be logged or blocked.

   This web page must reside on a web server that is accessible as a URL by LAN (WorkPort) users. This page must also contain a link that tells the SonicWALL appliance that the user agrees to having filtering enabled. To do this, create the following link:

   
   ```
   IPaddress/iAcceptFilter.html
   ```

   where `IPaddress` is the LAN (WorkPort) IP address of the SonicWALL appliance.

   Enter the URL of this page in the **Consent page URL (Mandatory Filtering)** field.

   Enter the IP address of a system that will be subject to mandatory filtering and click **Add**. Repeat this step for each system that will use mandatory filtering. Up to 128 IP addresses can be entered.

   To remove a system from the mandatory filtering list, highlight its IP address and click **Delete Address**.

9. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
Websense and N2H2 Content Filtering

This section describes additional filtering configuration options for N2H2 and Websense content filtering.

N2H2

To configure N2H2 content filtering options, follow these steps:
1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click N2H2. The N2H2 page appears (Figure 64).

   Figure 64: N2H2 Page

4. Enter the N2H2 server name or IP address in the Server Host Name or IP Address field.
5. Enter the port that the N2H2 server listens for N2H2 requests in the Listen Port field (default: 4005).
6. Enter the port that the N2H2 server uses to send packets to the SonicWALL appliances in the Reply Port field (default: 4005).
7. Enter the username associated with the N2H2 account in the User Name field.
8. Enter the size of the URL cache in the URL Cache Size field. A larger URL cache can improve browser response times.
9. Select the action that the SonicWALL appliance(s) will take if the N2H2 server is unavailable beyond the specified period of time:
   • To block traffic to all web sites, select Block traffic to all web sites.
   • To allow access to all web sites, select Allow traffic to all web sites.
10. Select one of the following:
    • Block Access to URL—Blocks access to restricted sites and logs access attempts.
    • Log Access to URL—Does not block access to restricted sites, but logs access. This enables organizations to monitor appropriate usage without restricting access.
11. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.
Websense

To configure Websense content filtering options, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Website Blocking tree and click Websense. The Websense page appears (Figure 65).

**Figure 65: Websense Page**

4. Enter the Websense server name or IP address in the **Server Host Name or IP Address** field.
5. Enter the port used for Websense packets in the **Server Port** field (default: 15666).
6. Enter the username associated with the Websense account in the **User Name** field.
7. Enter the size of the URL cache in the **URL Cache Size** field. A larger URL cache can improve browser response times.
8. Select the action that the SonicWALL appliance(s) will take if the Websense server is unavailable beyond the specified period of time:
   - To block traffic to all web sites, select **Block traffic to all web sites**.
   - To allow access to all web sites, select **Allow traffic to all web sites**.
9. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
To determine whether packets are allowed through the firewall, each SonicWALL checks the destination IP address, source IP address, and port against the network access rules.

**Note:** Network access rules take precedence over the default firewall functions. Because it is possible to disable all firewall protection or block all access to the Internet, use caution when creating or deleting network access rules. Network access rules do not disable protection from Denial of Service attacks such as SYN Flood, Ping of Death, LAND, and so on. However, it is possible to create vulnerabilities to attacks that exploit application weaknesses.

It is important to consider the purpose and ramifications of a rule before adding it to the network access rule list.

Use the following guidelines to determine the rule logic:

- What is the purpose of the rule? For example, “This rule will restrict all Internet Relay Chat (IRC) access from the LAN (WorkPort) to the Internet.” Or, “This rule will allow a remote Lotus Notes server to synchronize with our internal Notes server via the Internet.”
- Will the rule allow or deny traffic?
- What is the flow of the traffic: LAN (WorkPort) to Internet or Internet to LAN (WorkPort)?
- Which IP services will be affected?
- Which computers on the LAN (WorkPort) will be affected?
- Which computers on the Internet will be affected? Be as specific as possible. For example, if traffic is being allowed from the Internet to the LAN (WorkPort), it is better to only allow specific computers to access the LAN or WorkPort.

After determining the logic of the rule, consider the ramifications:

- Will this rule stop LAN (WorkPort) users from accessing important resources on the Internet? For example, if IRC is blocked, are there users who require this service?
- Can the rule be modified to be more specific? For example, if IRC is blocked for all users, will a rule that only blocks certain users be more effective?
- Will this rule allow Internet users to access LAN or WorkPort resources in a way that makes the LAN vulnerable? For example, if NetBIOS ports (UDP 137, 138, 139) are allowed from the Internet to the LAN, Internet users may be able to connect to PCs that have file sharing enabled.
- Does this rule conflict with other rules?
Understanding the Network Access Rules Hierarchy

The rule hierarchy uses two basic concepts:
- Specific rules override general rules.
- Equally specific Deny rules override Allow rules.

For example: a rule defining a specific service is more specific than the Default rule; a defined Ethernet link, such as LAN (WorkPort), or WAN, is more specific than * (all); and a single IP address is more specific than an IP address range.

Rules are listed in the LAN (WorkPort) Interface window from most specific to the least specific, and rules at the top override rules listed below.

To illustrate this, consider the Rules shown below.

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td>Chat (IRC)</td>
<td>206.18.25.4 (LAN)</td>
<td>148.178.90.55 (WAN)</td>
</tr>
<tr>
<td>2</td>
<td>Allow</td>
<td>Ping</td>
<td>199.2.23.0 - 199.2.23.255 (WAN)</td>
<td>206.18.25.4 (WAN)</td>
</tr>
<tr>
<td>3</td>
<td>Deny</td>
<td>Web (HTTP)</td>
<td>216.37.125.0 - 216.37.125.255 (WAN)</td>
<td>*</td>
</tr>
<tr>
<td>4</td>
<td>Allow</td>
<td>Lotus Notes</td>
<td>WAN</td>
<td>LAN (WorkPort)</td>
</tr>
<tr>
<td>5</td>
<td>Deny</td>
<td>News (NNTP)</td>
<td>LAN (WorkPort)</td>
<td>*</td>
</tr>
<tr>
<td>6</td>
<td>Deny</td>
<td>Default</td>
<td>*</td>
<td>LAN (WorkPort)</td>
</tr>
<tr>
<td>7</td>
<td>Allow</td>
<td>Default</td>
<td>LAN (WorkPort)</td>
<td>*</td>
</tr>
</tbody>
</table>

The Default Allow Rule (#7) at the bottom of the page allows all traffic from the LAN (WorkPort) out to the WAN. However, Rule #5 blocks all NNTP traffic from the LAN (WorkPort).

The Default Deny Rule (#6) blocks traffic from the WAN to the LAN (WorkPort). However, Rule #4 overrides part of this rule by allowing Lotus Notes into the LAN (WorkPort) from the WAN.

Defining Network Rules

After defining rules and understanding their ramifications, follow these steps:

1. Define a service. See “Adding a Service” on page 83.
2. Create one or more rules for the service. See “Creating Rules” on page 84.
3. Repeat this procedure for each service for which you would like to define rules.

Configuring General Access Settings

To configure general access settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Access tree and click General. The General page appears (Figure 66).
4. Computers running Microsoft Windows communicate with each other through NetBIOS broadcast packets. By default, SonicWALL appliances block these broadcasts. To configure the SonicWALL appliance(s) to allow NetBIOS packets to pass from the LAN (WorkPort) to the DMZ (HomePort), select the From LAN to DMZ or From WorkPort to HomePort check box.

5. To configure the SonicWALL appliance(s) to allow NetBIOS packets to pass from the LAN (WorkPort) to the WAN, select the From LAN to WAN or From WorkPort to WAN check box.

6. To enable stealth mode, select the Enable Stealth Mode check box. During normal operation, SonicWALL appliances respond to incoming connection requests as either “blocked” or “open.” During stealth operation, SonicWALL appliances do not respond to inbound requests, making the appliances “invisible” to potential hackers.

7. Hackers can use various detection tools to “fingerprint” IP IDs and detect the presence of a SonicWALL appliance. To configure the SonicWALL appliance(s) to generate random IP IDs, select the Randomize IP ID check box.

8. The Network Connection Inactivity Timeout option disables connections outside the LAN if they are idle for a specified period of time. Without this timeout, connections can stay open indefinitely and create potential security holes. To specify how long the SonicWALL appliance(s) wait before closing inactive connections outside the LAN, enter the amount of time in the Minutes field.

9. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.

Adding a Service

This section describes how to add a service.

To add a service, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Access tree and click Services. The Services page appears (Figure 67).
4. To add a known service (e.g., HTTP, FTP, News), select the service from the Service Name list box and click Add Known Service. Repeat this step for each service that you would like to add. A task is scheduled for each service for each selected SonicWALL appliance.

5. To add a custom service, enter its name in the Service Name field, enter the port range it uses in the Port Begin and Port End fields, select its protocol from the Protocol list box, and click Add Custom Service. Repeat this step for each service that you would like to add. A task gets scheduled for each service for each selected SonicWALL appliance.

6. To remove a service from the list, select its trash can check box and click Update. A task gets scheduled to update the services page for each selected SonicWALL appliance.

7. To clear all screen settings and start over, click Reset.

Creating Rules

This section describes how to define rules for defined services.

To create a rule, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Access tree and click Rules. The Rules page appears (Figure 68).

5. Select a service from the Service Name list box. If the service does not exist, see “Adding a Service” on page 83.

6. Select whether access to this service will be allowed or denied.

7. Select the SonicWALL interface to which this rule applies. Select whether this rule will apply to packets coming from the LAN (WorkPort), WAN, DMZ (HomePort), or all interfaces (*).
8. Specify the source IP address range. The rule will apply to requests originating from IP addresses within this range. For all IP addresses, enter an asterisk (*).

9. Specify the destination IP address range. The rule will apply to requests sent to IP addresses within this range. For all IP addresses, enter an asterisk (*).

10. Specify when the rule will be applied. By default, it is Always. To specify a time, enter the time of day (in 24-hour format) to begin and end enforcement. Then, enter the days of the week to begin and end rule enforcement.

11. Specify how long (in minutes) the connection may remain idle before the connection is terminated in the Inactivity Timeout field.

12. Fragmented packets are used in certain types of Denial of Service attacks and, by default, are blocked. You should only enable the Allow Fragmented Packets check box if users are experiencing problems accessing certain applications and the SonicWALL logs show many dropped fragmented packets.

13. SonicWALL appliances can manage outbound traffic using bandwidth management. To enable bandwidth management for this service, select the Enable Bandwidth Management check box.

   Enter the amount of bandwidth that will always be available to this service in the Guaranteed Bandwidth field. Keep in mind that this bandwidth will be permanently assigned to this service and not available to other services, regardless of the amount of bandwidth this service does or does not use.

   Enter the maximum amount of bandwidth that will be available to this service in the Maximum Bandwidth field.

   Select the priority of this service from the Bandwidth Priority list box. Select a priority from 0 (highest) to 7 (lowest).

   Note: In order to configure bandwidth management for this service, bandwidth management must be enabled on the SonicWALL appliance. For more information, see “Configuring Ethernet Settings” on page 105.

14. To add this rule to the rule list, click Update. Repeat Step 4 through Step 14 for each rule that you will add.

15. If the network access rules have been modified or deleted, you can restore the Default Rules. The Default Rules prevent malicious intrusions and attacks, block all inbound IP traffic and allow all outbound IP traffic. To restore the network access rules to their default settings, click Restore Rules to Defaults and click Update. A task is scheduled to update the rules page for each selected SonicWALL appliance.

16. If the network access rules for a SonicWALL appliance need to be uniform with access rules for other SonicWALL appliances in the same group, you can restore the group rules. To do this, click Restore Rules to Group Settings and click Update. A task is scheduled to overwrite the rules page for each selected SonicWALL appliance.

   If you want to append the group rules to the current rules, make sure the Append Services and Rules inherited from group check box is selected on the SGMS Settings page of the Console Panel.

   Note: This option is not available at the group or global level.

17. To modify a rule, select its notepad icon. The Add/Modify Rule dialog box appears. When you are finished making changes, click Update. SonicWALL GMS creates a task that modifies the rule for each selected SonicWALL appliance.

18. To disable a rule without deleting it, deselect its Enable Rule check box.

19. To delete a rule, select its trash can icon and click Update. SonicWALL GMS creates a task that deletes the rule for each selected SonicWALL appliance.

Creating Users

SonicWALL appliances can be configured to authenticate users through a Remote Authentication Dial-In User Service (RADIUS) server, a local user list, or a combination of both. If authenticated locally or a combination of locally and through RADIUS, SonicWALL appliances can also control user access privileges.

Note: In order for changes on this page to take effect, the SonicWALL(s) will automatically be restarted. We recommend configuring these options when network activity is low.

To add a user, follow these steps:

1. Start and log into SonicWALL GMS.

2. Select the global icon, a group, or a SonicWALL appliance.

3. Expand the Access tree and click Users. The Users page appears (Figure 70).
4. Specify the maximum amount of time (in minutes) a connection may remain idle before users are required to reestablish an authenticated session in the **User Idle Timeout** field. The timeout applies to both Remote Access and Bypass Filters. This value may range from 5 to 99 minutes.

5. Enter the maximum amount of time a user may remain logged in through the SonicWALL appliance in the **Maximum user login time** field. To allow indefinite access, enter 0.

6. To allow unauthenticated VPN users to access the DNS service, select the **Allow DNS access for unauthenticated VPN users** check box.

7. Select from the following:
   - To use RADIUS for all user authentication, select **Use RADIUS**.
   - To use RADIUS for all user authentication but only allow specific listed users, select **Use RADIUS and select the Allow only users listed below** check box.
   - To bypass RADIUS and authenticate the listed users locally, select **Authenticate users in list below**.

8. When you are finished, click **Update**. SonicWALL GMS creates a task that changes these settings for each selected SonicWALL appliance.

9. To add a user, do the following:
   - Enter the user name in the **User Name** field.
   - Enter the password in the **New Password** field and reenter it in the **Confirm Password** field.

   *Note: Passwords are case-sensitive.*

   - Select from the following user privileges:
     - **Remote Access**—enables the users to access LAN resources from the Internet. This option is only available in Standard mode.
     - **Bypass Filters**—enables Bypass Filters if the user can bypass Content Filtering settings.
     - **Access to VPNs**—enables the users to send information over the VPN Security Associations.
     - **Access from VPN Client with XAUTH**—use if a VPN client is using XAUTH for authentication.
     - **Limited Management Capabilities**—allows authorized users limited local management access to the SonicWALL interface. Access is limited to the General page (Status, Network, Time), the Log page (View Log, Log Settings, Log Reports), and the Tools page (Restart, Diagnostics minus Tech Support).
When you are finished, click Add. SonicWALL GMS creates a task that adds these users for each selected SonicWALL appliance. Repeat this step for each user that you want to add (up to 100 users).

10. To clear all screen settings and start over, click Reset.

Establishing an Authenticated Session

Authenticated sessions enable authorized users to access the LAN (WorkPort) via the Internet without restrictions. To establish an authenticated session, users must access the SonicWALL LAN (WorkPort) IP address through their browsers. This process is identical to the administrator login.

The user will be prompted for his or her user name and password, which will be verified using MD5 authentication. The password is never sent “in the clear” over the Internet, preventing password theft and replay attacks.

Once authenticated, remote users will be able to access all IP resources on the LAN or WorkPort, and users on the LAN will be able to bypass the Content Filter Lists. If user inactivity exceeds the configured time-out period, the remote user will be timed-out and will need to re-authenticate to access the LAN.

Note: Authenticated sessions create a log entry when established. However, no user activity is logged.

Configuring Management Settings

This section describes how to configure encryption and authentication settings used to establish secure communications between SonicWALL appliances and the SonicWALL GMS.

Note: Other than the encryption and authentication keys, do not modify the other fields on this page. These configuration changes will terminate the secure management tunnel between SonicWALL GMS and the SonicWALL appliance(s).

To configure the encryption and authentication settings for the SonicWALL appliance(s), follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Access icon and click Management. The Management page appears (Figure 71).

Figure 71: Management Page
4. Enter the key used for encryption in the Encryption Key field. The DES and ARCFOur Keys must be exactly 16 characters long and be composed of hexadecimal characters. Encryption keys less than 16 characters will not be accepted; keys longer than 16 characters will be truncated. If the SGMS on VPN check box is selected, this step is not necessary.

Note: Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

5. The authentication key must be exactly 32 characters long and be composed of hexadecimal characters. Authentication keys less than 32 characters will not be accepted; keys longer than 32 characters will be truncated. If the SGMS on VPN check box is selected, this step is not necessary.

Note: Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

6. When you are finished, click Update. SonicWALL GMS schedules a task to change the settings for the selected SonicWALL appliance. To clear the settings and start over, click Reset.

7. To allow SonicWALL GMS to create unique encryption and authentication keys, click Change Only SA Keys. SonicWALL GMS schedules a task to update the encryption and authentication keys for the selected SonicWALL appliance.

Note: At group or global level, SonicWALL GMS will create unique encryption and authentication keys for a group or all SonicWALL appliances.

Configuring SNMP Settings

Simple Network Management Protocol (SNMP) enables administrators to monitor the status of SonicWALL appliances from SNMP v1/v2c-compliant management systems.

To configure SNMP settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Access tree and click SNMP. The SNMP page appears (Figure 72).

Figure 72: SNMP Page

4. Select the Enable SNMP check box.
5. Enter the host name of the SonicWALL device, the system contact, and the location.
6. Enter the name of the administrator group that can view SNMP information in the **Get Community Name** field (default: public).
7. Enter the name of the administrator group that can view SNMP traps in the **Trap Community Name** field.
8. Enter the IP addresses or names of the SNMP management systems that will receive SNMP traps in the **Host** fields. Up to four management systems can be specified.

   **Note:** This field does not accept any special characters except period (.).
9. When you are finished, click **Update**. The settings are changed. To clear the screen settings and start over, click **Reset**.

---

### Configuring RADIUS

This section explains how to configure RADIUS, a standard protocol that enables remote servers to authenticate users through a central server.

VPN Client users that access the LAN (WorkPort) through a VPN tunnel may be required to authenticate through RADIUS before accessing LAN resources. This enables users to share VPN resources, but requires the users to authenticate with unique usernames and passwords.

RADIUS provides an additional layer of VPN security and can be centrally managed from a server that controls all remote access for your organization.

**Note:** SonicWALL's RADIUS implementation supports Steel-Belted RADIUS by Funk Software. A 30-day demo version of Steel-Belted RADIUS may be downloaded from [http://www.funk.com](http://www.funk.com).

To configure RADIUS, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Access tree and click **RADIUS**. The RADIUS page appears (Figure 73).

**Figure 73: RADIUS Page**

4. Enter the number of retries in the **RADIUS Server Retries** field. This field defines the number of times the SonicWALL will attempt to contact the RADIUS server. If the RADIUS server does not respond within the
specified number of retries, the VPN connection will be dropped. The RADIUS server retries can range from 0 to 30, but three retries is recommended.

5. Enter the amount of time that will elapse before the SonicWALL reattempts to contact the RADIUS server in the **RADIUS Server Timeout** field. The RADIUS server timeout can range from 1 to 60 seconds, but 5 seconds is recommended.

6. Enter the information for the primary and secondary (optional) RADIUS servers. This includes:
   - **IP Address/name**—IP address or domain name of the RADIUS server.
   - **Port Number**—UDP port that the RADIUS server listens on. By default, the Steel-Belted RADIUS server listens on port 1645.
   - **Shared Secret**—this field must match the shared secret or administrative password of the RADIUS server. The shared secret is alphanumeric and case-sensitive, and can range from 1 to 30 characters in length.

7. Select from the following privileges that will be available to RADIUS users:
   - **Remote Access**—enables the users to access LAN (WorkPort) resources from the Internet. This option is only available in Standard mode.
   - **Bypass Filters**—enables Bypass Filters if the user can bypass Content Filtering settings.
   - **Access to VPNs**—enables the users to send information over the VPN Security Associations.
   - **Access from the VPN Client with XAUTH**—enable this option if a VPN client is using XAUTH for authentication.
   - **Limited Management Capabilities**—allows authorized users limited local management access to the SonicWALL Management interface. This access is limited to the following pages:
     - **General**—Status, Network, Time
     - **Log**—View Log, Log Settings, Log Reports
     - **Tools**—Restart, Diagnostics minus Tech Support Report

8. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

**Note:** To test the RADIUS server now, enter a valid username and password in the RADIUS Client Test area and click **Test Authentication**.
Dynamic Host Configuration Protocol (DHCP) enables network administrators to automate the assignment of IP addresses from a centralized DHCP server. This conserves IP addresses and makes it easy for mobile users to move among different segments of the network without having to manually enter new IP addresses.

This chapter describes how to use the SonicWALL Global Management System (SonicWALL GMS) to configure SonicWALL appliances as DHCP servers.

Select from the following:

- To configure standard DHCP settings, see “Configuring DHCP” on page 94.
- To configure clients to obtain their IP addresses from a DHCP server at the other end of a VPN tunnel, see “Configuring DHCP Over VPN” on page 95.
Configuring DHCP

This section describes how to configure SonicWALL appliances as DHCP servers.

*Note:* In order for changes on this page to take effect, the SonicWALL(s) will automatically be restarted. We recommend configuring these options when network activity is low.

To configure one or more SonicWALL appliances as DHCP servers, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the DHCP tree and click Setup. The Setup page appears (Figure 74).

**Figure 74: DHCP Setup Page**

4. Select from the following:
   - To enable the DHCP server, select the **Enable DHCP Server** check box.
   - To disable the DHCP server, deselect the **Enable DHCP Server** check box.
   - To disable the DHCP server and configure computers on the LAN (WorkPort) to use a DHCP server outside the firewall, deselect the **Enable DHCP Server** check box and select the **Allow DHCP Pass Through** check box.

5. Enter the amount of time IP addresses will be available to users before they will be required to renew them in the **Lease Time** field. Try specifying a time that is roughly equivalent to the average amount of time users will spend on the network (default: 60 minutes).

6. Enter the IP address of the gateway used by LAN (WorkPort) clients to access the Internet in the **Default Gateway** field. If NAT is enabled, use the SonicWALL LAN (WorkPort) IP address.

7. Enter the registered domain name in the **Domain Name** field, for example “your-domain.com.”

8. Select from the following:
   - If you selected the NAT with DHCP Client configuration, choose the **DNS Servers Using SonicWALL’s Network Settings** option. For details, see “Configuring Network Settings” on page 56.
   - To add DNS servers manually, select **Specify DNS Servers Manually** and enter the DNS server IP addresses.
9. Enter a range of dynamic IP addresses that will be available to computers on the network in the **Dynamic Ranges** fields and click **Add**. Repeat this step for each range of dynamic IP addresses that you want to add.

10. Enter the IP addresses and MAC addresses of static network devices in the **Static Entries** fields. Static IP addresses are often required by network servers and services that must remain accessible at the same IP address.

11. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### Configuring DHCP Over VPN

DHCP over VPN enables clients of the SonicWALL appliance to obtain IP addresses from a DHCP server at the other end of the VPN tunnel or a local DHCP server.

To configure DHCP over VPN, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the DHCP tree and click **DHCP over VPN**. The DHCP over VPN page appears (Figure 75).

**Figure 75: DHCP Over VPN Page**

4. Select from the following:
   - To configure the SonicWALL appliance to forward DHCP requests through a VPN tunnel, select **Remote Gateway** from the **DHCP Relay Mode** list box and do the following:
     - Select the security association (SA) through which the DHCP server resides from the **Obtain using DHCP through this SA** list box.
     - Enter the IP address that will be inserted by the SonicWALL appliance as the IP address of the DHCP Relay Agent in the **Relay IP Address** field.
     - If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL blocks any traffic across the VPN tunnel that is spoofing an authenticated user’s IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is entered for the device.
     - If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local SonicWALL appliance. Once the tunnel is active, it will stop issuing leases. To enable this option, select the **Obtain temporary lease from local DHCP server if tunnel is down** check box.
When you enable this option, clients will be able to obtain IP addresses if the tunnel is unavailable. To ensure that clients use the remote DHCP server shortly after it becomes available, enter a short lease time in the Temporary Lease Time field. The default value is two minutes. Make sure to enable DHCP and enter an IP address range on the DHCP Setup page. Otherwise, the SonicWALL appliance will be unable to act as a DHCP server.

- To specify static IP addresses on the LAN (WorkPort), enter the IP address and MAC address and click Add. Repeat this step for each device that uses a static IP address.
- To specify a device that is not allowed to obtain an IP address through the SA, enter its MAC address and click Add. Repeat this step for each device that will not be allowed to obtain an IP address through the SA.
- To configure the SonicWALL appliance to forward DHCP requests to local servers, select Central Gateway from the DHCP Relay Mode list box and do the following:
  - To configure the SonicWALL appliance to send DHCP requests to specific DHCP servers, select the Send DHCP requests to the server addresses listed below check box. Then, enter the IP address of a DHCP server and click Add. Repeat this step for DHCP server that you want to add.
  - To configure the SonicWALL appliance to broadcast DHCP requests, deselect the Send DHCP requests to the server addresses listed below check box and leave the DHCP Servers field blank.

5. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.
Configuring Advanced Settings and Options

This chapter describes how to configure advanced SonicWALL options. Select from the following:

- **Proxy Settings**—describes how to configure SonicWALLs for use with proxy servers. See “Configuring Proxy Settings” on page 98.
- **Intranet Settings**—describes how to configure SonicWALLs to separate restricted systems from the rest of the network on the same subnet of an organization’s intranet. See “Configuring Intranet Settings” on page 99.
- **Route Settings**—describes how to configure SonicWALLs to recognize internal routers. See “Configuring Routes” on page 101.
- **DMZ (HomePort) Addresses**—describes how to define DMZ (HomePort) addresses. See “Configuring DMZ (HomePort) Addresses” on page 102.
- **One-to-one NAT**—describes how to map valid external IP addresses to internal addresses hidden by NAT. See “Configuring One-to-One Network Address Translation” on page 103.
- **Ethernet**—describes how to define Ethernet settings. See “Configuring Ethernet Settings” on page 105.

*Note: The Advanced options are not available at the global or group levels.*
Configuring Proxy Settings

A proxy server intercepts all requests to web servers on the Internet. As users access websites, the data is cached on the proxy server. This improves Internet response and lessens the load on the Internet link. For example, suppose a school is using the Internet for a research project. A student requests a certain Web page, and then sometime later, a second student requests the same page. Instead of forwarding the request to the Web server where the page resides, the proxy server returns the local copy of the page that was cached when the first student accessed the page.

The problem with a proxy server is that each client must be configured to support the proxy, creating unnecessary administrative problems. If a proxy server is already installed on the LAN (WorkPort), instead of configuring each client to point to the proxy server, move it to the WAN and enable automatic proxy forwarding. SonicWALLs can automatically forward all Web proxy requests to proxy servers without client configuration.

*Note: The proxy server must be located on the WAN; it may not be located on the LAN (WorkPort).*

**Configuration**

To configure automatic proxy forwarding, follow these steps:

*Note: In order for changes on this page to take effect, the SonicWALL(s) will automatically be restarted. We recommend configuring these options when network activity is low.*

To create proxy settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Advanced tree and click **Proxy Relay**. The Proxy Relay page appears (Figure 76).

*Figure 76: Proxy Relay Page*

4. Enter the IP address of the proxy server in the **Proxy Web Server** field.
5. Enter the web server port of the proxy server in the **Proxy Web Server Port** field.
6. Normally, if a proxy server fails, clients behind the SonicWALL appliance will not be able to access the Internet. To allow clients to bypass the proxy server in the event that it fails or becomes unavailable, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
7. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### Configuring Intranet Settings

SonicWALLs can be installed between LAN segments of intranets to prevent unauthorized access to certain resources. For example, if the administrative offices of a school are on the same network as the student computer lab, they can be separated by a SonicWALL.

Figure 77 shows how a SonicWALL appliance can be installed between two network segments on an Intranet.

**Figure 77: SonicWALL Intranet Configuration**

![SonicWALL Intranet Configuration Diagram]

*Note:* Devices connected to the WAN port do not have firewall or content filter protection. To protect these units, install another SonicWALL appliance between the Internet and devices connected to the WAN port of the other SonicWALL appliance.

### Configuration

Although the systems on the WAN and LAN links are separated, they are still on the same subnet. Consequentially, you must make the systems on the larger network aware of the systems on the smaller network. To do this, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Advanced tree and click **Intranet**. The Intranet page appears (Figure 78).
4. Select from the following:
   - If the SonicWALL is not used to separate LAN segments on the intranet, select **SonicWALL’s WAN link is connected to the Internet Router**.
   - If the smaller network is connected to the LAN, select **Specified addresses are attached to the LAN (WorkPort) link**.
   - If the smaller network is connected to the WAN, select **Specified addresses are attached to the WAN link**.

5. Enter the IP address or IP address range of a system or group of systems on the smaller network:
   - To enter a single IP address, enter the IP address in the **Addr Range Begin** field.
   - To enter a range of IP addresses, enter the starting IP address in the **Addr Range Begin** field and the ending IP address in the **Addr Range End** field.
   - Click **Add Range**.

6. Repeat Step 5 for each IP address or IP address range on the smaller network.

7. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

8. To define which services can be accessed from outside the restricted network segment, see Chapter 9, “Configuring Network Access Rules.”
Configuring Routes

If the LAN(s) have internal routers, their addresses and network information must be entered into the SonicWALL(s). To add an internal router, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Advanced tree and click Routes. The Routes page appears (Figure 79).

**Figure 79: Routes Page**

4. Select whether the router is connected to the LAN (WorkPort), WAN, or DMZ (HomePort) interface from the the **Link** list box.
5. Enter the destination network IP addresses in the **Destination Network** and **Subnet Mask** fields.
6. Enter the IP address of the router in the **Gateway** field.
7. Click **Add Route**. Repeat Step 4 through 6 for each route that you want to add.
8. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
Configuring DMZ (HomePort) Addresses

SonicWALL appliances protect users by preventing Internet users from accessing systems within the LAN (WorkPort). However, this security also prevents users from reaching servers intended for public access, such as web and mail servers.

To allow these services, many SonicWALL models have a special Demilitarized Zone (DMZ) port (also known as the HomePort) which is used for public servers. The DMZ sits between the LAN (WorkPort) and the Internet. Servers on the DMZ are publicly accessible, but are protected from denial of service attacks such as SYN Flood and Ping of Death.

Although the DMZ port is optional, it is strongly recommended for public servers or when connecting the servers directly to the Internet where they are not protected.

Configuration

Each server on the DMZ port or HomePort requires a unique, publishable Internet IP address. The ISP that provides your Internet connection should be able to provide these addresses.

To add DMZ (HomePort) IP addresses, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Advanced tree and click **DMZ Addresses** or **HomePort Addresses**.
4. The DMZ/HomePort Addresses page appears (Figure 80).

5. Select from the following:
   - If the devices on the DMZ will use fixed IP addresses, select **DMZ (HomePort) in Standard Mode**. Then, enter the starting IP address in the **Addr Range Begin** field, the ending IP address in the **Addr Range End** field, and click Add Range. Repeat this step for each range of IP addresses.

   *Note: To enter a single IP address, enter the IP address in the **Addr Range Begin** field.*
If the devices on the DMZ or HomePort will use NAT, select **DMZ (HomePort) in NAT Mode** and do the following:

- Enter the private internal IP address assigned to the DMZ or HomePort interface in the **DMZ (HomePort) Private Address** field.
- Assign a subnet mask in the DMZ or HomePort Subnet Mask field. The LAN (WorkPort) and DMZ (HomePort) can have the same subnet mask, but the subnets must be different. For instance, the LAN subnet can be 192.168.0.1 with a subnet mask of 255.255.255.0, and the DMZ subnet can be 172.16.18.1 with a subnet mask of 255.255.255.0.
- To define a DMZ or HomePort public IP address that will be used to access devices on the DMZ interface, enter an IP address in the **DMZ (HomePort) NAT Many to One Public Address** field (Optional).

6. Select from the following:

- To enter a single IP address, enter the IP address in the **Addr Range Begin** field.
- To enter a range of IP addresses, enter the starting IP address in the **Addr Range Begin** field and the ending IP address in the **Addr Range End** field.

7. Click **Add Range**.

8. To enter additional IP addresses and IP address ranges, repeat Steps 6 and 7.

9. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### Configuring One-to-One Network Address Translation

One-to-One NAT maps valid external IP addresses to internal addresses hidden by NAT. This enables you to hide most of your network by using internal IP addresses. However, some machines may require access. This enables you to allow direct access when necessary.

To do this, assign a range of internal IP addresses to a range of external IP addresses of equal size. The first internal IP address will correspond to the first external IP address, the second internal IP address to the second external IP address, and so on.

For example, if an ISP has assigned IP addresses 209.19.28.16 through 209.19.28.31 with 209.19.28.16 as the NAT public address and the address range 192.168.168.1 through 192.168.168.255 is used on the LAN (WorkPort), the following table shows how the IP addresses will be assigned.

<table>
<thead>
<tr>
<th>LAN Address</th>
<th>WAN Address</th>
<th>Accessed Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.168.1</td>
<td>209.19.28.16</td>
<td>Inaccessible, NAT public IP address</td>
</tr>
<tr>
<td>192.168.168.2</td>
<td>209.19.28.17</td>
<td>209.19.28.17</td>
</tr>
<tr>
<td>192.168.168.3</td>
<td>209.19.28.18</td>
<td>209.19.28.18</td>
</tr>
<tr>
<td>[…]</td>
<td>[…]</td>
<td>[…]</td>
</tr>
<tr>
<td>192.168.168.16</td>
<td>209.19.28.31</td>
<td>209.19.28.31</td>
</tr>
<tr>
<td>192.168.168.16</td>
<td>No corresponding IP address</td>
<td>No corresponding IP address</td>
</tr>
<tr>
<td>[…]</td>
<td>[…]</td>
<td>[…]</td>
</tr>
<tr>
<td>192.168.168.16</td>
<td>No corresponding IP address</td>
<td>No corresponding IP address</td>
</tr>
</tbody>
</table>

### Configuration

To configure One-to-One NAT, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Advanced tree and click **One-to-One NAT**.
4. The One-to-One NAT page appears (Figure 81).

**Figure 81: One-to-One NAT Page**

5. Select the **Enable One-to-One NAT** check box.

6. Enter the first IP address of the internal IP address range in the **Private Range Begin** field.

7. Enter the first corresponding external IP address in the **Public Range Begin** field.

   **Note:** Do not include the **NAT Public IP Address** in a range.

8. Enter the number of IP addresses in the range in the **Range Length** field.

9. Click **Add Range**.

10. To add additional IP address ranges, repeat Step 6 through 9 for each range. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
Configuring Ethernet Settings

This section describes how to configure Ethernet settings on each port of the SonicWALL appliance(s). To configure Ethernet settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Advanced tree and click Ethernet.
4. The Ethernet page appears (Figure 82).

Figure 82: Ethernet Page

5. Select from the following WAN Link settings:
   - To configure the WAN link to automatically negotiate Ethernet settings, select Auto Negotiate.
   - To specify WAN link settings, select Force and select the speed and duplex settings.

6. Select from the following DMZ (HomePort) Link settings:
   - To configure the DMZ (HomePort) to automatically negotiate Ethernet settings, select Auto Negotiate.
   - To specify DMZ (HomePort) link settings, select Force and select the speed and duplex settings.

7. Select from the following LAN (WorkPort) Link settings:
   - To configure the LAN link to automatically negotiate Ethernet settings, select Auto Negotiate.
   - To specify LAN link settings, select Force and select the speed and duplex settings.

8. If you are managing the Ethernet connection from the LAN (WorkPort) side of your network, select the Proxy Management Workstation Ethernet Address on WAN check box. The SonicWALL appliance will take the Ethernet address of the computer that is managing the SonicWALL appliance and will proxy the address on the WAN port of the SonicWALL. If you are not managing the SonicWALL appliance from the LAN side of your network, the firmware looks for a random computer on the LAN which can be a lengthy search process.

9. To limit the size of packets sent over the Ethernet WAN interface, select the Fragment Outbound Packets Larger than the WAN MTU check box and enter the maximum size in the WAN MTU field. If the maximum transmission unit (MTU) size is too large for a remote router, it may require more transmissions. If the packet size is too small, this could result in more packet header overhead and more acknowledgement that have to be processed. The default size is 1,500 MTU.
10. To enable bandwidth management, select the **Enable** check box and enter the bandwidth of the connection in the **Available Bandwidth** field.

11. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
A Virtual Private Network (VPN) is a private data network that uses encryption technologies to operate over public networks. Each node in a network can exchange data by establishing a VPN tunnel or a Security Association (SA) with one or more other nodes. Once a tunnel is established, the SA uses encryption and authentication keys to ensure data security and integrity.

A security key string is an encryption key that is used to encrypt and decrypt secure data. Both nodes must have the key to exchange data. For example, the announcer of the Little Orphan Show used the same key to encode the secret messages that the kids used to decode the messages.

Although an encrypted message cannot be read, it can be tampered with externally. Using an authentication key prevents external tampering. An authentication key is a hash function that is applied to the message content and is checked by the message recipient to verify the message was not modified in transit.

In order to ensure message security, it is very important that the security and authentication keys are not discovered by outside parties. Otherwise, the messages could be read in transit.

SonicWALL appliances can use the following methods to exchange security and authentication keys:

- **SonicWALL certificates**—each SonicWALL appliance obtains a certificate from the SonicWALL Certificate Authority (CA). Security and authentication keys are exchanged using public-key cryptography and authenticity of each node is verified by the SonicWALL CA.
  
  After the SA expires, the SonicWALL appliances will reestablish an SA using the same public keys, but the security and authentication keys will be different. If one set of security and authentication keys is compromised by an outside party, that party will be unable to compromise the next set of keys.

- **Third-party certificates**—the SonicWALL appliance and peer device obtain certificates from the third-party certificate authorities. Security and authentication keys are exchanged using public-key cryptography and authenticity of each node is verified by the third-party CA.
  
  After the SA expires, the peers will reestablish an SA using the same public keys, but will not use the same security and authentication keys.

- **Pre-shared secret**—each SonicWALL appliance has a shared secret that is used to establish an SA.
  
  After the SA expires, the SonicWALL appliances will reestablish an SA using the same public keys, but will not use the same security and authentication keys.

- **Pre-exchanged security and authentication keys**—keys are exchanged in advance.
  
  The SA will always use the same encryption and authentication keys. If the keys are compromised by an outside party, they will remain compromised until the keys are changed.

*Note:* For an explanation of VPN terms, see “Basic Terms and Concepts” on page 131.

*Note:* Some SonicWALL appliances include VPN and others require a VPN upgrade that must be purchased separately. For example, the SonicWALL TELE2 includes VPN and the SonicWALL SOHO2 does not.
Configuring VPN

To configure VPN on SonicWALL appliances, follow these procedures:

- Obtain and activate a VPN upgrade for each device—see “Adding Virtual Private Networking to SonicWALL Appliances” on page 159.
- Enable VPN for each SonicWALL appliance—see “Enabling VPN” on page 108.
- Configure security associations—see “Configuring Security Associations” on page 109.

Enabling VPN

After applying a VPN upgrade, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the VPN tree and click Summary. The VPN Summary page appears (Figure 83).

   Note: If VPN is already configured for the SonicWALL appliance, a list of current SAs appears. The unique firewall identifier also appears.

   Figure 83: VPN Summary Page

4. Select the Enable VPN check box.
5. To disable all NetBIOS broadcasts, select the Disable all VPN Windows Networking (NetBIOS) broadcast check box.
6. To improve interoperability with other VPN gateways and applications that use a large data packet size, select the Enable Fragmented Packet Handling check box. Packet fragmentation overburdens a network router by resending data packets and causes network traffic to slow down between networks.

   The Enable Fragmented Packet Handling option configures the SonicWALL appliance to listen to the intermediate router and, if necessary, send Internet Control Message Protocol (ICMP) messages to the router to decrease the size of the data packets. Enabling this option is recommended if the VPN tunnel logs contain many “Fragmented IPSec packets dropped” messages.
7. SonicWALL appliances can manage outbound traffic using bandwidth management. To enable bandwidth management for VPN tunnels, select the Enable Bandwidth Management check box.
Enter the amount of bandwidth that will always be available to VPN tunnels in the **VPN Guaranteed Bandwidth** field. Keep in mind that this bandwidth will be permanently assigned to VPN services and not available to other services, regardless of the amount of bandwidth that VPN uses.

Enter the maximum amount of bandwidth that will be available for VPN services in the **VPN Maximum Bandwidth** field.

Select the priority of VPN services in relation to other services from the **VPN Bandwidth Priority** list box. Select a priority from 0 (highest) to 7 (lowest).

*Note: In order to configure bandwidth management, bandwidth management must be enabled on the SonicWALL appliance. For more information, see “Configuring Ethernet Settings” on page 105.*

8. When you are finished, click **Update**. To clear all screen settings and start over, click **Reset**.

---

**Configuring Security Associations**

SonicWALL GMS supports several methods for establishing and maintaining security associations (SAs). These include:

- Internet Key Exchange (IKE) using SonicWALL certificates. See “Internet Key Exchange Using SonicWALL Certificates” on page 109.
- IKE using third-party certificates. See “Internet Key Exchange Using Third-Party Certificates” on page 114.
- IKE using a pre-shared secret. See “Internet Key Exchange Using Pre-Shared Secret” on page 120.

**Internet Key Exchange Using SonicWALL Certificates**

*Note: This section assumes that you are familiar with Public Key Infrastructure (PKI) and the implementation of digital certificates with VPN.*

A digital certificate is an electronic means to verify identity by using a trusted third party known as a Certificate Authority (CA). SonicWALL certificates are the easiest certificate solution for establishing the identity of peer VPN devices and users.

Internet Key Exchange (IKE) is an important part of IPSec VPN solutions, and it can use digital signatures to authenticate peer devices before setting up security associations. Without digital signatures, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices using digital signatures do not require configuration changes every time a new device is added to the network.

*Note: Although SAs can be established with most IPSec-compliant devices, SonicWALL Certificates can only be used between SonicWALL appliances.*

This section describes how to establish SAs between SonicWALL appliances that are managed by SonicWALL GMS and SonicWALL appliances that are not managed by SonicWALL GMS.

*Note: Before establishing SAs using SonicWALL certificates, you must obtain a Public Key Infrastructure (PKI) administrator certificate and apply it to each SonicWALL appliance. For more information, see “Adding PKI Administrator Certificates” on page 166.*

**When All Appliances are Managed by SonicWALL GMS**

To enable VPN using certificates, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 84).
4. Select IKE using SonicWALL Certificates.

5. Select from the following:
   - To add a new SA, select Add a new Security Association.
   - To delete an existing SA, select Delete an existing Security Association.
   - To edit an existing SA, select Modify an existing Security Association.

6. Select the Use Interconnected Mode check box.

7. Click Select Target.
   A dialog box that contains all SonicWALL appliances managed by this SonicWALL GMS appears.

8. Select the SonicWALL appliance or group to which you will establish SAs and click the Select button. The name of the target appears in the Target SonicWALL Group/Node field.

9. Select the Diffie-Hellman (DH) group that will be used when the VPN devices are negotiating encryption and authentication keys from the Phase 1 DH Group list box.
   
   Note: Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.

10. Select the Diffie-Hellman group that will be used when the VPN devices have established an SA from the Phase 2 DH Group list box.

11. Select the type of encryption and authentication keys used when the VPN devices are negotiating encryption and authentication keys from the Phase 1 Encryption/Authentication list box.

12. Select the type of encryption and authentication keys used for the SAs from the Phase 2 Encryption/Authentication list box.

13. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the Default LAN (WorkPort) Gateway field.
   
   A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the Route all Internet traffic through this destination unit check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming Internet Protocol Security (IPSec) packets for this SA.
Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN (WorkPort). If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

14. To specify how long the tunnel is active before being renegotiated, enter a value in the **SA Lifetime** field. We recommend a value of 28,800 seconds (8 hours).

15. To prevent repeated compromises of the same security key when reestablishing a tunnel, select the **Enable Perfect Forward Secrecy** check box.

16. To configure the VPN tunnel to remain open as long as there is network traffic on the SA, select the **Enable Keep Alive** check box.

17. Aggressive mode improves the performance of IKE SA negotiation by only requiring three packet exchanges. However, it provides no identity protection. To enable aggressive mode, select the **Use Aggressive Mode** check box.

18. To enable NetBIOS broadcasts across the SA, select the **Enable Windows Networking Broadcast** check box.

19. To allow the remote VPN tunnel to be included in the routing table, select the **Forward Packets to Remote VPNs** check box.

   Normally, inbound traffic is decrypted and only forwarded to the local LAN (WorkPort) or a manually specified route (see “Configuring Routes” on page 101). This option enables you to create a “hub and spoke” network configuration where all traffic is routed among branch offices via the corporate office.

   **Note:** To create a “hub and spoke” network, make sure to select the **Forward Packets to Remote VPNs** check box for each SA.

20. To force all network traffic to the WAN through a VPN to a central site, select the **Route all Internet traffic through destination unit** check box.

   When this option is selected, all traffic that is not destined for another SA is forwarded through this VPN tunnel. If this option is not specified and the destination does not match any SA, the packet is forwarded unencrypted to the WAN.

   **Note:** Only one SA can have this option enabled.

21. Select one of the following VPN termination options:

   - To configure the VPN tunnel to terminate at the LAN or WorkPort, select **LAN (WorkPort)**. Users on the other side of the SA will be able to access the LAN, but not the DMZ (HomePort).
   - To configure the VPN tunnel to terminate at the DMZ or HomePort, select **DMZ (HomePort)**. Users on the other side of the SA will be able to access the DMZ, but not the LAN (WorkPort).
   - To allow users on the other side of the SA to access both the LAN and DMZ, select **LAN/DMZ or WorkPort/HomePort**.

22. Select from the following NAT and Firewall Rules:

   - To disable NAT and not apply firewall rules to traffic coming through this SA, select **Disabled**.
   - To enable NAT and firewall rules for the selected SonicWALL appliance, select **Source**. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and network firewall rules will be applied to all traffic on this SA.
   - To enable NAT and firewall rules for the selected SonicWALL appliance and its peer, select **Source and Destination**. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and all traffic originating from its peer will appear to originate from a single IP address. Network firewall rules will be applied to all traffic on this SA.

   **Note:** Applying firewall rules can dramatically affect services that run between the networks. For more information, see Chapter 9, “Configuring Network Access Rules.”

23. Select how local users are authenticated:

   - To disable authentication for local users, select **Disabled**.
   - To configure local users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
   - To configure local users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
   - To authenticate local users both locally and on the destination network, select **Source and Destination**.
24. Select how remote users are authenticated:
- To disable authentication for remote users, select **Disabled**.
- To configure remote users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
- To configure remote users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
- To authenticate remote users both locally and on the destination network, select **Source and Destination**.

25. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

*Note: To disable this SA, select the **Disable this SA** check box and click **Update**.*

When One Appliance Is Not Managed by SonicWALL GMS

Although SAs can be established with most Internet Protocol Security (IPSec)-compliant devices, Certificates can only be used between SonicWALL appliances.

This section describes how to establish SonicWALL certificate-based SAs between SonicWALL appliances that are managed by SonicWALL GMS and SonicWALL appliances that are not managed by SonicWALL GMS.

To create SAs using certificates, follow these steps:
1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 85).

**Figure 85: VPN Configure Page**

4. Select **IKE using SonicWALL Certificates**.

5. Select from the following:
- To add a new SA, select **Add a new Security Association**.
- To delete an existing SA, select **Delete an existing Security Association**.
- To edit an existing SA, select **Modify an existing Security Association**.

---

112  SonicWALL Global Management System Configuration Guide
6. Enter the name of the remote firewall/VPN gateway in the **Security Association Name** field. This name must match exactly if the device has a dynamic IP address.

7. Enter the IP address of the remote firewall/VPN gateway in the **IPSec Gateway Address** field. This address must be valid and will be the public IP address if the remote LAN has NAT enabled. If the remote VPN gateway has a dynamic IP address, this field can be left blank if the name matches.

8. To specify how long the tunnel is active before being renegotiated, enter a value in the **SA Lifetime** field. We recommend a value of 28,800 seconds (8 hours).

9. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the **Default LAN (WorkPort) Gateway** field.

   A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the Route all internet traffic through destination unit check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

   Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

10. To configure the VPN tunnel to remain open as long as there is network traffic on the SA, select the **Enable Keep Alive** check box.

11. Aggressive mode improves the performance of IKE SA negotiation by only requiring three packet exchanges. However, it provides no identity protection. To enable aggressive mode, select the **Use Aggressive Mode** check box.

12. To prevent repeated compromises of the same security key when reestablishing a tunnel, select the **Enable Perfect Forward Secrecy** check box.

13. To enable NetBIOS broadcasts across the SA, select the **Enable Windows Networking Broadcast** check box.

14. To apply NAT and firewall rules to all traffic coming through this SA, select the **Apply NAT and firewall rules** check box.

   This feature is useful for hiding the LAN subnet from the corporate site. All traffic will appear to originate from a single IP address.

15. To allow the remote VPN tunnel to be included in the routing table, select the **Forward Packets to Remote VPNs** check box.

   This will enable the SonicWALL appliance to receive VPN traffic, decrypt it, and forward it to another VPN tunnel. This feature can be used to create a “hub and spoke” network configuration by routing traffic among SAs. To do this, make sure to enable this option for all SAs.

16. To require local users to authenticate locally before accessing the SA, select the **Require authentication of local users** check box.

17. To require remote users to authenticate with this SonicWALL appliance or the local RADIUS server before accessing resources, select the **Require authentication of remote users** check box.

18. Enter the serial number of the target SonicWALL appliance in the **Peer SonicWALL Serial #** field.

19. Select the Diffie-Hellman group that will be used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 DH Group** list box.

   Note: Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 3 specifies the currently most secure 1536-bit Diffie-Hellman value.

20. Select the Diffie-Hellman group that will be used when the VPN devices have established an SA from the **Phase 2 DH Group** list box.

