SonicWALL ViewPoint User's Guide

Contents

Copyright Notice

Software License Agreement for ViewPoint

This Software License Agreement (SLA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this SLA. If you do not agree to the terms of this SLA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

•The SOFTWARE PRODUCT is licensed as a single product.

•You may install and use one copy of the SOFTWARE PRODUCT, or any prior version for the same operating system. The installation script may install the SOFTWARE PRODUCT on more than one computer.

•You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network.

•You may not resell, or otherwise transfer for value, the SOFTWARE PRODUCT.

•You may not rent, lease, or lend the SOFTWARE PRODUCT.

•You may not remove any product identification, copyright, or other notices from the SOFTWARE PRODUCT.

•The SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this SLA.

•You agree and certify that neither the SOFTWARE PRODUCT nor any other technical data received from SonicWALL, nor the direct product thereof, will be exported outside the United States except as permitted by the laws and regulations of the United States which may require U.S. Government export approval/licensing. Failure to strictly comply with this provision shall automatically invalidate this License.

LICENSE

Subject to and conditional upon the terms of this SLA, SonicWALL grants you a non-exclusive, nontransferable license to use the SOFTWARE PRODUCT only in conjunction with a single SonicWALL Internet Security Appliance. Support for additional SonicWALL Internet Security Appliances is subject to a separate upgrade license.

OEM

If the SOFTWARE PRODUCT is modified and enhanced for a SonicWALL OEM partner, you must adhere to the software license agreement of the SonicWALL OEM partner.

SUPPORT SERVICES

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in "online" documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this SLA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

UPGRADES

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this SLA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

OWNERSHIP

As between the parties, SonicWALL retains all title to, ownership of, and all proprietary rights with respect to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and 'applets" incorporated into the

SOFTWARE PRODUCT) the accompanying printed materials, and any copies of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. The SOFTWARE PRODUCT is licensed, not sold. This SLA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this SLA.

U.S. GOVERNMENT RESTRICTED RIGHTS

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense ("DoD"), the Software is subject to "Restricted Rights", as that term is defined in the DOD Supplement to the Federal Acquisition Regulations ("DFAR") in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government's rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations ("FAR"). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions. Contractor/Manufacturer is: SonicWALL, Inc. 1160 Bordeaux Drive, Sunnyvale, California 94089.

LIMITED WARRANTY

Media. For a period of ninety (90) days from the date of license, SonicWALL warrants to you only that the media containing the SOFTWARE (but not the SOFTWARE itself) is free from physical defects.

NO OTHER EXPRESS WARRANTIES ARE MADE OR AUTHORIZED WITH RESPECT TO THE MEDIA. ALL IMPLIED WARRANTIES WITH RESPECT TO THE MEDIA, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. SOME STATES DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

PRODUCTS EXCLUDED FROM WARRANTY COVERAGE

Misuse, Damage, Etc. Products which have been abused, misused, damaged in transport, altered, neglected or subjected to unauthorized repair or installation as determined by SonicWALL are not covered by this Limited Warranty.

SOFTWARE PROGRAMS. SOFTWARE IS PROVIDED "AS IS" AND SONICWALL MAKES NO WARRANTY OR REPRESENTATION, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO

THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. WITH RESPECT TO ANY SOFTWARE, YOU BEAR THE ENTIRE RISK AS TO QUALITY AND PERFORMANCE. SHOULD THE SOFTWARE PROVE DEFECTIVE FOLLOWING LICENSE, YOU (AND NOT SONICWALL OR ANY DISTRIBUTOR OR RETAILER) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING OR REPAIR.

LIMITATION OF REMEDIES

SONICWALL'S ENTIRE LIABILITY AND LICENSEE'S EXCLUSIVE REMEDY FOR BREACH OF THE FOREGOING WARRANTY SHALL BE, AT SONICWALL'S OPTION AND EXPENSE: (1) REPAIR, (2) REPLACEMENT OR (3) REFUND (IF REPAIR OR REPLACEMENT IS IMPRACTICAL) OF MEDIA NOT MEETING SONICWALL'S "LIMITED WARRANTY'' WHICH IS RETURNED TO SONICWALL ACCORDING TO THE CLAIM PROCEDURE BE LOW. IN NO EVENT WILL SONICWALL BE LIABLE FOR ANY LOST PROFITS, COST OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH PRODUCT EVEN IF SONICWALL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU (LICENSEE).

WARRANTY CLAIM PROCEDURE

Any claim under this Limited Warranty must be submitted before the end of the warranty period to SonicWALL at the address listed below. SonicWALL will use reasonable commercial efforts to repair, replace or refund within thirty (30) days of receipt of the media.

THIS WARRANTY GIVES YOU (LICENSEE) SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

SonicWALL, Inc. 1160 Bordeaux Drive, Sunnyvale, California 94089, 408-745-9600

MISCELLANEOUS

This SLA represents the entire agreement concerning the subject matter hereof between the parties and supersedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This SLA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this SLA be declared void or unenforceable by any

court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

TERMINATION

This SLA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this SLA if you fail to comply with the terms and conditions of this SLA. In such event, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

The manufacturer is SonicWALL, Inc. with headquarters located at 1160 Bordeaux Drive, Sunnyvale, CA 94089-1209, USA.

1 Introduction

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. SonicWALL ViewPoint is supplement to the SonicWALL Internet security products by providing detailed and comprehensive reports of network activity.

