SonicWALL ViewPoint User's Guide

SONICWALL

CONTENTS

Copyright Notice 2
Software License Agreement 3

1 INTRODUCTION 5

2 GETTING STARTED 6
System Requirements 6
Network Configuration for ViewPoint 6

3 REGISTERING VIEWPOINT 7

4 UPDATING SONICWALL FIRMWARE 9

5 CONFIGURING THE SONICWALL 11

6 INSTALLING VIEWPOINT 12
Installing the ViewPoint Software 12

7 MANAGING VIEWPOINT 14
Logging into the ViewPoint Web Interface 14
Configuring ViewPoint Settings 15
Configuring SonicWALL Settings 16
Configuring Syslog Settings 18
Setting the ViewPoint Report Date 20

8 VIEWPOINT WEB INTERFACE 21

9 REPORT DESCRIPTIONS 23
General Reports 23
Bandwidth Reports 24
Services Reports 25
Web Usage Reports 26
Web Filter Reports 27
FTP Usage Reports 29
Mail Usage Reports 29
Attack Reports 30

10 ACCESSING VIEWPOINT REMOTELY 32

APPENDIX 33
Uninstalling ViewPoint 33
ViewPoint Server Across a VPN 33
ViewPoint Administrative Tools 34
ViewPoint Software Components 35
Active ViewPoint Services 35

NOTES 36

Copyright Notice

Under the 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. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) may be sold, given, or loaned to another person. 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 subject to change without 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").

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 LE GAL 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 supercedes 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.

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 compliments SonicWALL's Internet security offerings by providing detailed and comprehensive reports of network activity.

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

SonicWALL ViewPoint:

- 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 may be installed on a server running Windows 2000 or NT located on the SonicWALL's LAN. SonicWALL ViewPoint 1.1 is available as a standard feature for the SonicWALL PRO-VX and the SonicWALL GX and an optional upgrade for the SonicWALL PRO.

2 GETTING STARTED

SonicWALL ViewPoint is a software reporting solution that may be installed on any computer on the SonicWALL's LAN. The computer used to host the reporting software will be referred to as the "ViewPoint Server."

System Requirements

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

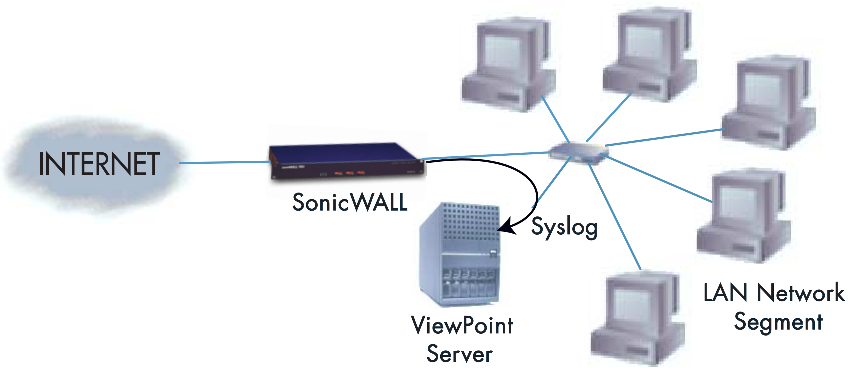
- Microsoft Windows 2000 or NT 4.0 Service Pack 4 or greater
- 500 MHz Processor
- 512 MB available disk space
- 256 MB memory
- Internet Explorer 4.0 or later or Netscape Navigator 4.0 or greater

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

Network Configuration for ViewPoint

The following diagram illustrates the network configuration for SonicWALL ViewPoint:

The SonicWALL ViewPoint Server may be any computer or server located on the SonicWALL's LAN running Windows 2000 or Windows NT 4.0 SP 4 or greater and meeting the minimum system requirements.



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

3 REGISTERING VIEWPOINT

The following instructions describe the procedure to register and activate the ViewPoint Upgrade for the SonicWALL PRO. Registering the ViewPoint Upgrade is not required for the SonicWALL PRO-VX or SonicWALL GX.

From a Web browser, go to the SonicWALL registration site at http://www.mysonicwall.com and enter your **User Name** and **Password** to login. If you do not have a mysonicwall.com user account, you will need to create one.

To register your SonicWALL Internet security appliance:

1. Select the **My Products** option on the menu at the top of the browser window. The SonicWALL Product Registration page will be displayed.