21. Select the type of encryption and authentication keys used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 Encryption/Authentication** list box.

22. Select the type of encryption and authentication keys used for the SAs from the **Phase 2 Encryption/Authentication** list box.

23. Select from the following:
   - To allow this SA to be used as the default route for all Internet traffic, select **Use this SA as default route for all Internet traffic**.
24. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.

Note: To disable this SA without deleting it, select the Disable this SA check box and click Update.

Internet Key Exchange Using Third-Party Certificates

Note: This section assumes that you are familiar with Public Key Infrastructure (PKI) and the implementation of digital certificates with VPN.

A digital certificate is an electronic means to verify identity by using a trusted third party known as a Certificate Authority (CA). SonicWALL now supports third party certificates in addition to the existing Authentication Service. The difference between third party certificates and the SonicWALL Authentication Service is the ability to select the source for your CA certificate. Using Certificate Authority Certificates and Local Certificates is a more manual process than using the SonicWALL Authentication Service; therefore, experience with implementing Public Key Infrastructure (PKI) is necessary to understand the key components of digital certificates.

Internet Key Exchange (IKE) is an important part of IPSec VPN solutions, and it can use digital signatures to authenticate peer devices before setting up security associations. Without digital signatures, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices using digital signatures do not require configuration changes every time a new device is added to the network.

SonicWALL has implemented X.509v3 as its certificate form and CRLv2 for its certificate revocation list. SonicWALL supports the following two vendors of Certificate Authority Certificates:

• VeriSign
• Entrust

Obtaining a Certificate

To obtain a certificate, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click Local Certs. The Local Certs page appears (Figure 86).
4. Complete the information in the **Generate Certificate Request** section and click **Generate Request**. The request appears in the **Current Certificate Requests** section.

5. Click **Export**. You are prompted to save the file. It will be saved in the PKCS 10 format.

6. Obtain a certificate from one of the approved certificate authorities using the PKCS 10 file.

7. After you receive the certificate file, locate and import the file by clicking **Browse** in the **Import Certificate With Private Key** section. Then click **Import**. The certificate will appear in the **Current Local Certificates** section.

**Note:** After you have obtained certificates for both devices, continue to “**When All Appliances are Managed by SonicWALL GMS**” on page 115 or “**When One Appliance Is Not Managed by SonicWALL GMS**” on page 118.

### When All Appliances are Managed by SonicWALL GMS

Setting up a VPN tunnel between appliances requires you to configure several parameters on both appliances. When setting up VPN tunnels between SonicWALL appliances managed by SonicWALL GMS, all selected appliances are automatically configured based on the settings that you entered.

To enable VPN using third-party certificates when both devices are managed by SonicWALL GMS, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 84).
4. Select IKE using 3rd Party Certificates.

5. Select from the following:
   - To add a new SA, select **Add a new Security Association**.
   - To delete an existing SA, select **Delete an existing Security Association**.
   - To edit an existing SA, select **Modify an existing Security Association**.

6. Select the **Use Interconnected Mode** check box.

7. Click **Select Target**.
   A dialog box that contains all SonicWALL appliances managed by this SonicWALL GMS appears.

8. Select the SonicWALL appliance or group to which you will establish SAs and click the **Select** button. The name of the target appears in the **Target SonicWALL Group/Node** field.

9. Select the Diffie-Hellman (DH) group that will be used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 DH Group** list box.

   **Note:** Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.

10. Select the Diffie-Hellman group that will be used when the VPN devices have established an SA from the **Phase 2 DH Group** list box.

11. Select the type of encryption and authentication keys used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 Encryption/Authentication** list box.

12. Select the type of encryption and authentication keys used for the SAs from the **Phase 2 Encryption/Authentication** list box.

13. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the **Default LAN (WorkPort) Gateway** field.

   A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the **Route all Internet traffic through this destination unit** check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming Internet Protocol Security (IPSec) packets for this SA.
Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

14. To specify how long the tunnel is active before being renegotiated, enter a value in the **SA Lifetime** field. We recommend a value of 28,800 seconds (8 hours).

15. To prevent repeated compromises of the same security key when reestablishing a tunnel, select the **Enable Perfect Forward Secrecy** check box.

16. To configure the VPN tunnel to remain open as long as there is network traffic on the SA, select the **Enable Keep Alive** check box.

17. Aggressive mode improves the performance of IKE SA negotiation by only requiring three packet exchanges. However, it provides no identity protection. To enable aggressive mode, select the **Use Aggressive Mode** check box.

18. To enable NetBIOS broadcasts across the SA, select the **Enable Windows Networking Broadcast** check box.

19. To allow the remote VPN tunnel to be included in the routing table, select the **Forward Packets to Remote VPNS** check box.

   Normally, inbound traffic is decrypted and only forwarded to the local LAN (WorkPort) or a manually specified route (see “Configuring Routes” on page 101). This option enables you to create a “hub and spoke” network configuration where all traffic is routed among branch offices via the corporate office.

   **Note:** To create a “hub and spoke” network, make sure to select the **Forward Packets to Remote VPNS** check box for each SA.

20. To force all network traffic to the WAN through a VPN to a central site, select the **Route all Internet traffic through destination unit** check box.

   When this option is selected, all traffic that is not destined for another SA is forwarded through this VPN tunnel. If this option is not specified and the destination does not match any SA, the packet is forwarded unencrypted to the WAN.

   **Note:** Only one SA can have this option enabled.

21. Select one the following VPN termination options:

   - To configure the VPN tunnel to terminate at the LAN or WorkPort, select **LAN (WorkPort)**. Users on the other side of the SA will be able to access the LAN, but not the DMZ (HomePort).
   - To configure the VPN tunnel to terminate at the DMZ or HomePort, select **DMZ (HomePort)**. Users on the other side of the SA will be able to access the DMZ, but not the LAN (WorkPort).
   - To allow users on the other side of the SA to access both the LAN and DMZ, select **LAN/DMZ or WorkPort/HomePort**.

22. Select from the following NAT and Firewall Rules:

   - To disable NAT and not apply firewall rules to traffic coming through this SA, select **Disabled**.
   - To enable NAT and firewall rules for the selected SonicWALL appliance, select **Source**. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and network firewall rules will be applied to all traffic on this SA.
   - To enable NAT and firewall rules for the selected SonicWALL appliance and its peer, select **Source and Destination**. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and all traffic originating from its peer will appear to originate from a single IP address. Network firewall rules will be applied to all traffic on this SA.

   **Note:** Applying firewall rules can dramatically affect services that run between the networks. For more information, see Chapter 9, “Configuring Network Access Rules.”

23. Select how local users are authenticated:

   - To disable authentication for local users, select **Disabled**.
   - To configure local users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
   - To configure local users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
   - To authenticate local users both locally and on the destination network, select **Source and Destination**.
24. Select how remote users are authenticated:
   - To disable authentication for remote users, select **Disabled**.
   - To configure remote users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
   - To configure remote users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
   - To authenticate remote users both locally and on the destination network, select **Source and Destination**.
25. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
   
   **Note:** To disable this SA, select the **Disable this SA** check box and click **Update**.

**When One Appliance Is Not Managed by SonicWALL GMS**

This section describes how to configure VPN when the target appliance is not managed by SonicWALL GMS. To create SAs using third-party certificates, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 85).

4. Select **IKE using 3rd Party Certificates**.
5. Select from the following:
   - To add a new SA, select **Add a new Security Association**.
   - To delete an existing SA, select **Delete an existing Security Association**.
   - To edit an existing SA, select **Modify an existing Security Association**.
6. Enter the name of the remote firewall/VPN gateway in the **Security Association Name** field. This name must match exactly if the device has a dynamic IP address.
7. Select the certificate to use from the **Select Certificate** list box.
8. Enter the IP address of the remote firewall/VPN gateway in the **IPSec Gateway Address** field. This address must be valid and will be the public IP address if the remote LAN has NAT enabled. If the remote VPN gateway has a dynamic IP address, this field can be left blank if the name matches.

9. To specify how long the tunnel is active before being renegotiated, enter a value in the **SA Lifetime** field. We recommend a value of 28,800 seconds (8 hours).

10. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the **Default LAN (WorkPort) Gateway** field.

A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the **Route all internet traffic through destination unit** check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

11. To configure the VPN tunnel to remain open as long as there is network traffic on the SA, select the **Enable Keep Alive** check box.

12. Aggressive mode improves the performance of IKE SA negotiation by only requiring three packet exchanges. However, it provides no identity protection. To enable aggressive mode, select the **Use Aggressive Mode** check box.

13. To prevent repeated compromises of the same security key when reestablishing a tunnel, select the **Enable Perfect Forward Secrecy** check box.

14. To enable NetBIOS broadcasts across the SA, select the **Enable Windows Networking Broadcast** check box.

15. To apply NAT and firewall rules to all traffic coming through this SA, select the **Apply NAT and firewall rules** check box.

This feature is useful for hiding the LAN subnet from the corporate site. All traffic will appear to originate from a single IP address.

16. To allow the remote VPN tunnel to be included in the routing table, select the **Forward Packets to Remote VPNs** check box.

This will enable the SonicWALL appliance to receive VPN traffic, decrypt it, and forward it to another VPN tunnel. This feature can be used to create a “hub and spoke” network configuration by routing traffic among SAs. To do this, make sure to enable this option for all SAs.

17. To require local users to authenticate locally before accessing the SA, select the **Require authentication of local users** check box.

18. To require remote users to authenticate with this SonicWALL appliance or the local RADIUS server before accessing resources, select the **Require authentication of remote users** check box.

19. Select one the following VPN termination options:

- **To configure the VPN tunnel to terminate at the LAN or WorkPort**, select **LAN (WorkPort)**. Users on the other side of the SA will be able to access the LAN, but not the DMZ (HomePort).
- **To configure the VPN tunnel to terminate at the DMZ or HomePort**, select **DMZ (HomePort)**. Users on the other side of the SA will be able to access the DMZ, but not the LAN (WorkPort).
- **To allow users on the other side of the SA to access both the LAN and DMZ**, select **LAN/DMZ or WorkPort/HomePort**.

20. Select the Diffie-Hellman group that will be used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 DH Group** list box.

*Note: Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 3 specifies the currently most secure 1536-bit Diffie-Hellman value.*

21. Select the Diffie-Hellman group that will be used when the VPN devices have established an SA from the **Phase 2 DH Group** list box.

22. Select the type of encryption and authentication keys used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 Encryption/Authentication** list box.

23. Select the type of encryption and authentication keys used for the SAs from the **Phase 2 Encryption/Authentication** list box.
24. Select whether the peer device uses a distinguished name, e-mail ID, or domain name as its certificate ID from the **Peer Certificate’s ID** list box.

25. Enter the peer device’s certificate ID in the **Peer Certificate’s ID** field.

26. Select from the following:
   - To allow this SA to be used as the default route for all Internet traffic, select **Use this SA as default route for all Internet traffic**.
   - If the destination network will receive its IP addresses on this network using DHCP, select **Destination network obtains IP addresses using DHCP**.
   - To specify destination networks, select **Specify destination networks below**. Then, click **Modify** and enter the destination network IP addresses and subnet masks.

27. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

   **Note:** To disable this SA without deleting it, select the **Disable this SA** check box and click **Update**.

**Internet Key Exchange Using Pre-Shared Secret**

When using IKE with a pre-shared secret, two VPN devices establish encryption and authentication keys using a shared secret. After the SA expires, the SonicWALL appliances will reestablish an SA using the same shared secret, but will not use the same security and authentication keys.

**When All Appliances are Managed by SonicWALL GMS**

Setting up a VPN tunnel between appliances requires you to configure several parameters on both appliances. When setting up VPN tunnels between SonicWALL appliances managed by SonicWALL GMS, all selected appliances are automatically configured based on the settings that you entered.

To configure an SA using IKE with pre-shared secrets, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 89).
4. Select IKE using Pre-shared Secret.

5. Select from the following:
   - To add a new SA, select Add a new Security Association.
   - To delete an existing SA, select Delete an existing Security Association.
   - To edit an existing SA, select Modify an existing Security Association.

6. Select the Use Interconnected Mode check box.

7. Click Select Target.
   A dialog box that contains all SonicWALL appliances managed by this SonicWALL GMS appears.

8. Select the SonicWALL appliance or group to which you will establish SAs and click the Select button. The name of the target appears in the Target SonicWALL Group/Node field.

9. Select the Diffie-Hellman group that will be used when the VPN devices are negotiating encryption and authentication keys from the Phase 1 DH Group list box.
   
   **Note:** Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 3 specifies the currently most secure 1536-bit Diffie-Hellman value.

10. Select the Diffie-Hellman group that will be used when the VPN devices have established an SA from the Phase 2 DH Group list box.

11. Select the type of encryption and authentication keys used when the VPN devices are negotiating encryption and authentication keys from the Phase 1 Encryption/Authentication list box.

12. Select the type of encryption and authentication keys used for the SAs from the Phase 2 Encryption/Authentication list box.

13. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the Default LAN (WorkPort) Gateway field.
   A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the Route all internet traffic through destination unit check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.
Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

14. To specify how long the tunnel is active before being renegotiated, enter a value in the SA Lifetime field. We recommend a value of 28,800 seconds (8 hours).

15. To prevent repeated compromises of the same security key when reestablishing a tunnel, select the Enable Perfect Forward Secrecy check box.

16. To configure the VPN tunnel to remain open as long as there is network traffic on the SA, select the Enable Keep Alive check box.

17. Aggressive mode improves the performance of IKE SA negotiation, by only requiring three packet exchanges. However, it provides no identity protection. To enable aggressive mode, select the Use Aggressive Mode check box.

18. To enable NetBIOS broadcasts across the SA, select the Enable Windows Networking Broadcast check box.

19. To allow the remote VPN tunnel to be included in the routing table, select the Forward Packets to Remote VPns check box.

Normally, inbound traffic is decrypted and only forwarded to the local LAN or a manually specified route (see “Configuring Routes” on page 101). This option enables you to create a “hub and spoke” network configuration where all traffic is routed among branch offices via the corporate office.

**Note:** To create a “hub and spoke” network, make sure to select the Forward Packets to Remote VPNs check box for each SA.

20. To force all network traffic to the WAN through a VPN to a central site, select the Route all internet traffic through destination unit check box.

When this option is selected, all traffic that is not destined for another SA is forwarded through this VPN tunnel. If this option is not specified and the destination does not match any SA, the packet is forwarded unencrypted to the WAN.

**Note:** Only one SA can have this option enabled.

21. Select one the following VPN termination options:

- To configure the VPN tunnel to terminate at the LAN or WorkPort, select LAN (WorkPort). Users on the other side of the SA will be able to access the LAN, but not the DMZ (HomePort).
- To configure the VPN tunnel to terminate at the DMZ or HomePort, select DMZ (HomePort). Users on the other side of the SA will be able to access the DMZ, but not the LAN (WorkPort).
- To allow users on the other side of the SA to access both the LAN and DMZ, select LAN/DMZ or WorkPort/HomePort.

22. Select from the following NAT and Firewall Rules:

- To disable NAT and not apply firewall rules to traffic coming through this SA, select Disabled.
- To enable NAT and firewall rules for the selected SonicWALL appliance, select Source. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and network firewall rules will be applied to all traffic on this SA.
- To enable NAT and firewall rules for the selected SonicWALL appliance and its peer, select Source and Destination. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and all traffic originating from its peer will appear to originate from a single IP address. Network firewall rules will be applied to all traffic on this SA.

**Note:** Applying firewall rules can dramatically affect services that run between the networks. For more information, see Chapter 9, “Configuring Network Access Rules.”

23. Select how local users are authenticated:

- To disable authentication for local users, select Disabled.
- To configure local users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select Source.
- To configure local users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select Destination.
- To authenticate local users both locally and on the destination network, select Source and Destination.
24. Select how remote users are authenticated:
   - To disable authentication for remote users, select **Disabled**.
   - To configure remote users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
   - To configure remote users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
   - To authenticate remote users both locally and on the destination network, select **Source and Destination**.

25. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

*Note: To disable this SA, select the **Disable this SA** check box and click **Update**.*

**When One Appliance Is Not Managed by SonicWALL GMS**

This section describes how to configure VPN when the target appliance is not managed by SonicWALL GMS.

To enable VPN using IKE with a pre-shared secret, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 90).

*Figure 90: VPN Configure Page*

4. Select **IKE using Pre-Shared Secret** in the IPSec Keying mode section.

5. Select from the following:
   - To add a new SA, select **Add a new Security Association**.
   - To delete an existing SA, select **Delete an existing Security Association**.
   - To edit an existing SA, select **Modify an existing Security Association**.

6. Enter the name of the remote firewall/VPN gateway in the **Security Association Name** field. This name must match exactly if the device has a dynamic IP address.
7. Enter the IP address of the remote firewall/VPN gateway in the **IPSec Gateway Address** field. This address must be valid and will be the public IP address if the remote LAN has NAT enabled. If the remote VPN gateway has a dynamic IP address, this field can be left blank if the name matches.

8. Enter the amount of time before an IKE SA will automatically negotiate (120 to 2,499,999 seconds).

9. To configure the VPN tunnel to remain open as long as there is network traffic on the SA, select the **Enable Keep Alive** check box.

10. Aggressive mode improves the performance of IKE SA negotiation by only requiring three packet exchanges. However, it provides no identity protection. To enable aggressive mode, select the **Use Aggressive Mode** check box.

11. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the **Default LAN (WorkPort) Gateway** field.

   A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the **Route all Internet traffic through destination unit** check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

   Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

12. To prevent repeated compromises of the same security key when reestablishing a tunnel, select the **Enable Perfect Forward Secrecy** check box.

13. To access remote resources within the Windows Network Neighborhood, select the **Enable Windows Networking (NetBIOS) Broadcast** check box.

14. To apply NAT and firewall rules to all traffic coming through this SA, select the **Apply NAT and firewall rules** check box.

   This feature is useful for hiding the LAN subnet from the corporate site. All traffic will appear to originate from a single IP address.

15. To allow the remote VPN tunnel to be included in the routing table, select the **Forward Packets to Remote VPNs** check box.

   This will enable the SonicWALL appliance to receive VPN traffic, decrypt it, and forward it to another VPN tunnel. This feature can be used to create a “hub and spoke” network configuration by routing traffic among SAs. To do this, make sure to enable this option for all SAs.

16. To require local users to authenticate locally before accessing the SA, select the **Require authentication of local users** check box.

17. To require remote users to authenticate with this SonicWALL appliance or the local RADIUS server before accessing resources, select the **Require authentication of remote users** check box.

18. Select one of the following VPN termination options:

   - To configure the VPN tunnel to terminate at the LAN or WorkPort, select **LAN (WorkPort)**. Users on the other side of the SA will be able to access the LAN, but not the DMZ (HomePort).
   - To configure the VPN tunnel to terminate at the DMZ or HomePort, select **DMZ (HomePort)**. Users on the other side of the SA will be able to access the DMZ, but not the LAN (WorkPort).
   - To allow users on the other side of the SA to access both the LAN and DMZ, select **LAN/DMZ or WorkPort/HomePort**.
   - To force inbound VPN clients to authenticate with the RADIUS server, select **Require VPN Clients with XAUTH** (only allows VPN Clients). Otherwise, select **Remote users behind VPN gateway**.

   **Note:** Only SonicWALL VPN clients can authenticate to a RADIUS server. Users tunneling from another VPN gateway will not be able to complete the VPN tunnel if this check box is selected.

19. Enter the shared secret in the **Shared Secret** field.

20. Select the Diffie-Hellman group that will be used when the VPN devices are negotiating encryption and authentication keys from the **Phase 1 DH Group** list box.

   **Note:** Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.
21. Select the Diffie-Hellman group that will be used when the VPN devices have established an SA from the Phase 2 DH Group list box.

22. Select the type of encryption and authentication keys used when the VPN devices are negotiating encryption and authentication keys from the Phase 1 Encryption/Authentication list box.

23. Select the type of encryption and authentication keys used for the SAs from the Phase 2 Encryption/Authentication list box.

24. Select from the following:
   - To allow this SA to be used as the default route for all Internet traffic, select Use this SA as default route for all Internet traffic.
   - If the destination network will receive its IP addresses on this network using DHCP, select Destination network obtains IP addresses using DHCP.
   - To specify destination networks, select Specify destination networks below. Then, click Modify and enter the destination network IP addresses and subnet masks.

25. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.

26. Create an SA in the remote VPN device for each SonicWALL appliance that you have configured.

   Note: To disable this SA without deleting it, select the Disable this SA check box and click Update.

Manual Keying

Manual keying involves exchanging keys in encryption and authentication keys in advance. Although this is the simplest method of establishing an SA between two VPN devices, the SA will always use the same encryption and authentication keys. If the keys are compromised by an outside party, they will remain compromised until the keys are changed.

When All Appliances are Managed by SonicWALL GMS

Setting up a VPN tunnel between appliances requires you to configure several parameters on both appliances. When setting up VPN tunnels between SonicWALL appliances managed by SonicWALL GMS, all selected appliances are automatically configured based on the settings that you entered.

To enable VPN using manual keying, follow these steps:
1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click Configure. The VPN Configure page appears (Figure 91).
4. Select Manual Key.

5. Select from the following:
   - To add a new SA, select Add a new Security Association.
   - To delete an existing SA, select Delete an existing Security Association.
   - To edit an existing SA, select Modify an existing Security Association.

6. Select the Use Interconnected Mode check box.

7. Click Select Target.
   A dialog box that contains all SonicWALL appliances managed by this SonicWALL GMS appears.

8. Select the SonicWALL appliance or group to which you will establish SAs and click the Select button. The name of the target appears in the Target SonicWALL Group/Node field.

9. Select one of the encryption methods from the Encryption Method list box.

10. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the Default LAN (WorkPort) Gateway field.

    A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the Route all Internet traffic through destination unit check box. The Default LAN (WorkPort) Gateway field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

    Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

11. To enable NetBIOS broadcasts across the SA, select the Enable Windows Networking (NetBIOS) Broadcast check box.

12. To allow the remote VPN tunnel to be included in the routing table, select the Forward Packets to Remote VPNs check box.
Normally, inbound traffic is decrypted and only forwarded to the local LAN or a manually specified route (see “Configuring Routes” on page 101). This option enables you to create a “hub and spoke” network configuration where all traffic is routed among branch offices via the corporate office.

*Note:* To create a “hub and spoke” network, make sure to select the **Forward Packets to Remote VPNs** check box for each SA.

13. To force all network traffic to the WAN through a VPN to a central site, select the **Route all Internet traffic through destination unit** check box.

When this option is selected, all traffic that is not destined for another SA is forwarded through this VPN tunnel. If this option is not specified and the destination does not match any SA, the packet is forwarded unencrypted to the WAN.

14. Select from the following NAT and Firewall Rules:

   - To disable NAT and not apply firewall rules to traffic coming through this SA, select **Disabled**.
   - To enable NAT and firewall rules for the selected SonicWALL appliance, select **Source**. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and network firewall rules will be applied to all traffic on this SA.
   - To enable NAT and firewall rules for the selected SonicWALL appliance and its peer, select **Source** and **Destination**. If NAT is enabled, all traffic originating from this appliance will appear to originate from a single IP address and all traffic originating from its peer will appear to originate from a single IP address. Network firewall rules will be applied to all traffic on this SA.

*Note:* Applying firewall rules can dramatically affect services that run between the networks. For more information, see Chapter 9, “Configuring Network Access Rules.”

15. Select how local users are authenticated:

   - To disable authentication for local users, select **Disabled**.
   - To configure local users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
   - To configure local users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
   - To authenticate local users both locally and on the destination network, select **Source** and **Destination**.

16. Select how remote users are authenticated:

   - To disable authentication for remote users, select **Disabled**.
   - To configure remote users to be authenticated locally, either through the SonicWALL device or the RADIUS server, select **Source**.
   - To configure remote users to be authenticated on the destination network, either through the SonicWALL device or the RADIUS server, select **Destination**.
   - To authenticate remote users both locally and on the destination network, select **Source** and **Destination**.

17. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

*Note:* To disable this SA, select the **Disable this SA** check box and click **Update**.

**When One Appliance Is Not Managed by SonicWALL GMS**

This section describes how to configure VPN when the target appliance is not managed by SonicWALL GMS.

To enable VPN using manual keying, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the VPN tree and click **Configure**. The VPN Configure page appears (Figure 92).
4. Select **Manual Key** in the IPSec Keying mode section.

5. Select from the following:
   - To add a new SA, select **Add a new Security Association**.
   - To delete an existing SA, select **Delete an existing Security Association**.
   - To edit an existing SA, select **Modify an existing Security Association**.

6. Enter a descriptive name for the SA in the **Security Association Name** field.

7. Enter the IP address of the remote firewall in the **IPSec Gateway Address** field. This address must be valid and will be the public IP address if the remote LAN has NAT enabled.

8. To specify the default LAN (WorkPort) gateway, enter the IP address of the gateway in the **Default LAN (WorkPort) Gateway** field. A Default LAN (WorkPort) Gateway is used at a central site in conjunction with a remote site using the **Route all Internet traffic through destination unit** check box. The **Default LAN (WorkPort) Gateway** field allows the network administrator to specify the IP address of the default LAN route for incoming IPSec packets for this SA.

   Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPSec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

9. To access remote resources within the Windows Network Neighborhood, select the **Enable Windows Networking (NetBIOS) Broadcast** check box.

10. To apply NAT and firewall rules to all traffic coming through this SA, select the **Apply NAT and firewall rules** check box.

   This feature is useful for hiding the LAN subnet from the corporate site. All traffic will appear to originate from a single IP address.

11. To allow the remote VPN tunnel to be included in the routing table, select the **Forward Packets to Remote VPNs** check box.
This will enable the SonicWALL appliance to receive VPN traffic, decrypt it, and forward it to another VPN tunnel. This feature can be used to create a “hub and spoke” network configuration by routing traffic among SAs. To do this, make sure to enable this option for all SAs.

12. Select one of the encryption methods from the **Encryption Method** list box.

13. Enter the key used for encryption in the **Encryption Key** field. The DES and ARCFour Keys must be exactly 16 characters long and be composed of hexadecimal characters. Encryption keys less than 16 characters will not be accepted; keys longer than 16 characters will be truncated.

   **Note:** Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

   This key must match the encryption key of the remote VPN gateway or client. If encryption is not used, this field is ignored.

14. Enter the key used for authentication in the **Authentication Key** field. The authentication key must be exactly 32 characters long and be composed of hexadecimal characters. Authentication keys less than 32 characters will not be accepted; keys longer than 32 characters will be truncated.

   **Note:** Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef1234567890abcdef.”

   This key must match the authentication key of the remote VPN gateway or client. If authentication is not used, this field is ignored.

15. Enter the Security Parameter Index (SPI) that the remote location will send to identify the Security Association used for the VPN Tunnel in the **Incoming SPI** field.

   **Note:** The SPI may be up to eight characters long and be composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f).

   The hexadecimal characters “0” to “ff” inclusive are reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. For example, a valid SPI would be “1234abcd.”

   **Note:** The SPI for an SA must be unique when compared to SPIs for other SAs. However, the Incoming SPI can be the same as the Outgoing SPI on the same SA.

16. Enter the Security Parameter Index (SPI) that the local SonicWALL VPN will transmit to identify the Security Association used for the VPN Tunnel in the **Outgoing SPI** field.

17. Select from the following:
   - To allow this SA to be used as the default route for all Internet traffic, select **Use this SA as default route for all Internet traffic**.
   - To specify destination networks, select **Specify destination networks below**. Then, click **Modify** and enter the destination network IP addresses and subnet masks.

18. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

19. Create an SA in the remote VPN device for each SonicWALL appliance that you have configured.

   **Note:** To disable this SA without deleting it, select the **Disable this SA** check box and click **Update**.

---

**Management of VPN Client users**

To configure VPN Clients on SonicWALL appliances, follow these procedures:

- Obtain and activate VPN Client licenses for each SonicWALL appliance—see “Adding VPN Client Licenses to SonicWALL Appliances” on page 161.
- Enable VPN Clients for each SonicWALL appliance—see “Enabling VPN Client” on page 129.

**Enabling VPN Client**

After applying a VPN Client license to one or more SonicWALL appliances, follow these steps:

1. Ensure that the Group VPN is enabled (Figure 93).
2. To email the SPD file to the SonicWALL GMS administrator or the VPN Client user, click Email SPD file. The file is attached to the email. A task is scheduled for each email.

   Note: A copy of the SPD file is also stored in the SonicWALL Agent's <sgms_directory\etc directory.

3. Once the SPD file is received, it can be loaded by the VPN Client software on the VPN Client user's computer.

4. If the user does not have the VPN Client software, you can send both the SPD file and the email client software by clicking Email SPD File and VPN Client.

   Note: Before the VPN client can be emailed to users, it must be downloaded to the <sgms_directory\etc directory from Mysonicwall.com.

**Downloading VPN Client Software**

To download the VPN Client software from Mysonicwall.com, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click SGMS License.
4. Click Login in a new window. This will open a new browser into the SGMS account on Mysonicwall.com.
5. Download the VPN Client software from Mysonicwall.com to a local directory.
6. Copy the VPN Client software to SonicWALL Agent's <sgms_directory\etc directory.
7. Rename the file to SWVpnClient.zip.
Basic Terms and Concepts

Before installing and configuring SonicWALL VPN, it is important to understand the following basic terms and concepts.

- **VPN Tunnel**
  Tunneling is the encapsulation of point-to-point transmissions inside IP packets. A VPN Tunnel is a term that is used to describe a connection between two or more private nodes or LANs over a public network, typically the Internet. Encryption is often used to maintain the confidentiality of private data when traveling over the Internet.

- **Encryption**
  Encryption is a mathematical operation that transforms data from “clear text” (something that a human or a program can interpret) to “cipher text” (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric “key” be supplied along with the clear text. The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms cipher text to clear text. Decryption also requires a key.

- **Key**
  A key is an alphanumeric string that is used by the encryption operation to transform clear text into cipher text. A key is composed of hexadecimal characters (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). A valid key would be 1234567890abcdef. Keys used in VPN communications can vary in length, but are typically 16 or 32 characters. The longer the key, the more difficult it is to break the encryption. The reason for this is that most methods used to break encryption involve trying every possible combination of characters, similar to trying to find someone’s telephone number by dialing every possible combination of phone numbers.

- **Asymmetric vs. Symmetric Cryptography**
  Asymmetric and symmetric cryptography refer to the keys used to authenticate, or encrypt and decrypt the data. Asymmetric cryptography, or public key cryptography, uses two keys for verification. Organizations such as RSA Data Security and VeriSign support asymmetric cryptography.
  With symmetric cryptography, or secret key cryptography, is usually faster than asymmetric cryptography. Therefore symmetric algorithms are often used when large quantities of data need to be exchanged.
  SonicWALL VPN uses symmetric cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- **Security Association (SA)**
  An SA is the group of security settings needed to create a VPN tunnel. All SAs require an encryption method, an IPsec gateway address, and a destination network address. IKE includes a shared secret. Manually keying includes two SPIs and an encryption and authentication key.
  SonicWALL PRO appliances supports up to 100 SAs. SonicWALL SOHO2 and SonicWALL XPRS2 appliances support 10 and 25 SAs, respectively. Different SAs may be created to connect branch offices, allow secure remote management, and pass unsupported traffic.

- **Internet Key Exchange (IKE)**
  IKE is a negotiation and key exchange protocol specified by the Internet Engineering Task Force (IETF). An IKE SA automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass IP traffic.

- **Manual Key**
  Manual keying allows the SonicWALL administrator to specify the encryption and authentication keys. SonicWALL VPN supports the ability to manually set up a security association as well as the ability to automatically negotiate an SA using IKE.

- **Shared Secret**
  A shared secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE SA. This field can be any combination of alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Precautions should be taken when delivering/exchanging this shared secret to assure that a third party cannot compromise the security of a VPN tunnel.
- **Encapsulating Security Payload (ESP)**
  ESP provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption may be in the form of ARCFour (similar to the popular RC4 encryption method), DES, etc.

  The use of ESP typically increases the processing requirements and communications latency. The increased latency is primarily due to the encryption and decryption required for each IP packet containing an ESP.

  ESP typically involves encryption of the packet payload using standard encryption mechanisms, such as RC4, ARCFour, DES, or 3DES.

  ESP has no mechanism for providing strong integrity and authentication of the data.

- **Authentication Header (AH)**
  The authentication header is a mechanism for providing strong integrity and authentication for IP packets. The Authentication Header does not offer confidentiality and protection from traffic analysis.

  The IP authentication header provides security by adding authentication information to an IP packet. This authentication information is calculated using all header and payload data in the IP packet. This provides significantly more security than is currently present in IP.

  Use of an AH will increase the processing requirements of SonicWALL VPN and will also increase the communications latency. The increased latency is primarily due to the calculation of the authentication data by the sender and the calculation and comparison of the authentication data by the receiver for each IP packet.

- **Data Encryption Standard (DES)**
  When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. The SonicWALL DES encryption algorithm uses a 56-bit key.

  The DES Key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

- **Triple Data Encryption Standard (3DES)**
  3DES is the same as DES, except that it applies three DES keys in succession and is significantly more secure. However, 3DES has significantly more processing requirements than DES.

  The 3DES Key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

- **ARCFour**
  ARCFour is used for communications with secure Web sites using the SSL protocol. Many banks use a 40-bit key ARCFour for online banking, while others use a 128-bit key. SonicWALL VPN uses a 56-bit key for ARCFour.

  The ARCFour key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

- **Security Parameter Index (SPI)**
  The SPI is used to establish a VPN tunnel. The SPI is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption, and key values that the administrator associated with the SPI to establish the tunnel.

  The SPI must be unique, is from one to eight characters long, and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, valid SPLs would be 999 or “1234abcd.”
Configuring Anti-Virus Settings

SonicWALL Global Management System (SonicWALL GMS) offers anti-virus protection on a subscription-basis through a partnership with McAfee.

*Note:* SonicWALL appliances are entitled to a one-month anti-virus trial subscription. To enable the trial subscription, see “Adding Anti-Virus Protection to SonicWALL Appliances” on page 164.

Select from the following:

- To change the anti-virus password, see “Changing Anti-Virus Password” on page 134.
- To change standard anti-virus settings, see “Configuring Anti-Virus Settings” on page 134.
- To configure the anti-virus email filter, see “Configuring Anti-Virus Email Filter Settings” on page 136.
- To create a License Sharing Group that can be used to share anti-virus licenses among multiple SonicWALL appliances, see “Creating License Sharing Groups” on page 138.
Changing Anti-Virus Password

This section describes how to configure the Anti-Virus password for SonicWALL appliances.

To configure the Anti-Virus password for one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Anti-Virus tree and click Password. The AV Password page appears (Figure 94).

**Figure 94: AV Password Page**

4. Select from the following:
   - If a single SonicWALL appliance is selected, enter a new password and click Change Anti-Virus Password. The password is changed.
   - If the global or group view is selected, click Change Anti-Virus Password(s) Randomly. The password(s) are changed.

Configuring Anti-Virus Settings

This section describes how to configure Anti-Virus settings for SonicWALL appliances.

To configure Anti-Virus settings for one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Anti-Virus tree and click Configure. The Configure page appears (Figure 95).
4. Select the **Enable Anti-Virus** check box.

5. To enforce Anti-Virus protection on the DMZ port or HomePort (if available), select the **Enable DMZ (HomePort) Policing** check box.

6. SonicWALL GMS automatically downloads the latest virus definition files. To configure the maximum number of days that can pass before SonicWALL GMS downloads the latest files, select the number of days from the **Maximum Days Allowed Before Forcing Update** list box.

7. Significant virus events can occur without warning (e.g., Melissa, ILOVEYOU, and others). When these occur, SonicWALL GMS can be configured to block network traffic until the latest virus definition files are downloaded. To configure this feature, determine which types of events will require updating. Then, select the **Low Risk**, **Medium Risk**, or **High Risk** check boxes.

8. To configure the SonicWALL appliance(s) to only check for updates once a day, select the **Reduce AV Traffic for ISDN connections** check box. This is useful for low bandwidth connections or connections that are not “always on.”

9. To enable infected email attachment blocking on inbound SMTP and POP3 e-mail protocols, select the **Enable E-mail Attachment Filtering Alert Service** check box. The SonicWALL appliance will block viruses that are discovered by the virus signature files and filenames that are known to be infected during an outbreak even before Anti-Virus signature (DAT) files are available.

This feature also provides full filename blocking of virus files. The full filename attachment filtering allows SonicWALL to block only malicious attachments, while enabling all other attachments through. For example, during a virus outbreak, only the virus file is blocked while other productive files (such as Word documents and Excel spreadsheets) are allowed through.

*Note: Only files that were discovered to be infected will be blocked. If a message contains uninfected attachments, those will be forwarded to the recipient.*

10. Select from the following:
   - **To configure the SonicWALL appliance(s) to provide Anti-Virus enforcement for all computers on the network,** select **Enforce Anti-Virus policies for all computers.**
   - **To configure the SonicWALL appliance(s) to provide Anti-Virus enforcement for a specific list of computers,** select **Include specific address ranges in the Anti-Virus enforcement** and enter ranges of IP addresses in the **Addr Range Begin** and **Addr Range End** fields.
To configure the SonicWALL appliance(s) to provide Anti-Virus enforcement for all computers except those listed, select **Exclude specific address ranges in the Anti-Virus enforcement** and enter ranges of IP addresses in the **Addr Range Begin** and **Addr Range End** fields.

11. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### Configuring Anti-Virus Email Filter Settings

This section describes how to configure SonicWALL appliances to automatically scan email messages for viruses.

To configure email filter settings for one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Anti-Virus tree and click **EMail Filter**. The EMail Filter page appears (Figure 96).

#### Figure 96: Email Filter Page

4. Select the **Enable Email Attachment Filtering** check box.
5. To add an extension to scan for viruses, enter the extension in the Extensions field and click **Add**. Hackers commonly spread viruses through Visual Basic and Windows Executable files, therefore "vbs" and "exe" are provided as default extensions for this feature.
6. To configure the SonicWALL appliance(s) to disable infected attachment files as they pass through the SonicWALL by changing their extensions, select **Disable forbidden file by altering the file extension**. The SonicWALL appliance replaces the third character of file extensions with "_". If the email attachment is a valid file, the message recipient may return the attachment to its original file extension without damaging the file.
7. To configure the SonicWALL appliance(s) to delete infected files, select **Delete forbidden file**.
8. Enter warning text that will be attached to the message and forwarded to the message recipient (maximum 256 characters).
9. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

The SonicWALL appliance will block viruses that are discovered by the virus signature files and filenames that are known to be infected during an outbreak.
Note: Only infected files will be blocked. If a message contains uninfected attachments, those will be forwarded to the recipient.
Creating License Sharing Groups

Anti-Virus License Sharing allows you to share an Anti-Virus license among multiple SonicWALL appliances. License sharing assigns a License Sharing Group (LSG) to a SonicWALL appliance from which this feature is activated. You may then add other SonicWALL appliances to the LSG and assign them Anti-Virus licenses from the pool of remaining available licenses.

Select from the following:
- To create an LSG, see “Creating a License Sharing Group” on page 138.
- To add SonicWALL appliances to an existing LSG, see “Adding a SonicWALL Appliance to an Existing Group” on page 139.
- To change the number of licenses that a SonicWALL appliance uses, see “Changing the Number of Licenses” on page 140.

Creating a License Sharing Group

To create an LSG, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance that has an anti-virus license to share. If no appliance has a license to share, see “Adding Anti-Virus Protection to SonicWALL Appliances” on page 164.
3. Expand the Register/Upgrades tree and click Anti-Virus Upgrade. The Anti-Virus Upgrade page appears (Figure 97).

Figure 97: Anti-Virus Upgrade Page

4. Click Join a License Sharing Group. The Join a License Sharing Group dialog box appears (Figure 98).
5. Select **Create a new License Sharing Group With** and select another SonicWALL appliance that will belong to the group. Then, enter a name for the group and click **Accept**. SonicWALL GMS initiates a task that creates a new group which will use the licenses from this SonicWALL appliance.

This SonicWALL appliance will start with no anti-virus licenses. To select the number of licenses it will use, see “Changing the Number of Licenses” on page 140.

### Adding a SonicWALL Appliance to an Existing Group

To add a SonicWALL appliance to an existing LSG, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Register/Upgrades tree and click **Anti-Virus Upgrade**. The Anti-Virus Upgrade page appears (Figure 99).

   **Figure 99: Anti-Virus Upgrade Page**

4. Click **Join a License Sharing Group**. The Join a License Sharing Group dialog box appears (Figure 100).
5. Select **Join Existing License Sharing Group** and select an LSG from the list box.

6. Click **Accept**. SonicWALL GMS initiates a task that will assign this SonicWALL appliance to the group.

   This SonicWALL appliance will start with no anti-virus licenses. To select the number of licenses it will use, see “Changing the Number of Licenses” on page 140.

### Changing the Number of Licenses

To change the number of licenses that a SonicWALL appliance will use, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance that is assigned to an existing LSG.
3. Expand the Register/Upgrades tree and click **Anti-Virus Upgrade**. The Anti-Virus Upgrade page appears (Figure 101).

   **Figure 101: Anti-Virus Upgrade Page**

4. Enter a new value and click **Change License count**. SonicWALL GMS initiates a task that changes the license count.
Configuring High Availability Settings

The high availability feature configures a pair of SonicWALL PRO or PRO-VX appliances as a primary and backup. The backup monitors the primary through a series of heartbeats. If the backup detects that the primary is unavailable or has failed, it will replace the primary.

This chapter describes how to use the SonicWALL Global Management System (SonicWALL GMS) to configure high availability.

To configure high availability, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the High Availability tree and click **Configure**. The Configure page appears (Figure 102).

   ![Figure 102: Configure Page](image)

4. Enter the LAN (WorkPort) and WAN IP addresses of the primary.
5. Select the **Enable High Availability** check box.
6. Enter the serial number of the backup.
7. Enter the LAN (WorkPort) and WAN IP addresses of the backup SonicWALL appliance.
8. To configure the primary SonicWALL appliance to take over from the backup SonicWALL appliance when it becomes available, select the Preempt Mode check box. Otherwise, the backup SonicWALL appliance will remain active.

9. Enter the heartbeat interval (in seconds) in the Heartbeat Interval field.

10. When a SonicWALL appliance becomes active after startup, it looks for an active SonicWALL appliance that is configured for High Availability. If the other appliance is active, it transitions to Idle mode. Sometimes, due to network latency and other issues, it may take a while to find the other SonicWALL appliance.

   To specify how long the SonicWALL appliance will look, enter the number of seconds in the Detection Delay Time field. You can enter a value between 0 and 300 seconds, but the default value of 0 seconds is sufficient in most cases.

11. Specify how long the backup waits before replacing the primary (in seconds) in the Failover Trigger Level field.

12. When changes are made to the Primary or Backup firewall, the changes are automatically synchronized between the two firewalls. To cause the synchronization to occur now, click Synchronize Now. The Backup SonicWALL will restart and become temporarily unavailable while it updates its settings.

   Note: If you change the IP address of either SonicWALL appliance, synchronization cannot occur between the two SonicWALL appliances without updating the changes manually on the High Availability page.

13. When you are finished, click Update. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click Reset.
Configuring PKI Options

This chapter describes how to use the SonicWALL Global Management System (SonicWALL GMS) to import, export, and revoke Public Key Infrastructure (PKI) administration certificates and to modify or revoke end user certificates.

Working with PKI Administrator Certificates

This section describes the procedures for importing, exporting, and revoking administrator certificates.

If a SonicWALL appliance that currently has an administrator certificate is added to SonicWALL GMS, you can export its administrator certificate to SonicWALL GMS. To do this, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the SonicWALL appliance.
3. Expand the PKI tree and click Admin Cert. The Admin Certificates page appears (Figure 103).

4. Enter the Certificate Management Password (CMP) for the SonicWALL appliance in the Correct password (CMP) To field. Do not use this field to change the CMP.
5. To export the administrator certificate for the SonicWALL appliance into the SonicWALL GMS database, click Export Admin Certificates from firewall(s) to SGMS.
6. Once SonicWALL GMS has the administrator certificate for the SonicWALL appliance, the certificate can be revoked at any time. To revoke the certificate, click Revoke.

Warning: If you revoke a certificate, you must purchase a new one.

7. If the SonicWALL appliance loses its administrator certificate, you can copy it from the SonicWALL GMS database to the SonicWALL appliance. To copy the certificate, click Import Admin Certificates from SGMS to firewall(s).

Note: You can import and revoke certificates for a group of SonicWALL appliances at the group level.

---

### Working with PKI End User Certificates

To make changes to one or more PKI end user certificates, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the PKI tree and click End-User Cert. The End-User Certificates page appears (Figure 104).

![Figure 104: End-User Cert Page](image)

4. Enter the first and last name of the user to whom this certificate will be assigned.
5. Enter the email address of the user.
6. Enter the organization, department, title, city, state, and country information for the user.
7. Enter the challenge phrase.
8. Enter the challenge response.
9. Select from the following:
   - To issue the certificate, select Issue.
   - To revoke the certificate, select Revoke.

Warning: If you revoke a certificate, you must purchase a new one.

10. When you are finished, click Update. The settings are changed for the selected SonicWALL appliance(s). To clear all screen settings and start over, click Reset.
Configuring Modem Options

This chapter describes how to configure the modem settings for SonicWALL SmartPath (SP) appliances. SonicWALL SP appliances have a WAN Failover feature. When the primary broadband connection becomes unavailable, SonicWALL SP appliances automatically use built-in modems to establish Internet connectivity. This is ideal when the SonicWALL appliance must remain connected to the Internet, regardless of network speed.

Configuring the Modem Profile

A profile is a list of modem connection settings that can be used by a SonicWALL SP appliance. To configure a profile, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the SonicWALL appliance.
3. Expand the Modem tree and click **Profile**. The Profile page appears (Figure 105).

![Figure 105: Profile Page](image)

4. To edit an existing profile or use an existing profile as a template, select a profile from the **Current Profile** list box.
5. Select from the following:
   - If this will be a new profile, enter the name of the profile in the **Name** field.


• If you are editing an existing profile, make sure the entry in the **Name** field matches the profile that you are editing.

6. Enter the primary phone number of the ISP in the **Primary phone number** field.
7. Enter the backup phone number in the **Secondary phone number** field.
8. Enter the username associated with the account in the **User** field.
9. Enter the password associated with the account in the **Password** and **Confirm Password** fields.
10. Select from the following IP address options:
    - If the account obtains an IP address dynamically, select **Obtain automatically**.
    - If the account uses a fixed IP address, select **Specify** and enter the IP address.
11. Select from the following DNS server options:
    - If the account obtains DNS server information from the ISP, select **Obtain automatically**.
    - If the account uses a specific DNS servers, select **Specify** and enter the DNS server IP addresses.
12. Enter a chat script (optional).
13. Select from the following connection options:
    - If the SonicWALL appliance(s) will remain connected to the Internet until the broadband connection is restored, select **Persistent Connection**.
    - If the SonicWALL appliance(s) will only connect to the Internet when data is being sent, select **Dial On Data**.
    - If the SonicWALL appliance(s) will connect to the Internet manually, select **Manual Dial**.
14. To specify how long the modem waits before disconnecting from the Internet, enter the amount of time in the **Inactivity Timeout** field.
15. To specify a maximum connection speed, select the speed from the **Max connection speed** list box. Otherwise, make sure Auto is selected.
16. To disable call waiting, select **Disable Call Waiting** and select the touch tone disabling code.
17. If the modem is unable to connect to the ISP, specify the number of retries in the **Dial Retries per phone number** field.
18. To specify how long the modem waits between retries, specify how long in the **Delay between Retries** field.
19. When you are finished, click **Update**. The profile is added. To clear all screen settings and start over, click **Reset**.

---

**Configuring the Modem**

To configure the WAN Failover feature for one or more SonicWALL SP appliances, follow these steps:
1. Start and log into SonicWALL GMS.
2. Select the SonicWALL appliance.
3. Expand the Modem tree and click **Configure**. The Configure page appears (Figure 106).
4. Select the first profile that the SonicWALL appliance will attempt to use when the broadband connection is not available from the Primary Profile list box.

5. Select the second profile that the SonicWALL appliance will attempt to use when the broadband connection is not available from the Secondary Profile list box.

6. Select the volume of the speaker from the Speaker volume list box.

7. Enter any AT commands that the modem will need to use to establish a connection in the AT Commands field.

8. Enable the WAN Failover feature by selecting the Enable WAN Failover check box.

9. Enter the IP address that the SonicWALL appliance will use to test Internet connectivity in the Probe Target field. We recommend using the IP address of the WAN Gateway.

10. Specify how often the IP address will be tested in the Probe Interval field.

11. Specify how many times the probe target must be unavailable before the SonicWALL appliance fails over to the modem in the Failover Trigger Level field.

12. Specify how many times the SonicWALL appliance must successfully reach the probe target to reactivate the broadband connection in the Successful probes to reactivate Primary field.

13. When you are finished, click Update. WAN Failover is enabled for the selected SonicWALL SP appliances. To clear all screen settings and start over, click Reset.
Maintaining SonicWALL Appliances

This chapter describes SonicWALL appliance maintenance procedures. These procedures include the following:

- How to upgrade firmware for one or more SonicWALL appliances—see “Upgrading SonicWALL Appliances” on page 149.
- How to restart SonicWALL appliances—see “Restarting SonicWALL Appliances” on page 150.
- How to synchronize one or more SonicWALL appliances with SonicWALL GMS—see “Synchronizing Now” on page 151.
- How to request diagnostics for SonicWALL appliances—see “Requesting Diagnostics for SonicWALL” on page 152.
- How to configure a SonicWALL appliance to inherit settings from a group—see “Inheriting Group Settings” on page 153.