SonicWALL ViewPoint is a software application that creates dynamic, Web-based network reports, both real-time and historical, to offer a complete view of all activity through your SonicWALL Internet security appliance. With SonicWALL ViewPoint, you can monitor network access, enhance security, and anticipate future bandwidth needs for your network.

SonicWALL ViewPoint Features

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site

SonicWALL ViewPoint software can be installed on a server running Windows XP, 2000, or NT located on the LAN of your SonicWALL. SonicWALL ViewPoint 1.1 is available as a standard feature for the SonicWALL PRO 300 and the SonicWALL GX. It is an optional upgrade for the SonicWALL TELE3, SOHO3, PRO 100, and PRO 200.

2 Getting Started

SonicWALL ViewPoint software is a reporting solution that can be installed on any computer on the SonicWALL LAN. The computer used to host ViewPoint is referred to as the “ViewPoint Server”.

System Requirements

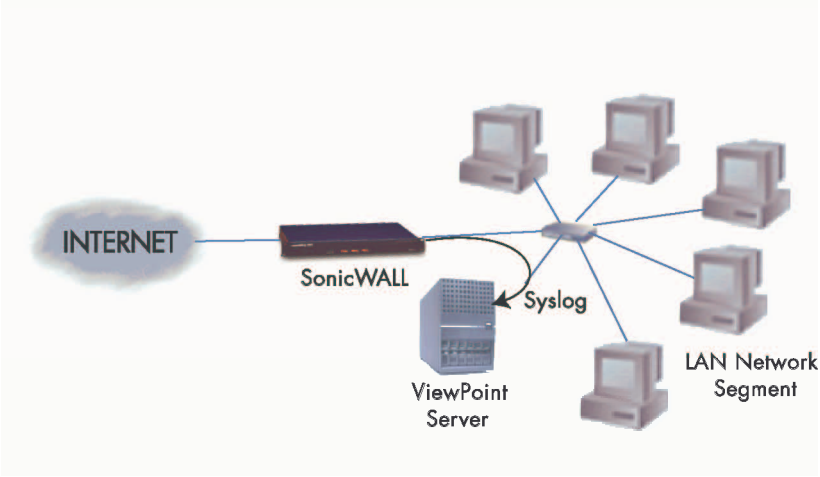
The following is a list of requirements for the ViewPoint Server:

- Microsoft Windows XP, 2000 or NT with Service Pack 4 or later
- 500 MHz Processor
- 512 MB available disk space
- 256 MB RAM
- Microsoft Internet Explorer 4.0 or later, or Netscape Navigator 4.0 or later

***Note**: More disk space may be required for larger networks.*

Network Configuration for ViewPoint

The following diagram illustrates the network configuration for SonicWALL ViewPoint:



The SonicWALL ViewPoint Server can be any computer or server with Windows XP, 2000, or NT, located on the SonicWALL LAN. It must meet the minimum requirements listed in the System Requirements section.

***Note**: The ViewPoint Server must have a static IP address.*

3 Registering ViewPoint

The following instructions describe the procedure to register and activate your ViewPoint Upgrade for your SonicWALL TELE3, SOHO3, PRO 100, and PRO 200. Registration is not necessary for the SonicWALL PRO 300 and SonicWALL GX.

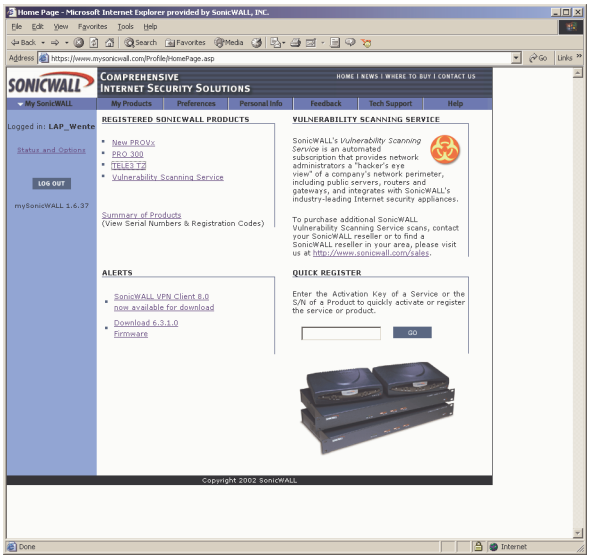
Using your Web browser, enter **http://www.mysonicwall.com** and enter your mysonicwall.com **User Name** and **Password** to access your user account. If you do not have a user account, you must register and create one.

To register your SonicWALL Internet security appliance, follow these steps:

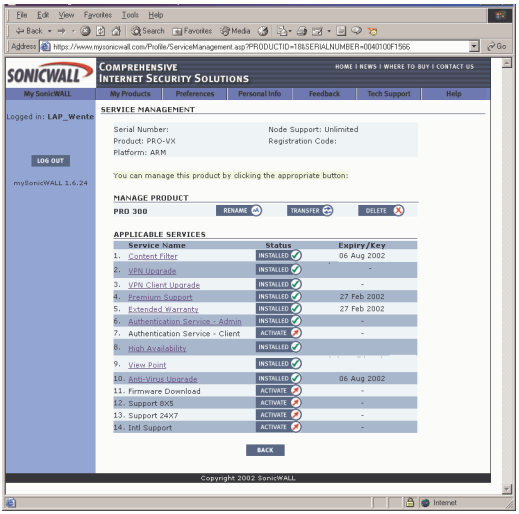
1. After logging into your user account, select **My Products** to display the SonicWALL **Product Registration** page.
2. Enter your SonicWALL serial number in **Add New Products** section.
3. Enter a **Friendly Name** to identify your SonicWALL.
4. Click **Register**.

