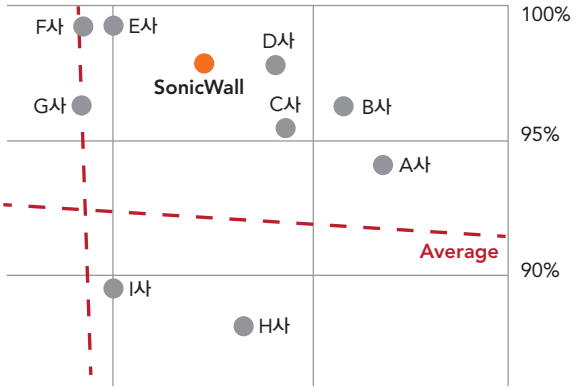
소닉월 솔루션 가이드

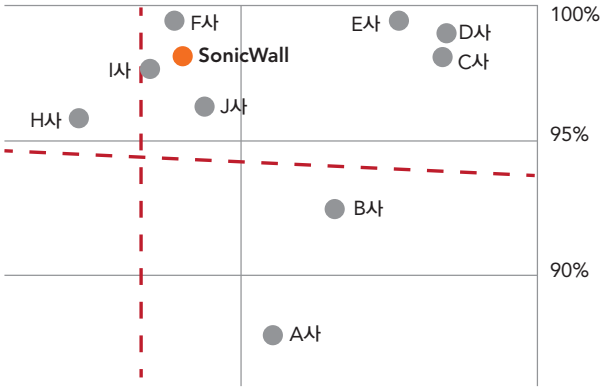
SONICWALL™

소닉월
- 4년 연속 리더그룹의 차세대 방화벽

소닉월 차세대 방화벽은 혁신적인 멀티 코어 아키텍처와 특허 기술인 Reassembly-Free Deep Packet Inspection(RF-DPI) 기반의 위협 차단 엔진을 사용하여 애플리케이션, 사용자, 콘텐츠 등에 대해 최고의 보안성과 성능을 제공하는 차세대 방화벽입니다 . 글로벌 테스트 인증 기관인 NSS Labs에서 4년 연속 리더그룹에 선정된 최상의 차세대 방화벽입니다.



[2015년 NSS Labs 테스트 결과]



[2016년 NSS Labs 테스트 결과]

주요 특징 및 기능

애플리케이션 정책 설정 및 침입 보안을 위한 통합 기능 제공

Application 제어

- Application 인지 및 제어
- 차단, Packet 모니터, QoS 등 다양한 제어 Action 제공
- 약 4,700개 이상의 시그니처
- 사용자 정의 시그니처 지원

AV, IPS, Anti-Spyware

- HTTP, FTP, IMAP, SMTP, POP3, CIFS/Netbios, TCP Stream 에 대한 Anti-Virus 지원
- 파일 사이즈에 제한이 없는 Scanning 지원
- 약 20,000 개의 시그니처 내장
- 약 4,600만개의 Cloud AV 제공

VPN

- IPSec : Site to Site 및 Client VPN 지원, Split 터널 및 다중 터널 Failover 지원, 주요 VPN 벤더와 상호 호환
- SSL-VPN : Windows, Linux, Android, IOS 등 다양한 OS 지원, Local user, AD, LDAP, Radius 사용자 인증 지원 등

콘텐츠 필터

- URL 기반 접근 차단
- Keyword 기반 접근 차단
- ActiveX, Java, Cookies, Proxy 차단 지원
- 사용자 정의 URL 차단 지원
- Category 기반 URL 차단 지원
- White list를 통한 예외처리

Anti-Spam

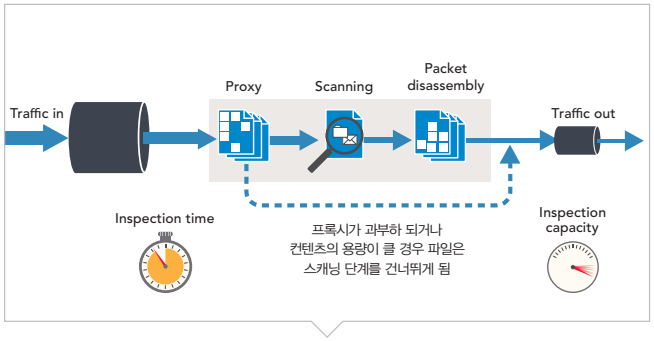
- 다양한 차단 방식 제공
  - Sender IP Address
  - Message 내용
  - Message 구조
  - URL 링크
  - 연락처, 첨부파일
- Junk Box, RBL Filter 지원

