



보안웹게이트웨이를 이용한 비업무사이트와 웹 어플리케이션 제어



2021.11.03

Contents

보안웹게이트웨이를 이용한
비업무사이트와 웹 어플리케이션 제어

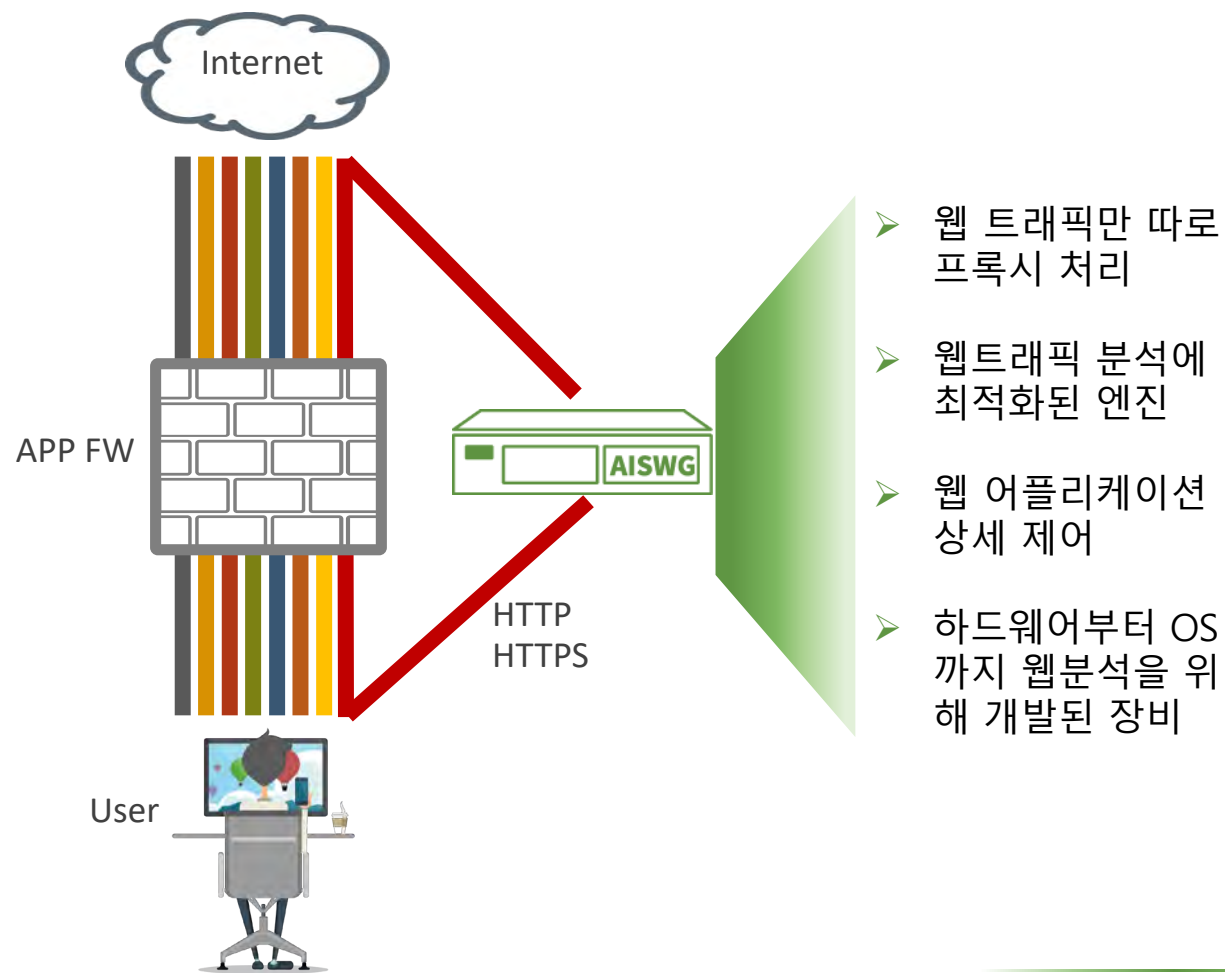
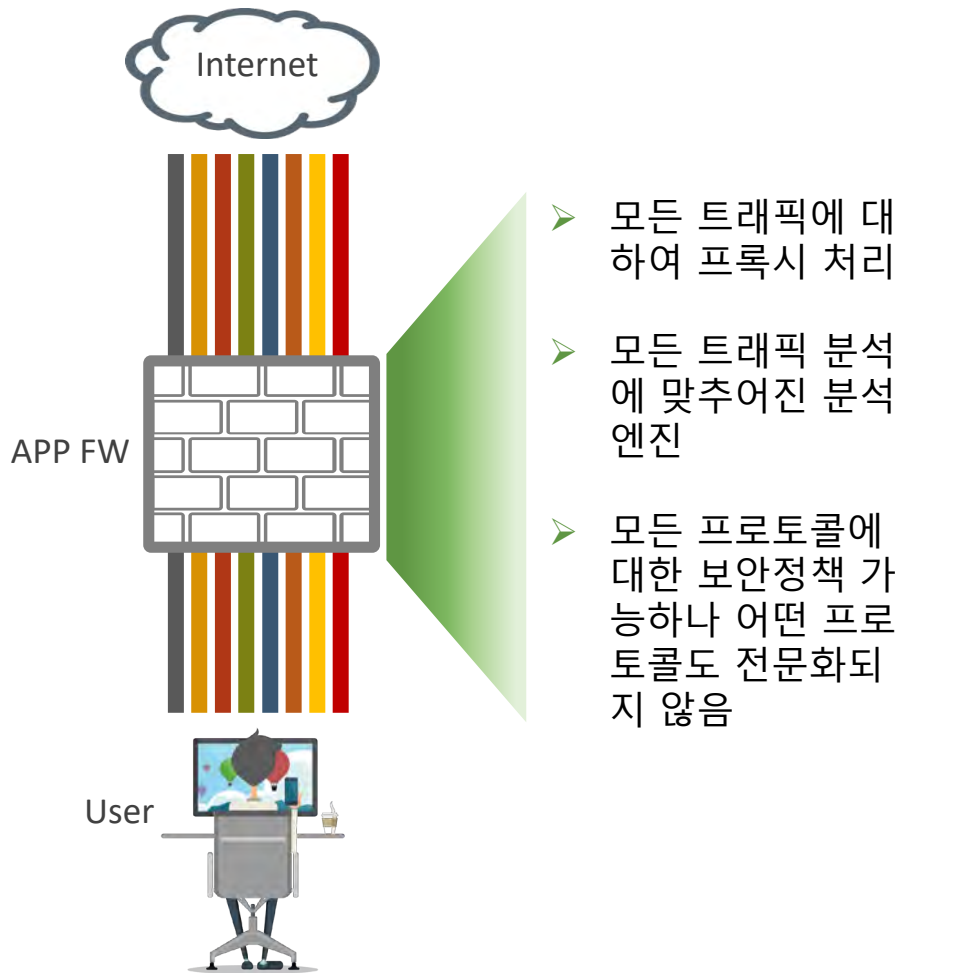