To activate your SonicWALL ViewPoint Upgrade:

1. Return to the home page by selecting **MySonicWALL**.



2. Select the **Friendly Name** created for your SonicWALL to display the registration information.



3. On the MySonicWALL Service Management page, select **Activate** next to the **ViewPoint** service. An **Activate Service** window appears.
4. Enter the ViewPoint Activation Key displayed on the back of this manual in the **Activation Key** field.
5. Click **Submit**.

***Note**: If you are not using SonicWALL firmware version 6.1.0.0 or later, download the latest firmware from the Service Management page. For instructions on upgrading your SonicWALL firmware, see your SonicWALL Internet Security Appliance User's Guide.*

Once the Activation Key is registered, a ViewPoint License Key is displayed. Record the **License Key** carefully or copy and paste into your Windows clipboard.

1. Log into the SonicWALL Management interface.
2. Click **Log**, and then **ViewPoint**. The **ViewPoint Upgrade** page is displayed.
3. Enter the License Key from the MySonicWALL.com registration site into the **Enter upgrade key** field.
4. Click **Update**, and restart the SonicWALL for the change to take effect.

4 Installing ViewPoint

You can install ViewPoint using the ViewPoint Installation CD or you can download the ViewPoint software files from the SonicWALL,Inc. Web site.

The ViewPoint Server must be running Windows XP, 2000, or NT with Service Pack 4 or higher. The ViewPoint Server must also have a static IP address.

***Note**: The Windows DNS configuration must be properly configured or domain and host names are not displayed in the ViewPoint reports*.

Before you attempt installation, confirm that your computer or server meets the minimum system requirements on page 12.

CD Installation

To install ViewPoint from the ViewPoint CD, load the CD into a Windows XP, 2000, or NT server. The ViewPoint setup program launches automatically.

Internet Installation

To download and install the software from the SonicWALL Web site, save the ViewPoint executable (*.exe) file to your hard drive on your computer, and then double click the file to start the installation of the software.

Software License Agreement

Before the program files are installed on your system, the Software License Agreement is displayed.

- If you agree to the stated terms, click **Yes**.
- If you do not agree, click **No**, and the setup program exits without installing the ViewPoint software.

***Note**: Before installing ViewPoint on the server, close any open applications on it.*

The Installation Wizard guides you the set up as it installs the ViewPoint Reporting software and Syslog server. It also installs the Tomcat Web Server, and MySQL database. Please refer to the Appendix for more information on these applications.

The ViewPoint setup program detects whether the default Web, syslog, or MySQL ports are in use on the computer. The Installation Wizard prompts you to define the ViewPoint Web Server port. The default Web (HTTP) port is port 80. If the default Web port is active, the setup program automatically recommends an alternative Web port, 8080. If the syslog port 514 or MySQL 3306 are active, the ViewPoint setup program displays an error message.

***Note**: If you currently have a syslog server installed on your computer, you must remove the existing program and install the syslog server provided with SonicWALL ViewPoint.*

The Installation Wizard prompts you to define additional settings such as the SonicWALL LAN IP address and the SonicWALL Administrator password. Once the programs are installed, you can close the Installation Wizard and restart your computer for the changes to take effect on your computer.

5 Managing ViewPoint

Logging into ViewPoint

You must configure several settings in ViewPoint in order to review network reports.

From a Web browser, enter http://Local Host or http://<ViewPoint Server IP Address> into the Location or Address field. Or, you can launch ViewPoint from the SonicWALL folder in the Windows **Start** menu. The Authentication window is displayed.

N*ote*: *If you configured the ViewPoint Web server to use a different port than the default port of 80, then add the port number to the URL. For example, http://<ViewPoint Server IP Address: 8080>*.

1. Enter the **User Name** and **Password**. The default **User Name** is *Admin*, and the default **Password** is *password*. The **Password** is case-sensitive.

Note: *The password configured during the ViewPoint Installation is used to authenticate your ViewPoint Server to your SonicWALL. It does not provide access to ViewPoint.*

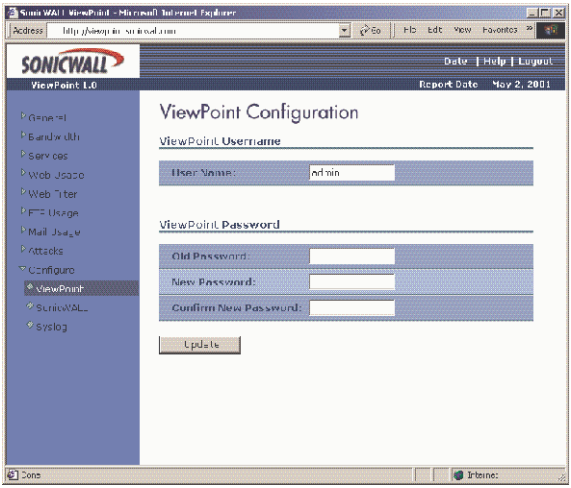
2. Click **Login** to access the ViewPoint interface.

Note: *Confirm that the **Authentication** screen has finished loading before attempting to log into ViewPoint.*

Configuring ViewPoint Settings

ViewPoint requires that you successfully authenticate to access reports. The authentication process prevents unknown users from accessing sensitive network data. The **ViewPoint Configuration** page allows you to modify the ViewPoint user name and password.

