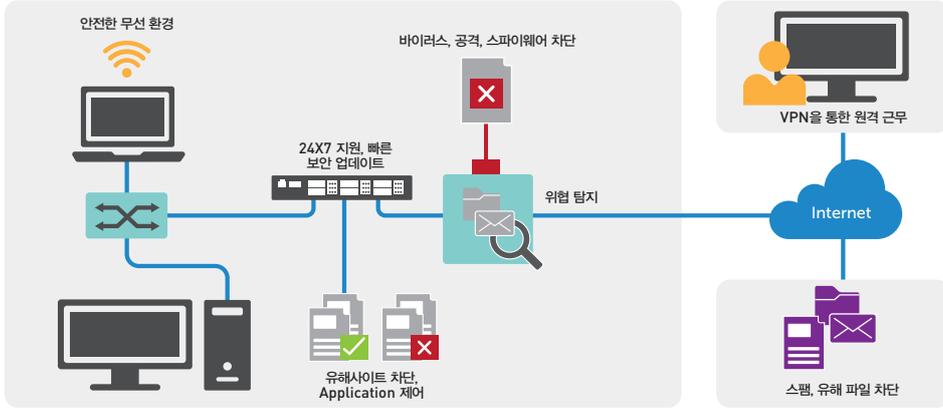


- 4년 연속 리더그룹의 차세대 방화벽

Reassembly-Free Deep Packet Inspection® (RFDPI) 특허 기반의 위협 차단 엔진을 적용한 고성능의 차세대 애플리케이션/통합보안 시스템



SonicWall 보안 네트워크



오늘날 기업들은 지금까지와는 다른 수준의 보안 위협에 노출되어 있습니다. 더욱 정교해진 대규모 전산 공격은 기업과 개인의 데이터는 물론 고객의 데이터까지 유실시키고 지적 재산에 피해를 입힘으로써 생산성을 저하시키고 기업 이미지에 치명적인 타격을 입히게 됩니다.

이러한 가운데 보안 시스템은 대단히 복잡해지고 있습니다. 대안을 고려할 때 가장 중요한 것은 우선순위를 명확히 파악하는 것입니다. BYO (bring your own) 돌풍과 함께 스마트폰, 태블릿 등 네트워크에 접근하는 개인 기기의 수가 폭증함에 따라 네트워크의 성능 및 생산성이 저하되고 있습니다. 또한 소셜 미디어 및 영상 스트리밍을 위한 모바일 애플리케이션은 상당한 수준의 대역폭을 소비합니다. 결국 IT 관리자들은 네트워크 성능을 유지하기 위해 보안 관련 기능을 포기하는 경우가 발생하게 됩니다.

SonicWall은 이러한 고민을 가진 기업 고객들을 위해 네트워크 성능을 희생시키지 않고 안전성과 생산성을 모두 만족시킬 수 있는 방법을 제공합니다. SonicWall 차세대 보안 시스템은 업계 최고 수준의 성능과 안정성을 보장하는 차세대 방화벽 솔루션으로서 엔터프라이즈급 보안 및 성능과 더불어 SonicWall 고유의 사용 편의성과 고부가가치를 제공합니다. 수년간의 연구 개발 과정을 거쳐 탄생하게 된 차세대 시리즈는 데이터 센터, 엔터프라이즈 분산 환경, SMB, 대학, 공공 기관 등 다양한 분야에서 활용이 가능합니다.

주요 기능 및 특징

자동화된 차세대 방화벽

사용자의 개입없이 자동으로 애플리케이션 및 사용자를 인식하며, 사용자/그룹, 애플리케이션에 대한 최소/최대 대역폭 할당 및 우선순위 할당 등을 통해 다양한 사용자의 애플리케이션을 실시간으로 제어하고 실시간으로 모니터링합니다.