- 1. 보안웹게이트웨이 필요성
- 2. AISWG 제품 소개 및 특징점
- 3.비업무사이트 차단과 웹 어플리케이션 제어
- 4. 다양한 구축 방안과 연동 사례

1. 보안웹게이트웨이 필요성

01 보안웹게이트웨이 필요성

◆ 웹 트래픽에 전문화된 보안웹게이트웨이



01 보안웹게이트웨이 필요성

◆ SSL을 이용한 Malware의 증가

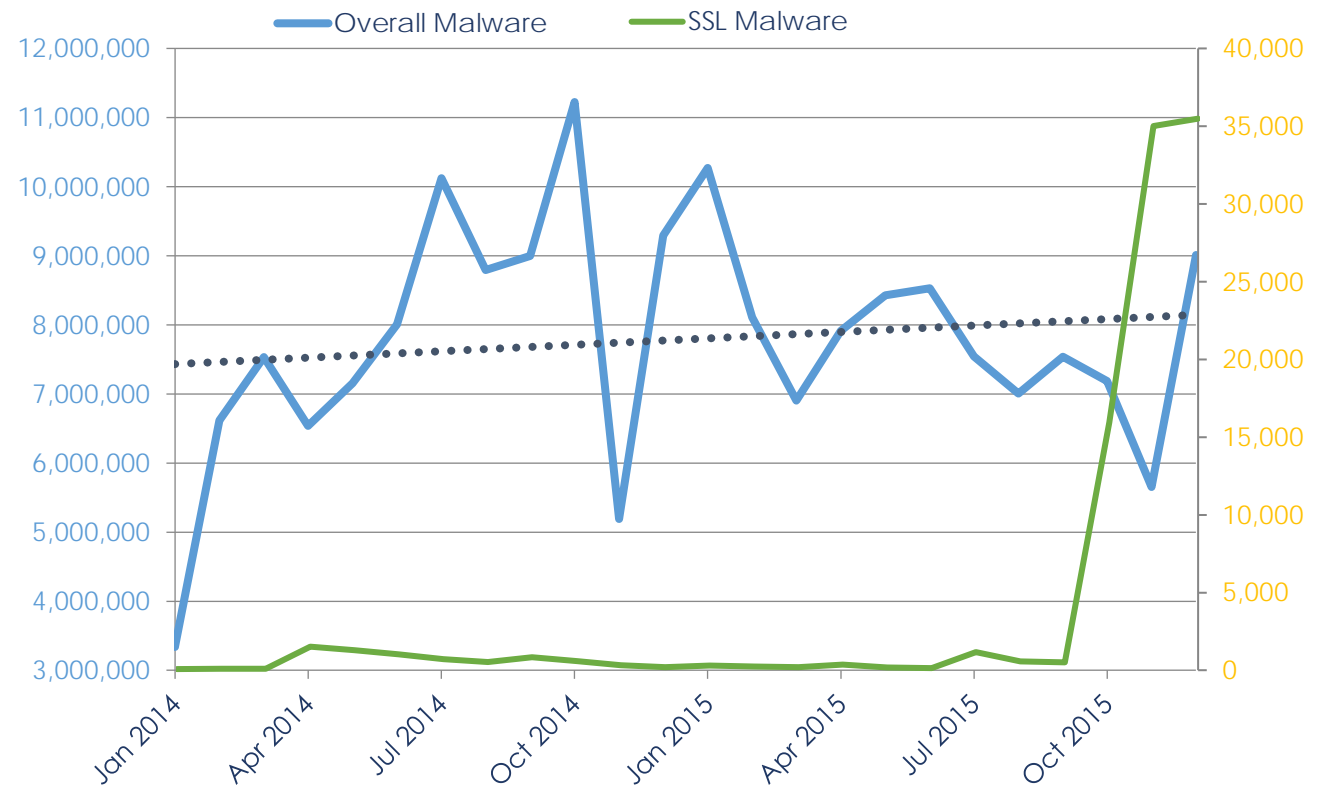
- 전체적인 멀웨어는 steady한 증가세
- SSL 블랙리스트 기반으로 멀웨어 추이를 보면 2015년을 기점으로 폭발적인 증가

Dridex	Spambot	Tinba
KINS	Retefe	Gozi
Shylock	TeslaCrypt	VMZeus
URLzone	CryptoLocker	Redyms
TorrentLocker	Bebloh	Qadars
CryptoWall	Gootkit	Vawtrack
Upatre	Geodo	Emotet

* Samples observed on VirusTotal

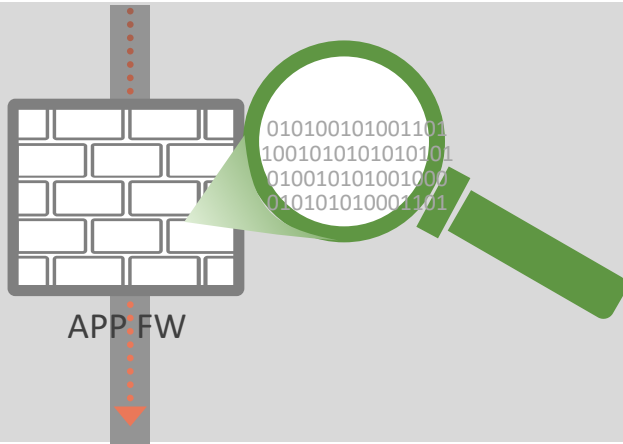
† SSL Blacklist can be viewed at <https://sslbl.abuse.ch>

Malware Sample Occurrence



01 보안웹게이트웨이 필요성

◆ 알지못하는 의심스런 트래픽(unknown tcp) 대처



⇒ 어플리케이션으로 인지하지 못하는 트래픽은 기본 허용

- 어떤 포트의 어떤 어플리케이션인지 모르기 때문에 의심스럽더라도 우선 통신 허용
- 방화벽 한계
- 인지못한 트래픽으로 공격이 들어올 경우 이로 인한 보안 hole 발생 가능성