1. Using the ViewPoint Web interface, expand **Configuration** and then click **ViewPoint**.



2. To change the ViewPoint User Name, enter the new User Name in the **User Name** field.
3. To change the password, enter the current password in the **Old Password** field.
4. Enter the new password in the **New Password** and **Confirm Password** fields.

***Note**: When setting the ViewPoint password for the first time, remember that the default password is "password".*

5. Click **Update** to refresh the ViewPoint Configuration.

***Note**: If you lose or forget the ViewPoint user name or password, you must uninstall and reinstall the ViewPoint software.*

Configuring SonicWALL Settings

ViewPoint transparently authenticates to your SonicWALL for status and state information. ViewPoint uses the SonicWALL administrator's password and IP address configured during installation to authenticate. If the SonicWALL IP address or password is changed, changes must be made to the ViewPoint settings in order for ViewPoint to authenticate to the SonicWALL.

1. On the ViewPoint Web interface, expand **Configure** and click **SonicWALL**.

2. Enter the LAN IP Address of your SonicWALL in the **IP Address** field.
3. Enter the SonicWALL serial number in the **Serial Number** field. The twelve (12) character, alphanumeric serial number is displayed on the General Status page of the SonicWALL Management interface as well as on the bottom of the SonicWALL.

***Note**: The Serial Number field is not case-sensitive.*

4. Enter the current SonicWALL administrator password in the **Old Password** field.
5. Enter the new SonicWALL administrator password in the **New Password** and **Confirm Password** fields.

***Note**: This password must match the password of your SonicWALL.*

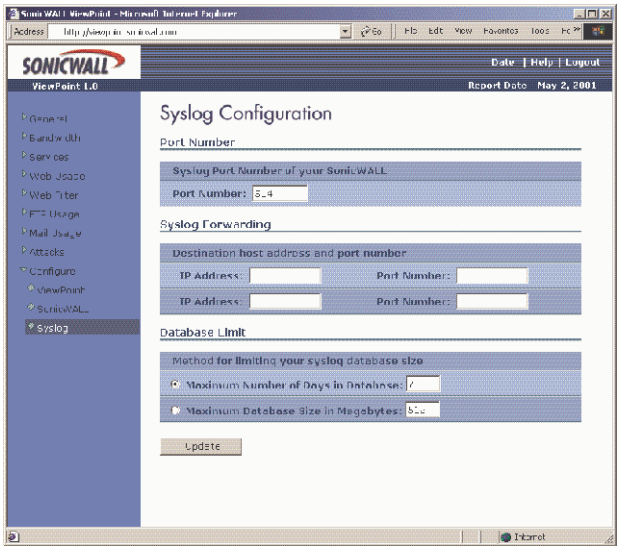
6. Click **Update** to refresh the configuration. Log out of ViewPoint and reauthenticate in order for these changes to take effect.

***Note**: If you lose or forget the password defined in the SonicWALL Configuration settings, and ViewPoint cannot authenticate to the SonicWALL, you must uninstall ViewPoint and reinstall it to configure the correct SonicWALL password.*

Configuring ViewPoint Syslog Settings

The **Syslog Configuration** page allows you to change the UCP port number for the ViewPoint Syslog server to listen on, and configure ViewPoint to forward syslog data to other servers. It also allows you to limit the size of the database.

1. On the ViewPoint Web interface, expand **Configuration** and click **Syslog**.



2. To change the UCP port for the syslog server, enter the new port number in the **Port Number** field. The default port value for the SonicWALL is 514.
3. To forward syslog data to a backup server, enter the IP address of the secondary server in the **IP Address** field.
4. Enter the port number that the syslog data is sent in the **Port Number** field.

5. To limit the database by the number of days that syslog messages are saved, select **Maximum Number of Days in Database**, and enter the number of days that syslog messages are saved in the corresponding field. The default value is seven (7) days.
6. To limit the database by size, select **Maximum Database Size in Megabytes** and enter a value in MB of memory that the database stores in the corresponding field.
7. Click **Update** to refresh the ViewPoint Configuration.

***Note**: Maintenance on the ViewPoint database is completed every night after midnight. Changes to the database size do not take effect until database maintenance is performed.*

Setting the ViewPoint Report Date

The ViewPoint Report date can be changed easily and quickly using these simple steps:

1. To change the report date, click **Date** on the ViewPoint Web interface.

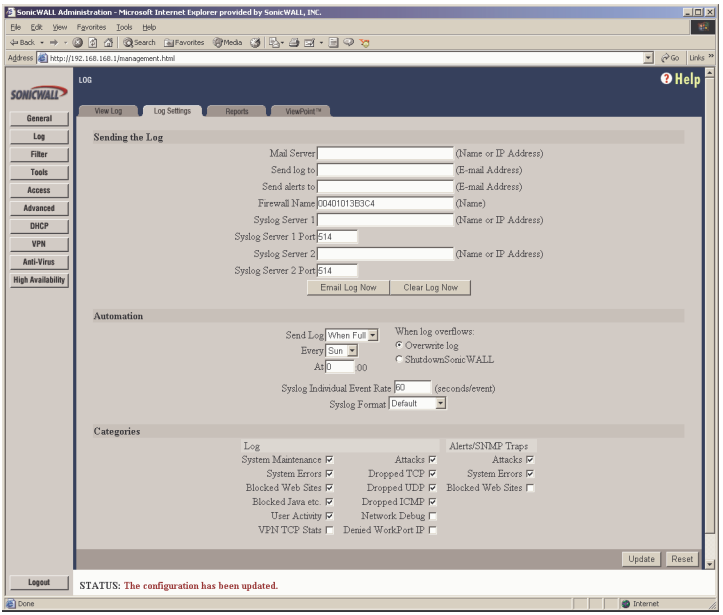
2. The current report date is highlighted in red on the ViewPoint date calendar. Select the desired month and year from the **Month** and **Year** menus.
3. Select the desired day in the ViewPoint calendar. The new report date is displayed in the upper right corner of the ViewPoint Report window. The ViewPoint report table and chart are also updated to reflect the new date.
4. Click **Close** after changing the date.