Analyzer

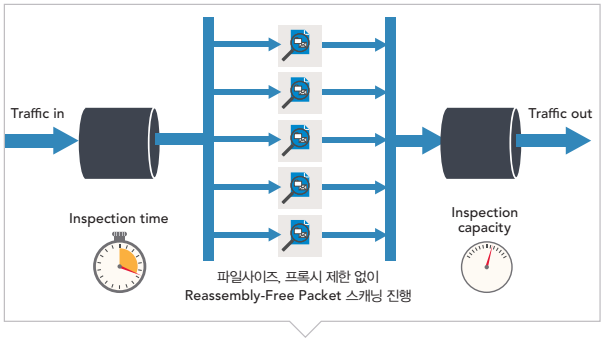
- Application, User, URL 등 다양한 기준의 사용량 제공
- 사용량, PPS, CPS, CCS등 제공
- AppFlow, Threat 보고서 제공
- User 모니터링 제공
- 실시간 Connection 모니터링
- Local Log 저장 및 Syslog 지원

안정적인 성능을 제공하기 위한 특허 기술(RF-DPI)

- ✓ 소닉월은 자체 특허기술인 RF-DPI를 통하여 과부하로 인한 성능의 저하 현상 방지
- ✓ 네트워크 환경에서 패킷의 재조합 없이 Scan 시간을 최소화하여 성능 극대화
- ✓ 실시간 지연에 민감한 파일에 대해 사이즈 제약 없이 우수한 정밀검사 제공