Upgrading SonicWALL Appliances

SonicWALL firmware is updated on a periodic basis to offer new functionality and address any known issues. After a SonicWALL appliance is added to SonicWALL GMS management, its auto-update feature is disabled. SonicWALL GMS periodically polls Mysonicwall.com site for new firmware versions. Once a new version of firmware is detected and available, SonicWALL GMS sends an email notification to the SonicWALL GMS administrator.

Note: If you want to disable firmware notifications, see “Configuring SonicWALL GMS Settings” on page 220.

To upgrade to the latest firmware, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the Register/Upgrades tree and click Firmware Upgrade.
4. Click the Firmware Upgrade button. SonicWALL GMS schedules a firmware update task for each SonicWALL appliance.

When SonicWALL GMS runs a firmware update task, it checks the firmware version of the SonicWALL appliance and determines whether there is a newer version available on the SonicWALL website.

If it finds a newer version, it downloads the file to the \Firmware\Current subdirectory of the SonicWALL GMS directory and applies it to the SonicWALL appliance. Additionally, SonicWALL GMS copies the old firmware files to the \Firmware\Old subdirectory of the SonicWALL GMS directory.

If a newer firmware version is not found, SonicWALL GMS logs a message that indicates the SonicWALL appliance already has the latest firmware.

Unlike firmware major and minor releases, SonicWALL firmware patches are generally not posted to the web. To upgrade to a firmware patch, follow these steps:

1. Copy the firmware patch to the \Firmware\Current subdirectory of the SonicWALL GMS directory.
2. Start and log into SonicWALL GMS.
3. Click the Console tab.
4. Expand the Login tree and click SGMS Settings.
5. Select Enable Local SonicWALL Firmware Download and click Update.
6. Click the Policies tab.
7. Click the SonicWALLs tab.
8. Select the global icon, a group, or a SonicWALL appliance.
9. Expand the Register/Upgrades tree and click Firmware Upgrade.
10. Click the Firmware Upgrade button. SonicWALL GMS schedules a firmware update task for each SonicWALL appliance.

In this case, when SonicWALL GMS runs a firmware update task, it checks the firmware patch in the \Firmware\Current subdirectory of the SonicWALL GMS directory and applies it to the SonicWALL appliance. Additionally, SonicWALL GMS copies the old firmware files to the \Firmware\Old subdirectory of the SonicWALL GMS directory.

## Restarting SonicWALL Appliances

Some SonicWALL GMS changes require the SonicWALL appliance(s) to automatically be restarted after changes are applied. However, there may be instances when you want to restart the SonicWALL appliance(s) manually.

**Note:** We recommend restarting the SonicWALL appliance(s) when network activity is low.

To restart one or more SonicWALL appliances, follow these steps:
1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the General tree and click Tools. The Tools page appears (Figure 107).

**Figure 107: Tools Page**

4. To restart the selected SonicWALL appliance(s), click Restart SonicWALL.
Synchronizing Now

If a change is made to the SonicWALL appliance from the local interface, SonicWALL GMS will be notified of the change through the syslog data stream. After this notification is received, SonicWALL GMS will schedule a task to synchronize its database with the local change. After the task successfully executes, the current configuration (prefs) file is read from the SonicWALL appliance and loaded into the database.

**Note:** After receiving and processing the localesync status message from syslog, SonicWALL GMS drops the status message and does not store it in the ViewPoint database. Also if syslog is forwarded from SonicWALL GMS to another syslog server, SonicWALL GMS will still not retain the localesync status message.

Auto synchronization automatically occurs whenever SonicWALL GMS receives a local change notification status syslog message from a SonicWALL appliance.

You can also force an auto synchronization at any time for a SonicWALL appliance or a group of SonicWALL appliances. To do this, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the General tree and click **Tools**. The Tools page appears (Figure 107).

**Figure 108: Tools Page**

4. To synchronize the selected SonicWALL appliance(s), click **Synchronize Now**. SonicWALL GMS schedules a task to synchronize the selected SonicWALL appliances.

**Note:** The auto synchronization feature can be disabled on the Login/SGMS Settings page.
Requesting Diagnostics for SonicWALL

To request diagnostics for one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance.
3. Expand the General tree and click **Tools**. The Tools page appears (Figure 107).

   **Figure 109: Tools Page**

4. To request diagnostics for the selected SonicWALL appliance(s), click **Request Diagnostics**. SonicWALL GMS schedules a task to immediately request diagnostics for the selected SonicWALL appliances.

5. To view the diagnostics, see “Viewing the Snapshot or Diagnostics” on page 233.
Inheriting Group Settings

If you move SonicWALL appliances between groups, the SonicWALL appliances can inherit the settings from the new group.

To move one or more SonicWALL appliances inheriting the group settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the SonicWALL appliance.
3. Expand the General tree and click Tools. The Tools page appears (Figure 110).

![Figure 110: Tools Page](image)

4. Click Inherit Settings from Group.
   You are prompted to continue.

5. To inherit the settings from the new group, click OK. To cancel without applying the group settings, click Cancel.
   One or more tasks are scheduled and the SonicWALL appliance(s) will receive the group settings.

   *Note: For the Access/Services and Access/Rules pages, by default, inheriting group settings overwrites the values at the unit level with the group values. If you wish for SonicWALL GMS to append the group settings to the values at the unit level, you need to enable the Append Group Settings option on the General/SGMS Settings page on the Console Panel.*

Adding Contact Information

To add contact information for a SonicWALL appliance, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select a SonicWALL appliance.
3. Expand the General tree and click Info. The Info page appears (Figure 111).
4. Enter the contact information in the provided fields.
5. Click **Update**.
6. To clear all screen settings and start over, click **Reset**.
Upgrading SonicWALL Appliances

This chapter describes the procedures for upgrading SonicWALL appliances. The following functionality can be added to SonicWALL appliances connected to the SonicWALL Global Management System (SonicWALL GMS):

- Additional Nodes—see “Adding Nodes to SonicWALL Appliances” on page 155.
- Content Filter List Subscription—see “Adding the Content Filter List to SonicWALL Appliances” on page 157.
- Virtual Private Network (VPN) Functionality—see “Adding Virtual Private Networking to SonicWALL Appliances” on page 159.
- VPN Client Upgrades—see “Adding VPN Client Licenses to SonicWALL Appliances” on page 161.
- Anti-Virus Licenses—see “Adding Anti-Virus Protection to SonicWALL Appliances” on page 164.
- PKI Administrator Certificate—see “Adding PKI Administrator Certificates” on page 166.
- PKI End User Certificate—see “Adding PKI End User Certificates” on page 168.

When a SonicWALL GMS subscription service (i.e., warranty support, anti-virus, or content filtering) is about to expire, the SGMS administrator will receive expiration notifications via email prior to the expiration. The email notification is sent once a day (if applicable) and lists all managed SonicWALL appliances with expiring subscription services.

Adding Nodes to SonicWALL Appliances

To enable organizations to support additional systems within their network as they grow, SonicWALL appliances can be upgraded to support additional nodes. This section describes how to purchase and apply this functionality.

Purchasing Node Upgrades

To purchase node upgrades, follow these steps:

1. Contact your SonicWALL sales representative.
   You will receive an activation code for each node upgrade that you purchase.
2. After receiving the activation codes for the SonicWALL node upgrade, continue to the next section.

Licensing Node Upgrades

To license node upgrades, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click SonicWALL Upgrades. The SonicWALL Upgrades page appears (Figure 112).
4. Select **Node Upgrade** from the **Category** list box.

5. Select the size of the node upgrade from the **Type** list box.

6. Enter the activation code in the **Activation Code** field.

7. Click **Add Activation Code**.

   The license is added to SonicWALL GMS license pool.

8. Repeat Step 4 through 7 for each node upgrade that you want to add.

9. To activate the node upgrade(s), continue to the next section.

### Activating Node Upgrades

To activate node upgrades for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.

2. Select the global icon, a group, or a SonicWALL appliance. If you select a group, all SonicWALL appliances within that group will be upgraded. If the node upgrade does not apply to a SonicWALL appliance within the group, the upgrade will not be applied to that appliance.

3. Expand the Register/Upgrades tree and click **Node Upgrade**. The Node Upgrade page appears (Figure 113).
4. Verify that this is the SonicWALL appliance or group of appliances that you want to upgrade by checking the Current Status section.

5. To upgrade the appliance, click the Upgrade button.

### Adding the Content Filter List to SonicWALL Appliances

Each SonicWALL appliance comes with a free one-month trial subscription to the content filter list. The content filter list contains a list of potentially objectionable material that SonicWALL appliances can block based on administrator-configured options. For more information, see Chapter 8, “Configuring Website Blocking.”

To activate a content filter subscription, complete each procedure in this section. To activate a one-month trial subscription, follow the steps in “Activating Subscriptions for SonicWALL Appliances” on page 158.

### Purchasing Content Filtering Subscriptions

To purchase content filter list subscriptions, follow these steps:

1. Contact your SonicWALL sales representative.
   
   You will receive an activation code for each content filter list subscription that you purchase.

2. After receiving the activation codes, continue to the next section.

### Licensing Subscription Upgrades

To license content filter list subscription upgrades, follow these steps:

1. Start and log into SonicWALL GMS.

2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.

3. Expand the Licenses tree and click SonicWALL Upgrades. The SonicWALL Upgrades page appears (Figure 114).
4. Select **Content Filter Subscription** from the **Category** list box.
5. Select the size of the upgrade from the **Type** list box.
6. Enter the activation code in the **Activation Code** field.
7. Click **Add Activation Code**.
   
   The license is added to SonicWALL GMS license pool.
8. Repeat Step 4 through 7 for each content filter list subscription that you want to add.
9. To activate the subscriptions for SonicWALL appliances, continue to the next section.

**Activating Subscriptions for SonicWALL Appliances**

To activate content filter list or one-month trial subscriptions for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the content filter list subscription. If a SonicWALL appliance is already licensed for a content filter list, it will be skipped.
3. Expand the Register/Upgrades tree and click **Content Filter List**. The Content Filter List page appears (Figure 115).
4. Verify this is the SonicWALL appliance or group of appliances for which you want to configure content filter list by checking the Current Status section.

5. To upgrade the appliance(s), click Upgrade.

6. To activate the one-month trial subscription(s), click Free Trial.

---

**Adding Virtual Private Networking to SonicWALL Appliances**

SonicWALL appliances can be upgraded to support VPN. A VPN is a private network that uses encryption technologies to exchange data over public networks (e.g., the Internet). For more information, see Chapter 12, “Configuring Virtual Private Networking.”

**Purchasing VPN Upgrades**

To purchase VPN upgrades, follow these steps:

1. Contact your SonicWALL sales representative.
   
   You will receive an activation code for each VPN upgrade that you purchase.

2. After receiving the activation code(s), continue to the next section.

**Licensing a VPN Upgrade**

To license VPN upgrades, follow these steps:

1. Start and log into SonicWALL GMS.

2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.

3. Expand the Licenses tree and click **SonicWALL Upgrades**. The SonicWALL Upgrades page appears (Figure 116).
4. Select VPN Upgrade from the Category list box.
5. Select the size of the upgrade from the Type list box.
6. Enter the activation code in the Activation Code field.
7. Click Add Activation Code.
   The license is added to the SonicWALL GMS license pool.
8. Repeat Step 4 through 7 for each VPN upgrade that you want to add.
9. To activate the VPN upgrades for SonicWALL appliances, continue to the next section.

**Activating VPN Upgrades for SonicWALL Appliances**

To activate VPN upgrades for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the VPN upgrade. If a SonicWALL appliance is already licensed for VPN, that appliance will be skipped.
3. Expand the Register/Upgrades tree and click VPN Upgrade. The VPN Upgrade page appears (Figure 117).
4. Verify that this is the SonicWALL appliance or group of appliances to which you want to apply the VPN upgrade by checking the Current Status section.

5. To upgrade the appliance(s), click Apply VPN Upgrade.

### Adding VPN Client Licenses to SonicWALL Appliances

Support for VPN client licenses is available for SonicWALL appliances. This section describes how to purchase and activate VPN client licenses.

#### Purchasing VPN Client Licenses

To purchase VPN clients, follow these steps:

1. Contact your SonicWALL sales representative.
   
   You will receive an activation code for each VPN client license that you purchase.

2. After receiving the activation code(s), continue to the next section.

#### Licensing VPN Clients

To license VPN clients, follow these steps:

1. Start and log into SonicWALL GMS.

2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.

3. Expand the Licenses tree and click **SonicWALL Upgrades**. The SonicWALL Upgrades page appears (Figure 118).
4. Select **VPN Client Upgrade** from the **Category** list box.
5. Select the number of VPN clients to support from the **Type** list box.
6. Enter the activation code in the **Activation Code** field.
7. Click **Add Activation Code**.
   
   The license is added to SonicWALL GMS license pool.
8. Repeat Step 4 through 7 for each VPN client that you want to add.
9. To activate the VPN clients, continue to the next section.

**Activating VPN Clients**

To activate VPN clients for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the VPN clients. If a SonicWALL appliance already has an appropriate VPN client license, that appliance will be skipped.
3. Expand the Register/Upgrades tree and click **VPN Client Upgrade**. The VPN Client Upgrade page appears (Figure 119).
4. Verify that this is the SonicWALL appliance that you want to upgrade by checking the Current Status section.
5. To add the VPN client license upgrade, click Upgrade.
Adding Anti-Virus Protection to SonicWALL Appliances

This section describes how to obtain and activate an anti-virus subscription or a one-month trial for one or more SonicWALL appliances. For information on configuring anti-virus protection, see Chapter 13, “Configuring Anti-Virus Settings.”

To activate an anti-virus subscription, complete each procedure in this section. To activate a one-month trial subscription, follow the steps in “Activating Anti-Virus Subscriptions” on page 165.

*Note:* Anti-virus licenses can be shared among multiple SonicWALL appliances. For more information, see “Creating License Sharing Groups” on page 138.

Purchasing Anti-Virus Subscriptions

To purchase anti-virus subscriptions, follow these steps:

1. Contact your SonicWALL sales representative.
   You will receive an activation code for each anti-virus subscription that you purchase.
2. After receiving the activation codes, continue to the next section.

Licensing Anti-Virus Upgrades

To license anti-virus subscription upgrades, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the *Console Panel* tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click *SonicWALL Upgrades*. The SonicWALL Upgrades page appears (Figure 120).

   **Figure 120: SonicWALL Upgrades Page**

   ![SonicWALL Upgrades Page](image)

4. Select *Network Anti-Virus* from the *Category* list box.
5. Select the size of the upgrade from the *Type* list box.
6. Enter the activation code in the *Activation Code* field.
7. Click *Add Activation Code*. 
The license is added to SonicWALL GMS license pool.

8. Repeat Step 4 through 7 for each anti-virus subscription that you want to add.

9. To activate the upgrades, continue to the next section.

Activating Anti-Virus Subscriptions

To activate anti-virus subscriptions or free trials for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.

2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the anti-virus upgrade. If a SonicWALL appliance is already licensed for an anti-virus subscription, it will be skipped.

3. Expand the Register/Upgrades tree and click Anti-Virus Upgrade. The Anti-Virus Upgrade page appears (Figure 121).

Figure 121: Anti-Virus Upgrade Page

4. Verify that this is the SonicWALL appliance or group of appliances to which you want to add anti-virus protection by checking the Current Status section.

5. To upgrade the appliance(s), click Upgrade Anti-Virus Subscription. The Upgrade button can also be used when adding additional anti-virus licenses or when anti-virus subscriptions are expired.

6. To activate the free trial(s), click Free Trial.

7. To reactivate the anti-virus subscription if the firmware was corrupted, click Reactivate.

8. To renew anti-virus subscriptions before they expire, click Renew Anti-Virus Subscription.
Adding PKI Administrator Certificates

This section describes how to obtain and activate a Public Key Infrastructure (PKI) administrator certificate for one or more SonicWALL appliances.

Purchasing PKI Administrator Certificates

To purchase PKI administrator certificates, follow these steps:

1. Contact your SonicWALL sales representative.
   
   You will receive an activation code for each certificate that you purchase.

2. After receiving the activation codes, continue to the next section.

Licensing PKI Administrator Certificate Upgrades

To license PKI administrator certificates, follow these steps:

1. Start and log into SonicWALL GMS.

2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.

3. Expand the Licenses tree and click SonicWALL Upgrades. The SonicWALL Upgrades page appears (Figure 122).

4. Select PKI Administrator Certificate from the Category list box.

5. Select the type of the SonicWALL appliance to which the certificate will be applied from the Type list box.

6. Enter the activation code in the Activation Code field.

7. Click Add Activation Code. The license is added to SonicWALL GMS license pool.

8. Repeat Step 4 through 7 for each certificate you want to add.

9. To activate the certificate(s), continue to the next section.
Activating PKI Administrator Certificates

To activate PKI administrator certificates for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.

2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the PKI upgrade. If a SonicWALL appliance is already licensed for an PKI subscription, it will be skipped.

3. Expand the Register/Upgrades tree and click PKI Upgrade. The PKI Upgrade page appears (Figure 123).

4. Enter the name and email address of the administrator.

5. To upgrade the appliance, click Upgrade.
**Adding PKI End User Certificates**

This section describes how to obtain and activate PKI end user certificates for one or more SonicWALL appliances.

**Purchasing PKI End User Certificates**

To purchase PKI certificates, follow these steps:
1. Contact your SonicWALL sales representative.
   You will receive an activation code for each certificate that you purchase.
2. After receiving the activation codes, continue to the next section.

**Licensing a PKI End User Certificate Upgrade**

To license PKI end user certificates, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click **SonicWALL Upgrades**. The SonicWALL Upgrades page appears (Figure 124).

4. Select **PKI End User Certificate** from the **Category** list box.
5. Select the number of nodes for the certificate from the **Type** list box.
6. Enter the activation code in the **Activation Code** field.
7. Click **Add Activation Code**.
   The license is added to SonicWALL GMS license pool.
8. Repeat Step 4 through 7 for each certificate you want to add.
9. To activate the upgrades, continue to the next section.
Activating PKI End User Certificates

To activate PKI end user certificates for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the PKI upgrade. If a SonicWALL appliance is already licensed for a PKI subscription, it will be skipped.
3. Expand the Register/Upgrades tree and click **PKI Upgrade**. The PKI Upgrade page appears (Figure 125).

![Figure 125: PKI Upgrade Page]

4. Verify that this is the SonicWALL appliance or group of appliances that you want to upgrade by checking the Current Status section.
5. Enter the name and email address of the administrator.
6. To upgrade the appliance, click **Upgrade**.
Adding High Availability to SonicWALL Appliances

This section describes how to obtain and activate high availability upgrades for one or more SonicWALL Pro or Pro-VX appliances. For information on configuring high availability settings, see Chapter 14, “Configuring High Availability Settings.”

Purchasing High Availability Subscriptions

To purchase high availability upgrades, follow these steps:
1. Contact your SonicWALL sales representative.
   You will receive an activation code for each High Availability upgrade that you purchase.
2. After receiving the activation codes, continue to the next section.

Licensing High Availability Upgrade

To license High Availability upgrades, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click **SonicWALL Upgrades**. The SonicWALL Upgrades page appears (Figure 126).
   
   **Figure 126: SonicWALL Upgrades Page**

   4. Select **HA Upgrade** from the **Category** list box.
   5. Select the model of the SonicWALL appliance from the **Type** list box.
   6. Enter the activation code in the **Activation Code** field.
   7. Click **Add Activation Code**. The license is added to SonicWALL GMS license pool.
   8. Repeat Step 4 through 7 for each high availability upgrade that you want to add.
   9. To activate the upgrades, continue to the next section.
Activating High Availability Subscriptions

To activate high availability upgrades for SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.

2. Select the global icon, a group, or a SonicWALL appliance. If a group is selected, all SonicWALL appliances within that group will be upgraded for the high availability upgrade. If a SonicWALL appliance is already licensed for an high availability subscription, it will be skipped.

   **Note:** The high availability upgrade is only available for SonicWALL Pro and Pro-VX appliances.

3. Expand the Register/Upgrades tree and click **HA Upgrade**. The HA Upgrade page appears (Figure 127).

   **Figure 127: HA Upgrade Page**

4. Verify that this is the SonicWALL appliance or group of appliances to which you want to add the high availability upgrade by checking the Current Status section.

5. To upgrade the appliance(s), click **Apply HA Upgrade**.
Section III
Ravlin Devices
To prepare one or more Ravlin devices for SonicWALL Global Management System (SonicWALL GMS) management, you must update their firmware, configure them for SonicWALL GMS management, decide how they will be grouped, and add them to the SonicWALL GMS UI.

To configure one or more Ravlin devices for SonicWALL GMS management, follow these steps:

- Update the Ravlin devices to firmware version 3.8 or later. For more information, refer to the documentation that accompanied the Ravlin devices.
- Prepare Ravlin devices for SonicWALL GMS. For more information, see “Configuring Ravlin Devices” on page 176.
- Create fields that will be used to organize Ravlin devices. For more information on creating fields, see “Creating Ravlin Fields and Views” on page 181.
- Add the Ravlin device(s) to SonicWALL GMS. For more information, see “Adding Ravlin Devices to SonicWALL GMS” on page 185.
Configuring Ravlin Devices

Before a Ravlin device can be administered from the SonicWALL GMS UI, the following must occur:

- The firmware must be updated to version that is compatible with SonicWALL GMS (Version 3.8 or later). For more information, refer to the documentation that accompanied the Ravlin device.
- The devices must be configured for management by SonicWALL GMS. For more information, see “Configuring Devices for SonicWALL GMS Management” on page 176.

Configuring Devices for SonicWALL GMS Management

To configure the Ravlin device for remote management by SonicWALL GMS, open the Ravlin Node Manager and complete the following procedures:

- Set up the manual keys—see “Setting up Manual Keys” on page 176.
- Configure the policy settings—see “Configuring Policy Settings” on page 177.
- Configure the SonicWALL GMS settings— see “Setting up Manual Keys” on page 179.

Setting up Manual Keys

Once configured, the Ravlin device and SonicWALL GMS will communicate through a VPN tunnel. To configure the manual key settings so the Ravlin device and SonicWALL GMS will be able to communicate, follow these steps:

1. Open Policy Database, Key Management, and select Manual (Figure 128).

   **Figure 128: Ravlin Node Manager**

2. Right-click Manual and select Insert from the pop-up menu. The Manual Key Information dialog box appears (Figure 129).
3. Enter the following:

- **Encryption Key**
  
  Enter the key used for encryption in the **Encryption Key** fields. Make sure to enter the same key in both the **Inbound** and **Outbound** fields. The keys must be exactly 16 characters long and be composed of hexadecimal characters. Encryption keys less than 16 characters will not be accepted; keys longer than 16 characters will be truncated.

  **Note:** Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be "1234567890abcdef."

  This key must match the encryption key of the SonicWALL GMS agent.

- **Authentication Key**
  
  Enter the authentication key in the **Authentication Key** fields. Make sure to enter the same key in both the **Inbound** and **Outbound** fields. The authentication key must be exactly 32 characters long and be composed of hexadecimal characters. Authentication keys less than 32 characters will not be accepted; keys longer than 32 characters will be truncated.

  **Note:** Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be "1234567890abcdef1234567890abcdef."

  This key must match the authentication key of the SonicWALL GMS agent.

- **SPI**
  
  Enter the Ravlin device’s local Media Access Control (MAC) address as the Security Parameter Index (SPI). The SPI identifies the Security Association (SA) used for the VPN tunnel. Make sure to enter the local MAC address in both the **Inbound** and **Outbound** fields.

4. When you are finished, click **OK**. The manual key information is now configured. To clear the settings and start over, click **Cancel**.

### Configuring Policy Settings

Once configured, the Ravlin device and SonicWALL GMS will communicate through a VPN tunnel. To configure the policy that will be used, follow these steps:

1. Open **Policy Database** and select **Policy Data Entries** (Figure 130).
2. Right-click **Policy Data Entries** and select **Insert** from the pop-up menu. A new entry appears beneath **Policy Data Entries**.

3. Select and rename the entry (e.g., “SonicWALL GMS” or “SGMS”).

4. Expand the tree of the new entry and select **Peer Info** (Figure 131).

5. Complete the following information in the **Peer Info** page:
   - **Type**—select **VPN Gateway**.
   - **IP Address**—enter the SGMS Gateway’s WAN IP address.
   - **Distinguished Name**—do not change this setting (default: Not Available).
   - **Local IP Address**—do not change this setting (default 0.0.0.0).

6. Select **Key Management** and complete the following information:
   - **Type**—select **Manual**.
   - **Index**—do not change this setting (default: 1).
7. Select **IPSEC Settings** and complete the following information:
   - Index—from the **IPSEC Protocol Table** dialog box, select an Index that contains only Proposal ID 15.
   - Lifetime—do not change this setting.

8. Select **Network Tables** (Figure 132).

**Figure 132: Ravlin Node Manager**

9. Select **Local Networks** and complete the following information:
   - Network Number—enter the LAN IP address of the Ravlin device.
   - Network Mask—enter the corresponding network mask.

10. Select **Peer Networks** and complete the following information:
    - Network Number—enter the SonicWALL GMS agent IP address.
    - Network Mask—enter the corresponding network mask.

