

SONICWALL

Vulnerability Scanning Service



Public Web, E-mail and FTP servers provide an important link for many organizations to the outside world, but they also make an inviting target for hackers. While firewalls protect a company's private network from intruders, there are other risks faced by companies. Server operating system and application software vulnerabilities are routinely discovered and network perimeter devices, such as routers and gateways, are also potential points of attack. These security "holes" expose an organization to network downtime, stolen, altered, or destroyed confidential information, and financial losses.

SonicWALL Vulnerability Scanning Service offers:

- *Comprehensive assessment of vulnerabilities*
- *Performs scheduled and on-demand scans*
- *Simple Web-based management*

SonicWALL Vulnerability Scanning Service is an automated, subscription-based vulnerability assessment service that provides a "hacker's eye view" of a network perimeter, including public servers, routers and gateways, and remote ends of VPN connections. This service integrates with SonicWALL's industry leading Internet security appliances.

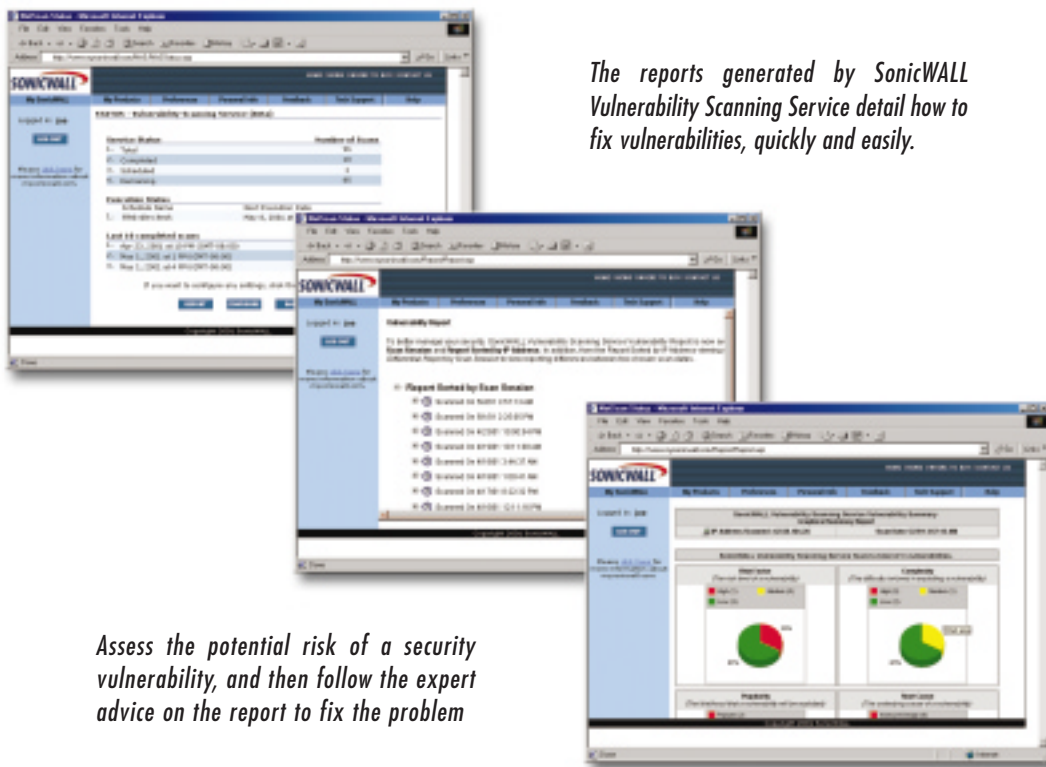
SonicWALL Vulnerability Scanning Service examines a network perimeter for weaknesses on an ongoing basis and provides administrators with in-depth guidance on how to address the risks to eliminate opportunities for hackers. Vulnerability scans

can be scheduled on a regular basis, such as once per month, as well as run on demand when policies are changed or new equipment is deployed. SonicWALL Vulnerability Scanning Service is easy to configure and run using SonicWall's integrated, Web-based security portal at www.mysonicwall.com.

SonicWALL Vulnerability Scanning Service enhances the comprehensive protection available to network administrators in one easy to manage, integrated security solution that reduces management headaches and delivers peace of mind.

SonicWALL Vulnerability Scanning Service Features and Benefits

- **Comprehensive Vulnerability Assessment.** SonicWALL Vulnerability Scanning 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.** Administrators can easily schedule scans and configure the service using your own Web-based security portal at www.mysonicwall.com. There is no software to install
- **Flexible Reporting Options.** Reports can be sorted by risk level and other criteria to allow administrators to prioritize which vulnerabilities to address first
- **Customizable Scheduling.** Administrators can schedule periodic or on-demand vulnerability scans
- **State-of-the-Art Updates.** Security updates for SonicWALL Vulnerability Scanning Service security are backed by NAI (Network Associates) Labs, the world leader in advanced security technology
- **Assured Security.** This service delivers peace of mind for network administrators that their public servers are being checked for security vulnerabilities on an ongoing basis
- **Instant Expertise.** SonicWALL Vulnerability Scanning Service provides expert remedies to fix detected security vulnerabilities



The reports generated by SonicWALL Vulnerability Scanning Service detail how to fix vulnerabilities, quickly and easily.

Assess the potential risk of a security vulnerability, and then follow the expert advice on the report to fix the problem

SonicWALL Vulnerability Scanning Service Part Numbers

01-SSC-2840 SonicWALL Vulnerability Scanning Service(Small Business Pack) 1 scan/quarter; 4 on-demand scans; 1 IP address

01-SSC-2841 SonicWALL Vulnerability Scanning Service(Enterprise Pack) 1 scan/month; 4 on-demand scans; up to 6 IP addresses

01-SSC-2842 SonicWALL Vulnerability Scanning Service(Distributed Enterprise Pack) 1 scan/month; 4 on-demand scans; up to 25 IP addresses

© 2001 SonicWALL, Inc. 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.