SonicWALL Vulnerability Scanning Service User's Guide

A User's Guide for the Network Vulnerability Assessment Service

Contents

Limited Warranty

SonicWALL, Inc. warrants that SonicWALL SonicWALL Vulnerability Scanning Service performs in accordance to the accompanying written materials for a period of ninety (90) days from the date of receipt.

SonicWALL Inc.'s and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the PRODUCT has resulted from accident, abuse, or misapplication. Any replacement PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

In no event shall SonicWALL or its suppliers be liable for any damages whatsoever (including, without limitation, special, incidental, indirect, or consequential damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the PRODUCT.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL's liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state.

By using this Product, you agree to these limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

No dealer, agent, or employee of SonicWALL is authorized to make any extension or addition to this warranty.

Introduction

While public servers provide an important link to the outside world, they also make an inviting target for hackers. Server operating system and application software vulnerabilities are routinely discovered and addressed with new software updates, but delays in applying updates can give hackers a window of opportunity to strike.

SonicWALL Vulnerability Scanning Service is an automated, web-based service that provides network administrators a "hacker's eye view" of a company's network perimeter, including public servers, routers and gateways. This service examines a network perimeter for security weaknesses on an ongoing basis, reports all vulnerabilities detected, and provides administrators with in-depth, expert guidance to quickly close up any security holes.

The subscription-based service offers vulnerability assessment scans that can scheduled on a regular basis or run on demand when policies change or new equipment is deployed.

SonicWALL Vulnerability Scanning Service is easy to configure using SonicWALL's integrated, Web-based security portal at http://www.mysonicwall.com.

Features and Benefits

- **Comprehensive Vulnerability Assessment -** This service checks for more than 730 types of vulnerabilities. It detects operating system security "holes," DNS, HTTP, FTP, SMTP server vulnerabilities, network device vulnerabilities (routers, printers, bridges, switches, etc), TCP/IP port openings and more.
- **Simple to Administer -** SonicWALL Vulnerability Scanning Service is easy to use and integrated with SonicWALL Internet security appliances. It's a Web-based service so there is no software to install. You can easily schedule scans and configure the service to fit your needs from your own security portal at www.mysonicwall.com.
- **Flexible Reporting Options -** You can sort reports by risk level and other criteria to allow you prioritize which vulnerabilities to address.
- **Customizable Scheduling -** You can schedule security assessment scans periodically or on-demand.
- **State-of-the-Art Updates -** Security updates for SonicWALL Vulnerability Scanning Service security are backed by NAI (Network Associates) Labs, a leader in advanced security technology.
- **Instant Expertise -** SonicWALL Vulnerability Scanning Service provides expert remedies to fix detected security vulnerabilities.

- **Assured Security -** This service delivers peace of mind for network administrators as their public servers are checked for security vulnerabilities on an ongoing basis.

Getting Started

Before You Start

Using the Vulnerability Scanning Service requires that you register your SonicWALL Internet Security Appliance at http://www.mysonicwall.com. You can create a user account to activate and manage services for all of your SonicWALL Internet Security Appliances.

> ***Note****: For the latest version of this manual and other SonicWALL documentation, go to http://www.sonicwall.com/products/documentation.html*

What is mySonicWALL.com?

mySonicWALL.com delivers a convenient, centralized way to register all your SonicWALL Internet Security Appliances and Security Services. It eliminates the hassle of registering individual SonicWALL appliances and upgrades to streamline the management of all your SonicWALL security services. Instead of registering each SonicWALL product individually, using mySonicWALL.com allows you to have a single user profile where you can manage all you product registrations and security services.

What Can I Do with mySonicWALL.com?

You can use MySonicWALL.com to:

- Register all your SonicWALL appliances and services in one place
- Access firmware and security service updates
- Get SonicWALL alerts on services, firmware, and products
- Check status of your SonicWALL services and upgrades linked to each registered SonicWALL Internet security appliance
- Manage (activate, change or delete) your SonicWALL security services online

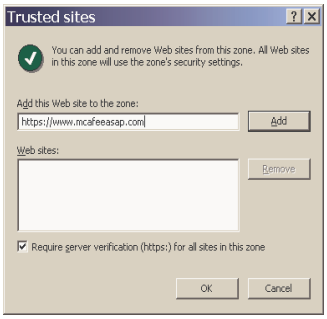
How do I Get Started with mySonicWALL.com?