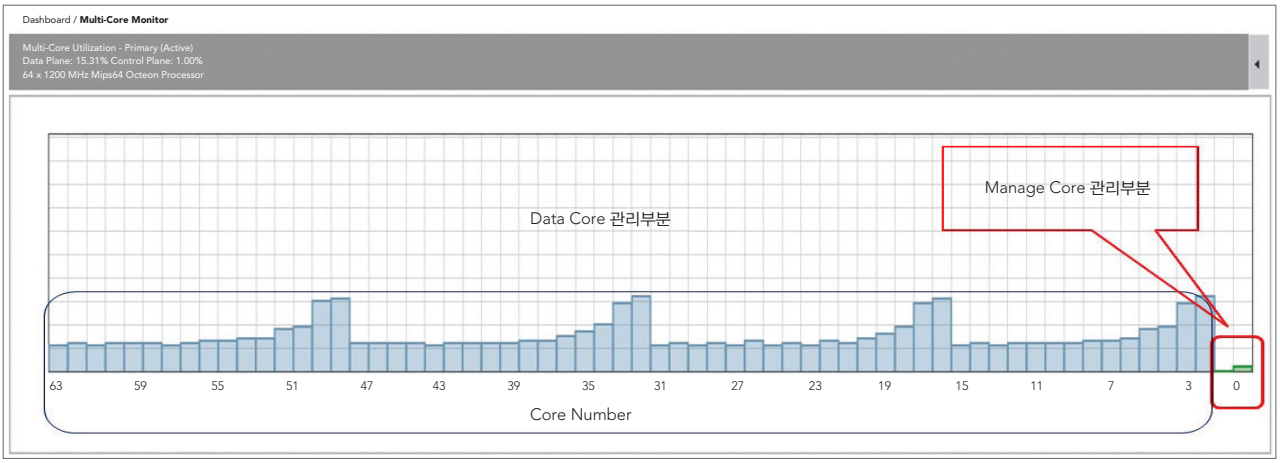
경쟁사 아키텍쳐



소닉월 아키텍쳐

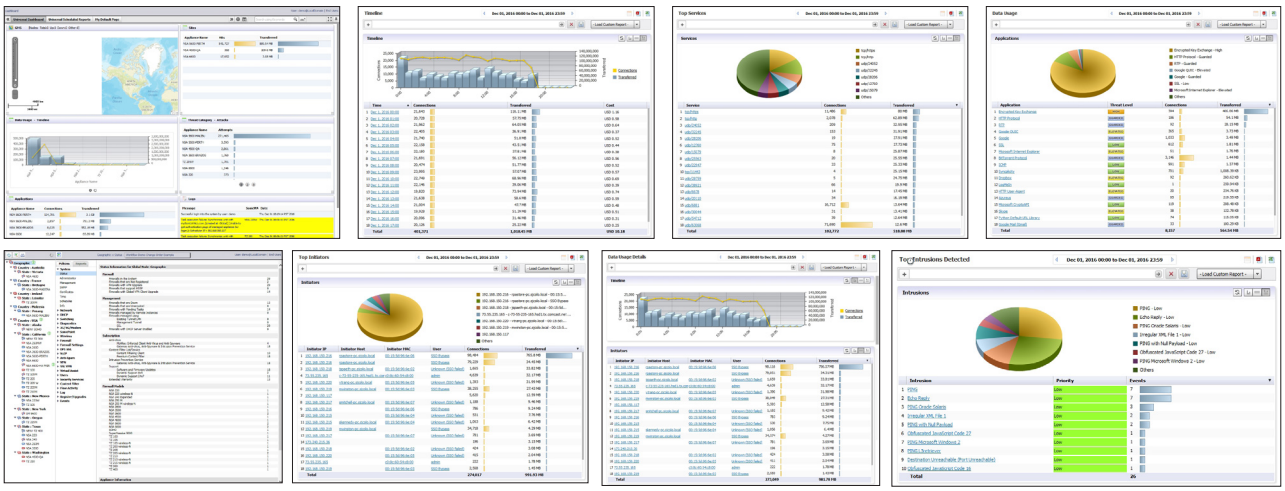
멀티코어(Multi-Core) 기반의 프로세스 처리

- ✓ 소닉월은 통합 보안 기능을 수행하기에 가장 적합한 멀티 코어 기술로 프로세스 처리



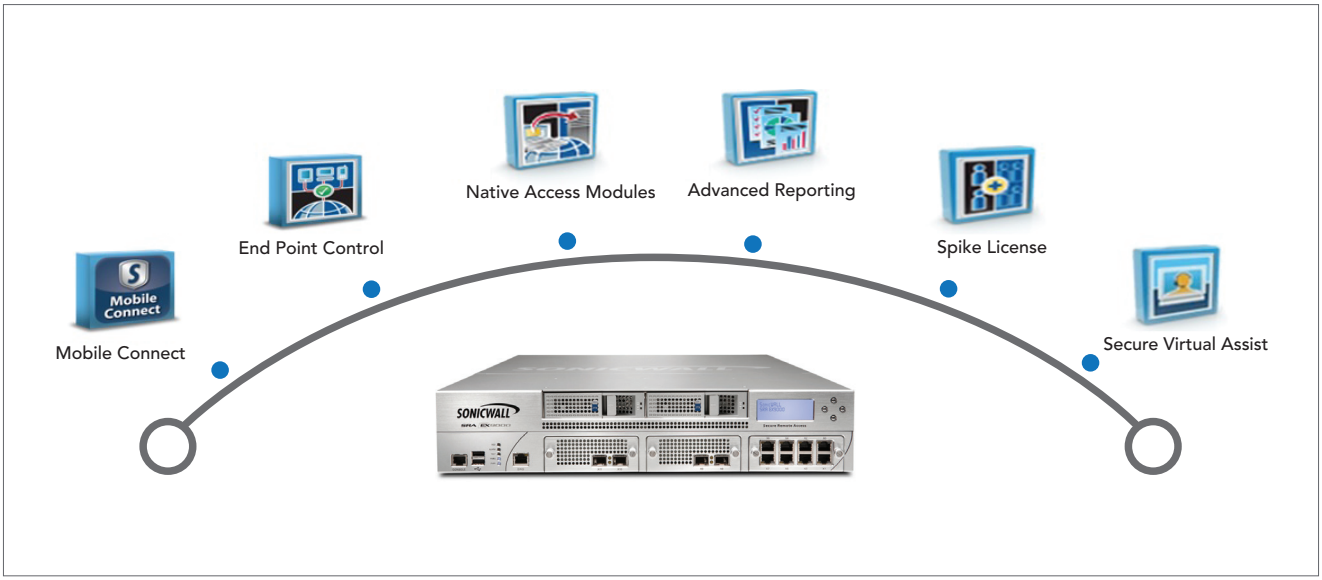
중앙 집중 관리 및 모니터링(GMS)