⇒ http나 https를 인지하여 자동 정책 적용 및 비표준 프로토콜 제어

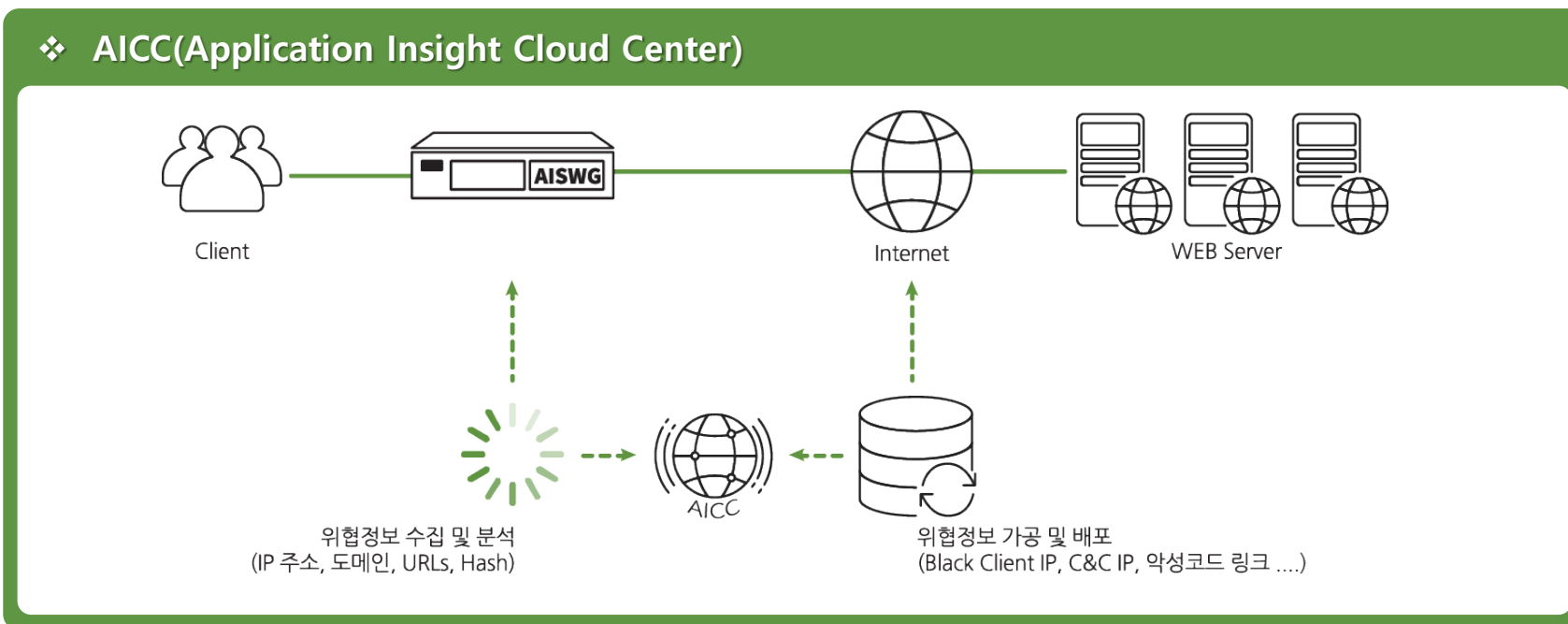
- TCP Port를 지정하지 않아도 Web Traffic 인지
- 80 or 443으로 들어오는 트래픽 중 웹이 아닌 Traffic에 대한 차단 or Bypass
- 비표준 프로토콜 제어

