



SonicWALL Application Intelligence and Control

FIREWALL

Granular application control, intelligence and real-time visualization

- **Application intelligence**
- **Application control**
- **Application visualization**
- **Data leakage prevention**
- **Application-level bandwidth management**
- **Automated signature updates**
- **Deep packet inspection for SSL traffic**

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. Boiling it down, stateful packet inspection firewalls cannot sort out the good from the bad.

Scanning every byte of every packet of all network traffic, SonicWALL® provides complete application intelligence and control, regardless of port or protocol, by determining exactly what applications are being used and who is using them. SonicWALL Next-Generation Firewalls leverage a continuously expanding threat signature database that currently recognizes over 3,000 applications and detects millions of pieces of malware to protect the network automatically and seamlessly. The solution detects and eliminates malware, intrusions, data leakage and policy violations before they cause harm to a company's network or its users.

SonicWALL Application Intelligence and Control puts power back into the hands of IT administrators with new levels of management and ease-of-use, allowing them to maintain granular control of applications and users. 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. As new applications are created, new signatures are pushed to the firewalls and the appropriate policies are automatically updated without IT spending costly time and effort to update rules and application objects. Administrators must also be able to visualize application traffic to properly control network use and to adjust network policy based on critical observations. The SonicWALL Application Flow Monitor provides real-time graphs of application activity allowing administrators to modify policies to increase network productivity.

Application intelligence and control is available along with SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention as a one, two or three year subscription, or is included in SonicWALL Comprehensive Gateway Security Suite subscriptions for the TZ 210, NSA and E-Class NSA Series firewalls.

Features and Benefits

Application intelligence leverages SonicWALL's Reassembly-Free Deep Packet Inspection™ to scan every packet to identify applications in use and who is using them. SonicWALL maintains a signature database to protect networks automatically and seamlessly.

Application control enables flexible, configurable application policies to throttle or block applications and files, URLs, and email attachments based upon application type, network user, schedules, custom signatures, and more.

Application visualization provides real-time graphs of applications, ingress and egress bandwidth consumed, users, currently visited Web sites and more. In addition, it is possible export the same data to any NetFlow/IPFIX analyzer for offline monitoring, troubleshooting and diagnostics of historical network activity.

Data leakage prevention blocks and controls transmission of sensitive, data via FTP uploads, or as attachments to personal Web mail services such as Hotmail® or Gmail®, as well as corporate SMTP and POP3 email.

Application-level bandwidth management ensures Quality of Service (QoS) by dedicating throughput for mission-critical applications or groups at specific times of the day.

Automated signature updates ease administration by ensuring that the network is protected against the latest threats.

Deep Packet Inspection for SSL traffic extends protection to the SSL encrypted traffic, enabling enhanced compliance, content filtering, data leak prevention and can eliminate another vector for malware. Encrypted traffic is decrypted, inspected and re-encrypted transparently to the user and can be configured for both inbound and outbound connections.*

* DPI SSL Upgrade Licenses available for NSA 240 and above.



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Application Intelligence, Control and Visualization

Identify

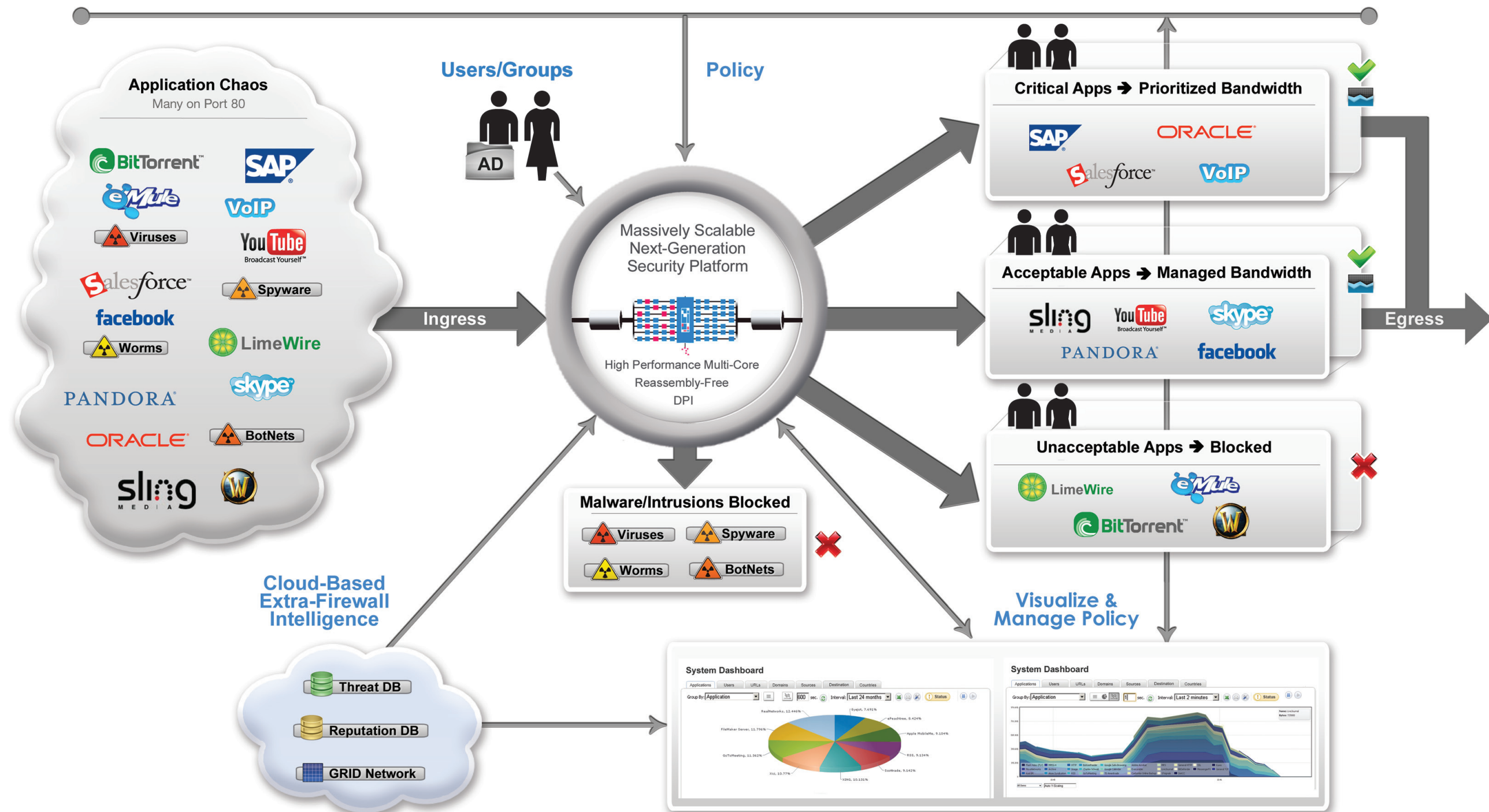
- By Application
 - Not by Port and Protocol
- By User/Group
 - Not by IP
- By Content Inspection
 - Not by Filename

