# DELL SonicWALL

# *SonicWALL* NSA Series

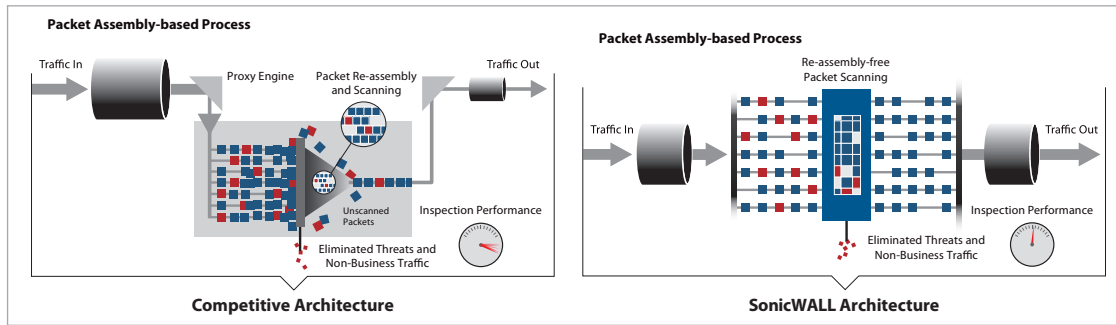| 뛰어난 확장성 | 강화된 성능 | 차세대 방화벽 |
|:---:|:---:|:---:|

## 확장성: 특허 기술 (RFDPI)

미국특허 *7,310,815 - A method and apparatus for data stream analysis and blocking.*
실시간과 지연에 민감한 어플리케이션들 및 트래픽에 대한 정밀검사

**Packet Assembly-based Process**

Traffic In — Proxy Engine — Packet Re-assembly and Scanning — Traffic Out

Unscanned Packets
Inspection Performance
Eliminated Threats and Non-Business Traffic

**Competitive Architecture**

**Packet Assembly-based Process**

Traffic In — Re-assembly-free Packet Scanning — Traffic Out

Inspection Performance
Eliminated Threats and Non-Business Traffic

**SonicWALL Architecture**

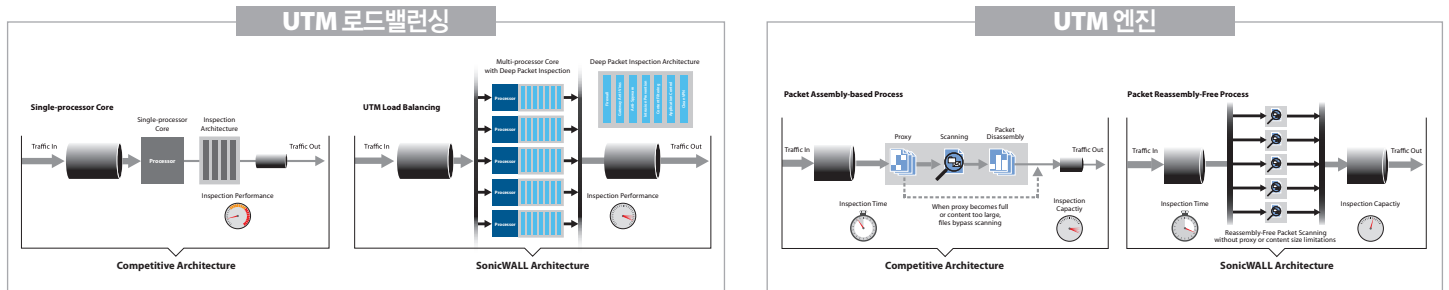### Re-Assembly Free Inspection

**Technology**
- 메모리에 데이터 복사없이 트래픽상의 파일 및 컨텐츠 검사
- 패킷 도착 순서에 관계없이 처리

**Benefit**
- 지연 감소
  – 실시간 스캐닝이 우수함
- 메모리 용량 부족에 의한 파일 크기 및 세션 제한이 없음.

## 강화된 성능 – "Multi-core"

차세대 멀티코어 기술 : 입력되는 네트워크 트래픽은 할당된 보안 멀티 코어 프로세서에 의해서 부하가 분산됨

**UTM 로드밸런싱**

Single-processor Core
Traffic In — Single-processor Core — Processor — Inspection Architecture — Traffic Out
Inspection Performance

**Competitive Architecture**

Multi-processor Core with Deep Packet Inspection
Deep Packet Inspection Architecture
UTM Load Balancing
Traffic In — Processor — Traffic Out
Inspection Performance

**SonicWALL Architecture**

**UTM 엔진**

**Packet Assembly-based Process**
Traffic In — Proxy — Scanning — Packet Disassembly — Traffic Out
Inspection Time
When proxy becomes full or content too large, files bypass scanning
Inspection Capacity

**Competitive Architecture**

**Packet Reassembly-Free Process**
Traffic In — Traffic Out
Inspection Time
Reassembly-Free Packet Scanning without proxy or content size limitations
Inspection Capacity