The first step to using mySonicWALL.com is creating a user account. Go to http://www.mysonicwall.com and follow the instructions for setting up a new user account.

Microsoft® Internet Explorer 6.0

Microsoft® Internet Explorer 5.x is recommended for viewing your Service Reports. If you are using IE 6.0 as a web browser, you must configure it appropriately using the following steps:

1. Open IE 6.0, and select **Tools** from the menu bar, and then select **Internet Options**.
2. Select the **Security** tab, and click the **Trusted Sites** icon. Click the **Sites...** button.
3. Type the URL https://www.mcafeeasap.com into the **Add this Web site to the zone:** field. Click **Add**, and then **OK**.



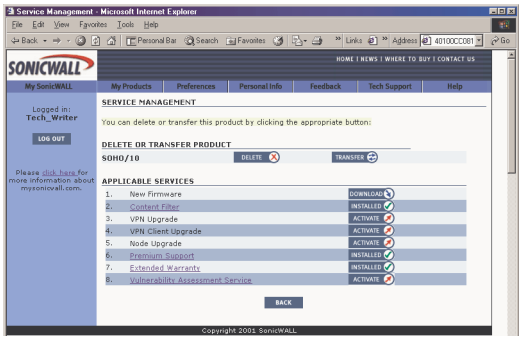
If you continue to experience problems with your Vulnerability Scanning Service, contact SonicWALL tech support at <http://techsupport.sonicwall.com/vsstech.html.

Activating the SonicWALL Vulnerability Scanning Service

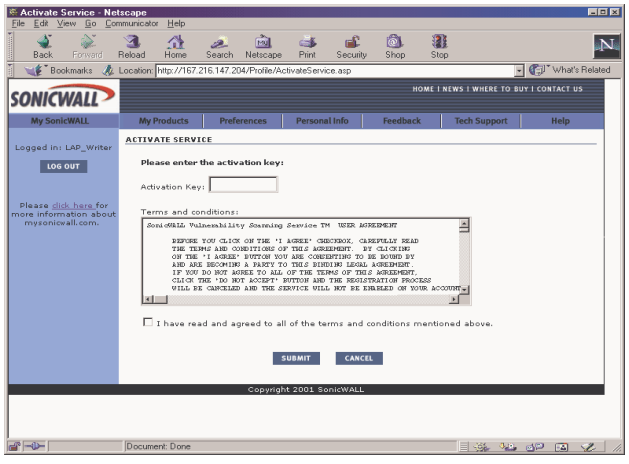
1. Log into http://www.mysonicwall.com using your username and password.

   Note: *If you do not have a user account at mysonicwall.com, see the* ***Before You Start*** *section of this manual.*

2. Click on your SonicWALL Internet Security Appliance and review the list of services.



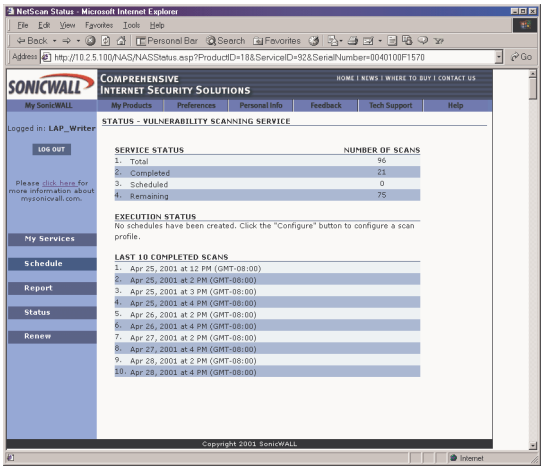
3. Locate the service **SonicWALL Vulnerability Scanning** and click **Activate**. The **Activation** screen is displayed.



4. To activate your subscription, enter the **Activation Key** located on the back of this manual and review the terms and conditions of the service. Check the **I have read and agreed to all of the terms and conditions mentioned above.** box, then click **Submit**. Your **Vulnerability Scanning Service** is now activated.

