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

Built upon SonicWALL’s patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology* and multi-core architecture, the SonicWALL® E-Class Network Security Appliance (NSA) Series provides high-performance Next-Generation Firewall protection and advanced application control for the most demanding networks. Combining application intelligence, control and visualization with multiple layers of network security technology, advanced bandwidth management and a suite of high availability features, the E-Class NSA E7500, E6500 and E5500 appliances offer a broad range of scalable solutions for enterprise deployments in data centers, campus networks and distributed environments.

The E-Class NSA Series is a key part of SonicWALL’s portfolio of enterprise-class products and services for network security, email security and secure remote access. All E-Class solutions offer outstanding protection and performance, while delivering intelligence, elegant simplicity and unparalleled value. SonicWALL’s E-Class delivers the high-performance protection required by enterprise-class networks in a solution that is engineered to drive the cost and complexity out of running a secure network.

**Features and Benefits**

- **Next-Generation Firewall**
- **Powerful intrusion prevention**
- **Application intelligence, control and visualization**
- **Reassembly-Free Deep Packet Inspection technology**
- **Flexible deployment**
- **Deep Packet Inspection of SSL-encrypted traffic (DPI SSL)**
- **SonicWALL Global Response Intelligent Defense (GRID) Network**

SonicWALL’s Next-Generation Firewall including Reassembly-Free Deep Packet Inspection™ (RFDPI) tightly integrates intrusion prevention, malware protection, and newly enhanced application intelligence and control with real-time visualization.

Powerful intrusion prevention protects against a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities, application exploits, and other malicious code.

Application intelligence, control and visualization provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity.

Reassembly-Free Deep Packet Inspection technology provides control for over 2,800 applications and detects millions of pieces of malware to protect the network automatically and seamlessly, while inspecting hundreds of thousands of connections simultaneously across all ports, with near zero latency and unlimited stream size.

Flexible deployment as either a traditional gateway or an inline solution allows administrators to keep their existing network infrastructure, while adding application intelligence and control as an extra layer of security and visibility.

Deep Packet Inspection of SSL-encrypted traffic (DPI SSL) transparently decrypts and scans both inbound and outbound HTTPS traffic using SonicWALL RFDPI. The traffic is then re-encrypted and sent to its original destination if no threats or vulnerabilities are discovered.

The SonicWALL Global Response Intelligent Defense (GRID) Network continually updates threat protection, intrusion detection and prevention and application control services on a 24x7 basis to maximize security. The full suite of threat prevention services can defend against over a million unique malware attacks.

* U.S. Patent 7,310,815 – A method and apparatus for data stream analysis and blocking.
SonicWALL Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. An integrated feature of SonicWALL Next-Generation Firewalls, it uses Reassembly-Free Deep Packet Inspection technology to identify and control applications in use, regardless of port or protocol. With a continuously expanding threat signature database that currently recognizes over 2,800 applications and millions of malware threats, it can maintain granular control over applications, prioritize or throttle bandwidth and deny Web site access. Application Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active Website connections and user activity, and can continuously send data to NetFlow/IPFIX analyzers.

**Reassembly-Free Deep Packet Inspection Engine**

The SonicWALL Reassembly-Free Deep Packet Inspection engine delivers a scalable application inspection engine that can analyze files and content of any size in real-time without reassembling packets or application content. This means of inspection is designed specifically for real-time applications and latency sensitive traffic, delivering control without having to proxy connections. Using this engine design, high-speed network traffic is inspected more efficiently and reliably for an improved end user experience.

**Central-site Gateway**

Deployed as a central-site gateway, the E-Class NSA Series provides a high-speed scalable platform, providing network segmentation and security using VLANs and security zones. Redundancy features include WAN Load balancing, ISP failover and Active/Active DPI.