Categorize

- By Application
- By Application Category
- By Destination
- By Content
- By User/Group

Control

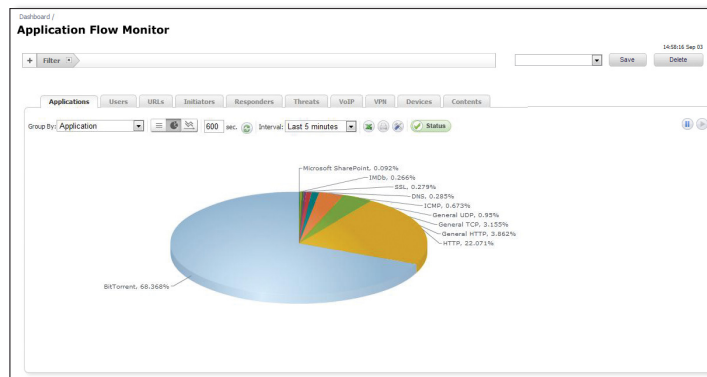
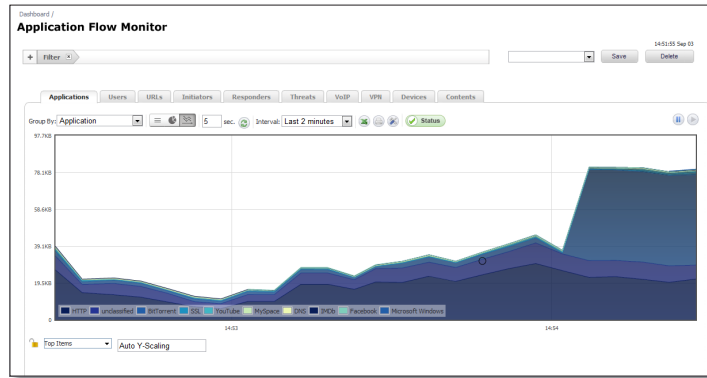
- Prioritize Applications by Policy
- Manage Applications by Policy
- Block Applications by Policy
- Detect and Block Malware
- Detect and Prevent Intrusion Attempts



Specifications

Application Visualization

Real-time graphs of applications, ingress and egress bandwidth, Web sites visited and all user activity enables administrators to modify application rules to conform to network policies.



Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service

NSA E7500 (1-year)
01-SSC-6130

NSA E6500 (1-year)
01-SSC-6131

NSA E5500 (1-year)
01-SSC-6132

NSA 5000 (1-year)
01-SSC-6159

NSA 4500 (1-year)
01-SSC-6133

NSA 3500 (1-year)
01-SSC-6134

NSA 2400 (1-year)
01-SSC-6135

NSA 240 Series (1-year)
01-SSC-6162

TZ 210 Series (1-year)
01-SSC-6165

Multi-year Subscription Services are available. To access SKUs for the complete line of SonicWALL network security appliances, please visit www.sonicwall.com.

Feature List

Application Intelligence Capabilities

- Scans and identifies all traffic independently of ports or protocols for complete control
- Data leakage functionality with user defined content to monitor
- Application-level bandwidth management provided by a rich and constantly expanding application signature database and powerful rule creation
- Predefined and custom actions such as Bandwidth Manage, Log, Log and Block, Custom User Messages, Bypass DPI
- Deep Packet Inspection of traffic tunneling over SSL encrypted protocols

Signature Database

- Dynamically-updated database containing thousands of application and content-based signatures

Logging and Reporting

- Real-time logging and alerting
- Granular reports through SonicWALL ViewPoint and Global Management System
- Netflow/IPFIX with Extensions logging for additional off-the-box traffic analysis and visualization

Scalability

- Able to scan large numbers of concurrent downloads of unlimited file size

For more information on SonicWALL's suite of value-added security services including Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Application Intelligence and Control, Comprehensive Anti-Spam Service, Enforced Client Anti-Virus and Anti-Spyware and Content Filtering Service, please visit our Web site at <http://www.sonicwall.com>.

SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY	SECURE REMOTE ACCESS	WEB AND E-MAIL SECURITY	BACKUP AND RECOVERY	POLICY AND MANAGEMENT



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™