파일사이즈와 프로토콜에 제한없는 안티 바이러스 및 위협 차단

혁신적인 멀티 코어 아키텍처와 특허 기술인 Reassembly-Free Deep Packet Inspection® (RFDPI) 기반의 싱글 패스 위협 차단 엔진이 통합 적용되어 있습니다. 이를 통해 업계 최고 수준의 보호 및 성능, 확장성을 보장하며 다양한 동시 커넥션 및 낮은 레이턴시와 함께 파일 크기에 제한 없이 최고 수준의 초당 연결 속도를 제공합니다. 또한, 시중의 레거시 방화벽 및 침입 방지 기술과 차별화된 수준으로 포트 및 프로토콜에 관계 없이 모든 트래픽을 감시합니다.

가장 많은 시그니처 내장 및 제공

모든 차세대 보안 시스템은 업계 최다인 약 20,000 개의 시그니처를 내장하고 있습니다. 3,760개 이상의 애플리케이션 시그니처, 8,150개 이상의 IPS/Spyware 시그니처, 20,000개 이상의 안티 바이러스 시그니처를 내장하고 있으며, 4,700만개 이상의 클라우드 시그니처와 연동하여 Zero-day Attack 및 Botnet/APT 공격을 차단합니다.

암호화된 트래픽 제어

업계에서 가장 높은 수준의 SSL 해독률을 보유한 차세대 시리즈는 암호화 데이터를 복호화하여 애플리케이션 탐지, 안티 바이러스, IPS/Spyware, 웹/URL 필터링 등의 다양한 보안 기능을 통해 사용자 및 시스템을 보호합니다.

통합 관리

SonicWall Global Management System (GMS) 은 엔터프라이즈 분산 환경에서 여러 개의 SonicWall 보안 시스템을 단일 창에서 통합 관리할 수 있도록 지원함으로써 관리 편의성을 높이고 총소유비용을 절감할 수 있습니다. 종합적인 실시간 시각화 기능이 제공되는 온/오프 리포트를 통해 네트워크의 상황을 정확하게 파악할 수 있도록 돕습니다.

- 차세대 방화벽 기반의 최고 수준의 보안 기능
- 고성능 멀티코어 아키텍처
- 파일 사이즈와 프로토콜에 제한없는 안티바이러스
- 유해트래픽 차단
- URL 필터링
- DPI SSL
- IPSec VPN 및 SSL VPN
- 무선랜 지원
- 중앙집중형 관리

제품 세부 사양

Model	SOHO	TZ300	TZ400	TZ500	TZ600	NSA2600	NSA3600	NSA4600	NSA5600	NSA6600	SM9200	SM9400	SM9600	SM9800	SM-E10400	SM-E10800
PERFORMANCE																
Firewall Throughput	300M	750M	1.3G	1.4G	1.5G	1.9G	3.4G	6.0G	9.0G	12G	15G	20G	20G	40G	20G	40G
Threat Prevention Throughput	100M	300M	900M	1.0G	1.1G	700M	1.1G	2.0G	3.0G	4.5G	5.0G	10G	11.5G	24G	15G	30G
Full DPI(Anti Virus) Throughput	50M	100M	300M	400M	500M	300M	500M	800M	1.6G	3.0G	3.5G	4.5G	5.0G	10G	6.0G	12G
IPSecVPN Throughput	100M	300M	900M	1.0G	1.1G	1.1G	1.5G	3.0G	4.5G	5.0G	5.0G	10G	11.5G	18G	7.5G	11G
Maximum Sessions	10K	50K	100K	125K	150K	225K	325K	400K	562.5K	750K	1.25M	1.25M	1.5M	3.0M	6.0M	12M
New Connections/Sec	1,800	5,000	6,000	8,000	12K	15K	20K	40K	60K	90K	100K	130K	130K	280K	320K	640K
IPSecVPN Tunnel	10	10	20	25	50	75	800	1500	4000	6000	10,000	10,000	10,000	10,000	10,000	10,000
IPSecVPN Client(Max)	5	10	25	25	25	250	1,000	3,000	4,000	6,000	4,000	6,000	10,000	10,000	10,000	10,000
SSL VPN Client(Max)	10	50	100	150	200	250	350	500	1,000	1,500	3000	3000	3000	50	50	50
HARDWARE																
10/100/1000 Interface	5	5	7	8	10	8	12	12	12	8	8	8	8	8	-	-
1G SFP Interface	-	-	-	-	-	-	4	4	4	8	8	8	8	12	16	16
10G SFP+ Interface	-	-	-	-	-	-	2	2	2	4	4	4	4	4	6	6
Size	Desktop	Desktop	Desktop	Desktop	Desktop	1U	1U	1U	1U	1U	1U	1U	1U	2U	4U	4U
Power	Single										Redundant					
SonicPoints supported (Maximum)	2	8	16	16	24	32	48	64	96	128	128	128	128	-	-	-