**Layer 2 Bridge Mode**

Layer 2 bridge mode provides inline intrusion detection and prevention, adds an additional level of zone-based security to network segments or business units and simplifies layered security. Additionally, this enables administrators to limit access to sensitive data by specific business unit or database server.
Remote Site Protection
The E-Class NSA Series incorporates ultra-high performance Virtual Private Networks (VPNs) that easily scale to thousands of endpoints and branch offices. Innovative SonicWALL Clean VPN™ technology prevents vulnerabilities and malicious code by decontaminating traffic before it enters the corporate network, in real-time and without user intervention.

Gateway Protection
Easily integrated into existing environments, E-Class NSAs centralize gateway-level protection across all incoming and outgoing applications, files and content-based traffic, while controlling bandwidth and applications, without significantly impacting performance or scalability.

Internal Protection
The highly-configurable E-Class NSA Series extends protection over the internal network by inspecting traffic over LAN interfaces and VLANs. Specifically designed for LAN network threats, the E-Class NSA Series monitors and responds to internally spreading malware, denial of service attacks, exploited software vulnerabilities, confidential documents, policy violations and network misuse.

Desktop and Server Protection
In addition to network and gateway based protection, the E-Class NSA Series provides additional endpoint protection for workstations and servers through an enforced anti-virus and anti-spyware client with advanced heuristics. This enforced client solution delivers network access control by restricting Internet access on endpoints that do not have the latest signature or engine updates. When enforcement is enabled on the appliance, each endpoint is directed to download the enforced anti-virus and anti-spyware client without any administrator intervention, automating the deployment of endpoint security.

Subscription Services
Each E-Class Network Security Appliance supports an expanding array of dynamic subscription-based services and software designed to integrate seamlessly into any network.

Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service delivers intelligent, real-time network security protection against sophisticated application layer and content-based attacks including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows. Application Intelligence and Control provides real-time visualization of network traffic, customizable policies and highly granular control over applications and users.

Enforced Client Anti-Virus and Anti-Spyware delivers comprehensive virus and spyware protection for laptops, desktops and servers using a single integrated client and offers automated network-wide enforcement of anti-virus and anti-spyware policies, definitions and software updates.

Content Filtering Service enforces protection and productivity policies by employing an innovative rating architecture, utilizing a dynamic database to block over 56 categories of objectionable Web content.

Centralized Policy Management
The SonicWALL Global Management System (GMS®) provides flexible, powerful and intuitive tools to centrally manage E-Class NSA configurations across distributed enterprises, view real-time monitoring metrics and integrate policy and compliance reporting.

ViewPoint is an easy-to-use Web-based reporting tool that provides instant insight into network performance and security. Delivered through a series of historical reports using dashboards and detailed summaries, ViewPoint helps organizations of all sizes track Internet usage, fulfill regulatory compliance requirements and monitor the security status of their network.

E-Class Support 24x7 is designed specifically for E-Class customers, E-Class Support 24x7 delivers enterprise-class support features and quality of service. E-Class Support 24x7 includes direct access to a team of highly-trained senior support engineers for telephone and Web-based technical support on a 24x7x365 basis, software and firmware updates and upgrades, Advance Exchange hardware replacement, access to electronic support tools and moderated discussion groups, and more.

Deep Packet Inspection for of SSL-Encrypted Traffic (DPI SSL) transparently decrypts and scans both inbound and outbound HTTPS traffic using SonicWALL RFDPI. The traffic is then re-encrypted and sent to its original destination if no threats or vulnerabilities are discovered.
### SonicWALL NSA E5500

- **SonicWALL NSA E5500**
  - 01-SSC-7008
- **SonicWALL NSA E6500 TotalSecure**
  - 01-SSC-7028

### SonicWALL NSA E7500

- **SonicWALL NSA E7500**
  - 01-SSC-7029

### SonicWALL NSA E5500 Security Services

- **SonicWALL NSA E5500 Security Services**
  - SonicWall Content Filtering Service Premium Business Edition for NSA E5500 (1-year) 01-SSC-7033
  - SonicWall GAV / IPS / Application Intelligence for NSA E5500 (1-year) 01-SSC-7030
  - SonicWall Comprehensive Gateway Security Suite for NSA E5500 (1-year) 01-SSC-9220
  - SonicWall E-Class Support 24x7 for NSA E5500 (1-year) 01-SSC-7254