2. In the "Add New Product" section, enter the **Serial Number** of your SonicWALL.

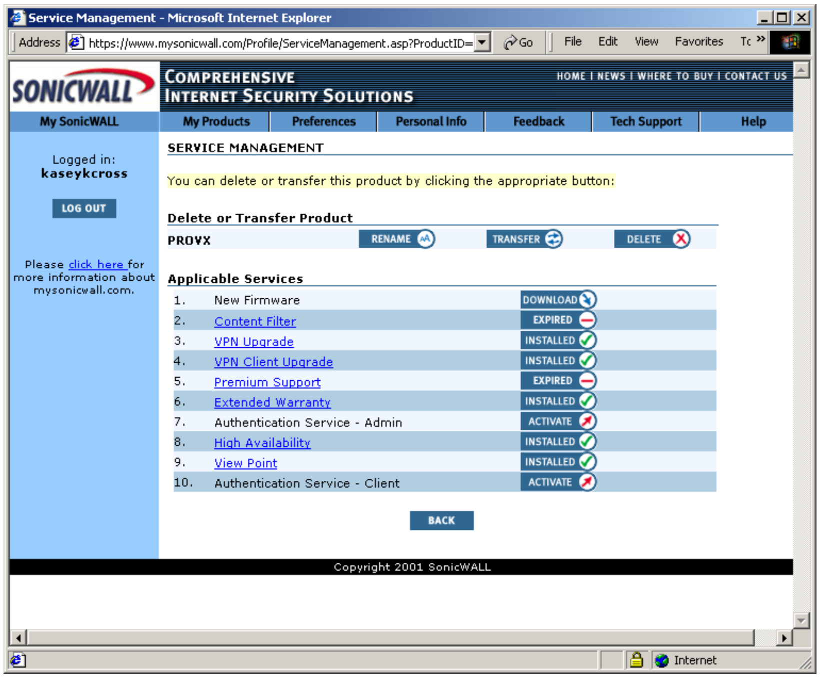
3. Enter a **Friendly Name** that you will use to identify your SonicWALL.

4. Click the **Register** button.

To activate your ViewPoint Upgrade:

1. Return to the home page by selecting **My SonicWALL**.

2. Select the friendly name that you created for your SonicWALL to display the registration information. A window similar to the following will be displayed.


Service Management - Microsoft Internet Explorer
Address https://www.mysonicwall.com/Profile/ServiceManagement.asp?ProductID=
Go
File Edit View Favorites
SONICWALL
COMPREHENSIVE INTERNET SECURITY SOLUTIONS
HOME I NEWS I WHERE TO BUY I CONTACT US
My SonicWALL
My Products
Preferences
Personal Info
Feedback
Tech Support
Help
LOG OUT
RENAME
TRANSFER
DELETE
BACK
Internet

Logged in:
kaseykcross

Please click here for more information about mysonicwall.com.

SERVICE MANAGEMENT

You can delete or transfer this product by clicking the appropriate button:

Delete or Transfer Product

PROVX

Applicable Services

1.	New Firmware	DOWNLOAD
2.	Content Filter	EXPIRED
3.	VPN Upgrade	INSTALLED
4.	VPN Client Upgrade	INSTALLED
5.	Premium Support	EXPIRED
6.	Extended Warranty	INSTALLED
7.	Authentication Service - Admin	ACTIVATE
8.	High Availability	INSTALLED
9.	View Point	INSTALLED
10.	Authentication Service - Client	ACTIVATE

Copyright 2001 SonicWALL

3. In the "My SonicWALL Service Management" window, select the **Activate** button displayed next to the **ViewPoint** service. An "Activate Service" window will be displayed.

4. Enter the ViewPoint Activation Key displayed on the back of this manual in the **Activation Key** field.

5. Click the **Submit** button.

Once the Activation Key has been registered, a ViewPoint License Key will be displayed. Record this activation key carefully or copy the License Key to your Windows Clipboard.

1. Log into SonicWALL Web Management Interface.

2. Click the **Log** button on the left side of the browser window and then click the **ViewPoint** tab at the top of the window. The ViewPoint Upgrade window will be displayed.

3. Enter the ViewPoint License Key displayed on the mysonicwall.com registration site into the **Enter upgrade key** field in the SonicWALL PRO.