Status - Vulnerability Scanning Service

After the Vulnerability Scanning Service is activated, the following screen appears.



The Navigation Bar

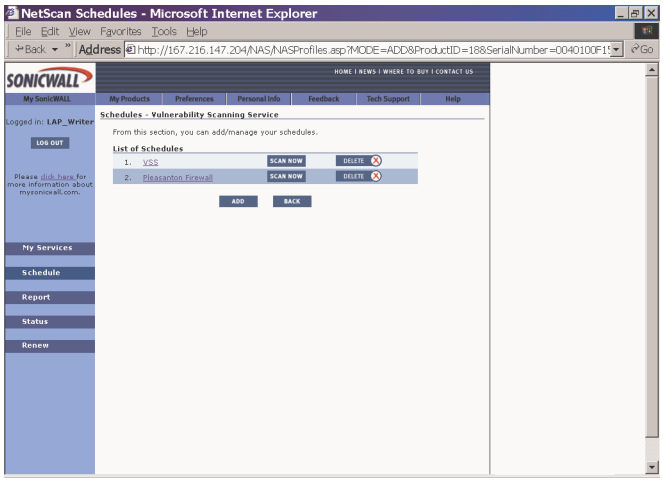
The Navigation bar located on the left side of the window allows you to perform the following functions:

- **My Services** - **My Services** allows you to display another service for your Internet security appliance.
- **Schedule** - **Schedule** displays your list of **Profile Names** and you can add additional profiles in this view.
- **Report** - **Report** displays the **Vulnerability Scan Report** list for your **Profile Names**.
- **Status** - Selecting **Status** displays the **Service Status**, **Execution Status**, and the last 10 completed scans of your network.
- **Renew** - To renew your scanning service, click **Renew** and type in your Activation key.

Creating Scanning Profiles

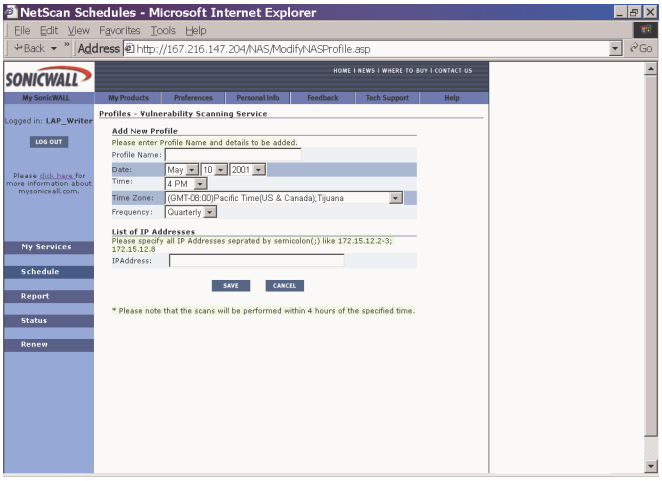
1. Log into **http://www.mysonicwall.com** using your username and password. Click on the product name on which you have activated the Vulnerability Scanning Service.

2. Click on **Vulnerability Scanning Service**. The **Status** screen is displayed in the browser window. Click **Schedule** to begin scheduling IP addresses for vulnerability scanning. The following screen is displayed:



3. This screen displays all profiles that have been previously configured. To add profiles to the **Schedules** section, click **Add** located in the navigation bar.

The **Add a New Profile** screen is displayed as shown below:



