

Executive brief: When it comes to security, protection and performance matter

Five things your next-generation firewall must do



Introduction

These days, cybercrime is big business. All types of data are being traded, whether it is medical information, credit card information, or the secret designs of your new product, app, or service.

Malware is becoming more sophisticated and today it's commonly hidden inside a larger file, or encrypted so a firewall device can't decrypt it. Meanwhile, the price of cyber-hacking tools is going down, so denial of service attacks, eavesdropping software, and Wi-Fi interception devices are less expensive and more readily available.

Given the maturity and sophistication of malware, businesses of every size and industry are at risk. At the same time, firewalls are becoming more mature and sophisticated, and are better integrated into the network, going beyond security to help improve network efficiency. A high-performing firewall can protect against advanced attacks, as well as control traffic on your network. However, the firewall you had last year probably isn't going to guard you from this year's threats. A firewall has

to protect more than assets — it also has to protect people, networks and productivity, and it has to give you granular controls into complex applications.

1. Protect assets and people

Firewalls were originally designed only to secure assets, but modern threats are so much more sophisticated that your firewall must now extend to protecting both assets and people. By functioning as a management hub for people and applications, next-generation firewalls (NGFWs) now allow you to get the type of network performance employees need, so you can get the level of security the business requires. A smoothly running network is one that has blocked spam, which can consume network resources, and restricts non-productive bandwidth-consuming activities such as video downloads.

2. Protect networks

It's easy to have a false sense of security once you install a firewall or cyber-protection program, but too many businesses

Given the maturity and sophistication of malware, businesses of every size and industry are at risk.

have learned the hard way that just owning the software isn't enough. Effective network security requires you to enable all program functions, including antivirus detection, intrusion prevention, and content filtering. Firewalls must be able to analyze entire files, including encrypted files and large file sizes. Finally, after the firewall is installed, it's critical that you test it regularly.

3. Protect productivity

NGFWs feature aggressive countermeasures and high-speed performance. This reduces risks, management complexity, and costs, through automated, dynamic security measures that are optimized to protect network performance.

4. Provide granular controls

Firewall control must also be granular enough to manage application functions

without disrupting productivity. Firewall zones should also allow you to isolate groups to minimize data leaks or breaches.

5. Provide scalability and performance

Traditional firewalls often lack the scalability and power to deliver comprehensive protection or the granular control required to keep your organization safe in today's complex, and potentially hostile, IT environment.

Regardless of the size of your business or type of industry, don't let an outdated firewall put your entire business at risk.

Learn more

SonicWall offers comprehensive, powerful, next-generation firewalls for organizations of any size. Read our white paper: "[How to prevent security breaches in your retail network.](#)"



© 2016 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING,

BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com