2. APPLICATION INSIGHT SWG 제품 소개 및 특징점

02 AISWG 소개 및 특징점

◆ 보안 규칙만으로 해결 할 수 없는 다양한 위협에 대한 선제적 대응

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

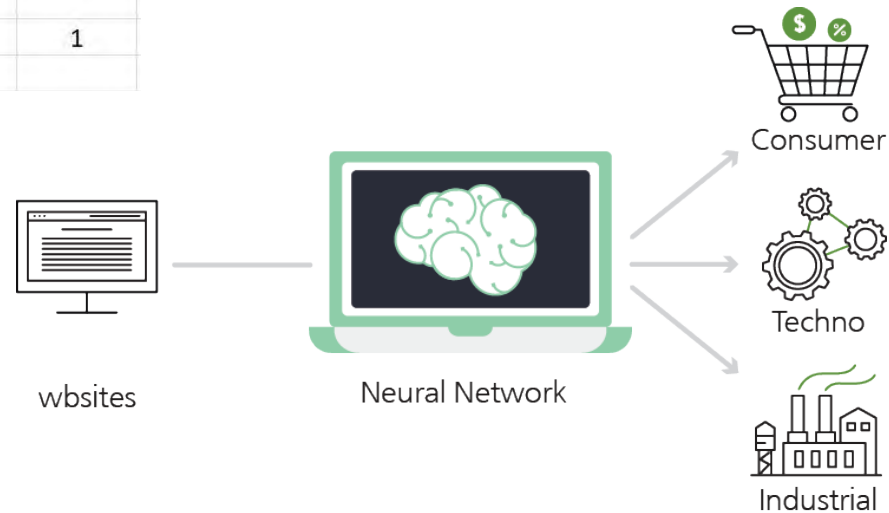
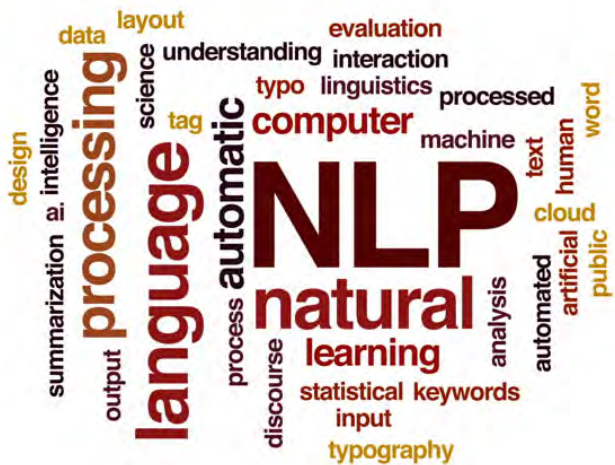


02 AISWG 소개 및 특징점

◆ 형태소 분석 및 머신러닝을 통한 URL 카테고리 분류

- 웹 사이트 내 콘텐츠 파악 및 분석을 통하여 여러 종류의 카테고리 중에서 가능 적절한 카테고리 군 판단.
- AISWG 시스템과의 실시간 카테고리 정보 공유

Training examples		Features	
	love	programming	also
1 → I love programming	1	1	0
2 → Programming also loves me	1	1	1



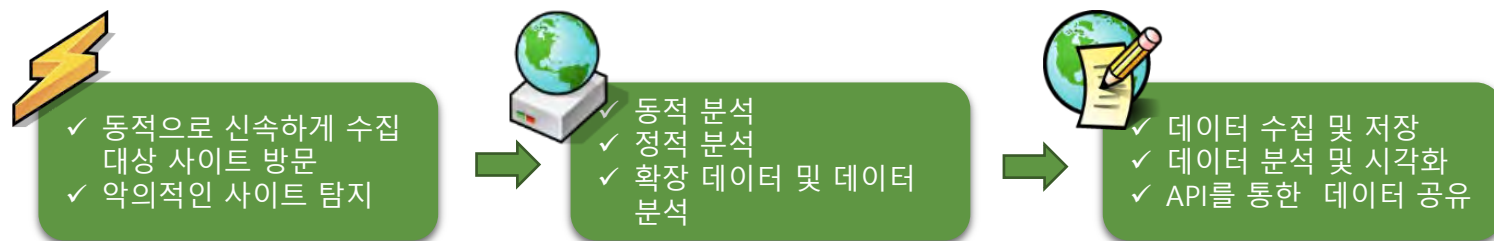
02 AISWG 소개 및 특징점

◆ 웹 사이트 직접 방문을 통해 인코딩 및 난독화 코드를 포함한 행위기반 분석 수행

▶ 악성 URL 분석 및 탐지

- 프로세스 삽입, 레지스트리 삽입, 파일자동 실행 등 OS 이벤트를 통해 Exploit 검출
- 웹 브라우저, 플러그인, 플래시, 자바취약점 등으로 인해 발생하는 Drive-by-down 탐지
- Landing Site 및 Distribute Site 추적