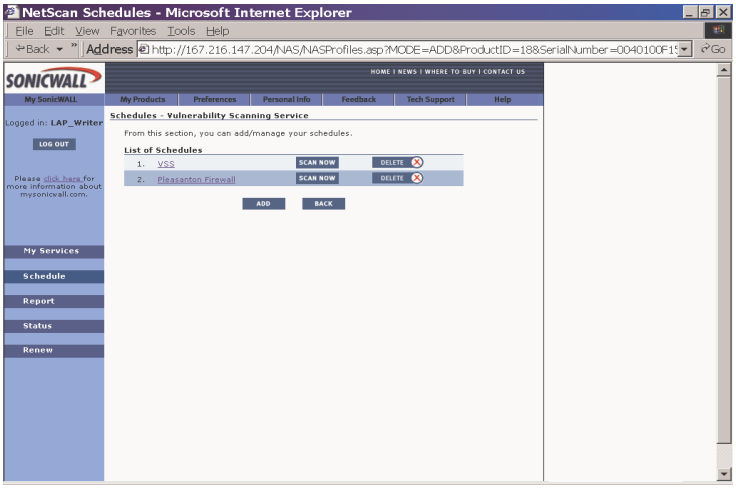
4. Create a name for the profile such as “Server Group”, “Remote Server Group”, “San Francisco Network”, by typing the name into the **Profile Name** box.
5. Select the date of the first scan for this profile using the **Date** menu boxes.
6. Select the time of the scan using the **Time** and **Time Zone** menus.
7. Select the **Frequency** of scanning for this profile.
8. Enter one or more IP addresses in the **IP Address** field. IP addresses can be added as a single address, a group of addresses, or as a range of addresses. Groups of IP addresses must have semi-colons separating the addresses. For instance, a group of addresses can be entered as follows: 172.172.172.2;172.172.172.100. Or, 172.172.172.2-6;172.172.172.100.

   Note: *The IP address to be scanned must be a public, routable address for the scanning service to be able to scan for vulnerabilities.Private addresses such as 192.168.168.168 and 10.0.0.1 should not be entered in a profile for scanning.*
9. Click **Save** to store the profile or click **Cancel** to discard the profile.

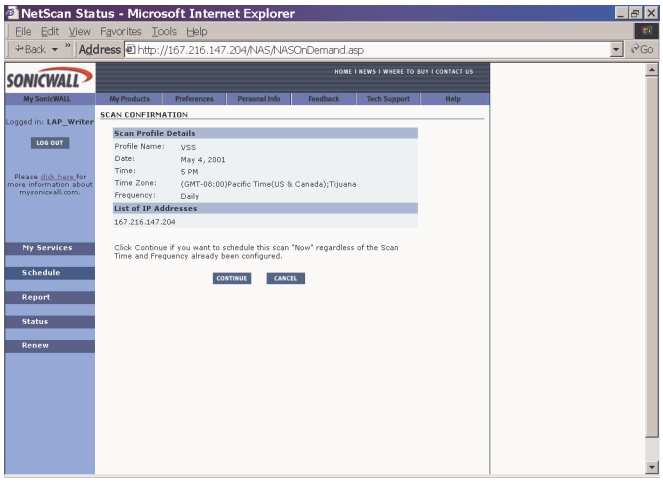
Scheduled Vulnerability Scanning Service Notification

From the **Profile Summary** screen, you can submit a profile for a vulnerability scan at anytime by clicking **Scan Now**.

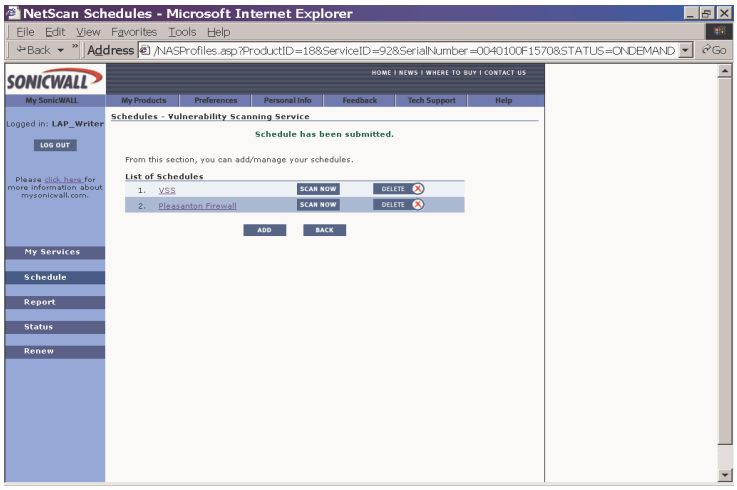
> ***Note**: You can also click on the **Profile Name** and select **Scan Now** from **Modify Profile** screen.*



After clicking **Scan Now**, a confirmation screen is displayed. Click **Continue** to submit the **Scan Profile**.