- ✓ 엔터프라이즈 분산 환경에서 다수의 소닉월 장비에 대한 통합 관리 제공
- ✓ 종합적인 실시간 시각화 기능이 제공되는 리포트를 통해 네트워크 상황을 정확하게 파악 가능
- ✓ 사용자별, 애플리케이션별, IP별 등의 다양한 리포트를 일간, 주간, 월간 리포트 제공



소닉월 SMA
- 유무선 통합 SSL VPN 전용 솔루션

소닉월 Secure Mobile Access(SMA) 장비는 기업용 SSL VPN 전용 솔루션입니다. 최근 기업의 모바일 업무 영역의 확대에 따라서 SSL VPN의 요구 범위도 유무선을 통합할 수 있는 기능으로 확장되고 있습니다. SMA는 Window, Linux, Mac, Android, iOS 등의 다양한 유무선 업무 환경의 단말을 포괄적으로 지원함으로써 통합 SSL VPN을 구축하고자 하는 고객에게 최적의 대안입니다.



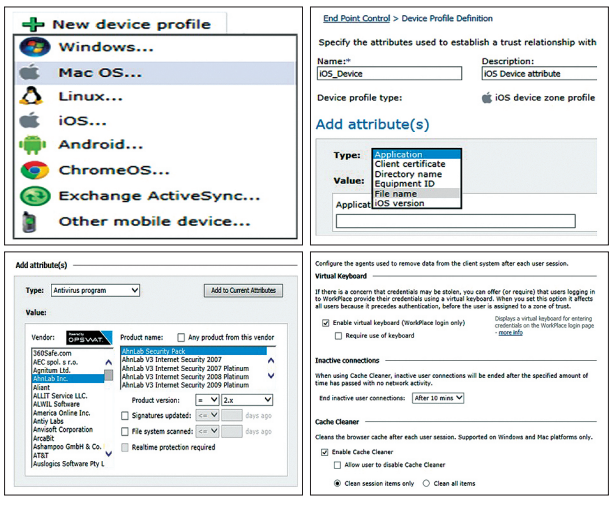
유무선 통합 SSL VPN인 소닉월 SMA를 통하여 기업의 보안 업무 네트워크 구축

주요 특징 및 기능

강력한 End Point 보안 기능 제공

- ✓ End Point Control을 통한 유무선 단말의 보안상태 감지
- ✓ Android 기기의 루팅 및 iOS 기기의 탈옥 상태 모니터링
- ✓ Virtual Keyboard 기능 및 CAPTCHA를 통해 Bots 공격 방어

엔드포인트 무결성 감지



디바이스 프로파일
- 윈도우
- MAC OS
- 리눅스
- iOS / Android
- ChromeOS
- Exchange ActiveSync
- 다른 모바일 기기