**SonicWALL Architecture**

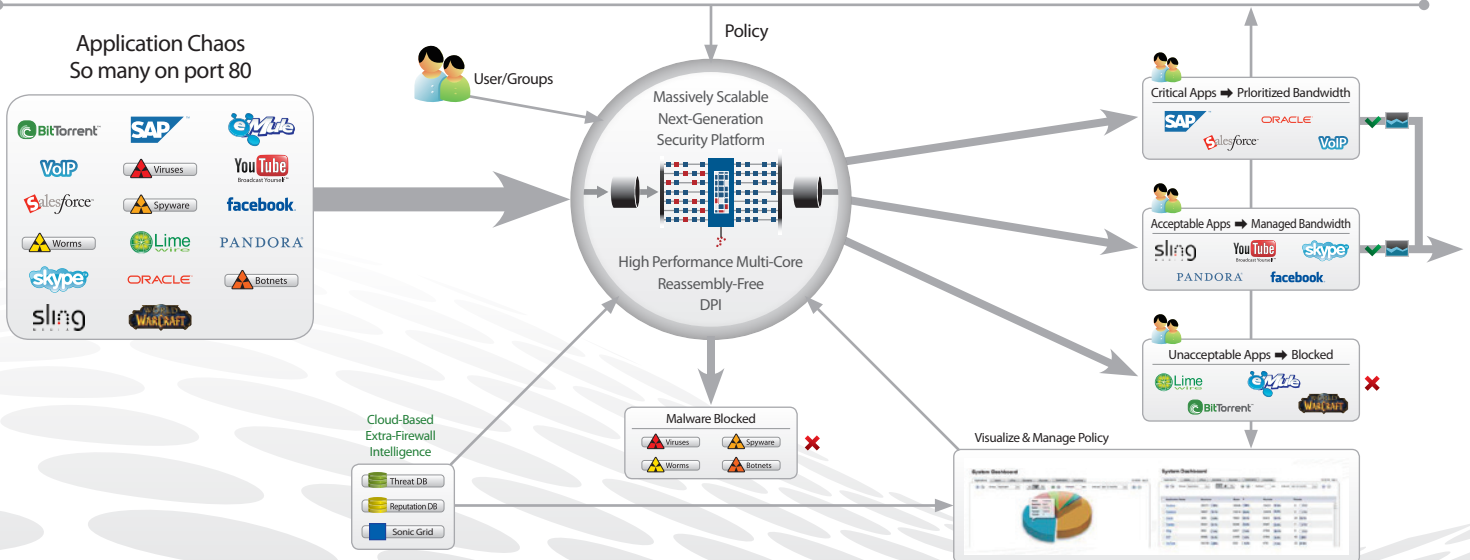## Next-Generation Firewall

### Identity
By Application - Not by Port & 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 Apps by Policy
Manage Apps by Policy
Block Apps by Policy
Detect and Block Malware
Detect & prevent Intrusion Attempts

Application Chaos
So many on port 80

BitTorrent, SAP, eMule, VoIP, Viruses, YouTube Broadcast Yourself, salesforce, Spyware, facebook, Worms, Limewire, PANDORA, Skype, ORACLE, Botnets, sling