**Setting up Manual Keys**

Once configured, the Ravlin device and SonicWALL GMS will communicate through a VPN tunnel. To specify the IP address and port of the SonicWALL GMS that will be used to manage the Ravlin device, follow these steps:

1. Open **Settings** and select **Global Management Settings** (Figure 133).
2. Enter the following information:
   - Global Management Server IP Address—enter the IP address of the SonicWALL GMS agent server.
   - Global Management Server Port—enter the port used by the SonicWALL GMS agent server. For Windows, the default setting is 514. For UNIX, you must look up this information.
Creating Ravlin Fields and Views

The SonicWALL GMS uses the same method for organizing Ravlin devices as it does for SonicWALL appliances. Ravlin devices are not forced into specific, limited, rigid hierarchies. Simply create a set of fields that define criteria that separate Ravlin devices (e.g., country, city, state). Then, create and use views to display and sort appliances on the fly.

To organize Ravlin devices, follow these steps:

- Create custom fields that will be useful to your organization. See “Creating Custom Fields” on page 181.
- Review the standard Ravlin fields. See “Standard Fields” on page 182.
- Create views that will make your job easier. See “Setting Up Views” on page 183.

Creating Custom Fields

When first configuring SonicWALL GMS, you will create custom fields that will be entered for each Ravlin device. SonicWALL GMS supports up to ten custom fields.

Note: Although SonicWALL GMS supports up to ten custom fields, only seven fields can be used to sort Ravlin devices at any given time.

Note: If you already configured these fields for SonicWALL appliances, you may not need to make any changes.

The following are examples of custom fields that you can use:

- Geographic—useful for organizing Ravlin devices geographically. Especially useful when used in combination with other grouping methods. Geographic fields may include:
  - Country
  - Time Zone
  - Region
  - State
  - City
- Customer-based—useful for organizations that are providing managed security services for multiple customers. Customer-based fields may include:
  - Company
  - Division
  - Department
- Configuration-based—useful when Ravlin devices will have very different configurations.
- User-type—different service offerings can be made available to different user types. For example, engineering, sales, and customer service users can have very different configuration requirements.

SonicWALL GMS is pre-configured with four custom fields: Country, Company, Department and State. These fields can be modified or deleted. To add, modify, or delete fields, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console tab.
3. Expand the Management tree and click Custom Groups (Figure 134).
4. Right-click **Custom Groupings** in the right pane.

5. Select Add Group from the pop-up menu.

6. Enter the name of the first field.

7. Select the newly created field and select Add Group from the pop-up menu.

8. Enter the name of the new field.

9. Repeat Steps 6 through 8 for each field that you want to create. You can create up to ten fields.

After you have defined fields, you will be prompted to select them for each Ravlin device and SonicWALL appliance that you add to SonicWALL GMS.

**Note:** Although the fields appear to be in a hierarchical form, this has no effect on how the fields will appear within a view. To define views, see “Setting Up Views” on page 183.

### Standard Fields

SonicWALL GMS includes standard fields that can be used to sort Ravlin devices based on their model, their firmware version, and other criteria. SonicWALL GMS fields currently include:

- **Firmware**—creates a group for each Firmware version and places each Ravlin device into its corresponding group.
- **Model**—creates a group for each Ravlin model and places each Ravlin device into its corresponding group.
- **Nodes**—creates a group for each node range and places each Ravlin device into its corresponding group.
- **Registered**—places the Ravlin devices into two groups: devices that are registered and devices that are not.
- **Warranty Status**—places the Ravlin devices into two groups: devices that have current warranties and devices that do not.
Setting Up Views

After creating custom fields and reviewing SonicWALL GMS fields, SonicWALL GMS administrators can set up views to perform different functions.

*Note: Each view can show a maximum of seven fields.*

Some of these views can include the following:

- **Standard Geographic Views**

  When the number of Ravlin devices managed by SonicWALL GMS becomes large, you can divide the devices geographically among SonicWALL administrators.

  For example, if one administrator will be responsible for each time zone in the United States, you can choose the following grouping methods:

  - Administrator 1: Country: USA, Time Zone: Pacific, State, City.
  - Administrator 2: Country: USA, Time Zone: Mountain, State, City.
  - Administrator 3: Country: USA, Time Zone: Central, State, City.
  - Administrator 4: Country: USA, Time Zone: Eastern, State, City.

- **Firmware Views**

  To ensure that all Ravlin devices are using the current firmware, you can create a view to check and update firmware versions and batch process firmware upgrades when network activity is low.

  For example, if you want to update all Ravlin devices to the latest firmware at 2:00 A.M., you can use the following grouping method:

  - Firmware Version, Time Zone

  If you want to update Ravlin devices only for companies that have agreed to the upgrade and you want the upgrades to take place at 2:00 A.M., you can use the following grouping method:

  - Company, Firmware Version, Time Zone

- **Registration Views**

  To ensure that all Ravlin devices are registered, you can create a registration view and check it periodically. To create a registration view, you can use the following grouping method:

  - Registration Status, any other grouping fields
Creating a View

To create a view, follow these steps:

1. Start and log into SonicWALL GMS.
2. Right-click anywhere in the left pane of the SonicWALL GMS window and select Edit View from the pop-up menu. The Edit View dialog box appears (Figure 135).

![Figure 135: Edit View Dialog Box](image)

3. Enter the name of the new view in the **View Name** field.
4. Select the first field that will be used to sort Ravlin devices from the **Group Category** list box. This can be a custom field or a SonicWALL GMS field. For a list of SonicWALL GMS fields and their meanings, see “Standard Fields” on page 182.
5. To add additional matching criteria, click **Add Level** and repeat Step 4.
6. To delete a level, select the level and click **Delete Level**.
7. To change a category, select it, make any changes, and click **Modify View**.
8. When you are finished, click **Add View** and click **Done**. To exit without saving changes, close the Edit View dialog box.

Changing Views

To change views from within the SonicWALL GMS UI, follow these steps:

1. Start and log into SonicWALL GMS.
2. Right-click anywhere in the left pane of the SonicWALL GMS window and select Change View from the pop-up menu. The Change View dialog box appears (Figure 136).

![Figure 136: Change View Dialog Box](image)

3. Select a view and click **OK**. The new view is displayed.
Adding Ravlin Devices to SonicWALL GMS

SonicWALL GMS communicates with Ravlin devices through VPN tunnels. After a Ravlin device is added to the SonicWALL GMS User Interface (UI), they will establish communications and SonicWALL GMS will begin monitoring and managing the Ravlin device.

To add a Ravlin device to the SonicWALL GMS UI, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Ravlins tab. The Status page appears (Figure 137).

Figure 137: Adding a Ravlin device

3. Right-click in the left pane of the SonicWALL GMS UI and select Add Unit from the pop-up menu. The Add Unit dialog box appears (Figure 138).

Figure 138: Add Unit Dialog Box

4. Enter a descriptive name for the Ravlin device in the Ravlin Name field.
5. Enter the password used to access the Ravlin device in the Ravlin Password field.
6. Enter the Ravlin Device’s SNMP Write String.
7. Select from the following:
8. Enter the MAC address or serial number of the Ravlin device in the **LAN MAC Serial Number** field.

9. Enter a 16-character encryption key in the **SA Encryption Key** field. The key must be exactly 16 characters long and composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

   **Note:** This key must match the encryption key of the Ravlin device.

10. Enter a 32-character authentication key in the **SA Authentication Key** field. The key must be exactly 32 characters long and composed of hexadecimal characters. For example, a valid key would be “1234567890abcdef1234567890abcdef.”

   **Note:** This key must match the authentication key of the Ravlin device.

11. Enter the IP address of the SonicWALL GMS server that will manage the Ravlin device in the **Agent IP Address** field:

12. Click **Properties**. The Unit Properties dialog box appears (Figure 139).

    **Figure 139: Unit Properties Dialog Box**

    ![Image of Unit Properties Dialog Box]

13. Enter the name of each group to which the Ravlin device belongs. For information on creating groups, see “Creating Ravlin Fields and Views” on page 181.

14. Click **OK**. You are returned to the Add Unit dialog box.

15. Click **OK**. The new Ravlin devices will appear in the SonicWALL GMS UI and will have red icons.

    The SonicWALL GMS will then attempt to establish separate management VPN tunnels to the appliances, read their configurations, and acquire them for management. This will take a few minutes.

    After the Ravlin devices are successfully acquired, their icons will turn blue, their configuration settings will be displayed at the unit level, and their settings will be saved to `<sgms_directory>/etc/Prefs`. 
Configuring Ravlins

The Ravlin configuration section of the SonicWALL Global Management System (SonicWALL GMS) user interface (UI) is similar to the SonicWALL appliances section of the SonicWALL GMS UI. Configuration changes are created as tasks, placed in a task queue, and sent to the Ravlin devices. After a Ravlin device receives a task, it will reconfigure itself accordingly and send an acknowledgement to the SonicWALL GMS.

Note: Although the Ravlin devices have been updated to work with SonicWALL GMS, the Ravlin section retains much of the configuration style and terminology of the original Ravlin Node Manager.

SonicWALL GMS offers the ability to push configuration settings to a single Ravlin device, a group, or all Ravlin devices being managed by the SonicWALL GMS. For example, to clear the ARP cache for a group of Ravlin appliances, select the group, expand the General tree, and click Tools. The Tools page appears (Figure 140).

Figure 140: Tools Page

Click Clear ARP Cache. The changes become tasks and are applied to all Ravlin devices within the group.

To view the status of these tasks, click the Console tab. Then expand the SonicWALL GMS Tasks tree and click Scheduled Tasks. The Scheduled Tasks page appears (Figure 141).
The task appears in the Scheduled Tasks page. After a task is successfully applied to a Ravlin device, it will be removed from the page.

Configuring Network Settings

This section describes how to configure network settings. Select from the following:

- **IP Settings**—describes how to configure the IP address settings of the Ravlin device(s). See “Configuring IP Settings” on page 188.
- **Routes**—describes how to configure routes for the Ravlin devices. See “Configuring Routes” on page 189.

  **Note:** You must set at least one route for each Ravlin device. This is generally the default route and points to the gateway router.
- **PPPoE**—describes how to configure PPPoE (optional). See “Configuring PPPoE” on page 191.
- **Packet Handling**—describes how to configure various packet handling options. See “Configuring Packet Handling Options” on page 191.
- **Miscellaneous**—describes how to configure general network settings. See “Configuring Miscellaneous Network Settings” on page 193.

Configuring IP Settings

**Note:** In order for changes on this page to take effect, the Ravlin devices will drop all current connections. If this will have a significant effect on your network, we recommend scheduling this task to run when network activity is low.

This section describes how to change the IP addresses of a Ravlin device. To change IP the addresses, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select a Ravlin device.
4. Expand the Network tree and click **IP Settings**. The IP Settings page appears (Figure 142).

**Figure 142: IP Settings Page**

5. Select from the following LAN Settings:
   - **DHCP Enabled**—The LAN interface will receive its IP address from the DHCP server.
   - **Static**—The LAN interface will use the following static settings:
     - **IP Address**—IP address assigned to the LAN interface. This address is also used for configuration and monitoring.
     - **Subnet Mask**—Specifies the subnet to which the LAN IP address belongs.

6. To enable the tunneling of DHCP requests between Ravlin devices, select the **Tunnel Local Host’s DHCP Request** check box.

7. Select from the following WAN Settings:
   - **DHCP Enabled**—The WAN interface will receive its IP address from the DHCP server.
   - **Static**—The WAN interface will use the following static settings:
     - **IP Address**—Public IP address used to access the Internet. All activity on the Internet will appear to originate from this address. This IP address must be valid and is generally supplied by your Internet Service Provider (ISP).
     - **Subnet Mask**—Specifies the subnet to which the WAN IP address belongs.

8. When you are finished, click **Update**. The settings are changed for the selected Ravlin device. To clear all screen settings and start over, click **Reset**.

*Note:* If there are SAs between this Ravlin device and other Ravlin devices, you will need to update the other devices to use the new IP address.

**Configuring Routes**

Whether the Ravlin device runs in bridge mode or router mode depends on the IP address and subnet mask values you specify for the device’s LAN and WAN interfaces. The unit runs in bridge mode if the LAN and WAN network addresses are the same; otherwise, the unit runs in router mode.
A router is a computer, a workstation, or a dedicated hardware device set up to route IP packets between two or more networks. Depending on its configuration, the router can allow or deny access to these networks.

Each router contains a routing table, which lists available networks. When the router receives packets to transmit, it consults the routing table and forwards the packets to the corresponding router or gateway.

This section describes how to define routes for a Ravlin device.

**Note:** The Ravlin device relies on the network route to support Routing Information Protocol (RIP), Border Gateway Protocol (BGP), or Open Shortest Path First (OSPF).

**Note:** Ravlin routing tables provide static routing capability as required for some networking topologies. However, a default route (denoted by the IP address 0.0.0.0) is sufficient in many instances.

**Note:** At a minimum, you should create a default route on the WAN interface. To create a default route, specify 0.0.0.0 in the Destination Network field, 0.0.0.0 in the Subnet Mask field, and the IP address of the ISP’s gateway router in the Gateway field.

To configure routes for a Ravlin device, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select a Ravlin device.
4. Expand the Network tree and click **Routes**. The Routes page appears (Figure 143).

**Figure 143: Routes Page**

![Routes Page](image)

5. Select whether the route will be on the LAN or the WAN interface from the **Link** list box.
6. Specify the destination network by entering its IP address and subnet mask.
7. Specify where packets for this network will be sent in the **Gateway** field.
8. Click **Add Route**.
9. Repeat Step 5 through 8 for each route that you want to add.
10. When you are finished, click **Update**. The settings are changed for the selected Ravlin device. To clear all screen settings and start over, click **Reset**.
Configuring PPPoE

To configure the Point-to-Point Protocol over Ethernet (PPPoE) settings of a Ravlin device, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Ravlins tab.
3. Select a Ravlin device.
4. Expand the Network tree and click PPPoE. The PPPoE page appears (Figure 144).

**Figure 144: PPPoE Page**

5. Select the Enable PPPoE check box.
6. To configure the Ravlin device to only connect when there is network traffic, select the Connect on Demand check box.
7. If you selected Connect on Demand, specify how long the Ravlin device will wait before disconnecting if there is no network traffic in the Idle Time in Minutes field.
8. If the service name is required by your ISP, enter it in the Service Name field. Otherwise, leave this field blank.
9. If the concentrator name is required by your ISP, enter it in the Concentrator Name field. Otherwise, leave this field blank.
10. Enter the IP addresses of the Domain Name Servers (DNS) in the Domain Name Server fields.
11. Enter the username and password associated with this PPPoE account in the User Configuration area.
12. When you are finished, click Update. The settings are changed for the Ravlin device. To clear all screen settings and start over, click Reset.

Configuring Packet Handling Options

This section describes how to define packet handling rules for the Ravlin device(s).

To configure packet handling options, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Ravlins tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the Network tree and click **Packet Handling**. The Packet Handling page appears (Figure 145).

**Figure 145: Packet Handling Page**

5. Select from the following packet handling options:
   - **Forward non-IP Traffic in Bridge Mode**—when this option is enabled and the router is configured in bridge mode, non-IP traffic will be forwarded between the LAN and WAN interface.
   - **Forward MAC Broadcast in Bridge Mode**—when this option is enabled and the router is configured in bridge mode, Media Access Control (MAC) broadcasts will be forwarded between the LAN and WAN interface.
   - **Remote Port ARP Proxy**—by default, the Local and Remote interfaces proxy Address Resolution Protocol (ARP) requests automatically.
     If two Ravlin devices are bridged across a network and a client on that network makes an ARP request for a server behind one of the Ravlin devices, it will receive two ARP replies. One reply will be from the Ravlin device that is acting as a gateway for the server and the other will be from the peer Ravlin device.
     In these cases, it is recommended to disable this setting.
   - **Ignore Do not Fragment Bit**—some IP packets contain a Don’t Frag Bit setting. When this bit is set, it warns network devices not to fragment the packet. To ignore this bit and instruct the Ravlin device(s) to fragment large packets anyway, select this check box.
   - **Firewall and Internet Sharing**—enables network address translation (NAT). NAT provides anonymity to machines on the LAN by connecting the entire network to the Internet using a single IP address. This provides security to the internal machines by hiding them from the outside world and conserves IP addresses.
   - **SNMP Management from WAN Interface**—allows the Ravlin device to be managed from the WAN interface.
   - **Listen to Unsolicited ARP on LAN Port**—allows the Ravlin device to update its ARP cache when it receives unsolicited ARP updates.
     When a Ravlin device receives a request for an IP address, it checks its ARP cache for the associated MAC address. If it does not find an entry, it makes an ARP request and places the information in its cache.
If the requested device fails and has a standby, the Ravlin device will need to know the MAC address of the standby server. To receive this information, the Ravlin device must be able to receive unsolicited ARP updates.

If you have devices on the network that are configured in a failover configuration, select this check box. Otherwise, deselect the check box.

- **Cascade Packets to Other Tunnels**—enables cascading of packets between VPN tunnels. When this option is enabled, the Ravlin device checks each packet that it receives, determines whether it is destined for another VPN tunnel, and handles it accordingly. This is useful when connecting multiple hub-and-spoke or peer networks.

If the network is a single hub-and-spoke network where all branch offices connect through the main office, you should probably disable this option as it can slow network performance.

6. When you are finished, click **Update**. The settings are changed for each selected Ravlin device. To clear all screen settings and start over, click **Reset**.

**Configuring Miscellaneous Network Settings**

This section describes how to configure general network settings for the Ravlin device(s). This includes information such as the location of the DHCP server, ARP cache cleanout intervals, and tunnel monitoring settings.

To configure miscellaneous network settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the Network tree and click **Miscellaneous**. The Miscellaneous page appears (Figure 146).

**Figure 146: Miscellaneous Page**

5. Select from the following DHCP options:
   - If the Ravlin device or its soft clients will obtain their IP addresses from a specific DHCP server, select **DHCP Server Address** and enter the DHCP server IP address.
• If the Ravlin device or its soft clients will obtain their IP addresses by broadcasting the requests, select **Broadcast DHCP requests** and select whether the request will be broadcast to the LAN or WAN interface from its list box (default: LAN).

6. To request an IP address range to use for DHCP requests, enter an IP address from an available range on the DHCP server in the **Client DHCP Relay Gateway IP** field. All addresses in that range will be available except the IP address that you enter.

If you enter 0.0.0.0, the DHCP server will use the range to which the Ravlin device’s LAN interface belongs.

7. When the **DHCP Relay for Failover** check box is enabled, the Ravlin device does not maintain DHCP state information. Because this information can consume a lot of memory, enabling this option is recommended for large networks that have many IP addresses.

8. Specify how often the ARP cache is cleared in the **ARP Cache Cleanout Interval** fields.

9. Specify the maximum length of a client session in the **Authentication Timeout** fields. Clients connected longer than this period will automatically be logged out.

10. Configure the following tunnel status settings:
- **Polling Time Interval**—specifies how often the Ravlin device will use ping to test the state of the VPN tunnel.
- **Reporting Time Interval**—specifies how often the Ravlin device will report the results of the tests.
- **Warning Trap Threshold**—specifies when to generate an SNMP warning trap. For example, if you set this to 50% and five or more of the last ten pings failed, an SNMP warning trap will be generated.

11. When you are finished, click **Update**. The settings are changed for each selected Ravlin device. To clear all screen settings and start over, click **Reset**.

---

**Configuring Log Settings**

In order for Ravlin devices to send syslog messages to syslog servers and SNMP traps to SNMP servers, you must specify the syslog and SNMP settings.

Select from the following:
- To configure SNMP settings, see “Configuring SNMP Settings” on page 194.
- To configure syslog settings, see “Configuring Syslog Server Settings” on page 195.

**Configuring SNMP Settings**

To configure SNMP trap receiver settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the Log tree and click **SNMP Settings**. The SNMP Settings page appears (Figure 147).
5. Enter the IP address and community string of an SNMP trap receiver and click Add SNMP Trap Receiver. Repeat this step for each SNMP trap receiver that you would like to add.

Note: You can enter up to five SNMP trap receivers.

6. When you are finished, click Update. The settings are changed for each selected Ravlin device. To clear all screen settings and start over, click Reset.

Configuring Syslog Server Settings

To configure syslog server settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Ravlins tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the Log tree and click Syslog Servers. The Syslog Servers page appears (Figure 148).
5. Enter the IP address and port of syslog server. Then, select the minimum type of syslog messages that it will receive (i.e., Critical, Severe, Error, Warning, Normal, Debug) from the **Priority** list box. For example, if you select **Error**, it will receive Error, Severe, and Critical syslog messages.

Click **Add Syslog Server**.

Repeat this step for each syslog server that you would like to add.

**Note:** *You can enter up to five syslog servers.*

6. When you are finished, click **Update**. The settings are changed for each selected Ravlin device. To clear all screen settings and start over, click **Reset**.
A Virtual Private Network (VPN) is a private data network that uses encryption technologies to operate over public networks. Each node in a network can exchange data by establishing a VPN tunnel or a Security Association (SA) with one or more other nodes.

Once a tunnel is established, the SA uses encryption and authentication keys to ensure data security and integrity. A security key string is an encryption key that is used to encrypt and decrypt secure data. Both nodes must have the key to exchange data. For example, the announcer of the Little Orphan Show used the same key to encode the secret messages that the kids used to decode the messages.

Although an encrypted message cannot be read, it can be tampered with externally. Using an authentication key prevents external tampering. An authentication key is a hash function that is applied to the message content and is checked by the message recipient to verify that the message was not modified in transit.

Although the security and authentication keys will ensure the security and integrity of the data, these keys must be exchanged securely. Otherwise, the information could be intercepted and read in transit. Ravlin devices can use the following methods to securely exchange security and authentication keys:

- **ISAKMP**—each Ravlin device has a shared secret that is used to establish an SA. After the SA expires, the Ravlin devices will reestablish an SA using the same pre-shared secret, but the security and authentication keys will be different. If one set of keys is compromised by an outside party, that party will be unable to compromise the next set of keys.

- **Manual keys**—keys are exchanged in advance. The SA will always use the same encryption and authentication keys. If the keys are compromised by an outside party, they will remain compromised until the keys are changed.

- **Certificates (Ravlin soft clients only)**—each Ravlin soft client obtains a certificate from the SonicWALL Certificate Authority (CA). Security and authentication keys are exchanged using public-key cryptography, and authenticity of each node is verified by the SonicWALL CA. After the SA expires, the SonicWALL appliances will reestablish an SA using the same public keys, but the security and authentication keys will be different. If one set of security and authentication keys is compromised by an outside party, that party will be unable to compromise the next set of keys.

*Note: For an explanation of VPN terms, see “Basic Terms and Concepts” on page 208.*
Configuring VPN

This section describes how to configure SAs so Ravlin devices can communicate secure information over VPN tunnels.

To configure SAs, complete the following procedures:

- Set up the routing table. See “Configuring Routes” on page 189.
- Configure key management and protocol options. See “Configuring Key Management and Protocol Options” on page 198.
- Configure one or more SAs. See “Configuring One or More Security Associations” on page 203.
- Enable VPN mode on the Ravlin device. See “Enabling VPN” on page 205.
- Create a compatible policy data entry on the peer Ravlin device. If you are using a Ravlin device, repeat these steps. Otherwise, follow the directions provided with the device.

Configuring Key Management and Protocol Options

Before configuring an SA, you must determine the types of configuration options that will be available to the Ravlin device. For example, you might decide that only triple-DES will be allowed or you might decide to make a number of choices available.

After choosing which configurations will be available to the Ravlin device, you can create SAs. Each SA contains the following configuration options:

- A type of key management (manual or ISAKMP)
  A Ravlin device can establish an SA using a manual key or ISAKMP. Because a manual key is a mutually agreed-upon value, it does not require exchange of digital certificates or the generation of a session key as an ISAKMP-generated key does.
- A type of encryption (if any) the Ravlin device performs on the IP traffic exchanged during the SA
  Ravlin devices can perform 56-bit DES, and the three-key 168-bit Triple DES encryption.
- A hashing algorithm the Ravlin device uses during authentication
  Ravlin devices can use MD5 or SHA-1 hashing. MD5 is a 128-bit hashing function designed for optimization with microprocessor-based systems such as Intel. SHA-1 is a 160-bit hash function, established by the National Institute for Standards Technology (NIST), with security mechanisms similar to MD5. Because SHA generates a 160-bit hash, it is considered safer from brute-force cryptographic attacks than MD5.
- The operational mode used during the SA.
  Ravlin devices can run in IPsec modes such as authentication header (AH) or encapsulating security payload (ESP) tunneling.

Policy Data Entry Creation Overview

The process of creating one or more SAs consists of three basic steps:

1. Create at least one entry in the Key Management table.
   Each Key Management entry is a profile that describes the kind of key to use when establishing an SA, the type of hashing to use, and the kind of encryption to perform. An entry in the Key Management table has no direct effect when the Ravlin device builds an SA. It only contains possible settings for a policy data entry.

2. Create at least one entry in the Protocol table.
   Each Protocol Table entry is a profile that determines which IPSec protocol to use (AH or ESP). As with Key Management table entries, an entry in the Protocol Table has no direct effect when the Ravlin device builds an SA. It only contains possible settings for a policy data entry. You create policy data entries later in the Policy Data Entries subcomponent (described in Step 3).