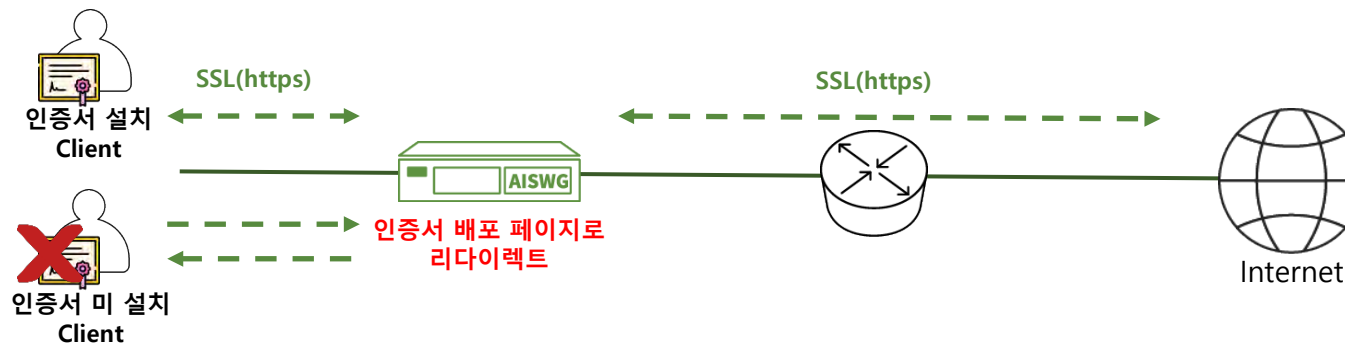
▶ AISWG 시스템과의 실시간 통신을 통한 악성 URL 접근 탐지에 활용



02 AISWG 소개 및 특징점

◆ HTTPS 암호화 트래픽 복호화 및 인증서 자동 배포

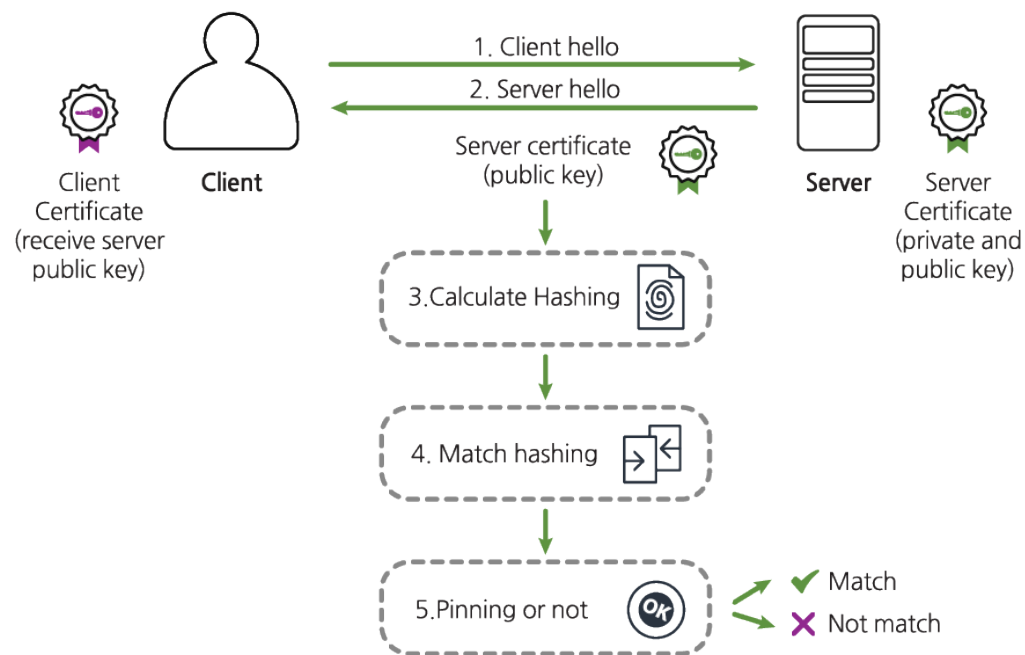
- APPLICATION INSIGHT SWG는 별도의 IP 부여 없이 Stealth-mode로 운영
- 하드웨어 자체 바이패스 기능 모듈 장착하여, 시스템 이상 발생 시 물리적 바이패스 기능 제공
- 클라이언트에 인증서 설치를 위한 인증서 자동 배포 기능 제공