6 Configuring Your SonicWALL

To use ViewPoint for reporting events on your SonicWALL, you must configure the **Syslog** settings on your SonicWALL. After configuring the **Syslog** settings, the syslog events are sent to the ViewPoint Server.

Use the following steps to configure your SonicWALL **Syslog** settings:

1. Log into your SonicWALL Management Station. Click **Log**, and then **Log Settings**.



2. Enter the domain name or IP Address of the ViewPoint Server in the **Syslog Server 1** field. Leave the port number at the default value of 514.

***Note**: The ViewPoint Server must have a static IP address. Confirm the IP address on the server using Network Properties of the operating system.*

3. Enter **0** in the **Syslog Individual Event Rate** field.
4. Confirm that **Default** is selected from the **Syslog Format** menu.
5. Click **Update** for the changes to take effect on the SonicWALL.

7 ViewPoint Web Interface

The ViewPoint Web Interface can be accessed from any computer located on the same network as the ViewPoint Server. This section describes the interface and the Web-based help options.

***Note**: Use Microsoft Internet Explorer 4.0 or higher, or Netscape Navigator 4.0 or higher to log in and manage ViewPoint. Confirm that your Web browser is configured to allow cookies and Java code.*

General, **Bandwidth**, **Services**, **Web Usage**, **Web Filter**, **FTP Usage**, **Mail Usage**, **Attacks**, and **Configure** appear on the left of the browser window. You can navigate through the Web-based ViewPoint reports by selecting and expanding the menu options and then selecting the desired ViewPoint report. The ViewPoint Web interface is intuitive and easy to navigate using a tree-structured menu design.

The ViewPoint Web interface also includes options at the top of the window. The options are **Date**, **Help**, and **Logout**.

- **Date** opens a Calendar that allows you to change the report date.
- **Help** displays comprehensive instructions for installing, configuring, and troubleshooting ViewPoint.
- **Logout** terminates the management session and redisplays the **Authentication** page. If Logout is clicked, it is necessary to reauthenticate to use ViewPoint.

***Note**: The ViewPoint Administrator is automatically logged out of ViewPoint after 5 minutes of inactivity.*

The current report date is displayed at the top of the ViewPoint page.

ViewPoint Report Layout

Most ViewPoint reports include a chart and a table. The chart displays information such as the amount of bandwidth through the SonicWALL over a period of time. The table provides a summary of the data displayed in the chart. The exceptions to this layout are **General Status** reports which displays state information retrieved directly from the SonicWALL, the **Bandwidth Monitor** and **Service Monitor** reports which display dynamic, real-time graphs of network activity through the SonicWALL, and the **Admin Login**, **User Login**, **Failed Login**, **VPN Events**, and **System Events** reports display a list of pertinent event sorted by time.

Next/Previous

Some reports contain thousands of records which is more data than can be displayed in a single table. These reports include **Next** and **Previous** links at the top of the table that allow you to view subsequent or preceding report data.

Source

The **Source** is the domain name, host name, or IP address of the device that initiated an event.

Destination

The **Destination** is the domain name, host name, or IP address that the event targeted.

Event/Hit

There are two primary methods to measure network activity through the SonicWALL: the amount of data transferred in bytes or the number of individual events. Depending on the type of report, events can be called “hits”, “events”, or “connections”. All of these terms describe a single IP connection from one location to another location through the SonicWALL.

KBytes/MBytes

Most ViewPoint reports display data in terms of KBytes or MBytes. KBytes, an abbreviation for kilobytes, and MBytes, an abbreviation for megabytes, describe the amount of data that was transferred through the SonicWALL.

8 Report Descriptions

General Reports

Status

The General Status report displays comprehensive information about the current status of the SonicWALL. The Status report includes the SonicWALL serial number, firmware version, ROM version, enabled upgrades, the number of users connected to the SonicWALL, and other status information.

Admin Login

The Administrative Login report displays successful administrative authentications to the SonicWALL that occurred during the report period. The Administrative Login report helps identify misuse and unauthorized management of your SonicWALL.

The Administrative Login report table displays the time and the name or IP address of the computer that authenticated to the SonicWALL.

User Login

The User Login report list successful authentications to the SonicWALL to bypass content filtering or to remotely access local network resources. User names, passwords, and user privileges are defined on the Users page of the SonicWALL Management interface. The User Login report illustrates the location and frequency of authenticated user sessions.

The User Login report table displays the time, and the name or IP address of the computer that authenticated to the SonicWALL.

Failed Login

The Failed Login report lists all attempts to log into your SonicWALL Internet security appliance. Failed authentication attempts include unsuccessful administrative and user logins. The Failed Login report identifies unauthorized authentication attempts and uncovers malicious activity.

The Failed Login report table displays the time and the name or IP address of the computer that attempted to authenticate to the SonicWALL.

VPN Events

The VPN Events report lists all VPN events, including VPN SA negotiation attempts, VPN key exchanges, VPN heartbeat messages, and VPN connection errors. The VPN Events report illustrates the cause of VPN negotiation failures, and identifies unknown or suspicious VPN activity.