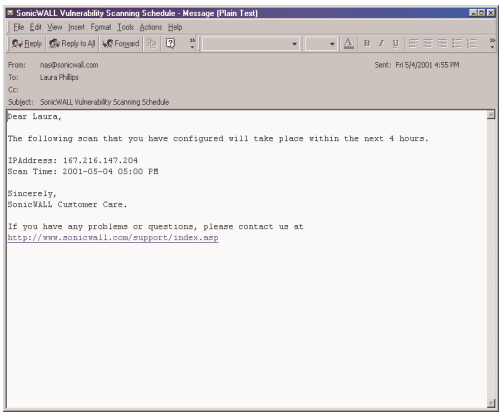
The **Scan Profile** is submitted for scanning and the following screen is displayed.

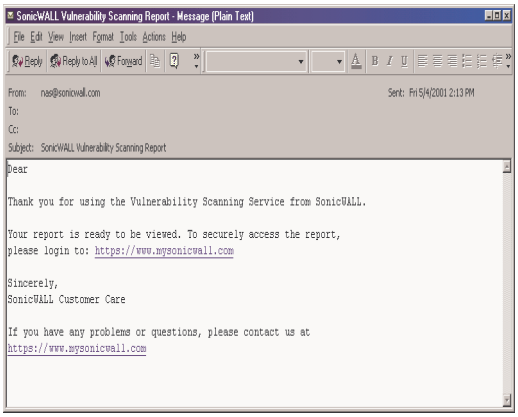


The **Vulnerability Scanning Service** scans the IP address within the next four hours and notifies you when your scan report is ready. After a scan profile is submitted for execution, using either **Scan Now** or a scheduled scan, an e-mail message is generated for the following events:

- A vulnerability scan is pending
- A vulnerability scan is completed.

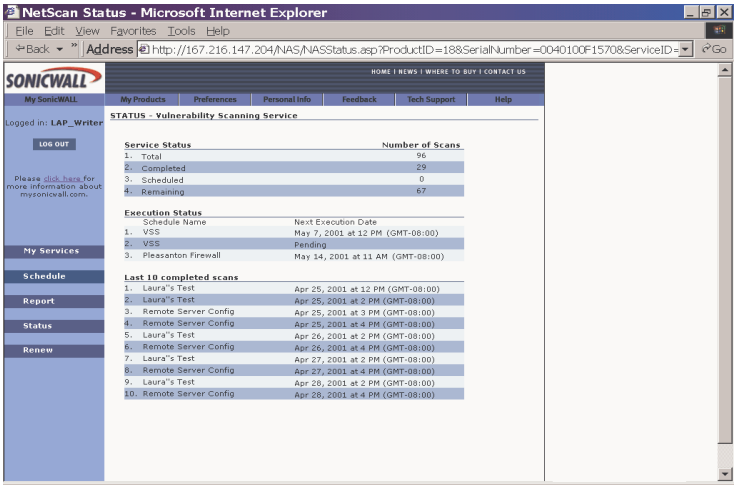
Samples of the e-mail messages are shown below.




SonicWALL Vulnerability Scanning Report - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward
From: nas@sonicwall.com
Sent: Fri 5/4/2001 2:13 PM
To:
Cc:
Subject: SonicWALL Vulnerability Scanning Report
Dear
Thank you for using the Vulnerability Scanning Service from SonicWALL.
Your report is ready to be viewed. To securely access the report,
please login to: https://www.mysonicwall.com
Sincerely,
SonicWALL Customer Care
If you have any problems or questions, please contact us at
https://www.mysonicwall.com

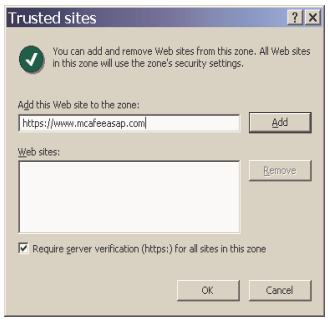
Viewing Vulnerability Scanning Service Reports

To view scan reports, log back into www.mysonicwall.com and view the **Status** page again. The **Status** window is displayed below:



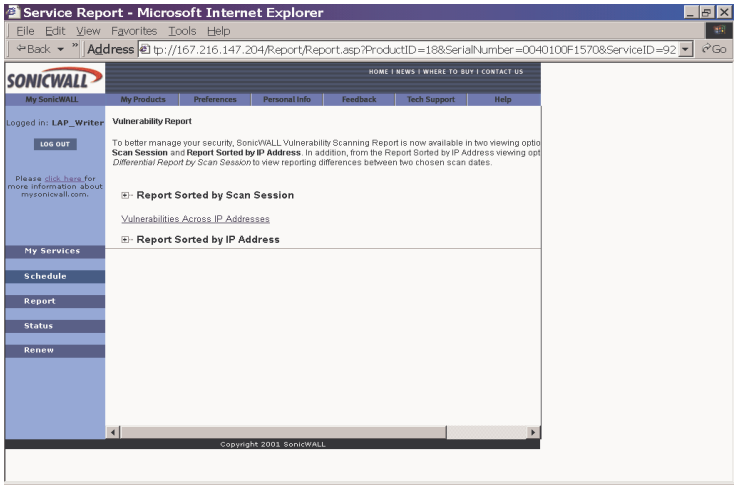
Microsoft® Internet Explorer 5.x is recommended for viewing your Service Reports. If you are using IE 6.0 as a web browser, you must configure it appropriately using the following steps:

1. Open IE 6.0, and select **Tools** from the menu bar, and then select **Internet Options**.
2. Select the **Security** tab, and click the **Trusted Sites** icon. Click the **Sites...** button.
3. Type the URL https://www.mcafeeasap.com into the **Add this Web site to the zone:** field. Click **Add**, and then **OK**.



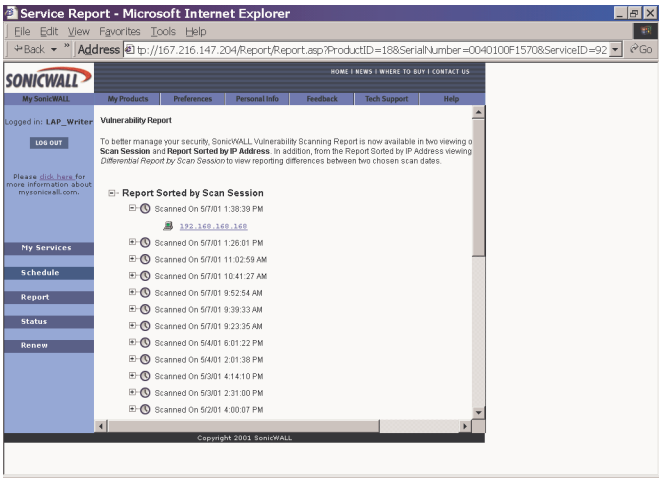
If you continue to experience problems with your Vulnerability Scanning Service, contact SonicWALL tech support at http://techsupport.sonicwall.com/vsstech.html.

Click **Report** in the navigation bar of the **Vulnerability Assessment Service** window. A **Report** screen appears with the three types of reports: by **Report Sorted by Scan Sessions**, **Vulnerabilities Across IP Addresses,** and **Report Sorted by IP Address.**

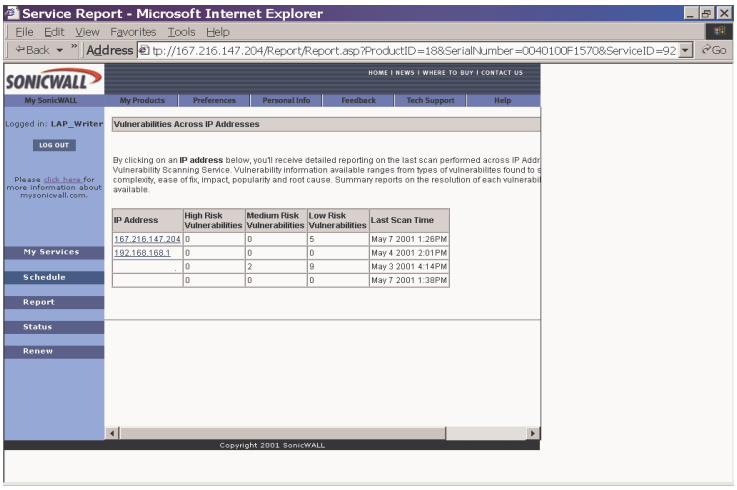


Reports Sorted by Scan Sessions

Reports Sorted by Scan Sessions lists the vulnerability scans by the date an IP address is scanned. To view a report, click on the **Scan Session** to be reviewed and then the IP address of the computer.