### SonicWALL NSA E6500 Security Services

- **SonicWALL NSA E6500 Security Services**
  - SonicWall Content Filtering Service Premium Business Edition for NSA E6500 (1-year) 01-SSC-7033
  - SonicWall GAV / IPS / Application Intelligence for NSA E6500 (1-year) 01-SSC-7030
  - SonicWall Comprehensive Gateway Security Suite for NSA E6500 (1-year) 01-SSC-9220
  - SonicWall E-Class Support 24x7 for NSA E6500 (1-year) 01-SSC-7254

### SonicWALL NSA E7500 Security Services

- **SonicWALL NSA E7500 Security Services**
  - SonicWall Content Filtering Service Premium Business Edition for NSA E7500 (1-year) 01-SSC-7033
  - SonicWall GAV / IPS / Application Intelligence for NSA E7500 (1-year) 01-SSC-7030
  - SonicWall Comprehensive Gateway Security Suite for NSA E7500 (1-year) 01-SSC-9220
  - SonicWall E-Class Support 24x7 for NSA E7500 (1-year) 01-SSC-7257

### Specifications

- **Firewall**
  - SonicOS Version: SonicOS Enhanced 5.6 (or Higher)
  - Stateful Throughput: 7.3 Gbps
  - Full DPI/Gateway AV Throughput: 3.3 Gbps
  - Global VPN Client Licenses (Maximum): 2,000
  - Bundled SSL VPN Licenses (Maximum): 2 (50)
  - Virtual Router Bundled (Maximum): 1 (25)
  - Encryption, Authentication/DH Groups: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1/DH Groups 1, 2, 5, 14
  - Application bandwidth management and control, prioritize or block application traffic
  - HTTP URL, HTTPS IP, keyword and content scanning
  - ActiveX, Java Applet, and Cookie blocking
  - unrestricted

- **Management and Configuration**
  - Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit/64 bit, Windows 7
  - Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware and Application Intelligence
  - Comprehensive Anti-Spam Service
  - SonicWALL Comprehensive Gateway Security Suite for NSA E5500 (1-year)
  - SonicWALL E-Class Support 24x7 for NSA E5500 (1-year)
  - SonicWALL E-Class Support 24x7 for NSA E6500 (1-year)
  - SonicWALL E-Class Support 24x7 for NSA E7500 (1-year)
  - SonicWALL NSA E5500 TotalSecure (1-year) 01-SSC-7029
  - SonicWALL NSA E6500 TotalSecure (1-year) 01-SSC-7028
  - SonicWALL NSA E7500 TotalSecure (1-year) 01-SSC-7029

- **Technical Specifications**
  - 3DES/AES Throughput: 1.7 Gbps, 2 Gbps, 3 Gbps
  - Site-to-Site VPN Tunnels: 4,000, 6,000, 10,000
  - Bundled Global VPN Client Licenses (Maximum): 2,000 (4,000), 2,000 (6,000), 2,000 (10,000)
  - Bundled SSL VPN Licenses (Maximum): 2 (50), 7 (100), 2 (50)
  - Virtual Router Bundled (Maximum): 1 (25), 2 (50), 1 (25)
  - Encryption, Authentication/DH Groups: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1/DH Groups 1, 2, 5, 14
  - Key Exchange: IKE, ECX, ActiveKey, PKI (X.509), L2TP over IPSEC
  - Route-based VPN: 960 (6), 2,000 (4), 2,000 (6), 2,000 (10)
  - Certificate Gateway: VeriSign, Thawte, CyberTrust, RSA Net, Entrust, and Microsoft CA for SSL/WaysLab/SecureCard/VNL/VPNC/IGEP
  - Redundant VPN Gateway: Yes
  - SSL V PN Platforms Supported: Microsoft® Windows 2000, Windows XP (Microsoft® Vista 2.0 identity key, Microsoft 7)