User/Groups

Policy

Massively Scalable Next-Generation Security Platform

High Performance Multi-Core Reassembly-Free DPI

Critical Apps ➡ Prioritized Bandwidth
SAP, ORACLE, salesforce, VoIP

Acceptable Apps ➡ Managed Bandwidth
sling, YouTube, skype, PANDORA, facebook

Unacceptable Apps ➡ Blocked
Lime wire, eMule, BitTorrent, WARCRAFT ✕

Malware Blocked
Viruses, Spyware, Worms, Botnets ✕

Visualize & Manage Policy

Cloud-Based Extra-Firewall Intelligence
Threat DB
Reputation DB
Sonic Grid

**NSA4500**

**NSA 3500**

**NSA 2400**

**NSA 250M**

**NSA 220**

## Specifications

| Feature | NSA 220/W | NSA 250M/W | NSA 2400 | NSA 3500 | NSA 4500 |
|---|---|---|---|---|---|
| **Firewall** | | | | | |
| SonicOS Version | SonicOS 5.8.1.1 | | SonicOS Enhanced 5.6 (or higher) | | |
| Stateful Throughput[1] | 600 Mbps | 750 Mbps | 775 Mbps | 1.5 Gbps | 2.75 Gbps |
| GAV Performance[2] | 115 Mbps | 140 Mbps | 160 Mbps | 350 Mbps | 690 Mbps |
| IPS Performance[2] | 195 Mbps | 250 Mbps | 275 Mbps | 750 Mbps | 1.4 Gbps |
| UTM Performance[2] | 110 Mbps | 130 Mbps | 150 Mbps | 240 Mbps | 600 Mbps |
| IMIX Performance[2] | 180 Mbps | 210 Mbps | 235 Mbps | 580 Mbps | 700 Mbps |
| Maximum Connections[3] | 85,000 | 110,000 | 225,000 | 325,000 | 500,000 |
| Maximum UTM Connections | 32,000 | 64,000 | 125,000 | 175,000 | 250,000 |
| New Connections/Sec | 2,200 | 3,000 | 4,000 | 7,000 | 10,000 |
| Nodes Supported | Unrestricted | | | | |
| Denial of Service Attack Prevention | 22 classes of DoS, DDoS and scanning attacks | | | | |
| SonicPoints Supported (Maximum) | 16 | 24 | 32 | 48 | 64 |
| **VPN** | | | | | |
| 3DES/AES Throughput[5] | 150 Mb | 200 Mbps | 300 Mbps | 625 Mbps | 1.0 Gbp |
| Site-to-Site VPN Tunnels | 25 | 50 | 75 | 800 | 25/50[4] |
| Bundled Global VPN Client Licenses (Maximum) | 2 (25) | 2 (25) | 10 (250) | 50 (1,000) | 2 (25) |
| Bundled SSL VPN Licenses (Maximum) | 2 (15) | 2 (15) | 2 (25) | 2 (30) | 2 (15) |
| Virtual Assist Bundled (Maximum) | 1 30-day Trial (5) | 1 30-day Trial (5) | 1 (5) | 2 (10) | 1 30-day Trial (5) |
| Encryption/Authentication/DH Groups | DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1/DH Groups 1, 2, 5, 14 | | | | |
| Key Exchange | Key Exchange IKE, IKEv2, Manual Key, PKI (X.509), L2TP over IPSec | | | | |
| Route-based VPN | Yes (OSPF, RIP) | | | | |
| Certificate Support | Verisign, Thawte, Cybertrust, RSA Keon, Entrust, and Microsoft CA for SonicWALL-to-SonicWALL VPN, SCEP | | | | |
| Dead Peer Detection | Yes | | | | |
| DHCP Over VPN | Yes | | | | |
| IPSec NAT Traversal | Yes | | | | |
| Redundant VPN Gateway | Yes | | | | |
| Global VPN Client Platforms Supported | Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32/64-bit, Windows 7 32/64-bit | | | | |
| SSL VPN Platforms Supported | Microsoft® Windows 2000 / XP / Vista 32/64-bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE | | | | |
| **Security Services** | | | | | |
| Deep Packet Inspection Service | Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control | | | | |
| Content Filtering Service Premium Edition | (CFS) HTTP URL,HTTPS IP, keyword and content scanning ActiveX, Java Applet, and cookie blocking bandwidth management on filtering categories, allow/forbid lists | | | | |
| Gateway-enforced Client Anti-Virus and Anti-Spyware | McAfee® or Kaspersky® | | | | |
| Comprehensive Anti-Spam Service | Supported | | | | |
| Application Intelligence and Control | Application bandwidth management and control, prioritize or block application by signatures, control file transfers, scan for key words or phrases | | | | |
| DPI-SSL[6] | Provides the ability to decrypt HTTPS traffic transparently, scan this traffic for threats using SonicWALL's Deep Packet Inspection technology (GAV/AS/IPS/ Application Intelligence/CFS), then re-encrypt the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both clients and servers. | | | | |
| **Networking** | | | | | |
| IP Address Assignment | Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay | | | | |
| NAT Modes | 1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode | | | | |
| VLAN Interfaces (802.1q) | 25 | 35 | 25 | 50 | 200 |
| Routing | OSPF, RIPv1/v2, static routes, policy-based routing, Multicast | | | | |
| QoS | Bandwidth priority, maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1p | | | | |
| IPv6 | Yes | | | | |
| Authentication | XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix | | | | |
| Internal Database/Single Sign-on Users | 100/100 Users | 150/150 Users | 250/250 Users | 300/500 Users | 1,000/1,000 Users |
| VoIP | Full H.323v1-5, SIP, gatekeeper support, outbound bandwidth management, VoIP over WLAN, deep inspection security, full interoperability with most VoIP gateway and communications devices | | | | |
| Switching Features(2400MX Only) | VLAN Trunking, Rapid Spanning Tree, Layer 2 Discovery, Link Aggregation, Port Mirroring, Layer 2 QoS, Rate Control, Port Security | | | | |
| **Hardware** | | | | | |
| Interfaces | (7) 10/100/1000 Copper Gigabit Ports, 2 USB, 1 Console Interface | (5) 10/100/1000 Copper Gigabit Ports, 2 USB, 1 Console Interface Module Slot | (6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB | | |
| Memory (RAM) | 512 MB | | | | |
| Flash Memory | 32 MB Compact Flash | | 512 MB Compact Flash | | |
| Fans | No Fan/1 Internal Fan | 2 Internal Fans | 2 Fans | | |
| Certifications | VPNC, ICSA Firewall 4.1 | | EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2 | | |

**Certifications**

Common Criteria EAL4+ CERTIFIED

FIPS 140-2

ICSAlabs CERTIFIED FIREWALL-CORPORATE

[1] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.
[2] UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.
[3] Actual maximum connection counts are lower when UTM services are enabled.
[4] Only with the NSA 240 Stateful HA and Expansion Upgrade.
[5] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.
[6] Supported on the NSA 3500 and higher.