3. Create a policy data entry in the Policy table.
   A policy data entry is a specification the Ravlin device uses to build an SA. Because the unit can establish and run multiple SAs simultaneously, you might need to create more than one such entry.

   **Note:** When you create a policy data entry, you invoke entries previously made in the Key Management table and the Protocol table. Consequently, you must create the necessary entries in those tables before you can create a policy data entry.
Creating a Key Management Table Entry

To create an entry in the Key Management table, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a Ravlin device.
4. Select one of the following key types:
   - Manual (to specify a pre-arranged, manual key).
   - ISAKMP (for generating a session key using ISAKMP and the Diffie-Hellman algorithm).

Manual Key

Ravlin devices support one set of manual keys. These keys are reserved for use by SonicWALL GMS. Unless you want to use the same key for other SAs, it is recommended to use ISAKMP for all SAs.

To create a manual key, follow these steps:

*Note*: If you change the manual key settings, you must also change them for SonicWALL GMS. For more information, see “Adding SonicWALL Appliances to SonicWALL GMS” on page 36.

1. Expand the VPN tree and click **Manual Keys**. The Manual Keys page appears (Figure 149).

**Figure 149: Manual Keys Page**

2. Enter the key used for encryption in the Inbound and Outbound **Encryption Key** fields. The DES and ARC-Four Keys must be exactly 16 characters long and be composed of hexadecimal characters. Encryption keys less than 16 characters will not be accepted; keys longer than 16 characters will be truncated.

*Note*: Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef”.

This key must match the encryption key of the remote VPN gateway or client. If encryption is not used, this field is ignored.

3. Enter the key used for authentication in the Inbound and Outbound **Authentication Key** fields. The authentication key must be exactly 32 characters long and be composed of hexadecimal characters. Authentication keys less than 32 characters will not be accepted; keys longer than 32 characters will be truncated.
Note: Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef1234567890abcdef.”

This key must match the authentication key of the remote VPN gateway or client. If authentication is not used, this field is ignored.

4. Enter the Security Parameter Index (SPI) that the remote location will send to identify the SA used for the VPN Tunnel in the SPI Inbound field. To work with SonicWALL GMS, this must be the MAC address of the Ravlin Device.

Note: The SPI may be up to eight characters long and be composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (e.g., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f).

The hexadecimal characters ‘0’ to ‘ff’ inclusive are reserved by the Internet Engineering Task Force (IETF) and are not allowed for use as an SPI. For example, a valid SPI would be 1234abcd.

Note: The SPI for an SA must be unique when compared to SPIs for other SAs. However, the Incoming SPI can be the same as the Outgoing SPI on the same SA.

5. Enter the Security Parameter Index (SPI) that the local SonicWALL VPN will transmit to identify the SA used for the VPN Tunnel in the SPI Outbound field. To work with SonicWALL GMS, this must be the MAC address of the Ravlin Device.

6. When you are finished, click Update. The settings are changed for the selected Ravlin device. To clear all screen settings and start over, click Reset.

ISAKMP Key

To use an ISAKMP key (recommended), follow these steps:

1. Expand the VPN tree and click ISAKMP Keys. The ISAKMP Keys page appears (Figure 150).

Figure 150: ISAKMP Keys Page

2. To create a new entry, click the notebook icon of a blank entry. To edit an existing entry, click its notebook icon.

The ISAKMP Key Management Page appears.
3. Enter the number of times that the Ravlin device will attempt to establish an SA in the **Retries** field.
4. Enter the Pre-shared Key used to negotiate encryption and authentication keys.
5. To use Perfect Forward Secrecy (PFS), select the **Enable Perfect Forward Secrecy** check box.
   With PFS, the Ravlin device does not derive new keys from the original or previous key. In addition, if the Ravlin device derived the key from any other keying material, the unit does not use that material to derive any more keys. This prevents intruders from using information about one key to discover subsequent keys.
6. Select an ISAKMP proposal from the **Proposals** list box.
   The Group 1 and Group 2 items refer to the Diffie-Hellman groups. Group 1 specifies a 768-bit Diffie-Hellman value, while Group 2 specifies a 1024-bit Diffie-Hellman value. Group 2 is considered more secure than Group 1.
7. When you are finished, click **Accept**. To exit without saving, click **Cancel**. You are returned to the ISAKMP Keys page.
8. To add another entry, repeat Steps 2 through 8.
9. When you are finished, click **Update**. The settings are changed for the selected Ravlin device. To clear all screen settings and start over, click **Reset**.

**Creating a Protocol Table Entry**

Entries in the Protocol table specify operational modes that SAs can use. These operational modes include Authenticated Headers (AH) and Encapsulating Security Payload (ESP).

- While running in the Authentication Header (AH) security mode, the Ravlin device provides integrity and authentication without confidentiality. AH mode ensures proper authentication by inserting an authentication header in the packet between the IP header and the payload. Because neither the packet's payload nor its IP address is encrypted, AH mode is widely acceptable even where the export, import, or use of encryption is regulated or prohibited.
  While running in the AH tunneling security mode, the Ravlin device encapsulates the original IP packet and attaches an AH header and a new IP header. As with normal AH mode, no encryption takes place.
- While running in the Encapsulating Security Payload (ESP) security mode, the Ravlin device encrypts the entire IP packet, authenticates it, encapsulates it, and gives it a new IP header. When two Ravlin devices establish a security association in ESP mode, the communication link between the units is referred to as an ESP tunnel. Because ESP tunnel mode encapsulates and encrypts the original IP header along with the payload, intruders cannot capture routing information and use it to attack the system.
While running in ESP transport security mode, the Ravlin device encrypts only the payload and ESP trailer. It does not encrypt the source IP address. Because of low overhead, ESP transport mode usually gives high performance.

To create a protocol entry, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Ravlins tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the VPN tree and click IPSEC Protocols. The IPSEC Protocols page appears (Figure 152).

**Figure 152: IPSEC Protocols Page**

5. To create a new entry, click the notebook icon of a blank entry. To edit an existing entry, click its notebook icon. The IPSEC Protocol Management Page appears.
6. Select from the following:
   - To use ESP, select **Encapsulating Security Payload (ESP)**.
   - To use AH, select **Authentication Header (AH)**.

7. Select an IPSEC Protocol from the **Proposals** list box.

8. When you are finished, click **Accept**. To exit without saving, click **Cancel**. You are returned to the IPSEC Protocols page.

9. To add another entry, repeat Steps 5 through 8.

10. When you are finished, click **Update**. The settings are changed for the selected Ravlin device. To clear all screen settings and start over, click **Reset**.

### Configuring One or More Security Associations

This section describes how to define the properties and behavior of an SA.

Every SA generated by a Ravlin device is based on a policy data entry. In turn, policy data entries use indexes created in the Key Management table and the Protocol table. Be sure to make the necessary entries in these tables before attempting to create a policy data entry as described below.

**Note:** Do not attempt to create a separate SA entry for each network or subnet protected by the Ravlin unit. For example, if a Ravlin device protects two different subnets, it is not necessary to create a separate SA entry for each. Use a single entry to protect multiple protected networks.

Before creating an SA entry, you need the following information:

- The Distinguished Name (DN) of the peer network security device to which the Ravlin device will establish the SA. If the network security device is a Ravlin device, the DN is equivalent to the unit's Security ID.
  
  If the Ravlin device has a front-panel display, you can get the Security ID by pressing the SID button (button 3). Otherwise, the Security ID is printed on the label on the bottom of each unit.

- The Remote interface IP address of the peer device (the device with which the Ravlin device will establish the SA).

- The IP address and subnet mask of the protected networks (the networks and subnets protected by the Ravlin device).

To create an SA, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the VPN tree and click **Configure**. The Configure page appears (Figure 154).

**Figure 154: Configure Page**

5. To configure a new SA, select **Add New VPN Policy** from the **Policies** list box. To edit an existing policy, select the policy from the **Policies** list box.

6. Enter a name for the policy in the **Name** field.

7. Select the type of SA from the **Type** list box:
   - VPN Host—Ravlin soft client.
   - VPN Gateway—peer Ravlin or VPN device.
   - Non-VPN Bypass—traffic to and from this peer will pass unencrypted.
   - Non-VPN Bypass Outbound Only—traffic to this peer will pass unencrypted if it originated inside the network. Traffic initiated from outside the network is blocked.

8. Enter the Distinguished Name (DN) of the peer network security device to which the Ravlin device will establish the SA. If the network security device is a Ravlin device, the DN is equivalent to the unit’s Security ID.

9. Enter the IP address of the peer device in the **Peer LAN IP** field.

10. Select the key management type from the **Key Management** list box. To add a key management type, see “Creating a Key Management Table Entry” on page 199.

11. Select the IPSEC protocol from the **IPSEC Protocol** list box. To add an IPSEC protocol, see “Creating a Protocol Table Entry” on page 201.

12. Specify how often the Ravlin device will renegotiate for IPSEC keys in the **IPSEC Lifetime** fields. A value of “0” will cause the device to never renegotiate IPSEC keys.

13. Specify how often the Ravlin device will renegotiate for ISAKMP keys in the **ISAKMP Lifetime** fields. A value of “0” will cause the device to never renegotiate ISAKMP keys.

14. To specify the next hop router for the WAN interface, select **WAN** from the **Routing Interface** list box and enter the next hop router in the **Routing Next Hop** field.

15. Specify destination networks that will be available to this SA by clicking **Modify** and entering the destination networks.

16. Specify local networks that will be available to the SA by clicking **Modify** and entering the local networks.
Enabling VPN

After configuring VPN, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Ravlins tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the VPN tree and click Summary. The Summary page appears (Figure 155).

5. Select from the following:
   - To enable VPN, select Apply Policies to All Traffic.
   - To disable VPN and configure the Ravlin device as a bridge, select Pass All Traffic.
   - To block all traffic through the Ravlin device, select Block All Traffic.

6. To specify the amount of time that must pass before inactive clients are disconnected, enter the time in the Inactive Client Timeout fields.

7. When you are finished, click Update. The settings are changed for each Ravlin device. To clear all screen settings and start over, click Reset.
Configuring RADIUS

This section explains how to configure Remote Authentication Dial-In User Service (RADIUS). RADIUS is a standard protocol that enables remote servers to communicate with a central server to authenticate users.

VPN Client users that access the LAN through a VPN tunnel may be required to authenticate through RADIUS before accessing LAN resources. This enables users to share VPN resources, but requires the users to authenticate with unique usernames and passwords.

RADIUS provides an additional layer of VPN security and can be centrally managed from a server that controls all remote access for your organization.

To configure RADIUS, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the VPN tree and click RADIUS. The RADIUS page appears (Figure 156).

![Figure 156: RADIUS Page](image)

5. To enable RADIUS authentication for the device(s), select the **Enable RADIUS Authentication** check box.
6. Enter the information for the primary, secondary (optional), and tertiary (optional) RADIUS servers. This includes the following:
   - **IP**—IP address of the RADIUS server.
   - **Port**—User Datagram Protocol (UDP) port that the RADIUS server listens on.
   - **Offset**—
   - **Secret**—this field must match the shared secret or administrative password of the RADIUS server. The shared secret is alphanumeric, case-sensitive, and can range from 1 to 30 characters in length.
   - **Retries**—defines the number of times the SonicWALL will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the VPN connection will be dropped. The RADIUS server retries can range from 0 to 30, but three retries is recommended.
   - **Priority**—sets the priority of the RADIUS server. Use this setting to configure the order in which the Ravlin device(s) will use the RADIUS servers.
When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.

### Adding Client Certificates

Ravlin soft clients can authenticate with Ravlin devices using certificates. This section explains how to add client certificates to Ravlin devices. To add certificates, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the VPN tree and click **Client Certs**. The Client Certs page appears (Figure 157).

**Figure 157: Client Certs Page**

To add a client certificate, follow these steps:

- Enter a name for the certificate in the **Name** field.
- Enter the path to the client certificate file or click **Browse** to locate the file.
- Click **Add**.

5. Repeat Step 5 for each client that you want to add.

6. To remove a certificate, select its trash icon.

7. When you are finished, click **Update**. The settings are changed for each selected SonicWALL appliance. To clear all screen settings and start over, click **Reset**.
Basic Terms and Concepts

Before installing and configuring SonicWALL VPN, it is important to understand the following basic terms and concepts.

- **VPN Tunnel**
  Tunneling is the encapsulation of point-to-point transmissions inside IP packets. A VPN Tunnel is a term that is used to describe a connection between two or more private nodes or LANs over a public network, typically the Internet. Encryption is often used to maintain the confidentiality of private data when traveling over the Internet.

- **Encryption**
  Encryption is a mathematical operation that transforms data from “clear text” (something that a human or a program can interpret) to “cipher text” (something that cannot be interpreted). Usually the mathematical operation requires that an alphanumeric “key” be supplied along with the clear text. The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms cipher text to clear text. Decryption also requires a key.

- **Key**
  A key is an alphanumeric string that is used by the encryption operation to transform clear text into cipher text. A key is composed of hexadecimal characters (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). A valid key would be “1234567890abcdef.” Keys used in VPN communications can vary in length, but are typically 16 or 32 characters. The longer the key, the more difficult it is to break the encryption. The reason for this is that most methods used to break encryption involve trying every possible combination of characters, similar to trying to find someone’s telephone number by dialing every possible combination of phone numbers.

- **Asymmetric vs. Symmetric Cryptography**
  Asymmetric and symmetric cryptography refer to the keys used to authenticate, or encrypt and decrypt the data. Asymmetric cryptography, or public key cryptography, uses two keys for verification. Organizations such as RSA Data Security and VeriSign support asymmetric cryptography. With symmetric cryptography, the same key is used to authenticate on both ends of the VPN. Symmetric cryptography, or secret key cryptography, is usually faster than asymmetric cryptography. Therefore symmetric algorithms are often used when large quantities of data need to be exchanged.

SonicWALL VPN uses symmetric cryptography. As a result, the key on both ends of the VPN tunnel must match exactly.

- **Security Association (SA)**
  An SA is the group of security settings needed to create a VPN tunnel. All SAs require an encryption method, an IPSec gateway address, and a destination network address. IKE includes a shared secret, manual keying includes two SPIs and an encryption and authentication key.

SonicWALL PRO appliances supports up to 100 SAs. SonicWALL SOHO2 and SonicWALL XPRS2 appliances support 10 and 25 SAs, respectively. Different SAs may be created to connect branch offices, allow secure remote management, and pass unsupported traffic.

- **Internet Key Exchange (IKE)**
  IKE is a negotiation and key exchange protocol specified by the Internet Engineering Task Force (IETF). An IKE SA automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass IP traffic.

- **Manual Key**
  Manual keying allows the SonicWALL administrator to specify the encryption and authentication keys. SonicWALL VPN supports the ability to manually set up a security association as well as the ability to automatically negotiate an SA using IKE.

- **Shared Secret**
  A shared secret is a predefined field that the two endpoints of a VPN tunnel use to set up an IKE SA. This field can be any combination of alphanumeric characters with a minimum length of 4 characters and a maximum of 128 characters. Precautions should be taken when delivering/exchanging this shared secret to assure that a third party cannot compromise the security of a VPN tunnel.
**Encapsulating Security Payload (ESP)**

ESP provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption may be in the form of ARCFour (similar to the popular RC4 encryption method), DES, etc.

The use of ESP typically increases the processing requirements and communications latency. The increased latency is primarily due to the encryption and decryption required for each IP packet containing an ESP.

ESP typically involves encryption of the packet payload using standard encryption mechanisms, such as RC4, ARCFour, DES, or 3DES.

ESP has no mechanism for providing strong integrity and authentication of the data.

**Authentication Header (AH)**

The authentication header is a mechanism for providing strong integrity and authentication for IP packets. The Authentication Header does not offer confidentiality and protection from traffic analysis.

The IP authentication header provides security by adding authentication information to an IP packet. This authentication information is calculated using all header and payload data in the IP packet. This provides significantly more security than is currently present in IP.

Use of an AH will increase the processing requirements of SonicWALL VPN and will also increase the communications latency. The increased latency is primarily due to the calculation of the authentication data by the sender and the calculation and comparison of the authentication data by the receiver for each IP packet.

**Data Encryption Standard (DES)**

When DES is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a message authentication code. The SonicWALL DES encryption algorithm uses a 56-bit key.

The DES Key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

**Triple Data Encryption Standard (3DES)**

3DES is the same as DES, except that it applies three DES keys in succession and is significantly more secure. However, 3DES has significantly more processing requirements than DES.

The 3DES Key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” inclusive (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

**ARCFour**

ARCFour is used for communications with secure Web sites using the SSL protocol. Many banks use a 40-bit key ARCFour for online banking, while others use a 128-bit key. SonicWALL VPN uses a 56-bit key for ARCFour.

The ARCFour key must be exactly 16 characters long and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be “1234567890abcdef.”

**Security Parameter Index (SPI)**

The SPI is used to establish a VPN tunnel. The SPI is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption, and key values that the administrator associated with the SPI to establish the tunnel.

The SPI must be unique, is from one to eight characters long, and is composed of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, valid SPIs would be 999 or 1234abcd.
Maintaining Ravlin Devices

This chapter describes Ravlin device maintenance procedures. These procedures include the following:

- How to upgrade firmware for one or more Ravlin devices—see “Upgrading Ravlin Devices” on page 211.
- How to restart Ravlin devices—see “Restarting Ravlin Devices” on page 212.
- How to clear active security associations—see “Clearing Security Associations” on page 213.
- How to clear the Address Resolution Protocol (ARP) caches—see “Clearing the ARP Caches” on page 214.

Upgrading Ravlin Devices

Ravlin firmware is updated on a periodic basis to offer new functionality and address any known issues. After a Ravlin device is registered, it is entitled to free firmware updates.

To upgrade to the latest firmware, follow these steps:

**Note:** In order for changes on this page to take effect, the Ravlin device(s) will automatically be restarted. We recommend scheduling the firmware update to run when network activity is low.

1. Copy the new firmware to the \Firmware\Current subdirectory of the SonicWALL GMS directory.
2. Start and log into SonicWALL GMS.
3. Click the Ravlins tab.
4. Select the global icon, a group, or a Ravlin device.
5. Expand the Register/Upgrades tree and click **Firmware Upgrade**. The Firmware Upgrade page appears (Figure 158).
6. Click the **Firmware Upgrade** button. SonicWALL GMS schedules a firmware update task for each Ravlin device.

When SonicWALL GMS runs a firmware update task, it checks the firmware in the \Firmware\Current subdirectory of the SonicWALL GMS directory and applies it to the Ravlin device. Additionally, SonicWALL GMS copies the old firmware file to the \Firmware\Old subdirectory of the SonicWALL GMS directory.

---

**Restarting Ravlin Devices**

Some SonicWALL GMS changes require the Ravlin device(s) to automatically be restarted after changes are applied. However, there may be instances when you want to restart the Ravlin device(s) manually.

*Note: It is recommended to restart the Ravlin device(s) when network activity is low.*

To restart one or more SonicWALL appliances, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a SonicWALL appliance.
4. Expand the General tree and click **Tools**. The Tools page appears (Figure 159).
5. To restart the selected SonicWALL appliance(s), click **Restart SonicWALL**.

## Clearing Security Associations

Occasionally, you might find it helpful to clear all active security associations. To do this, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the General tree and click **Tools**. The Tools page appears (Figure 160).
5. Click **Clear All Active Security Associations**. All active security associations are terminated and will need to be reestablished by the VPN devices.

### Clearing the ARP Caches

Ravlin devices store information on all devices with which they have communicated. By default, this information is cleared every 15 minutes.

*Note: To change this interval, see “Configuring Miscellaneous Network Settings” on page 193.*

To clear the ARP cache immediately, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Ravlins** tab.
3. Select the global icon, a group, or a Ravlin device.
4. Expand the General tree and click **Tools**. The Tools page appears (Figure 161).
5. Click Clear ARP Cache(s).
Section IV
SonicWALL GMS Configuration and Maintenance
CHAPTER 23

Configuring and Working with SonicWALL GMS

The SonicWALL Global Management System (SonicWALL GMS) Console Panel is used for configuring SonicWALL GMS settings, working with the SonicWALL GMS log, working with SonicWALL GMS tasks, and upgrading SonicWALL GMS.

This chapter describes the following:

- Changing the SonicWALL GMS password. See “Changing the SonicWALL GMS Password” on page 219.
- Setting the SonicWALL GMS user idle-logout period and email address. See “Configuring SonicWALL GMS Settings” on page 220.
- Configuring and viewing the SonicWALL GMS log. See “Viewing the SonicWALL GMS Log” on page 223.
- Configuring task settings and view pending tasks. See “Working with SonicWALL GMS Tasks” on page 224.
- Managing SonicWALL GMS sessions and configuring Agents. See “Managing SonicWALL GMS” on page 225.
- Adding SonicWALL GMS licenses to support additional SonicWALL appliances. See “Upgrading SonicWALL GMS” on page 228.

Changing the SonicWALL GMS Password

To change the SonicWALL GMS password, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS user interface (UI).
3. Expand the Login tree and click Change Password. The Change Password page appears (Figure 162).
4. Enter the old SonicWALL GMS password in the **Old SGMS Password** field.
5. Enter the new SonicWALL GMS password in the **New SGMS Password** field.
6. Reenter the new password in the **Confirm New Password** field.
7. When you are finished, click **Update**. The password is changed. To clear all screen settings and start over, click **Reset**.

**Note:** The maximum size of the SonicWALL GMS User ID is 24 alphanumeric characters. The password is one-way hashed and any password of any length can be hashed into a fixed 32 character long internal password.

### Configuring SonicWALL GMS Settings

The SGMS Settings page is used to configure general SonicWALL GMS settings.

To configure general SonicWALL GMS settings, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.
3. Expand the Login tree and click **SGMS Settings**. The SGMS Settings page appears (Figure 163).
4. The SGMS Inactivity Timeout period specifies how long SonicWALL GMS waits before logging out an inactive user. To prevent someone from accessing the SonicWALL GMS UI when SonicWALL GMS users are away from their desks, enter an appropriate value in the **SGMS Inactivity Timeout** field (default: 10 minutes).

   **Note:** This field can be set to a maximum of 120 minutes.

5. Enter the IP address of the Simple Mail Transfer Protocol (SMTP) server in the **SMTP Server Address** field.

6. Enter the email addresses of the SonicWALL GMS administrators in the **SGMS Admin Email Address** and **SGMS Admin Email Address 2** fields.

7. Enter the sender’s email address that will appear in messages sent from the SonicWALL GMS.

8. SonicWALL GMS provides a subscription expiry notification email that notifies the SonicWALL GMS administrator before warranty support, anti-virus, and content filtering services expire. By default, the email is sent to the SonicWALL GMS administrator 30 days and 7 days in advance of the firewall subscription service expiration dates. The email lists all managed SonicWALL appliances with expiring subscription services.

   To change when SonicWALL GMS administrators receive notifications of expiring subscriptions, enter new values in the **Subscription 1st Notice** and **Subscription 2nd Notice** fields.

9. Select how often the SonicWALL GMS administrators will be notified of SonicWALL appliances that have failed in the **Email Down Unit's Status** field.

10. Select how many times a task must fail before SonicWALL GMS administrators are notified in the **Email Task Failure Count** field (default: 25).

11. Select the amount of debug information that is stored from the **System Debug Level** field. For no debugging, enter 0. For verbose debugging, enter 3.

12. To append services and rules that are inherited from the group, select the **Append Services and Rules inherited from group** check box.

   At the unit level, SonicWALL GMS allows a SonicWALL appliance to inherit group settings. By default, SonicWALL GMS overwrites the parameters at the Unit level with the values set at the Group level. If you select this check box, the rules (Access/Rules) and services (Access/Services) settings will be appended to the current settings rather than replacing them.

13. To enable ViewPoint reporting, select the **Enable ViewPoint Reports** check box. For more information on ViewPoint, see the *SonicWALL Global Management System ViewPoint Guide*.

   **Note:** ViewPoint reporting can consume a significant amount of bandwidth.
14. To enable automated firmware updates to occur from the local drive, select the **Enable Firmware Upgrade From Local Drive** check box.

15. To notify the administrator when a SonicWALL appliance fails, select the **Email Administrator About Down Units** check box.

16. To notify the administrator when a new firmware is available, select the **Email Administrator when New Firmware is Available** check box.

17. To configure SonicWALL GMS to automatically synchronize with the local changes made to the SonicWALL appliances, select the **Enable Auto Synchronization** check box.

18. To create a copy of the AddUnit.xml file, including the entire SonicWALL GMS system TreeControl hierarchy, click **Create AddUnit XML File**. A new browser will pop up displaying the content of the AddUnit.xml file. You can save this file to a local directory and modify it at a later time. This will enable you to add new SonicWALL appliances or Ravlin devices to SonicWALL GMS using the command-line interface.

   **Note:** If need to reinstall SonicWALL GMS, you can use this file to reacquire the SonicWALL appliances or Ravlin devices from the newly installed SonicWALL GMS system.