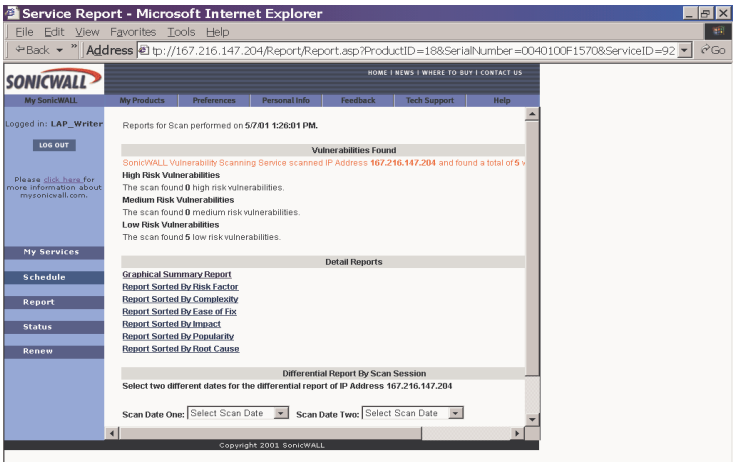


Reports can be viewed as **Vulnerabilities Across IP Addresses**. The report lists the IP address scanned, vulnerabilities according to High, Medium, or Low Risks, and the date of the last scan. An example report is displayed below:



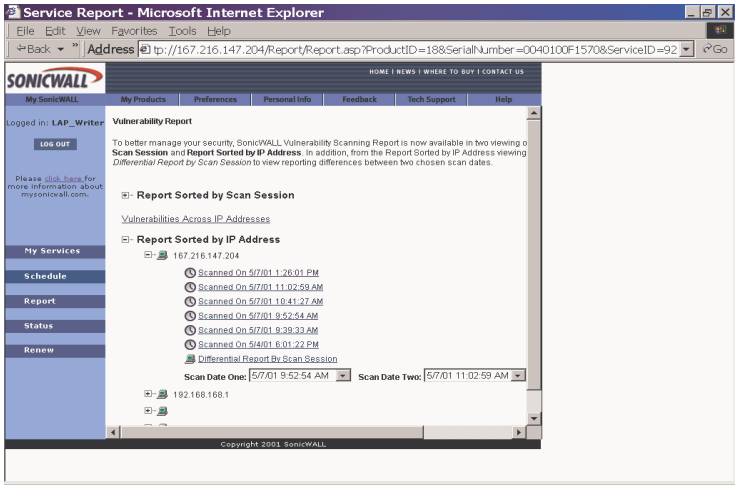
Reports Sorted By IP Address

By selecting one of the IP addresses in the IP Address list, you can view a vulnerability report for that IP address. Select an IP address to display the report.



Differential Report by Scan Session

You may also view Vulnerability Reports by choosing separate scan sessions to compare data. By selecting a range of dates, the report displays any new vulnerabilities that may result from any network administration, maintenance, or upgrades over a period of time. After selecting a range of dates, click **Differential Report by Scan Session** to review the report.