4. Click the **Update** button and then restart the SonicWALL for the change to take effect.

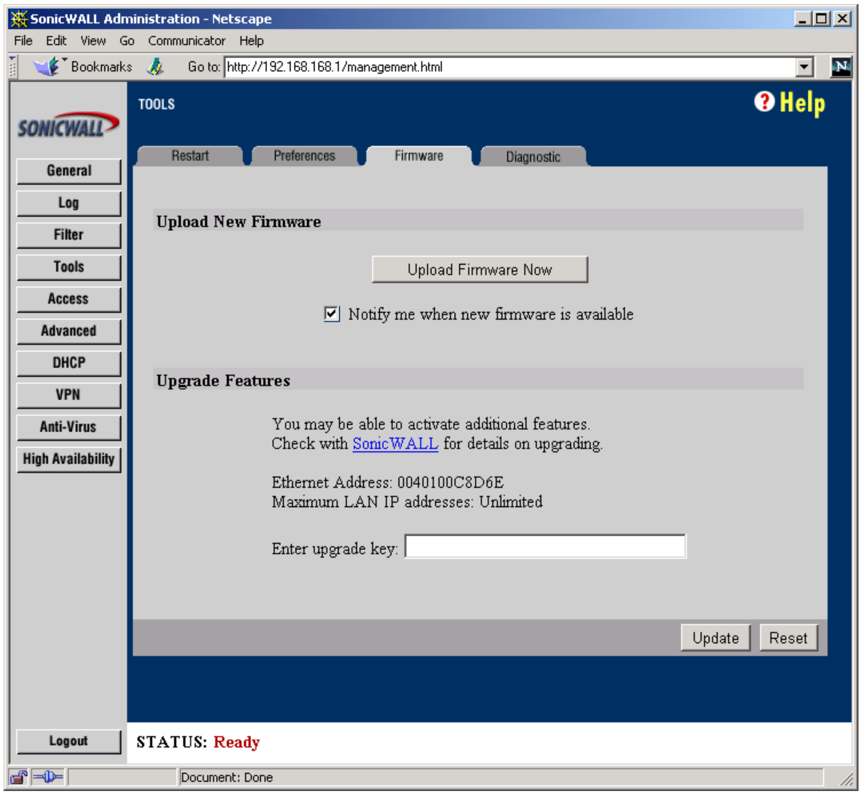
4 UPDATING SONICWALL FIRMWARE

You must upgrade the SonicWALL firmware to version 6.1.0.0 to support ViewPoint. You may skip this section if you are using firmware version 6.1.0.0 or greater.

1. From a Web browser, go to http://www.sonicwall.com and navigate to the Download Center to download the latest version of SonicWALL firmware to your local disk.

2. Login to your SonicWALL Internet security appliance.

3. Click the **Tools** button on the left side of the browser window and then click the **Firmware** tab at the top of the window. A window similar to the following will be displayed.



Upload New Firmware

☑ Notify me when new firmware is available

Upgrade Features

You may be able to activate additional features.
Check with SonicWALL for details on upgrading.

Ethernet Address: 0040100C8D6E
Maximum LAN IP addresses: Unlimited

Enter upgrade key:

STATUS: Ready

Note: *You must register your SonicWALL Internet security appliance at http://www.mysonicwall.com before you may upgrade firmware.*

4. Click the **Upload Firmware Now** button.

5. A **Save Preferences** window will appear. When firmware is updated, your SonicWALL's settings may be erased, so it is recommended to save the SonicWALL's preferences. If you have saved the SonicWALL's preferences file to your local disk, click **Yes**.

6. Click the **Browse** button and select the SonicWALL firmware file from your computer's local disk.

7. Click the **Upload** button to upload the firmware file.

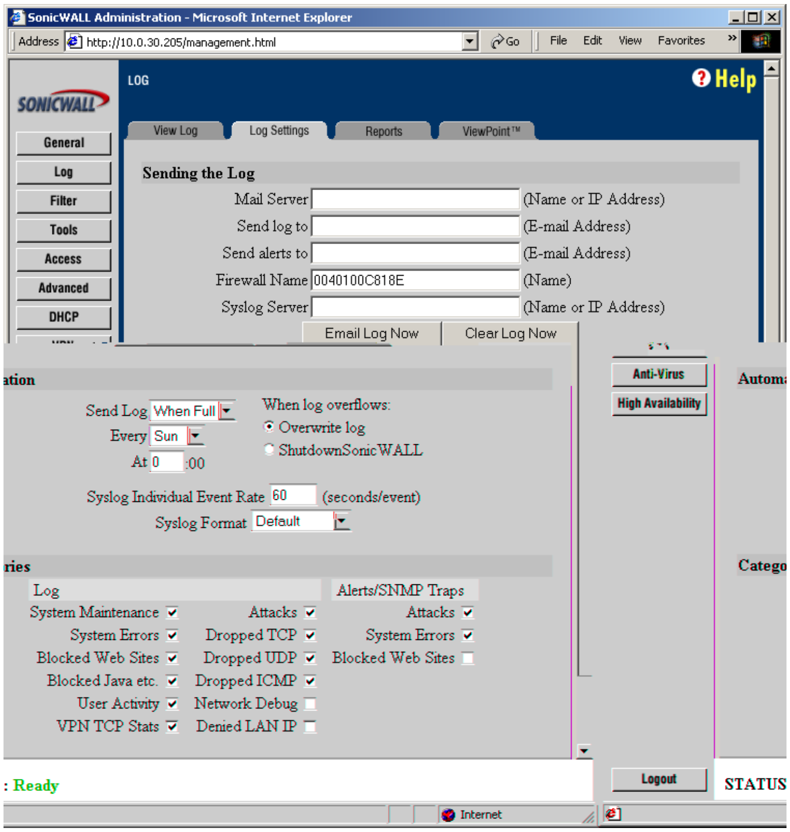
8. Restart the SonicWALL for the change to take effect.

Note*: When uploading firmware to the SonicWALL, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the SonicWALL firmware.*

5 CONFIGURING THE SONICWALL

Configure the SonicWALL to direct syslog to the ViewPoint Server.

1. Click the **Log** button on the left side of the browser window and then click the **Log Settings** tab at the top of the window. A window similar to the following will be displayed.