19. When you are finished, click **Update**. The settings are changed. To clear the screen settings and start over, click **Reset**.

---

**Deleting the SonicWALL GMS Logs**

To configure SonicWALL GMS to automatically delete old log files, follow these steps:

1. Start and log into SonicWALL GMS.

2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.

3. Expand the Log tree and click **Configuration**. The Configuration page appears (Figure 164).

   **Figure 164: Configuration Page**

4. Select a date from the list boxes.

5. Click **Delete Logs Older Than**. Log files older than the selected date will be deleted.
Viewing the SonicWALL GMS Log

The SonicWALL GMS log keeps track of changes made within the SonicWALL GMS UI, logins, failed logins, logouts, password changes, scheduled tasks, failed tasks, and completed tasks.

To view the SonicWALL GMS log, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS UI.
3. Expand the Log tree and click **View Log**. The View Log page appears (Figure 165).

**Figure 165: View Log Page**

4. Each log entry contains the following fields:
   - **Number**—specifies the number of the log entry.
   - **Date**—specifies the date of the log entry.
   - **Message**—contains a description of the event.
   - **Severity**—displays the severity of the event (Alert, Warning, or FYI).
   - **SonicWALL**—specifies the name of the SonicWALL appliance that generated the event (if applicable).
   - **User@IP**—specifies the user name and IP address.

5. To narrow the search, enter one or more of the following and click **Start Search**:
   - **Select Time of logs**—displays all log entries for a specified period of time.
   - **SonicWALL Node**—displays all log entries associated with the specified SonicWALL appliance.
   - **Message contains**—displays all log entries that contain the specified text.
   - **SGMS User**—displays all log entries with the specified user.
   - **Severity**—displays log entries with the matching severity level:
     - **All (Alert, Warning, and FYI)**
     - **Alert and Warning**
     - **Alert**

6. To configure how many messages are shown per screen, enter a new value (default: 10).
Working with SonicWALL GMS Tasks

As you move through the SonicWALL GMS UI and make changes, SonicWALL GMS creates and queues tasks and applies them to SonicWALL appliances managed by SonicWALL GMS.

As SonicWALL GMS processes the tasks, some SonicWALL appliances may be down or offline. When this occurs, SonicWALL GMS requeues the tasks and retries the updates after a fixed interval.

To view and manage pending tasks, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.
3. Expand the Tasks tree and click Scheduled Tasks. The Scheduled Tasks page appears (Figure 166).

4. Each task entry contains the following fields:
   - **Task ID**—specifies the number of the task entry.
   - **SonicWALL**—specifies the name of the SonicWALL appliance to which the task applies.
   - **Description**—contains a description of the task.
   - **Last Error**—if the task was not successfully executed, specifies the error.
   - **Creation Time**—specifies the date and time the task was generated.
   - **Last Attempt**—specifies the last time SonicWALL GMS attempted to execute the task.
   - **No. of Attempts**—specifies the number of times SonicWALL GMS has attempted to execute the task.
   - **Owner**—specifies the user who created the task.

5. To narrow the search, enter one or more of the following and click Start Search:
   - **Creation time of tasks**—displays all tasks created during the specified period of time.
   - **SonicWALL Node**—displays all tasks associated with the specified SonicWALL appliance.
   - **Description contains**—displays all tasks that contain the specified text.
   - **Owner**—displays all tasks with the specified owner.
   - **Task ID**—displays the task with the specified task ID.

6. To execute one or more tasks immediately, select their check boxes and click Execute the tasks selected now.
7. To reschedule one or more tasks for another time, select their check boxes and click **Re-schedule the tasks selected**. The SGMS Date Selector dialog box appears (Figure 167).

**Figure 167: SGMS Date Selector Dialog Box**

![SGMS Date Selector Dialog Box]

8. Select the date and time when the task will execute and click **OK**. The dialog box closes and the task will execute at the selected time.

   *Note:* The task(s) will execute based on the time setting of the SonicWALL GMS agent server, UTC, or local browser’s time.

9. To delete one or more tasks, select their Task IDs and click **Delete the tasks selected**. To delete all pending tasks, select the **Select all Tasks** check box and click **Delete the tasks selected**.

---

**Managing SonicWALL GMS**

This section describes how to perform SonicWALL GMS management functions.

**Managing Sessions**

On occasion, it may be necessary to log off other user sessions. To do this, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS user interface (UI).
3. Expand the Management tree and click **Sessions**. The Sessions page appears (Figure 168).
4. Select the check box of each user to log off and click **End selected sessions**. The selected users are logged off.

**Managing Agent Configurations**

The Agents page provides information for the SonicWALL GMS primary and backup agent servers that are managing the SonicWALL appliances. This page lists the IP address and status of each agent server, the IP address and password of the SGMS gateway for each agent server, and the number of firewalls under SonicWALL GMS management. You can also schedule all the tasks for each agent server to be executed during a specified time period.

To configure the Agents page, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the **Console Panel** tab at the bottom of the SonicWALL GMS user interface (UI).
3. Expand the Management tree and click **Agents**. The Agents page appears (Figure 169).
4. The summary section displays the number of installed and running agents.

5. Select the IP address of the Agent you want to view from the Agent IP list box.

6. To specify when tasks can run, select the start and stop times from the Begin Time and End Time list boxes. The time is based on the SonicWALL GMS agent server's local time.

   Note: By default, SonicWALL GMS schedules tasks for immediate execution.

7. To change the state of the server, select Up or Down and click Change Agent State to.

8. For each agent server, the SGMS Gateway IP address and password is displayed. If you change the SGMS gateway IP address or password, you must also change the settings on this page.

9. For each agent server, the Firewalls for Primary Management list box lists the SonicWALL appliances that are assigned to the agent server for primary management. The total number is also displayed.

10. For each agent server, the Firewalls for Standby Management list box lists the SonicWALL appliances that are assigned to the agent server for backup management. The total number is also displayed.

11. For each agent server, the Firewalls Under Active Management list box lists the SonicWALL appliances that are actively being managed by the agent server. The total number is also displayed.

12. When you are finished, click Update. The settings are changed. To clear the settings and start over, click Reset.
Upgrading SonicWALL GMS

This section describes how to upgrade a SonicWALL GMS demo license or add upgrade the SonicWALL GMS license to support additional SonicWALL appliances.

- To upgrade a demo license, see “Upgrading a Demo License to a Retail License” on page 228.
- To upgrade SonicWALL GMS to support additional SonicWALL appliances, see “Upgrading the Node License” on page 229.

Upgrading a Demo License to a Retail License

To upgrade a SonicWALL GMS demo license to a retail license, select from the following:

- To upgrade within the demo period, see “Upgrading within the Demo Period” on page 228.
- To upgrade after the demo period expires, see “Upgrading within the Demo Period” on page 228.

Upgrading within the Demo Period

To upgrade a SonicWALL GMS demo license to a retail license within the demo period, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS user interface (UI).
3. Expand the Licenses tree and click SGMS License. The SGMS License page appears (Figure 170).

   ![Figure 170: SonicWALL GMS License Page](image)

4. Enter the activation code in the Upgrade Activation Code field and click Perform Upgrade Now.
   The License Type will change to Retail License and the Current Noes Allowed will change from 10 to 25.

Upgrading Outside the Demo Period

To upgrade a SonicWALL GMS demo license to a retail license after the demo period expires, follow these steps:

1. Start SonicWALL GMS. The Registration page appears.
2. Enter the demo upgrade activation code and click Update. The Login appears and the license is upgraded.
Upgrading the Node License

Depending on the number of licenses you have ordered, you may need to add SonicWALL GMS licenses to configure and support additional SonicWALL appliances. This section describes how to perform a node license upgrade.

Upgrading the License

To upgrade SonicWALL GMS, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS user interface (UI).
3. Expand the Licenses tree and click SGMS License. The SGMS License page appears (Figure 171).
4. Select the Node License Upgrade option from the pull-down menu and enter the activation code in the Upgrade Activation Code field.
5. Click Perform Upgrade Now.
   The Current Nodes Allowed number will increase by the number of node license upgrades that you purchased.
6. If you have additional activation codes, repeat Steps 4 and 5 for each activation code.

Activating SonicWALL GMS Support

To activate SonicWALL GMS support, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click SGMS License. The SGMS License page appears (Figure 172).
4. Select the **SonicWALL GMS Support** option from the pull-down menu and enter the activation code in the **Upgrade Activation Code** field.

5. Click **Perform Upgrade Now**.

The selected SonicWALL GMS support with its expiration date will be displayed.

6. If you have additional activation codes, repeat Steps 4 and 5 for each activation code.

**Note:** For each SonicWALL GMS support option (Base, 24x7, or Software Maintenance), the CERT activation code must be activated before activating the activation codes for additional nodes.

---

**Log into Mysonicwall.com**

You can now automatically log into the SonicWALL registration site, Mysonicwall.com, from SonicWALL GMS. Follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the Console Panel tab at the bottom of the SonicWALL GMS UI.
3. Expand the Licenses tree and click **SGMS License**. The SGMS License page appears (Figure 173).
4. Click **Login in new window**. A new browser opens with the SonicWALL GMS account on Mysonicwall.com.
Performing a System Snapshot

In order for a technical support representative to troubleshoot a problem, you might be asked to take a snapshot of SonicWALL GMS or you might want to view the configuration yourself.

A system snapshot provides a detailed information about SonicWALL GMS, the SonicWALL GMS database, the system environment, licensing, and firewalls. This information includes:

- Data from the sgmsConfig.xml file (Console or Agent only)
  - Debug state
  - Build number
  - Version
  - Product Code
  - Database type
  - Database driver string
  - Database dbuser
  - Database password
  - Database URL
- SQLServer or Oracle state (Console or Agent only)—whether a database connection could be established
- Environment information
  - CLASSPATH, PATH variables
  - DISPLAY variable (for Solaris - Console only)
  - Web server listening port (Console only)
  - Country
  - Language
  - Operating System
  - IP Address
  - MAC Address
  - Machine data (memory size, etc.)
- Latte/Licensing (Console or Agent only)
  - Connectivity to Latte backend
  - Latte username/password
  - MS license information (Console only)
- Agent specific data
  - Managed units
  - Units states (active or standby)
  - Gateway firmware version
  - Gateway state
  - Ports (syslog, syslog parsing, etc.)
- Firewall data (Gateway or Unit only)
  - IP address
  - Data from status.xml
  - VPNs present (Gateway only)
  - Latte information (if registered)

Note: System Snapshots contain detailed information on SonicWALL GMS. To view information on a specific SonicWALL appliance, see “Requesting Diagnostics for SonicWALL” on page 152.

Performing the Snapshot

To take a snapshot of the system, follow these steps:
1. Start and log into SonicWALL GMS.
2. Click the **Console** tab at the bottom of the SonicWALL GMS UI.
3. Expand the Diagnostics tree and click **Request Snapshot**. The Request Snapshot page appears (Figure 163).
4. To take a snapshot of the SonicWALL GMS console, select **GMS Console**.
5. To take a snapshot of one or more SonicWALL GMS agents, select the **Agent** check box(es).
6. To take a snapshot of the SGMS Gateway, select **Gateway**.
7. Click **Submit Snapshot Request**. SonicWALL GMS takes the snapshot.
8. To view the snapshot, see “Viewing the Snapshot or Diagnostics.”

**Viewing the Snapshot or Diagnostics**

To view a snapshot or SonicWALL diagnostics, follow these steps:

1. Start and log into SonicWALL GMS.
2. Click the **Console** tab at the bottom of the SonicWALL GMS UI.
3. Expand the Diagnostics tree and click **Snapshot Status**. The Snapshot Status page appears (Figure 175).
4. Select the snapshot or diagnostics that you want to view from the **Diagnostics requested** list box.

5. To view the information, click **View Snapshot Data**.

6. To save the information to a file that you can send to technical support, click **Save Snapshot Data**.

7. To delete the information, click **Delete Snapshot Data**.

8. To refresh the information, click **Refresh Snapshot Data**.
Troubleshooting Tips

This appendix describes troubleshooting tips and other technical information.

**SonicWALL GMS Log Files**

SonicWALL GMS provides a number of log files that can be used for troubleshooting. These files are located in the SonicWALL GMS Logs directory and are:

- phase2install.log—Phase 2 Installation log
- schedulerDbg.txt—SGMS Scheduler log in debug mode
- schedulerLog.txt—SGMS Scheduler log in non-debug mode
- SGMSWebServerLog.txt—SGMS Web Server log
- tomcaterr.log—Tomcat log
- tomcatout.log—Tomcat log
- vpSchedulerDbg.txt—SGMS ViewPoint Scheduler log in debug mode
- vpSchedulerLog.txt—SGMS ViewPoint Scheduler log in non-debug mode
- vpSummarizerDbg.txt—SGMS ViewPoint Summarizer log in debug mode
- vpSummarizerLog.txt—SGMS ViewPoint Summarizer log in non-debug mode

The following log files are also available:

- `<sgms_directory>\SonicWALL_GMS_2.3_installLog.log`—Phase 1 Installation log
- C:\sgms23_uninstall.log—Uninstall log

**Encrypting the sgmsConfig.xml File**

To encrypt text for use in the sgmsConfig.xml and web.xml files, do the following:

1. Navigate to the `<sgms_directory>\bin` folder.
2. Enter the following command:
   ```java
   java -cp . TEAV text
   ```
   where `text` is the text string to encrypt.
   
   This command returns the encrypted string.
3. Add the encrypted string to the sgmsConfig.xml or web.xml file.

*Note: This procedure only performs encryption.*

**SonicWALL Information that Remains in the Database**

When a managed SonicWALL appliance is deleted from SonicWALL GMS management, all records pertaining to the managed SonicWALL appliance are removed from the database except for the following:

- SonicWALL GMS log for the managed SonicWALL appliance.
- ViewPoint related logs/summaries.
Resetting the Admin Password

To reset the admin user’s password to default value of ‘password’, enter the following from the command-line prompt:

```
osql -U DBuser -P DBpassword -q "exit(update sgmsdb.dbo.users set password = '5f4dcc3b5aa765d61d8327deb882cf99' where id like 'admin')"
```

where DBuser is the SGMSDB username and DBpassword is the SGMSDB password.

Using Remote Management feature with SonicWALL GMS

If you are trying to enable the Remote Management feature in a SonicWALL appliance that is under SonicWALL GMS management, ensure that you include the IP address of the machine from which you will remotely access the managed SonicWALL. This remote machine cannot be the SonicWALL GMS server.

Copying/Pasting into SonicWALL GMS

Java Plug-in 1.3 and later does not allow applets to access the user clipboards. To circumvent this, you need to explicitly allow applets to access your clipboard. To do this, follow these steps:

1. Open the java.policy file with a text editor. It is usually located in the following directory:
   `c:\Program Files\JavaSoft\JRE\1.3\lib\security`
2. Add the following line to the top of the file after the "// "standard" properties that can be read by anyone":
   ```
   permission java.awt.AWTPermission "accessClipboard", "write";
   ```
3. Save the java.policy file and exit.

Renewing/Extending a SonicWALL GMS Demo License

The SGMS demo license is valid for 30 days. To renew the demo license for another 30 to 60 days, contact SonicWALL Technical Support.

Transferring Appliances from Mysonicwall.com to SonicWALL GMS

During the initial registration of SonicWALL GMS, an account gets created for the SonicWALL GMS on the Mysonicwall.com. If you have one or more SonicWALL appliances that are registered under another Mysonicwall.com account, any attempt to register those appliances will fail because they are already registered to another user.

To manage the SonicWALL appliances with SonicWALL GMS, they need to be transferred from the old Mysonicwall.com account to the SonicWALL GMS account. To do this, follow these steps:

1. Login into your personal Mysonicwall.com account.
2. Select the registered SonicWALL appliance.
3. Choose the Transfer option.
4. Enter the SonicWALL GMS serial number (license) in the New User Name field, and the SonicWALL GMS administrator’s email address in the E-mail ID field.
   **Note:** The SonicWALL GMS email address is the email address that you entered in the SonicWALL GMS Registration page during the initial registration.
5. Schedule a task to automatically synchronize the SonicWALL GMS with the SonicWALL appliance’s local settings.

Encrypted Data

The sgmsConfig.xml and web.xml files contain encrypted data. The following information is encrypted using the Tiny Encryption technology:

- Database Password
Non-encrypted SGMS account password

The password for the SGMS account that was created on the SonicWALL registration site, Mysonicwall.com, is not encrypted. It is a cleartext password and is saved in the SonicWALL GMS database, SGMSDB.

Changing Task Execution Retries

During the SGMS Scheduler window of operation, some tasks may not get executed. These tasks are automatically reattempted after a specified period of time.

By default, SonicWALL GMS attempts to execute a failed task every ten minutes within the window of operation. To change this setting, open the sgmsConfig.xml with a text editor, change the schedulerTaskRetryWaitMinutes parameter, save the file, and exit.

To specify how many times SonicWALL GMS attempts to execute a task within the window of operation (default: 5), open the sgmsConfig.xml with a text editor, change the schedulerTaskRetries parameter, save the file, and exit.

Reducing Missed Heartbeat Messages Frequency

By default, SonicWALL appliances send heartbeat messages every sixty seconds to SonicWALL GMS. If SonicWALL GMS does not receive a heartbeat message within three minutes, the SonicWALL appliance will be marked as “Down.”

To change how long SonicWALL GMS waits before marking a SonicWALL appliance as “Down,” follow these steps:

1. Open the sgmsConfig.xml file with a text editor.
2. Add the following to the end of the file before the </Configuration> section.

   Parameter name="scheduler.missedreportthreshold" value=""

3. Enter a new value for the missed report threshold.
4. Save the file and exit.

Using the Import Feature from Applet

To use the SonicWALL GMS Import option from a remote browser, follow these steps:

1. Open the java.policy file with a text editor. It is usually located in the following directory:

   c:\Program Files\JavaSoft\JRE\1.1\lib\security

2. Add the following line to the end of the file:

   // permission granted to all domains to use GMS' Import option

   grant {
   permission java.io.FilePermission "<<ALL FILES>>", "read, write, delete, execute";
   permission java.util.PropertyPermission "user.home", "read, write";
   permission java.lang.RuntimePermission "modifyThread";
   };
   grant {
   permission java.lang.RuntimePermission "accessClassInPackage.sun.misc";
   };
3. Save the file and exit.
SonicWALL GMS File

SonicWALL Global Management System (SonicWALL GMS) stores its configuration information in the sgmsConfig.xml file.

The following table contains the contents of the sgmsConfig.xml file. Each of these parameters was configured during installation or can be configured from the SonicWALL GMS UI.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LANGUAGE</td>
<td>Specifies the language used by SonicWALL GMS (default: en).</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>Specifies the country (default: US).</td>
</tr>
<tr>
<td>debug</td>
<td>Specifies the debugging level (Levels 0, 1, 2, or 3). The default setting 0 specifies no debugging.</td>
</tr>
<tr>
<td>installDir</td>
<td>Specifies where SonicWALL GMS is installed.</td>
</tr>
<tr>
<td>dbtype</td>
<td>Specifies the type of database used.</td>
</tr>
<tr>
<td>dbhost</td>
<td>Specifies the IP address of the database server.</td>
</tr>
<tr>
<td>dbport</td>
<td>Specifies the database port.</td>
</tr>
<tr>
<td>dbname</td>
<td>Specifies the database name. This is encrypted using Tiny Encryption technology.</td>
</tr>
<tr>
<td>dbuser</td>
<td>Specifies the database username. This is encrypted using Tiny Encryption technology.</td>
</tr>
<tr>
<td>dbowner</td>
<td>Specifies the database owner. This is encrypted using Tiny Encryption technology.</td>
</tr>
<tr>
<td>datasource</td>
<td>Specifies the data source.</td>
</tr>
<tr>
<td>dbpassword</td>
<td>Specifies the database password. This is encrypted using Tiny Encryption technology.</td>
</tr>
<tr>
<td>dbconnections</td>
<td>Number of database connections (default: 20).</td>
</tr>
<tr>
<td>dbdriver</td>
<td>Specifies the database driver.</td>
</tr>
<tr>
<td>dburl</td>
<td>Specifies the URL of the database.</td>
</tr>
<tr>
<td>reportsOn</td>
<td>Indicates whether ViewPoint reporting is enabled. The value 0 indicates ViewPoint is disabled; the default setting 1 indicates ViewPoint is enabled.</td>
</tr>
<tr>
<td>licensPath</td>
<td>Path to the SonicWALL GMS license file.</td>
</tr>
<tr>
<td>licenseTimeout</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>GatewayVPNLimit</td>
<td>Number of security associations supported by the SGMS Gateway.</td>
</tr>
<tr>
<td>log.filePath</td>
<td>Specifies the path to the scheduler log file.</td>
</tr>
<tr>
<td>log.fileSize</td>
<td>Specifies the maximum log file size before truncation (in kilobytes).</td>
</tr>
<tr>
<td>scheduler.controlPort</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>scheduler.count</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>scheduler.scheduerPorts</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>scheduler.dispplayNames</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>scheduler.startHour</td>
<td>Specifies when the scheduler activity window begins.</td>
</tr>
<tr>
<td>scheduler.endHour</td>
<td>Specifies when the scheduler activity window ends.</td>
</tr>
<tr>
<td>scheduler.vpnGatewayIP</td>
<td>Specifies the IP address for the SGMS Gateway. This is encrypted using Tiny Encryption technology.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>scheduler.vpmGatewayPassword</td>
<td>Specifies the SGMS gateway password. This is encrypted using Tiny Encryption technology.</td>
</tr>
<tr>
<td>scheduler.prefsDir</td>
<td>Specifies where the firewall configuration files are saved.</td>
</tr>
<tr>
<td>scheduler.schedulerTaskRetries</td>
<td>Specifies the number of times the scheduler will attempt to execute a failed task (default: 5).</td>
</tr>
<tr>
<td>scheduler.schedulerTaskRetryWaitMinutes</td>
<td>Specifies how long the scheduler will wait before re-executing a task (default: 10 minutes).</td>
</tr>
<tr>
<td>syslog.syslogParserPort</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>syslog.syslogServerPort</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>syslog.launchSyslogServer</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>syslog.forwardToHost</td>
<td>Specifies another host that will receive syslog messages.</td>
</tr>
<tr>
<td>syslog.forwardToHostPort</td>
<td>Specifies the port of the host that will receive syslog messages.</td>
</tr>
<tr>
<td>scheduler.missedreportthreshold</td>
<td>Specifies the number of missed reports or intervals before SonicWALL GMS declares a managed SonicWALL appliance “Down” (default: 3).</td>
</tr>
</tbody>
</table>
SonicWALL GMS Screens

Some SonicWALL Global Management System (SonicWALL GMS) attributes can be inherited from the group to individual SonicWALL appliances. Other settings, such as network IP addresses, cannot be inherited. The following table describes which screens in the SonicWALL GMS UI are group-inheritable.

<table>
<thead>
<tr>
<th>Screen</th>
<th>Inheritable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access/General</td>
<td>Yes</td>
</tr>
<tr>
<td>Access/Management</td>
<td>No</td>
</tr>
<tr>
<td>Access/Rules</td>
<td>Yes</td>
</tr>
<tr>
<td>Access/Services</td>
<td>Yes</td>
</tr>
<tr>
<td>Access/SNMP</td>
<td>Yes</td>
</tr>
<tr>
<td>Access/Users</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced/DMZ Addresses</td>
<td>No</td>
</tr>
<tr>
<td>Advanced/Ethernet</td>
<td>No</td>
</tr>
<tr>
<td>Advanced/Intranet</td>
<td>No</td>
</tr>
<tr>
<td>Advanced/One-to-One NAT</td>
<td>No</td>
</tr>
<tr>
<td>Advanced/Proxy Relay</td>
<td>No</td>
</tr>
<tr>
<td>Advanced/Routes</td>
<td>No</td>
</tr>
<tr>
<td>Anti-Virus/Configure</td>
<td>No</td>
</tr>
<tr>
<td>Anti-Virus/EMail Filter</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP/Setup</td>
<td>No</td>
</tr>
<tr>
<td>Website Blocking/Consent</td>
<td>Yes</td>
</tr>
<tr>
<td>Website Blocking/Customization</td>
<td>Yes</td>
</tr>
<tr>
<td>Website Blocking/General</td>
<td>Yes</td>
</tr>
<tr>
<td>Website Blocking/Filter List</td>
<td>Yes</td>
</tr>
<tr>
<td>Website Blocking/URL Keywords</td>
<td>Yes</td>
</tr>
<tr>
<td>Website Blocking/Web Features</td>
<td>Yes</td>
</tr>
<tr>
<td>General/Network</td>
<td>No</td>
</tr>
<tr>
<td>High Availability/Configure</td>
<td>No</td>
</tr>
<tr>
<td>Log/Log Settings</td>
<td>Yes</td>
</tr>
<tr>
<td>VPN/Configure</td>
<td>No</td>
</tr>
<tr>
<td>VPN/RADIUS</td>
<td>Yes</td>
</tr>
<tr>
<td>VPN/Summary</td>
<td>Yes</td>
</tr>
</tbody>
</table>