The VPN Events table displays the time, the source and destination of the event, and the type of event that occurred.

System Events

The System Events report lists events and errors occurring on the SonicWALL Internet security appliance during the report period. System events include successful downloads of the Content Filter List, SonicWALL activations, DHCP messages, and PPPoE messages as well as High Availability failover activation. System errors listed include problems downloading the Content Filter List, difficulties obtaining a DHCP Client lease or PPPoE Client lease, deactivation of the SonicWALL because the syslog was full, and the number of simultaneous connections exceeding the limit.

The System Events report table displays the time, the source name or IP address, and the type of event. Since many events are created by the SonicWALL, the SonicWALL is the most common source of events and errors. Most events are normal SonicWALL operation and do not indicate network or SonicWALL problems.

Bandwidth Reports

Bandwidth Summary Report

The Bandwidth Summary report shows the level of traffic traveling through your SonicWALL over time. The report helps determine when to perform system maintenance on the SonicWALL. It also displays peak bandwidth usage times, and predicts future bandwidth needs.

The Bandwidth Summary report displays a bar graph of all IP traffic through the SonicWALL in MBytes transferred. The table displays the hour of the day, the number of events occurring during the hour, the number of MBytes transferred, and the MBytes as a percentage of the total MBytes for the report day. Both the report and table include outbound and inbound traffic through the LAN, WAN, and DMZ ports.

Bandwidth Monitor

The Bandwidth Monitor report displays a real-time graph of all network activity through the SonicWALL. The Bandwidth Monitor displays inbound and outbound IP traffic through the SonicWALL in either

KBytes or MBytes per second over the past five (5) minutes. The Bandwidth Monitor includes traffic through the LAN, WAN, and DMZ ports.

Top Users of Bandwidth

The Top Users of Bandwidth report shows the top users of bandwidth in Kbytes per second. This report displays the users on the LAN, WAN, or DMZ, with the greatest amount of bandwidth. This data helps provide inappropriate bandwidth use.

The Top Users of Bandwidth report includes a pie chart of the top users of bandwidth as a percentage of total MBytes transferred. The colors in the pie chart correspond with the users listed in the table. The report table displays the IP address, host or domain name of the top ten (10) users, the number of connections initiated by or directed to the users, the number of MBytes transferred by the users, and the MBytes transferred as a percentage of all MBytes transferred.

Service Reports

Service Summary

The Service Summary report displays the amount of bandwidth used by a Service. This report reveals inappropriate use of Internet bandwidth and can help determine network access policies enforced by your SonicWALL.

The Service Summary report displays a graph of FTP, HTTP, ICMP, NetBIOS, DNS, NTP, SMTP, and other service traffic by the number of events or IP connections that occurred on the SonicWALL. The report table lists the services displayed in the graph, the number of events per service, the number of KBytes transferred, and the KBytes as a percentage of the total KBytes for the report period.

Service Monitor

The Service Monitor report displays a real-time graph of network activity by a service over the past five (5) minutes. The Service Monitor shows FTP, HTTP, ICMP, NetBIOS, DNS, NTP, SMTP, and other services in KBytes or MBytes transferred per second. The Service Monitor reports traffic on the LAN, WAN, or DMZ ports.

Web Usage Reports

Web Usage Summary Report

The Web Usage Summary report displays the amount of Web (HTTP) traffic traveling through the SonicWALL over time. This report displays peak bandwidth usage times of Web traffic and provides information

about the number of Web site hits and bandwidth use during the report period.

The Web Usage Summary report displays a bar graph of Web traffic through the SonicWALL in MBytes transferred. The table displays the hour of the day, the number of Web hits that occurred during the hours, the number of MBytes transferred, and the MBytes as a percentage of the total MBytes for the report period.

Top Web Sites

The Top Web Sites report identifies the most popular Web sites accessed through your SonicWALL. This report provides a snap shot of the Web sites accessed by users through the LAN, WAN, or DMZ ports.

The Top Web Sites report displays a bar graph of the top 20 Web sites visited by the number of hits to the Web site. The table displays the name of the Web site, the number of hits to the Web site, the number of KBytes transferred, and the number of hits as a percentage of total hits during the report period.

***Note**: Each Web site listed in the table includes a link to the site, so that the ViewPoint administrator can view and evaluate the top Web sites in the report.*

Top Users of Web

The Top Users of Web report displays the most active users accessing Web sites on the Internet or on the LAN or DMZ network segments. The report displays the number of Web site hits and the amount of bandwidth transferred, identifying inappropriate or excessive Web usage.

The Top Users of the Web report displays a pie chart of the top ten (10) by the number of Web site hits. The report table lists the top ten (10) users displayed in the chart, the number of MBytes transferred by the user, and the number of hits as a percentage of the total Web hits during the report period.

Top Web Sites by User

The Top Web Sites by User report displays the top five (5) Web sites visited by the user. The report provides clear and in-depth information about Web activity by network user.

The Top Web Sites by User report displays a table listing the top users of the Web, the top five (5) Web sites visited by each user, and the KBytes transferred from the Web site by the user. Additional user Web activity can be displayed by clicking the **Next 5** link at the top of the

report table. This report includes LAN users accessing Internet sites, as well as WAN users accessing Web sites hosted on the LAN or DMZ.

***Note**: Each Web site displayed in the table includes a link to the site, so that the ViewPoint Administrator can view and evaluate the Web site.*

Web Filter Reports

Web Filter Summary Report

The Web Filter Summary report shows the number of attempts to access blocked Web sites over time. The Web Filter Summary report includes Web sites blocked by the SonicWALL Content Filter List, or customized Keyword or Domain Name filtering. The reports includes blocked Java, blocked cookies, and blocked Active X attempts.