Sending the Log

Mail Server		(Name or IP Address)
Send log to		(E-mail Address)
Send alerts to		(E-mail Address)
Firewall Name	0040100C818E	(Name)
Syslog Server		(Name or IP Address)

ation

Send Log When Full

Every Sun

At 0 :00

When log overflows:
● Overwrite log
○ ShutdownSonicWALL

Syslog Individual Event Rate 60 (seconds/event)

Syslog Format Default

ries

Log				Alerts/SNMP Traps	
System Maintenance	☑	Attacks	☑	Attacks	☑
System Errors	☑	Dropped TCP	☑	System Errors	☑
Blocked Web Sites	☑	Dropped UDP	☑	Blocked Web Sites	□
Blocked Java etc.	☑	Dropped ICMP	☑		
User Activity	☑	Network Debug	□		
VPN TCP Stats	☑	Denied LAN IP	□		

2. Enter the IP address or domain name of the ViewPoint Server in the **Syslog Server** field.

***Note**: The ViewPoint Server must have a static IP address. Confirm that the server has a permanent IP address in the server's **TCP/IP Properties** window.*

3. Enter "0" in the **Syslog Individual Event Rate** field to send all syslog messages without filtering.

4. Confirm that the **Syslog Format** menu is set to "Default".

5. Click the **Update** button at the bottom of the browser window, then restart your SonicWALL.

6 INSTALLING VIEWPOINT

Installing the ViewPoint Software

You may install ViewPoint from the ViewPoint Upgrade CD or you may download the ViewPoint software file from the SonicWALL, Inc. Web site.

The ViewPoint server must be running Windows 2000 or Windows NT SP 4 or greater and it must have a static IP address.

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

Before you attempt the installation, confirm that your server meets the system requirements described on page 6.

CD Installation

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

Internet Download Installation

To download and install the software from the Internet, save the ViewPoint executable file to your hard drive and then double click the file to run the executable.

Software License Agreement

Before the program files are copied to your system, the Software License Agreement is presented.

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

Note: *When you install ViewPoint, be sure to close all other applications on your computer.*

The installation wizard will guide you through the set up and install ViewPoint reporting software and syslog server, Tomcat Web Server, and MySQL Database. Please refer to the Appendix for more information about these software components.

The ViewPoint setup program will detect whether the default Web, syslog or MySQL ports are in use. If the default Web port is active, the setup program will automatically recommend an alternative Web port, port 8080. If either syslog port 514 or MySQL port 3306 are active, the ViewPoint setup program will display an error message.

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

The Installation Wizard will prompt you to define the ViewPoint Web Server port. The default Web (HTTP) port is port 80.

Note: *If you have a Web server already installed on your computer, then configure the ViewPoint's Web server to run on an unused HTTP port, such as the recommended port, 8080.*

The Installation Wizard will prompt you to define additional settings, such as the SonicWALL LAN IP address and the SonicWALL administrator password.

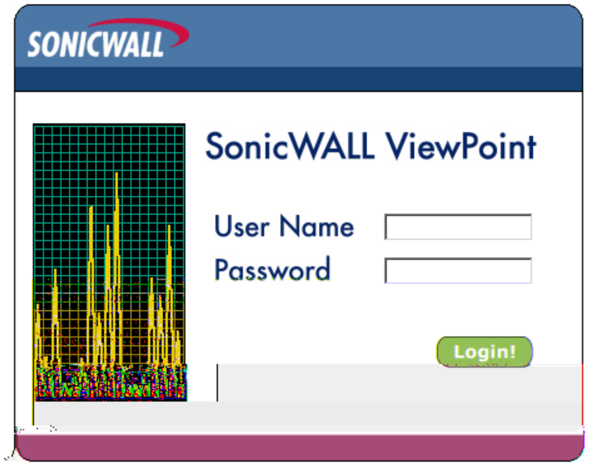
Once the programs have been installed, you may close the ViewPoint Installation Wizard window. You will need to restart your computer for the changes to take effect.

7 MANAGING VIEWPOINT

Logging Into the ViewPoint Web Interface

You will need to configure several settings in the ViewPoint Web Interface in order to view network reports.

From a Web browser, type http://LocalHost or http://<ViewPoint Server IP Address> into the **Location** or **Address** field or launch ViewPoint from the **SonicWALL** folder in the Windows **Start** menu. An authentication window similar to the following will be displayed.



Note: *If you configured the ViewPoint Web server to use a different port than port 80, then add the port number to the URL, for example, http://LocalHost:8080.*

1. Type the **User Name** and **Password**.

Note: *The default* ***User Name*** *is "admin" and the default* ***Password*** *is "password."*

Note*: The password that was configured during the ViewPoint installation is used to authenticate to your SonicWALL, it does not provide access to ViewPoint.*