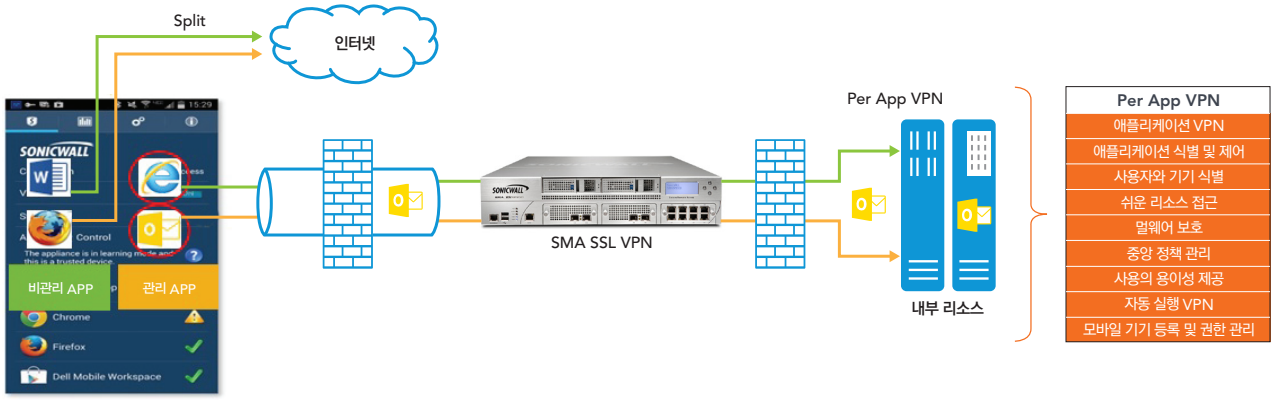
디바이스 식별
- 어플리케이션
- 크라이언트 인증서
- 디렉토리 이름
- 장비 ID
- 파일 이름
- OS 버전

디바이스 무결성
- 안티바이러스
- 안티스파이웨어
- 개인 방화벽
- 레지스트리 키
- 윈도우 OS 레벨
- 탈옥 / 루팅

데이터 보안
- 캐쉬 제어
- 가상 키보드
- 비활성 연결 제한

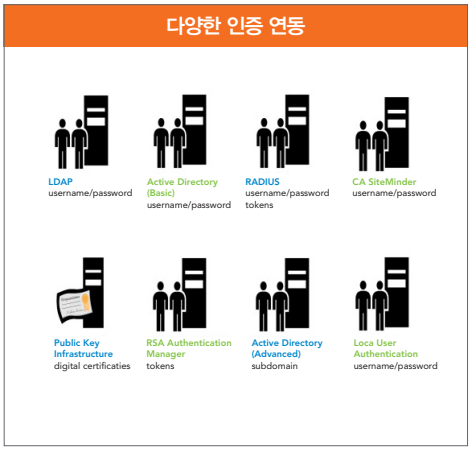
모바일 애플리케이션 단위 기반의 VPN 기능 (Per App VPN)

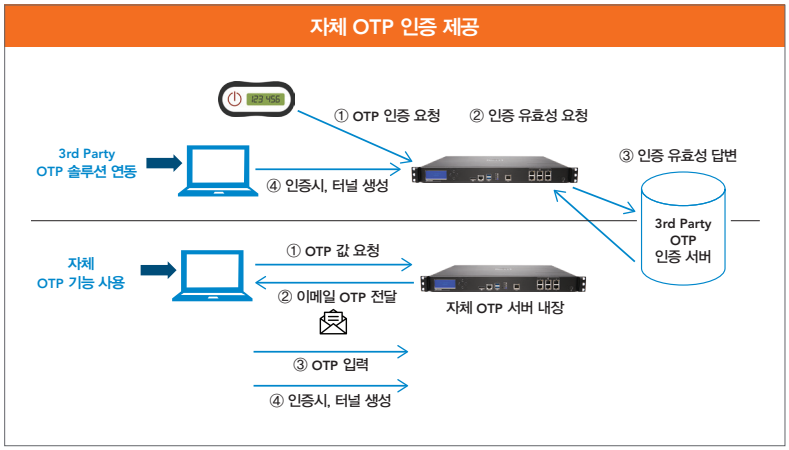
- ✓ 애플리케이션 단위 기반의 터널링을 통한 SSL VPN 환경 구축 가능
- ✓ 모바일 환경에서 기업용 App과 개인용 App을 구분하여 기업용 App만 내부 접근 통제
- ✓ Android 및 iOS 기기에 대해 속도 저하 없이 고성능 제공
- ✓ 최적의 비용으로 안전한 고객의 모바일 업무 환경 구축 가능