The Web Filter Summary report displays a bar graph of attempts to access objectionable Web sites by the number of blocked attempts. The report also displays the hour of the day, the number of attempts to access objectionable Web content during the hour, and the number of attempts during the report period.

Top Objectionable Web Sites

The Top Objectionable Web Sites report presents the top destinations that are blocked by the SonicWALL. The report allows you to see the sites that users attempting to access.

The Top Objectionable Web Sites report displays a pie chart of the top twenty (20) objectionable Web sites by the number of attempts to access the site. The table lists the top objectionable Web sites, the number of attempts to access the site, and the number of attempts as a percentage of total attempts during the report period.

***Note**: The Web sites displayed in the table include links to the blocked sites to allow the ViewPoint Administrator to evaluate and review blocked sites. However, the ViewPoint Administrator may also be blocked from accessing the sites if sufficient privileges are not granted to bypass the SonicWALL Content Filter List.*

Top Objectionable Web Sites by User

The Top Objectionable Web Sites by User report displays the top five (5) filtered Web sites by user. The report shows the Web sites that users attempted to visit and were blocked by the SonicWALL Content Filter policies.

The Top Objectionable Web Sites by User reports displays a table of the users blocked by the SonicWALL, the top five (5) Web sites the

users attempted to access, and the number of attempts to access each Web site. If more than five (5) users attempt to access objectionable Web sites, the additional activity can be displayed by clicking **Next 5** at the top of the report table.

FTP Usage Reports

FTP Usage Summary Report

The FTP Usage Summary Report shows the amount of inbound and outbound FTP traffic through the SonicWALL in KBytes per second. The report displays the peak bandwidth usage times for FTP traffic and provides detailed information about bandwidth use and the number of FTP sessions.

The FTP Usage Summary report displays a bar graph of FTP traffic through the SonicWALL in MBytes transferred. The table displays the hour of the day, the number of FTP events occurring during the hour, the number of MBytes transferred for FTP, and the number of MBytes as a percentage of the total MBytes for the report period.

Top Users of FTP

The Top Users of FTP report displays the most active users on the LAN, WAN, or DMZ transferring files via FTP. The report shows the number of FTP events and the amount of data transferred by individual users.

The Top Users of FTP report displays a pie chart of the top ten (10) users of FTP by the number of KBytes transferred. The report table lists the top ten (10) users displayed in the chart, the number of FTP events generated by the user, the number of KBytes transferred by the user, and the number of KBytes as a percentage of total KBytes of FTP during the report period.

Mail Usage Reports

Mail Usage Summary Report

The Mail Usage Summary Report shows the amount of E-mail traffic through the SonicWALL. The report displays peak bandwidth usage times for E-mail.

The Mail Usage Summary Report displays a bar graph of Mail traffic though the SonicWALL in KBytes transferred. The table displays the hour of the day, the number of mail events occurring during the hour, the number of KBytes transferred for mail, and the number of KBytes as a percentage of the total KBytes for the report period.

***Note**: Mail Usage includes SMTP, POP3, and IMAP traffic.*

Top Users of Mail

The Top Users of Mail report shows the most active users on the LAN, WAN, or DMZ sending or receiving E-mail messages. The report shows the number of E-mail files transferred by user in KBytes and the total number of E-mail events through the SonicWALL.

The Top Users of Mail report displays a pie chart of the top ten (10) users displayed in the chart, the number of KBytes transferred by the user, the number of mail events generated by the user, and the number of events as a percentage of the total Mail Events during the report period.

Attack Reports

Attack Summary Report

The Attack Summary report shows the number of attacks received by the SonicWALL during the reporting period. It displays Denial of Service (DoS) attacks, intrusions, probes, and all other malicious activity targeted against the SonicWALL or computers on the LAN or DMZ.

The Attack Summary report displays a bar graph of the number of attacks received by the SonicWALL. The table displays the hour of the day, the number of attacks that occurred during the hour, and the number of attacks as a percentage of the total attacks during the report period.

Top Sources of Attacks

The Top Sources of Attacks report show the top users that attacked the SonicWALL or devices on the network during the report period. Top sources of attacks reveal the IP addresses or host names of devices that generated the most attacks.

The Top Sources of Attacks displays a pie chart of the top ten (10) sources by the number of attacks. The report table lists the top ten (10) sources displayed in the chart, the number of attacks generated by the source, and the number of attacks as a percentage of the total attacks during the report period.

Number of Attacks by Category

The Number of Attacks by Category report presents attacks against the SonicWALL by category during the report period. Attack categories include IP spoof, Ping of Death, SYN flood, land, smurf, probe, and Trojan.

The Number of Attacks by Category report displays a pie chart of the top attack categories by number of attacks. The report table lists the top ten (10) attack categories displayed in the chart, the number of attacks for the category, and the number of total attacks during the report period.

Dropped Packets

The Dropped Packets report displays all IP packets dropped by the SonicWALL which include TCP, UCP, ICMP, IPSec, PPTP packets, Broadcast, and Fragmented packets. The Dropped Packets report includes blocked NetBIOS packets and other normal Internet activity as well as it signals unusual or suspicious connection attempts.

The Dropped Packets report displays a bar graph of the number of IP packets dropped by the SonicWALL. The table displays the hour of the day, the number of dropped packets during the hour of the day, and the number of dropped packets as a percentage of total dropped packets during the report period.