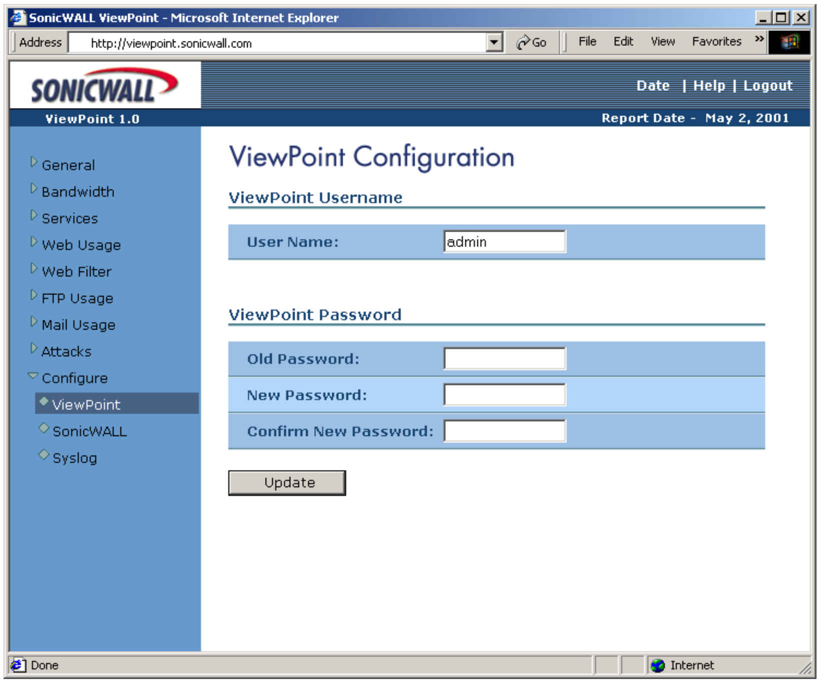
2. Click the **Login** button to login to the Web Interface.

Note*: Confirm that the authentication screen has finished loading before attempting to log in. Also note that the ViewPoint password is case-sensitive.*

Configuring ViewPoint Settings

ViewPoint requires that users successfully authenticate to access reports. This authentication mechanism prevents unknown users from viewing sensitive network data. The ViewPoint Configuration window allows you to modify the ViewPoint user name and password.

1. From the ViewPoint Web Interface, expand the **Configure** option on the left side of the browser window and then click **ViewPoint**. A window similar to the following will be displayed.



ViewPoint Configuration

ViewPoint Username

User Name: admin

ViewPoint Password

Old Password:

New Password:

Confirm New Password:

2. To change the ViewPoint user name, highlight the text in the **User Name** field and replace it with your new user name.

3. To change the ViewPoint password, enter your current ViewPoint password in the **Old Password** field.

4. Enter the new ViewPoint password in the **New Password** and **Confirm New Password** fields.

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

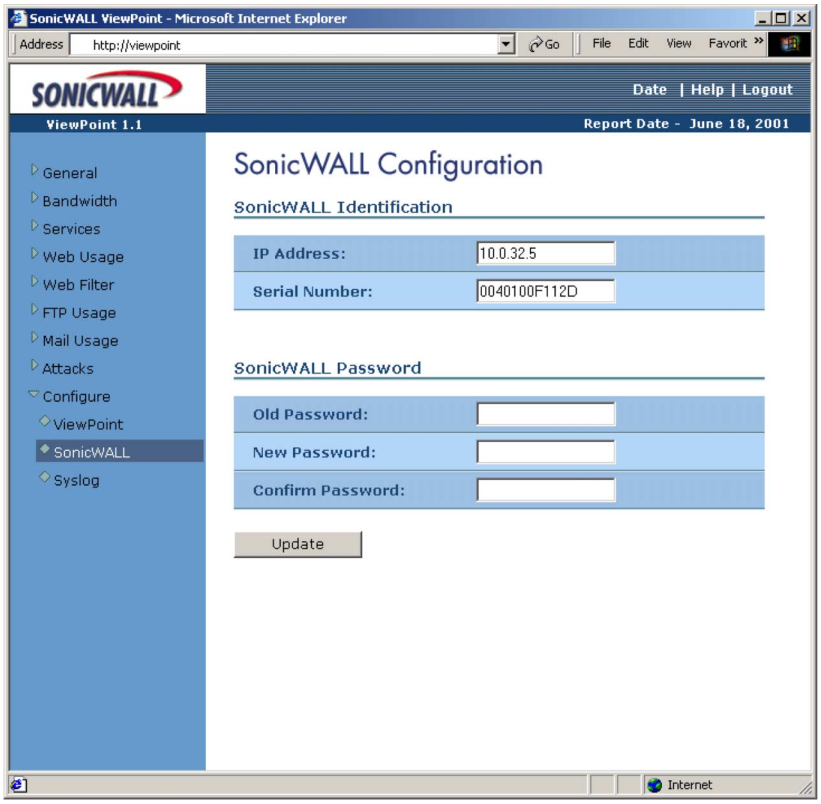
6. Click the **Update** button to update the configuration.

Note: *If you lose or forget the ViewPoint user name or password, you will need to uninstall and then reinstall the ViewPoint software.*

Configuring SonicWALL Settings

ViewPoint transparently authenticates to your SonicWALL Internet security appliance for status and state information. ViewPoint uses the SonicWALL administrator password and IP address configured during ViewPoint installation to authenticate. If the SonicWALL IP address or password is changed, you will need to modify the ViewPoint settings to reflect these changes.