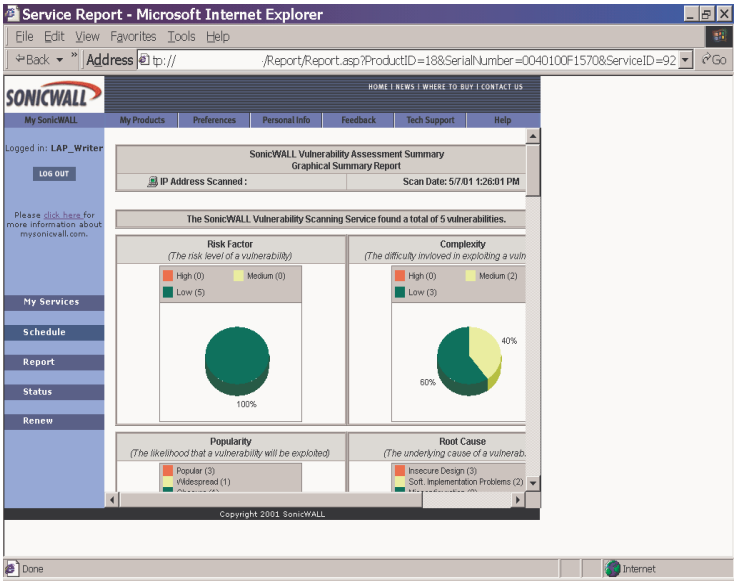


Vulnerability Report Output

If vulnerabilities are found by **SonicWALL Vulnerability Scanning Service**, a report is generated with the number vulnerabilities and the risk level of each vulnerability.The **Vulnerability Report** also lists several ways of viewing the report in detail:

- **Graphical Summary Report**
- **Report Sorted by Risk Factor**
- **Report Sorted by Complexity**
- **Report Sorted by Ease of Fix**
- **Report Sorted by Impact**
- **Report Sorted by Popularity**
- **Report Sorted by Root Cause**

A sample **Vulnerability Report** is show below:



Graphical Summary Report

The **Graphical Summary Report** displays the number of vulnerabilities found during an IP address scan in a graphical format.

Report Sorted By Risk Factor

The risk levels of vulnerabilities are sorted by **Low**, **Medium**, and **High Risk**.

Report Sorted by Complexity

Complexity describes the difficulty involved of exploiting a vulnerability.Some attacks against computer systems are more complicated than others; exploiting a vulnerability in a WWW CGI program may involve merely inserting a “magic” character in a form field, while other attacks may require a carefully coordinated series of interactions with obscure network services. Unfortunately, the complexity of an attack has more of an effect on the likelihood of it being defended, rather than the likelihood of an attacker using it as the attacker is probably wielding an arsenal of complex attacks to leverage against a computer system. Ironically, complex attacks are the most popular with hackers.

The **Vulnerability Scanning Service Report** sorts vulnerabilities by **Low**, **Medium**, and **High Complexity**. Each category is explained in the report.

Report Sorted by Ease of Fix

Ease of Fix describes the simplicity of a vulnerability fix. When faced with a large number of serious vulnerabilities, it is important that security problems be solved as efficiently as possible. Because some problems are easier to solve than others, quickly addressing the easy problems first may rapidly increase the security of a vulnerable system. Other fixes may pose the risk of disrupting services and require careful scheduling to resolve.

The report is sorted by the following categories: **Trivial**, **Simple**, **Moderate**, **Difficult**, and **Infeasible**. Each category is explained in the report.

Report Sorted by Impact

Impact describes the specific threat posed by a vulnerability. A security problem in a computer system can pose many different risks. Some problems are more serious than others. While all problems should be considered in an audit, it is more important that the most serious and far-reaching vulnerabilities be addressed before the minor ones. SonicWALL Vulnerability Scanning Service breaks down the implications of a vulnerability into several different categories. Each category represents an aspect of a computer system threatened by a security vulnerability.

The report is sorted by these categories: **System Integrity**, **Confidentiality, Availability, Accountability, Authorization, Data Integrity,** and **Intelligence**.

Report Sorted by Popularity

Popularity describes the likelihood that a vulnerability can be exploited. It is important to understand that all attackers are not equally capable. The presence of vulnerabilities is not a strong indicator that a system has been compromised. However, the presence of well-known, widely exploited problems may be cause for immediate concern.

The report is sorted by these categories: **Obscure, Widespread,** and **Popular.**

Report Sorted by Root Cause

Root Cause describes the underlying cause of vulnerability. Many security problems can be avoided, proactively, by maintaining security awareness in the planning and design stages of network engineering. Others may be the result of poor operational practice such as a lack of focus on network security. Identifying the root cause of vulnerabilities in a network allows patterns of vulnerability to be identified.

The report is sorted by these categories: **Misconfiguration, Software Implementation Problems,** and **Insecure Design.**

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 # 232-000130-00
Rev B 6/01