SonicOS 주요 기능

Firewall <ul style="list-style-type: none"> • Reassembly-Free Deep Packet Inspection • Deep packet inspection for SSL • Stateful packet inspection • TCP reassembly • Stealth mode • Common Access Card (CAC) support • DOS attack protection • UDP/ICMP/SYN flood protection 	Web content filtering <ul style="list-style-type: none"> • URL filtering • Anti-proxy technology • Keyword blocking • Bandwidth manage CFS rating categories • Unified policy model with app control • 56 Content filtering categories 	Wireless LAN <ul style="list-style-type: none"> • Built-in wireless controller • 802.11 a/b/g/n/ac • WPA/WPA2, TKIP, WEP • 802.1x, EAP-PEAP, EAP-TTLS
Intrusion prevention <ul style="list-style-type: none"> • Over 8,150 built-in IPS/Spyware signatures • Signature-based scanning • Automatic signature updates • Outbound threat prevention • IPS exclusion list • GeoIP and reputation-based filtering • Regular expression matching 	VPN <ul style="list-style-type: none"> • IPSec VPN for site-to-site connectivity • SSL VPN or IPSec client remote access • Redundant VPN gateway • Mobile Connect for Apple® iOS and Google® Android™ • Route-based VPN 	QoS <ul style="list-style-type: none"> • CoS designator, DSCP and 802.1p QoS Egress and Ingress bandwidth management Policy, Application, user based QoS
Anti-Virus <ul style="list-style-type: none"> • Over 20,000 built-in AV signatures • All TCP Stream-based AV scanning • No file size limitation • Gateway anti-virus • SSL decryption • Compressed file scanning • Bi-directional inspection • Over 47 Million CloudAV threat database 	Networking <ul style="list-style-type: none"> • Dynamic routing(RIP, OSPF, BGP) • Policy-based routing • Advanced NAT • NAT load balancing • DHCP server • Bandwidth management • Link aggregation • Port redundancy • Inbound/outbound load balancing • L2 bridge, wire mode, tap mode, NAT mode 	High Availability <ul style="list-style-type: none"> • Active/Passive high availability • Active/Active DPI • A/A clustering(Max 8 boxes) • Configuration and Session sync
Application control <ul style="list-style-type: none"> • Over 3,760 application signatures • Application control • Application component blocking • Application bandwidth management • Custom application signature creation • Application traffic visualization • Data leakage prevention • Application reporting over NetFlow/IPFIX • Single Sign-On (SSO) • User activity tracking • Comprehensive application signature database 	VoIP <ul style="list-style-type: none"> • Advanced QoS • Bandwidth management • DPI for VoIP traffic • H.323 gatekeeper and SIP proxy support 	Management and monitoring <ul style="list-style-type: none"> • Web GUI • Realtime application/user/traffic monitoring • Command line interface (CLI) • SNMPv2/v3 • Centralized management and reporting • Logging • Netflow/IPFIX exporting • App traffic visualization • LCD management screen • Centralized policy management • Terminal service/Citrix support • Solera Networks Forensics integration

소닉월코리아

서울특별시 강남구 테헤란로 445 본술빌딩10F
 전화 번호 02-3420-9000 | 팩스 번호 02-569-3600
 웹 사이트 www.sonicwall.com

© 2016 SonicWall, Inc. ALL RIGHTS RESERVED. SonicWall logo and products - as identified in this document - are registered trademarks of SonicWall, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

본 문서에 명시된 SonicWall의 로고와 제품들은 미국과 전세계에 SonicWall의 상표로 등록되어 있습니다. 모든 기타 상표 및 등록 상표는 SonicWall의 자산입니다.