1. From the ViewPoint Web Interface, expand the **Configure** option on the left side of the browser window and then click **SonicWALL**. A window similar to the following will be displayed.



SonicWALL Configuration

SonicWALL Identification

IP Address:	10.0.32.5
Serial Number:	0040100F112D

SonicWALL Password

Old Password:	
New Password:	
Confirm Password:	

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 12 character, alphanumeric serial number is displayed on the **General Status** window of the SonicWALL Web Management Interface.

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 New Password** fields.

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

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

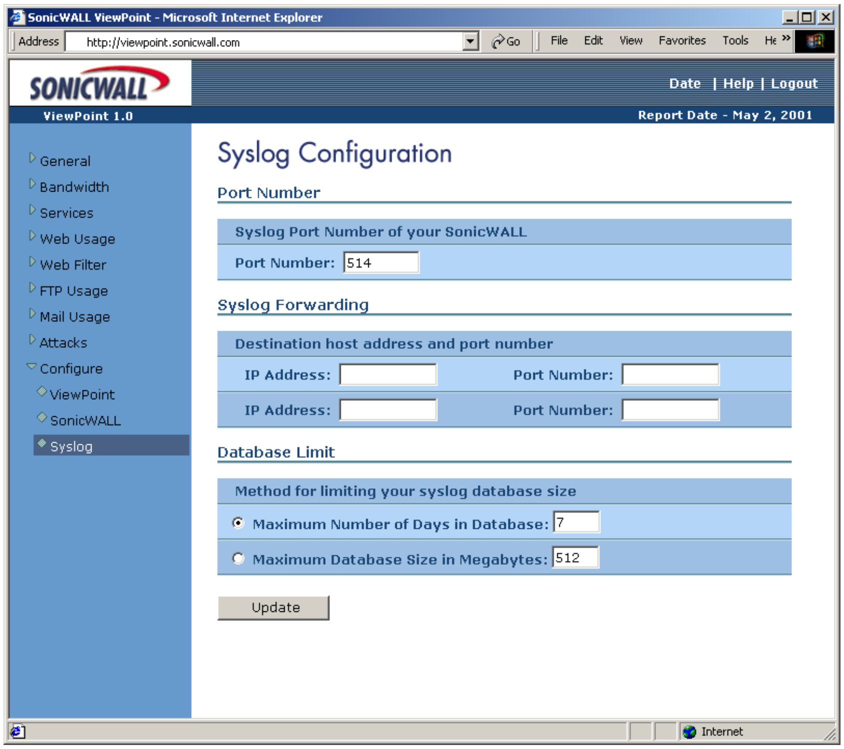
Click the **Update** button to update the configuration. Then logout of ViewPoint and reauthenticate in order for these changes to take effect.

Note: *If you lose or forget the password that had been defined in the SonicWALL Configuration window and ViewPoint cannot authenticate to your SonicWALL, you will need to uninstall and reinstall the ViewPoint software, and then define the correct SonicWALL administrator password.*

Configuring Syslog Settings

The Syslog Configuration window allows you to change the UDP port number that ViewPoint syslog server listens on, to configure ViewPoint to forward syslog data to other servers, and to limit the database size.

1. From the ViewPoint Web Interface, expand the **Configure** option on the left side of the browser window and then click **Syslog**. A window similar to the following will be displayed.



Syslog Configuration

Port Number

Syslog Port Number of your SonicWALL

Port Number: 514

Syslog Forwarding

Destination host address and port number

IP Address: Port Number:

IP Address: Port Number:

Database Limit

Method for limiting your syslog database size

● Maximum Number of Days in Database: 7

○ Maximum Database Size in Megabytes: 512

2. To change the UDP port number that the ViewPoint syslog server listens on, enter the new port number in the **Port Number** field.

Note: *SonicWALL Internet security appliances write syslog traffic on port number 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 will be sent on in the **Port Number** field.

5. You may configure the maximum size of the ViewPoint database. To limit the database by number of days, select the **Maximum Number of Days in Database** radio button and enter the number of days that syslog messages should be saved in the corresponding field.

   To limit the database by size, select the **Maximum Database Size in Megabytes** radio button and enter the number of megabytes of memory that the database will store in the corresponding field.

Note: *By default, Viewpoint will save database records for seven days.*

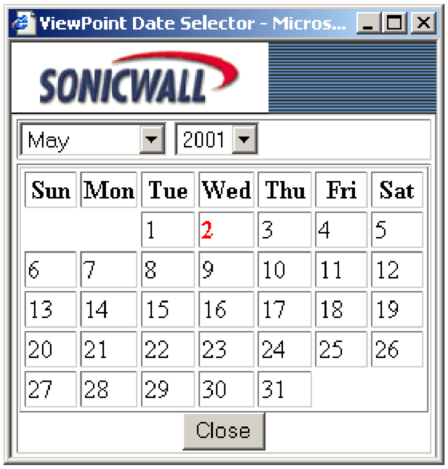
6. Click the **Update** button.