다양한 인증 및 연동 방안 제공

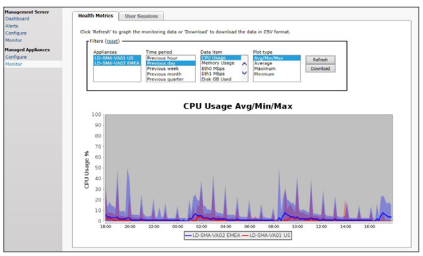
- ✓ LDAP, AD, RADIUS, RSA, CA, PKI, Local DB 등 고객에 맞는 다양한 인증 서버 연동
- ✓ 자체 OTP(One Time Password) 및 3rd Party OTP를 통한 Two factor 기능 구현
- ✓ 모바일 SDK 제공을 통한 다양한 연동 방안 제공

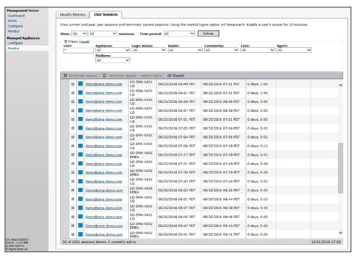




직관적인 관리 및 리포팅

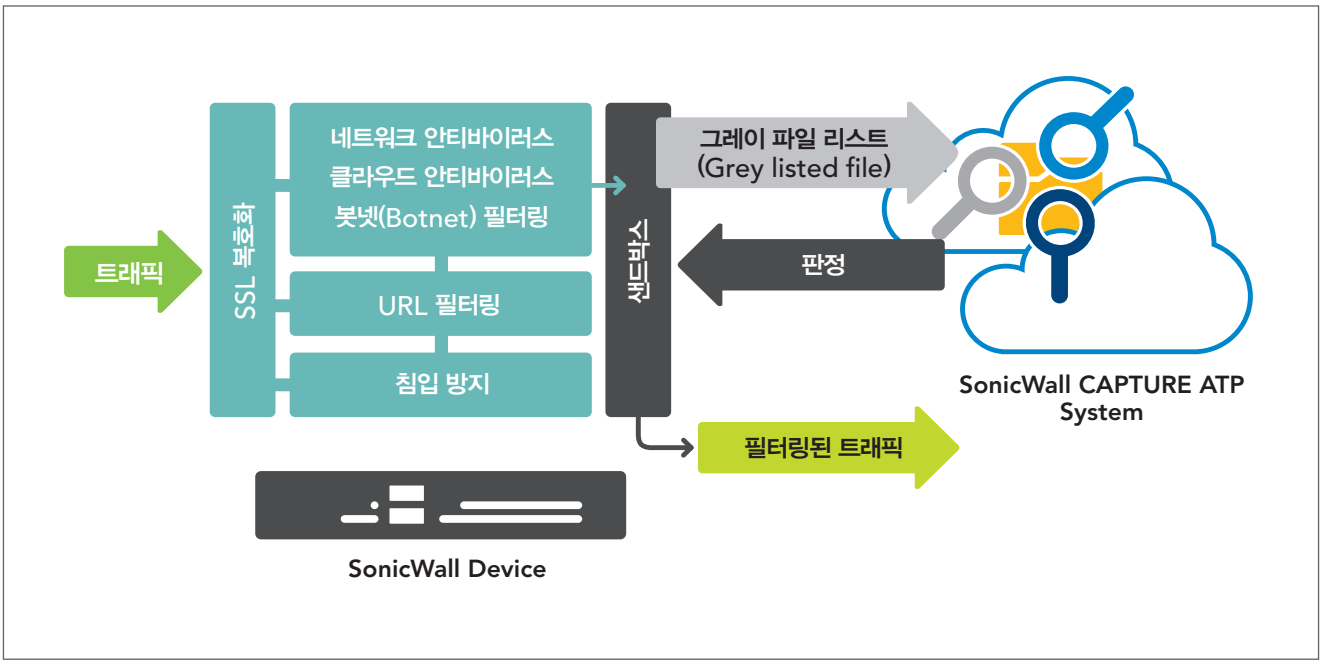
- ✓ 중앙 집중형의 풍부한 모니터링 기능을 통해 컴플라이언스 준수, 관리, 자원 계획 등 지원
- ✓ 사용자, 시간, 처리량, 영역, 커뮤니티, 구역, 에이전트 및 IP 주소 별로 모니터링 기능 지원





소닉월 CAPTURE
- APT 방어 전용 솔루션

소닉월 CAPTURE는 지능형 지속 공격인 APT의 방어 솔루션으로 멀티엔진 샌드박스 분석 기술을 통해 알려지지 않은 Zero-day 공격을 방어하여 높은 보안 효과를 제공합니다.