02 AISWG 소개 및 특징점

◆ Public Key Pining 목록 업데이트를 통한 서비스 가용성 확보

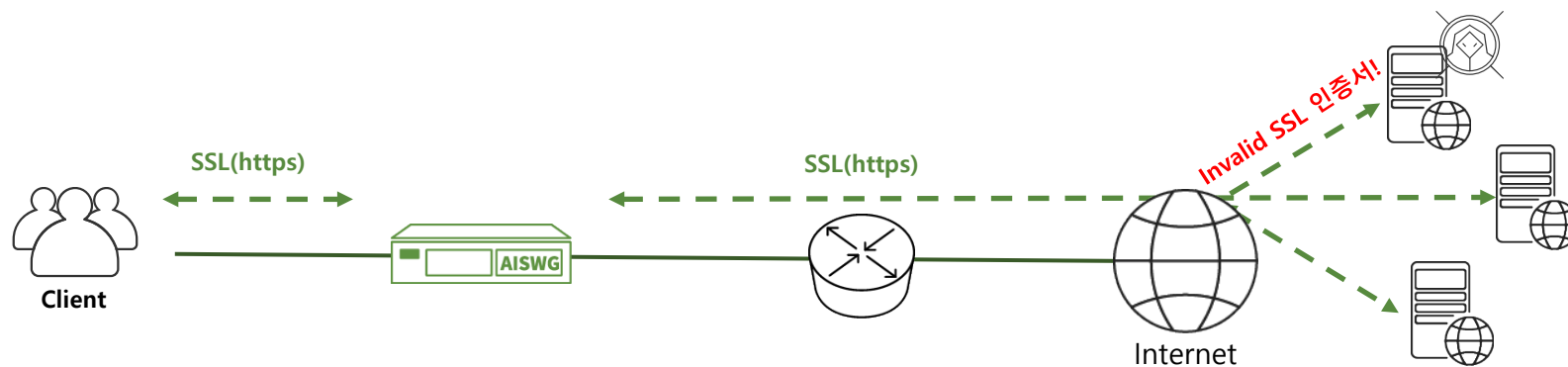
- HTTPS 복호화를 위하여 AISWG가 통신에 개입하는 경우 인증서 고정으로 인한 정상적인 통신 불가
- AISWG가 제공한 공개 키와 클라이언트 어플리케이션에 내장된 공개키가 불일치 하여 MITM 공격으로 간주
- PKP List를 정기적으로 업데이트하여 해당 목적지 트래픽에 대한 선택적 바이패스



02 AISWG 소개 및 특징점

◆ Invalid SSL 인증서 검출

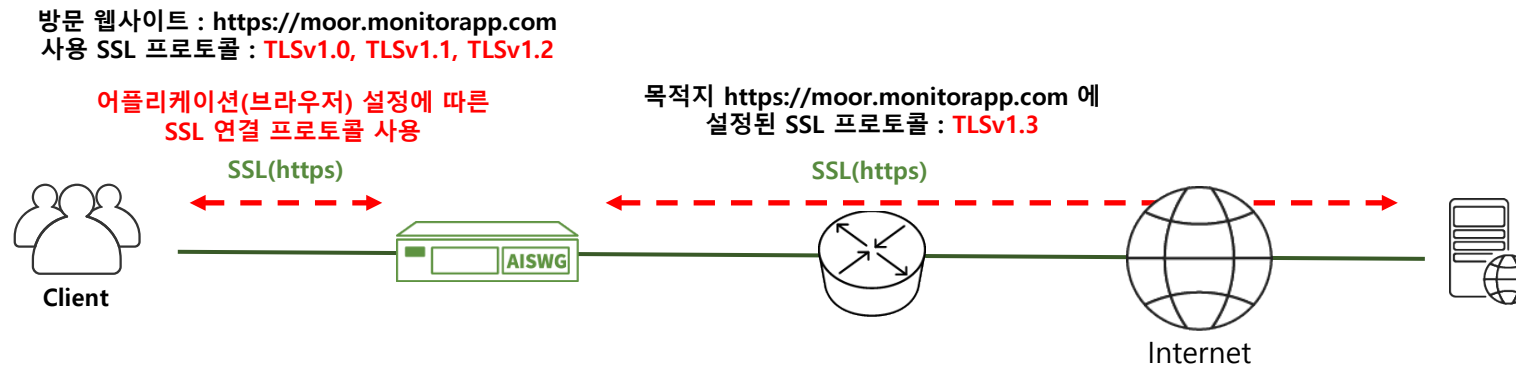
- ▶ 사용자가 통신하는 서버의 SSL 인증서가 Invalid 상태로 확인 되는 경우 해당 세션을 차단 하는 보안 기능
 - Invalid 인증서는 주로 악용된 웹 사이트에서 빈번하게 발생
- ▶ 사설 인증서, 유효 기간 만료, 웹 사이트 주소와 발급된 인증서 주소 미 일치, 인가되지 않은 Certificate authority 등 약 30 여가지 타입에 대한 Invalid 인증서 검출



