Deep Packet Inspection
Go beyond simple stateful inspection to ensure your network is protected

Introduction
Going far beyond simple stateful inspection, the Dell™ 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 Dell 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.
Ensure your network is protected from internal and external attacks as well as application vulnerabilities.

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

Dell 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, Dell 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. Dell 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.
For More Information
© 2014 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. (“Dell”).

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. 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 Dell 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 Dell products. EXCEPT AS SET FORTH IN DELL’S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES 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 DELL 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 DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes 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. Dell does not make any commitment to update the information contained in this document.

About Dell Software
Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

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

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.