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

Setting the ViewPoint Report Date

You may change the ViewPoint report date quickly and easily.

1. To change the report date, click the **Date** option in the top right corner of the browser window. A window similar to the following will appear.



May 2001

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

2. The current report date will be highlighted in the ViewPoint date calendar. Select the desired month and year from the **Month** and **Year** menus.

3. Select the desired day in the ViewPoint date calendar. The new report date will be displayed in the upper right corner of the ViewPoint Report window. The ViewPoint report table and chart will also be updated to show the new report date.

4. Click **Close** to close the ViewPoint Date Selector window.

8 VIEWPOINT WEB INTERFACE

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

Note: *Please use Internet Explorer 4.0 or greater or Netscape Navigator 4.0 or greater to login 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** options appear on the left side of the window. You may navigate through the Web-based ViewPoint reports by selecting and expanding the menu options on the left side of browser window and then selecting the desired ViewPoint report. The ViewPoint Web Interface should be intuitive and easy-to-navigate for anyone familiar with the tree-structure menu design.

The ViewPoint Web Interface also includes links at the top right corner of the browser window. These options are: **Date**, **Help**, and **Logout**.

- The **Date** option opens a new window. This window allows you to change the report date from a Web-based calendar.
- The **Help** option displays comprehensive instructions for installing, configuring and troubleshooting ViewPoint.
- The **Logout** option on the upper right side of the browser window terminates the management session and redisplays the Authentication window. If the Logout option is clicked, it will be necessary to reauthenticate to use ViewPoint.

Note: *The ViewPoint administrator will be automatically logged out of the ViewPoint User Interface after 5 minutes of inactivity.*

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

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 time. The table provides a summary of the data displayed in the chart. Several reports deviate from this layout: the **General Status** report presents state information retrieved directly from the SonicWALL, the **Bandwidth Monitor** and **Service Monitor** 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 all pertinent events sorted by time.

Next/Previous

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

Source

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

Destination

The **Destination** is the domain or host name or the IP address that the event was directed towards.

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 upon the report type, events may 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.

9 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 and subscriptions, the number of users connected to the SonicWALL, and other state 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 machine that authenticated to the SonicWALL.

User Login

The User Login report lists 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 window in the SonicWALL Web 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 machine that authenticated to the SonicWALL.

Failed Login

The Failed Login report lists all attempts to login 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 machine 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 helps illustrate the cause of VPN negotiation failures. It also 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 that occurred to the SonicWALL Internet security appliance during the report period. System events include successful downloads of the Content Filter List, SonicWALL activations, DHCP and PPPoE informational messages, and High Availability backup firewall activation. System errors listed include problems downloading the Content Filter List, difficulties obtaining a DHCP Client or PPPoE Client Lease, deactivation of the SonicWALL because the log was full, and the number of simultaneous connections exceeding the limit.

The System Events table displays the time, the source name or IP address, and the type of system event. Since many system events are created by the SonicWALL, the SonicWALL will be the most common source of events. Most events are results of 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. This report helps to 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 that occurred during the hour, the number of MBytes transferred, and the MBytes as a percentage of the total MBytes for the report day. Both the chart and the table include inbound and outbound traffic through the LAN, WAN, and DMZ interfaces.

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 5 minutes. The Bandwidth Monitor includes traffic through the LAN, WAN, and DMZ interfaces.

Top Users of Bandwidth

The Top Users of Bandwidth report shows the top users of bandwidth in KBytes per second. This report illustrates which users on the LAN, the WAN, or the DMZ are using the greatest amount of bandwidth. This data helps identify 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 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.

Services Reports

Service Summary

The Service Summary Report shows 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 have occurred. 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 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 includes traffic through the LAN, WAN, and DMZ interfaces.

Web Usage Reports

Web Usage Summary Report

The Web Usage Summary report shows the amount of Web (HTTP) traffic traveling through your 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 hour, 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 snapshot of the Web sites located on the LAN, WAN, or DMZ that users are visiting.

The Top Web Sites report displays a bar graph of the top 20 Web sites visited by the number of hits to the 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 the 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 may view and evaluate the top Web sites.*

Top Users of Web

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

The Top Users of Web report displays a pie chart of the top 10 users by the number of Web site hits. The report table lists the top 10 users displayed in the chart, the number of MBytes transferred by the user, the number of hits generated 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 shows the top 5 Web sites visited by user. This 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 Web, the top 5 Web sites visited by each user, and the KBytes transferred from the Web site to the user. Additional users' Web activity may 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 may view and evaluate the listed Web sites.*

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’s Content Filter List or by customized Keyword or Domain Name filtering. This report also includes blocked Java, blocked cookies and blocked ActiveX attempts.

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

Top Objectionable Web Sites

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

The Top Objectionable Web Sites report displays a pie chart of the top 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 the total attempts during the report period.