- **Security Services**
  - Deep Packet Inspection Service: Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware and Application Intelligence
  - Content Filtering (CF): Premium Edition: HTTP URL, HTTPS, IP keyword and content scanning, ActiveX, Java Applet, and cookie blocking
  - Enforced Client Anti-Virus and Anti-Spyware: HTTP/HTTPS, SMRT DEF, LMA, and TIP, enforced Microsoft® Client Email attachment blocking
  - Comprehensive Anti-Spam Service
  - Application intelligence and control

- **Networking**
  - IP Address Assignment: Static, DHCP, PPPoE, L2TP, and PPTP client
  - NAT Modes: NAT, Mann, manym, manyman, flexible NAT (overlapping IPv4, IPv6, transparent mode)
  - Routing: OSPF, RIP, RIPv2, static routes, policy-based routing, Multicast
  - QoS: Bandwidth priority, maximum bandwidth, bandwidth limit, DSCP marking, RSVP (IP)
  - Authentication: RADIUS, Active Directory, SSL (LOAD balancer, internal user database, Terminal Services, Citrix
  - IPv4: Yes
  - Internal Database/Single Sign-on Users: 1,500/500 Users, 2,900/1,000 Users
  - VoIP: Full H.323, H.225, SIP gateways support, automatic bandwidth management through 3GPP, deep inspection security, full interoperability with most VoIP gateways and communications devices
  - Link Aggregation: Yes
  - Port Redundancy: Yes

- **System**
  - Management and Monitoring: Web GUI (HTTP, HTTPS), Command Line (SSH, Console), SNMP, Management with installation, secure IP, and control over SONICWALL NSX E-Class and ViewPoint Reporting
  - VoIP: Full H.323, H.225, SIP gateways support, automatic bandwidth management through 3GPP, deep inspection security, full interoperability with most VoIP gateways and communications devices
  - Link Aggregation: Yes
  - Port Redundancy: Yes

- **Hardware**
  - Interfaces: 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface, 2 USB
  - Flash Memory: 32 GB Compact Flash
  - 3G Wireless/Modem: With 3G Adapter Module
  - Power Supply: Single 200W AC Power Supplies, Single 290W AC, Hot Swappable
  - Fans: Dual Fans, Hot Swappable
  - Display: Front LCD Display
  - Power Consumption: 300-240V, 60-30Hz
  - Power Consumption: 208 V, 60 Hz
  - Total Heat Dissipation: 1.6 Gbps 1.26 Gbps
  - Maximum Full DPI Connections: 1.1 Gbps 2.7 Gbps
  - IPS Performance: 3.9 Gbps, 5 Gbps, 5.6 Gbps
  - Total Durable Connections: 1.1 Gbps 1.4 Gbps
  - 3DES/AES Throughput: 1.7 Gbps, 2 Gbps, 3 Gbps
  - Site-to-Site VPN Tunnels: 4,000, 6,000, 10,000
  - Bundled Global VPN Client Licenses (Maximum): 2,000 (4,000), 2,000 (6,000), 2,000 (10,000)
  - Bundled SSL VPN Licenses (Maximum): 2 (50), 7 (100), 2 (50)
  - Virtual Router Bundled (Maximum): 1 (25), 2 (50), 1 (25)
  - Encryption, Authentication/DH Groups: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1/DH Groups 1, 2, 5, 14
  - Key Exchange: IKE, ECX, ActiveKey, PKI (X.509), L2TP over IPSEC
  - Route-based VPN: 960 (6), 2,000 (4), 2,000 (6), 2,000 (10)
  - Certificate Gateway: VeriSign, Thawte, CyberTrust, RSA Net, Entrust, and Microsoft CA for SSL/WaysLab/SecureCard/VNL/VPNC/IGEP
  - Redundant VPN Gateway: Yes
  - SSL V PN Platforms Supported: Microsoft® Windows 2000, Windows XP (Microsoft® Vista 2.0 identity key, Microsoft 7)

- **SonicWALL’s line-up of dynamic security solutions**

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