오늘날의 보안 위협은 더욱 지능화, 고도화되어 기존의 보안 솔루션을 우회하여 공격하도록 설계되고 있습니다. 알려진 위협에 대해서만 탐지가 가능한 기존 보안 솔루션은 지능화된 Zero-day 공격을 방어하는데 취약합니다.
매일 새롭게 발생하는 멀웨어 및 랜섬웨어의 행위를 분석하고 효과적으로 방어할 수 있는 기술은 최근 보안의 핵심 요구사항으로 발전하였습니다. 소닉월의 CAPTURE 서비스는 3개의 멀티엔진 기반의 샌드박스 기술을 이용하여 멀웨어, 랜섬웨어 등의 행위를 분석하고 위협을 차단 합니다.

주요 특징 및 기능

멀티 엔진기반의 지능형 위협 분석 기능

소닉월의 CAPTURE 서비스는 업계 최초로 3개의 강력한 멀티엔진 기반의 샌드박스 플랫폼을 개발하여 멀웨어, 랜섬웨어와 같은 APT 의 Zero-day 공격을 차단합니다. 3중의 강력한 멀티엔진은 기존 APT 솔루션보다 뛰어난 확장된 성능을 제공합니다.

- ✓ Virtual Sandboxing (SonicWall)
- ✓ Hypervisor 레벨 분석 (VMRAY)
- ✓ Full System Emulation (Lastline)

다양한 파일 타입 분석 지원

- ✓ 실행프로그램(PE), DLL, PDF, MS office 문서, 압축파일, APK 등 다양한 파일 형식 지원
- ✓ Windows 및 모바일 운영체제 환경 분석 지원
- ✓ 분석을 위한 수동 파일 Upload 지원

쉬운 구성 및 운영

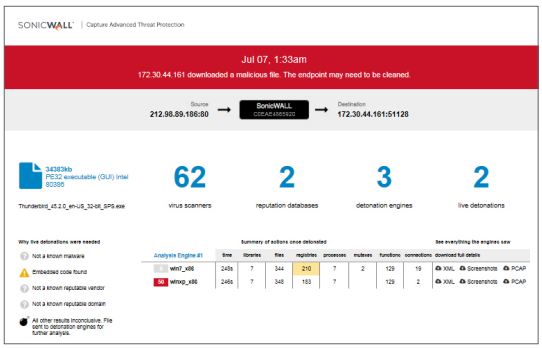
- ✓ 소닉월 방화벽과 CAPTURE 클라우드 연동을 통한 단순한 구성
- ✓ 간단한 설정을 통한 쉬운 운영

신속한 시그니처 업데이트

- ✓ 파일 분석 결과는 CAPURE 서비스를 사용하는 전세계 모든 소닉월 방화벽에서 신속하게 이용할 수 있도록 제공
- ✓ 글로벌 시큐리티 네트워크를 통하여 시그니쳐에 대한 신속한 업데이트 제공

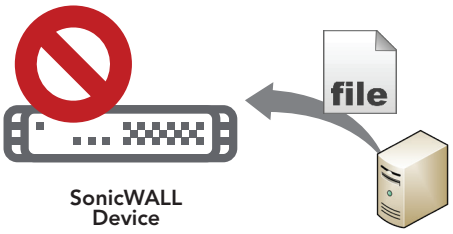
다양한 분석 보고서 및 경고 알림

- ✓ 분석된 악성코드에 대한 상세 보고서 제공
- ✓ 일별 탐지 파일 통계 및 Filter 제공
- ✓ 악성 코드의상세 행위 분석 보고서 및 스크린 샷 제공
- ✓ 악성코드 탐지 시 경고 메일 발송



