Deep Packet Inspection

Go beyond simple stateful inspection to ensure your network is protected

Introduction

Going far beyond simple stateful inspection, the SonicWall™ Reassembly-Free Deep Packet Inspection™ (RFDPI) engine scans against multiple application types and protocols to ensure your network is protected from internal and external attacks as well as application vulnerabilities. Unlike other scanning engines, the RFDPI engine is not limited by file size or the amount of concurrent traffic it can scan, making our solutions second to none. By working at the application layer, RFDPI protects against hidden application vulnerabilities that may be inadvertently letting attackers in through an unknown back door.

Simple, secure and cost-effective

The patented RFDPI engine is at the heart of every SonicWall network security solution. This patented technology unifies multiple security functions into a single integrated suite that inspects all files from local, remote and mobile users. This gives network administrators the ability to manage network security simply and cost-effectively. RFDPI increases productivity by allowing IT to create reusable and adaptive policy control. More than simply a security approach, RFDPI incorporates object-based contextual controls over user identity and access, application identity and access, data leakage, network optimization and granular reporting, auditing and forensics.

Controlling applications in the organization

It can be a real challenge for IT administrators to efficiently deliver critical corporate solutions while also contending with employee use of wasteful and often dangerous applications. Critical applications need bandwidth prioritization while social media and gaming applications need to be bandwidth throttled or completely blocked. Stateful packet inspection

Ensure your network is protected from internal and external attacks as well as application vulnerabilities.

firewalls used in many organizations rely on port and protocol; they cannot solve the problem because they are not able to identify applications.

SonicWall's Reassembly-Free Deep Packet Inspection engine examines all downloaded, emailed and compressed files at the application layer to protect against the more sophisticated attacks that target application vulnerabilities. Scanning every byte of every packet of all network traffic, SonicWall provides complete application identification and control, regardless of port or protocol, by determining exactly what applications are being used and who is using them. Administrators can easily create bandwidth management policies based on logical pre-defined categories (such as social media or gaming), individual applications, or even users and groups. SonicWall puts the power back in the hands of IT administrators.

Protection against both internal and external attacks

Deep packet inspection scans multiple application types and covers many protocols, including SMTP, POP3, IMAP, FTP, HTTP and NetBIOS. It also scans all network layers. As a result, your network is protected from both internal and external threats.

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