Note: *The Web sites displayed in the table include links to the blocked sites, so that the ViewPoint administrator may view and evaluate blocked Web sites. The ViewPoint administrator may also be blocked from accessing these sites if he or she does not have privileges to bypass the SonicWALL's Content Filter List.*

Top Users Attempting to Access Objectionable Web Sites

The Top Users Attempting to Access Objectionable Web Sites report shows the users most frequently blocked by the SonicWALL’s Content Filtering policies. This report presents a list of users that are trying to access inappropriate or objectionable material on the Internet.

The Top Users Attempting to Access Objectionable Web Sites report displays a pie chart of the top 10 users by the number of connection attempts. The report table lists the top 10 users displayed in the chart, the number of Web attempts by the user, and the number of attempts as a percentage of the total blocked attempts during the report period.

Top Objectionable Web Sites By User

The Top Objectionable Web Sites By User report shows the top 5 filtered Web sites by user. This report describes the Web sites users attempted to visit that were blocked by the SonicWALL’s Web Content Filtering policies.

The Top Objectionable Web Sites By User report displays a table of the users blocked by the SonicWALL, the top 5 Web sites the users attempted to access, and the number of attempts to access each Web site. If more than 5 users attempted to access objectionable Web sites, the additional users' Web activity may be displayed by clicking the **Next 5** link 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 traveling through the SonicWALL in KBytes per second. This report displays 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 that occurred 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 shows the most active users on the LAN, WAN, or DMZ transferring FTP files. This 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 10 users of FTP by the number of KBytes transferred. The report table lists the top 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 traveling 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 through the SonicWALL in KBytes transferred. The table displays the hour of the day, the number of Mail events that occurred 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. This 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 10 users by the number of Mail Events. The report table lists the top 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 the SonicWALL received over the report period. It displays Denial of Service 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 shows the top users that attacked the SonicWALL or devices on the network over 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 report displays a pie chart of the top 10 sources by the number of attacks. The report table lists the top 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 over 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 10 attack categories displayed in the chart, the number of attacks for the category, and the number of attacks for the category as a percentage of the total attacks during the report period.

Dropped Packets

The Dropped Packets report displays all IP packets dropped by your SonicWALL. IP packets dropped by the SonicWALL include: TCP Packets, UDP Packets, ICMP Packets, IPSec Packets, PPTP Packets, Broadcast Packets, and Fragmented Packets. The Dropped Packets report includes blocked NetBIOS packets and other normal Internet activity and it also 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 and the number of dropped packets as a percentage of the total dropped packets during the report period.

10 ACCESSING VIEWPOINT REMOTELY

Because the ViewPoint Interface is Web browser-based, any user on the SonicWALL's LAN may login and look at ViewPoint network reports. Even users located across a VPN or accessing network resources through applications such as pcAnywhere should be able to contact the ViewPoint Web Interface.

To access ViewPoint, the remote user should launch a Web browser, then type 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 port 80, add the port number after the IP address, for example, type http://<IP Address>:8080.*

Note: *Internet Explorer 4.0 or greater or Netscape Navigator 4.0 or greater should be used to login and manage ViewPoint. The Web browser must also be enabled for Java and cookies and support Java applets.*

1. Type the ViewPoint **User Name** and **Password**.

2. Click the **Login** button to login to the Web Interface.

The remote user will be 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 setup program.

1. If you installed ViewPoint from a CD, load the CD into your server and run the ViewPoint setup 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 can not locate the ViewPoint executable file, you may download it from http://www.sonicwall.com.

2. The ViewPoint setup program will automatically detect ViewPoint and display a window to confirm deletion of the software. To remove the ViewPoint software application and all of its components, select **OK**.

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

4. The ViewPoint uninstall program will also prompt you to delete the ViewPoint database data. To remove the data, click **Yes**. To keep 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 be located on the SonicWALL's LAN for performance issues, it may also be located remotely, across a VPN. The only requirement is that the ViewPoint Server must be able to access and login to the SonicWALL Web Management Interface.

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

ViewPoint Administrative Tools

The ViewPoint software includes several utilities to improve management and reliability. These 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 may become corrupt. When this occurs, affected ViewPoint reports will neither function nor 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 will cause an interruption to the ViewPoint service,and some loss of data may occur. The repair operation may take some considerable time to complete, and is best run when the system is lightly loaded.

You may 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 may cancel the program by pressing **Control-C** from your keyboard. It is advisable not to cancel the program while it is recovering files.

To avoid possible database corruption issues, be sure to use an uninterruptible power supply and always properly 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 or other purposes, it may be necessary to completely 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 the ViewPoint software services. The **Shutdown** command, also located in the **SonicWALL** directory in the Windows **Start** menu, safely closes the ViewPoint software services.

ViewPoint Software Components

The ViewPoint software program consists of several different components. These components include: MySQL Database, Tomcat Web server, a syslog server, and SonicWALL ViewPoint software files.

MySQL Database

MySQL is a relational database management system. It is open source software that uses SQL, or Structured Query Language, the most common standardized language used to access databases. To learn more about the MySQL database system, 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 software operates on Windows 2000 or Windows NT 4.0 Service Pack 4 or greater.

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**.

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

NOTES