평결 대기

- ✓ 파일 분석 결과를 받기 전까지 전송 보류
- ✓ 신규 악성파일의 기업 네트워크 진입 차단



소닉월 차세대 방화벽 제품 세부 사양 – 중소형 사업장

Model	SOHO	TZ300	TZ400	TZ500	TZ600	NSA2600	NSA3600	NSA4600
PERFORMANCE								
Firewall Throughput	300M	750M	1.3G	1.4G	1.5G	1.9G	3.4G	6.0G
Threat Prevention Throughput	100M	300M	900M	1.0G	1.1G	700M	1.1G	2.0G
Full DPI(Anti Virus) Throughput	50M	100M	300M	400M	500M	300M	500M	800M
IPSecVPN Throughput	100M	300M	900M	1.0G	1.1G	1.1G	1.5G	3.0G
Maximum Sessions	10K	50K	100K	125K	150K	225K	325K	400K
New Connections/Sec	1,800	5,000	6,000	8,000	12K	15K	20K	40K
IPSecVPN Tunnel	10	10	20	25	50	75	800	1500
IPSecVPN Client(Max)	5	10	25	25	25	250	1,000	3,000
SSL VPN Client(Max)	10	50	100	150	200	250	350	500
CAPTURE 지원		✓	✓	✓	✓	✓	✓	✓
HARDWARE								
10/100/1000 Interface	5	5	7	8	10	8	12	12
1G SFP Interface	-	-	-	-	-	-	4	4
10G SFP+ Interface	-	-	-	-	-	-	2	2
Size	Desktop	Desktop	Desktop	Desktop	Desktop	1U	1U	1U
Power	Single							
SonicPoints supported (Maximum)	2	8	16	16	24	32	48	64

소닉월 차세대 방화벽 제품 세부 사양 – 중대형 및 데이터센터

Model	NSA5600	NSA6600	SM9200	SM9400	SM9600	SM9800	SM-E10400	SM-E10800
PERFORMANCE								
Firewall Throughput	9.0G	12G	15G	20G	20G	40G	20G	40G
Threat Prevention Throughput	3.0G	4.5G	5.0G	10G	11.5G	24G	15G	30G
Full DPI(Anti Virus) Throughput	1.6G	3.0G	3.5G	4.5G	5.0G	10G	6.0G	12G
IPSecVPN Throughput	4.5G	5.0G	5.0G	10G	11.5G	18G	7.5G	11G
Maximum Sessions	562.5K	750K	1.25M	1.25M	1.5M	3.0M	6.0M	12M
New Connections/Sec	60K	90K	100K	130K	130K	280K	320K	640K
IPSecVPN Tunnel	4000	6000	10,000	10,000	10,000	10,000	10,000	10,000
IPSecVPN Client(Max)	4,000	6,000	4,000	6,000	10,000	10,000	10,000	10,000
SSL VPN Client(Max)	1,000	1,500	3000	3000	3000	50	50	50
CAPTURE 지원	✓	✓	✓	✓	✓			
HARDWARE								
10/100/1000 Interface	12	8	8	8	8	8	-	-
1G SFP Interface	4	8	8	8	8	12	16	16
10G SFP+ Interface	2	4	4	4	4	4	6	6
Size	1U	1U	1U	1U	1U	2U	4U	4U
Power	Single		Redundant					
SonicPoints supported (Maximum)	96	128	128	128	128	-	-	-

소닉월 SMA 제품 세부 사양

	SMA for SMB			SMA for Enterprise			
MODEL	SMA 500v (virtual)	SMA200	SMA400	SMA 8200v (virtual)	SMA6200	SMA7200	EX9000
Concurrent user	Max 250	Max 50	Max 250	Max 5,000	Max 2,000	Max 10,000	Max 20,000
Form factor	-	1U	1U	-	1U	1U	2U
Memory	-	2GB	4GB	-	8GB	16GB	32GB
Interfaces	-	2xGbE	4xGbE	-	6xGbE	2x10GbE, 6xGbE	4x10GbE, 8xGbE

	SMA Virtual Appliance (가상화 기반)
Hypervisor	ESX/ESXi (6.0, 7.x)
OS	Hardened Linux
Memory	2GB
HDD Size	80GB
Vmware Hardware Compatibility Guide	http://www.vmware.com/resources/compatibility/search.php

소닉월코리아
서울특별시 강남구 테헤란로 445 본솔빌딩10F
전화 번호 02-3420-9000 | 팩스 번호 02-569-3600
웹 사이트 www.sonicwall.com

SONICWALL™