9 Accessing ViewPoint Remotely

Because the ViewPoint interface is Web browser-based, any user on the SonicWALL LAN can login and access the ViewPoint reports. Users accessing network resources remotely using a VPN or not can access the ViewPoint Web interface.

To access ViewPoint, the remote user launches a Web browser, then enters http://<ViewPoint Server IP address> into the **Location** or **Address** field of the Web browser.

Note: If the ViewPoint Web interface uses a different port than the default port of 80, add the port number after the IP address. For example, http://<ViewPoint Server IP address>8080.

Note: Internet Explorer 4.0 or higher, or Netscape Navigator 4.0 or higher, must be used to log in and manage ViewPoint. The Web browser must also be enabled for cookies and Java as well as support for Java applets.

1. Enter the ViewPoint **User Name** and **Password**.
2. Click **Login** to access the ViewPoint interface.

The remote user is now able to view network reports and perform management functions.

Appendix

Uninstalling ViewPoint

Uninstall the ViewPoint program and all of its components from your system by relaunching the ViewPoint set up program.

1. If you installed ViewPoint from a CD, load the CD into your server and run the ViewPoint set up program.

   If you downloaded the ViewPoint executable file from the SonicWALL Web site, then select and launch the ViewPoint executable file from your local disk. If you cannot locate the ViewPoint executable file, you can downloaded it from http://www. sonicwall.com.

2. The ViewPoint set up program automatically detects ViewPoint and displays a window to confirm deletion of the software. To remove ViewPoint and all of its components, click **OK**.

3. The ViewPoint uninstall program prompts you to remove the MySQL Server and MySQL Clients. To remove the software, click **Yes**.

4. The ViewPoint also prompts you to delete the ViewPoint database. To remove the database, click **Yes**. To save the data for future use, click **No**.

5. Click **Finish** to complete the uninstallation process.

ViewPoint Server Across a VPN

While it is recommended that the ViewPoint Server is located on the SonicWALL LAN for optimal performance issues, it may also be located remotely across a VPN tunnel. The only requirement is that the ViewPoint Server can access and login to the SonicWALL Web Management interface.

***Note**: If your VPN tunnel is interrupted or temporarily disabled, report data can be lost.*

ViewPoint Administrative Tools

The ViewPoint software includes several utilities to improve management and reliability. The utilities include a Repair Database tool, and Startup and Shutdown commands.

ViewPoint Repair Database

If the ViewPoint server temporarily loses power, the ViewPoint database files can become corrupt. When this occurs, affect ViewPoint reports neither function or display report data. The SonicWALL folder in the Windows **Start** menu, includes a **ViewPoint Database Repair** utility. The Repair Database utility repairs affected database files by removing corrupt data and indexes.

To fix any problems, the database server must be temporarily halted. This causes an interruption to the ViewPoint Service, and some loss of data may occur. The repair operation may take considerable time to complete, so it is best to run it when the system is lightly loaded.

You can repair your database by launching the **ViewPoint Database Repair** utility from the **SonicWALL** directory in the Windows **Start** menu, and then selecting any key. You can cancel the program by pressing **Control -C** from your keyboard. It is recommended that you do not cancel the program while it is recovering files from your database.

To avoid possible database corruption, be sure to use an uninterruptible power supply, and always shut down your ViewPoint server.

Startup and Shutdown Commands

The ViewPoint software includes the following applications: a Web server, a syslog server, and a database. For administrative purposes or other reasons, it may be necessary to start or stop ViewPoint and all of its software components.

The **Startup** command, located in the SonicWALL directory in the Windows **Start** menu, launches all of the ViewPoint software services. The **Shutdown** command, located in the same directory, safely shuts down the ViewPoint software services.

ViewPoint Software Components

The ViewPoint software program consists of the following components:

- **MySQL Database**
- **Tomcat Web Server**
- **Syslog Server**
- **SonicWALL ViewPoint**

MySQL Database

MySQL is a relational database management system. It is open source software that uses SQL, Structured Query Language, the most common standardized language used to access databases. To learn more about MySQL database systems, visit http://www.mysql.com.

TomCat Web Server

TomCat is a Web Server and Java Servlet engine developed by the Apache Software Foundation. More specifically, Tomcat is a Java server that invokes servlets when JSP pages are requested. To learn more about Tomcat software or the Apache Software Foundation, visit http://www.apache.org.

SonicWALL ViewPoint Software

SonicWALL ViewPoint software includes proprietary HTML, Java, and servlet files as well as a Syslog Daemon. The SonicWALL Syslog Daemon receives syslog messages from a SonicWALL Internet security appliance on UDP port 514, and then forwards the messages to the MySQL database.

ViewPoint operates on Windows XP, 2000, and NT with Service Pack 4 or higher.

Active ViewPoint Services

For maintenance or other reasons, it may be necessary to start or stop ViewPoint services. ViewPoint-related services in the “Control Panel/ Administrative Tools/Services” directory include **ViewPoint**, **Syslogd**, and **MySQL**.

Process initiated by ViewPoint that appear in the Windows Task Manager include **mysqld-nt.exe**, **java.exe**, **syslogd.exe**, and **srvany.exe**.

Notes

Activation Key

SonicWALL, Inc.
1160 Bordeaux Dr.
Sunnyvale, CA 94089-1209
Phone: 408-745-9600
Fax: 408-745-9300
Email: sales@sonicwall.com
Web: www.sonicwall.com

Part # 232-000103-01
Rev A 4/02