02 AISWG 소개 및 특징점

◆ SSL 연결 프로토콜 지정

- ▶ 특정 서버로 향하는 SSL 프로토콜 버전 지정 가능
 - 지정된 외부 서버와 SSL 협상에 사용되는 SSL 프로토콜 버전을 강제로 지정할 수 있도록 기능 제공
- ▶ Proxy 타입으로 운영 되어, 내부 사용자들의 취약한 SSL 프로토콜을 대신하여 상위 SSL 프로토콜 지정 가능



02 AISWG 소개 및 특징점

◆ HTTP/2 트래픽 지원

- 외부에 서비스 되고 있는 웹 사이트들의 HTTP/2 비율은 매해 증가하고 있음
 - 2019년 5월 경 37.4% → 2020년 9월 경 **47.9%** → 2021년 4월 경 **50.8%**
- HTTP/2는 HTTP/1.1과 전혀 다른 구조의 프로토콜로 암호화(HTTPS) 통신만 지원
- HTTP/2 트래픽에 대해 완전한 Parsing 및 모든 보안 기능 동일 적용 지원

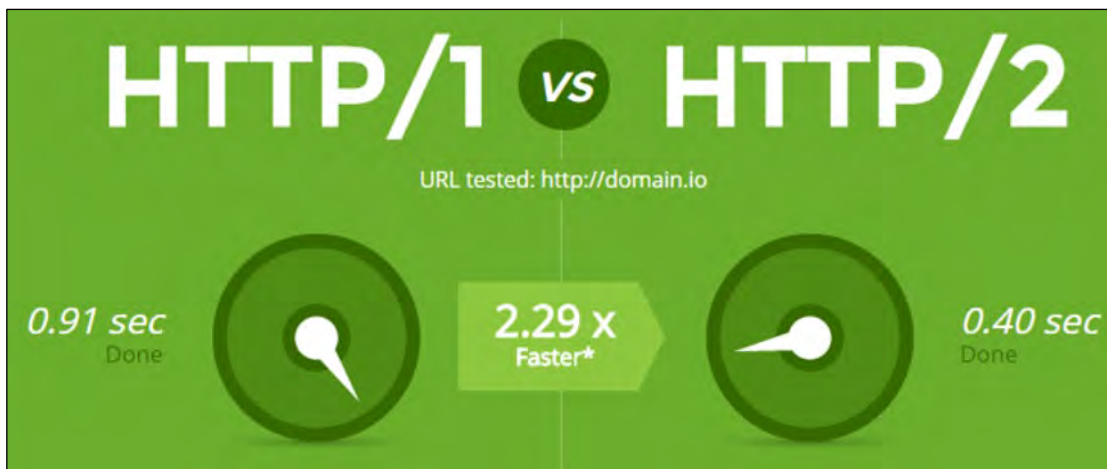
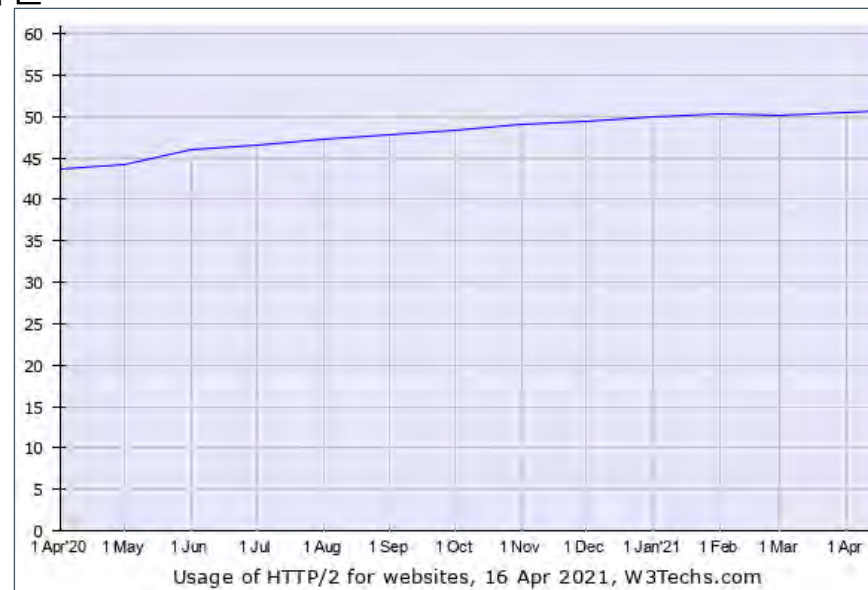


그림 출처 : <https://www.webfandom.com/introduction-http-2>

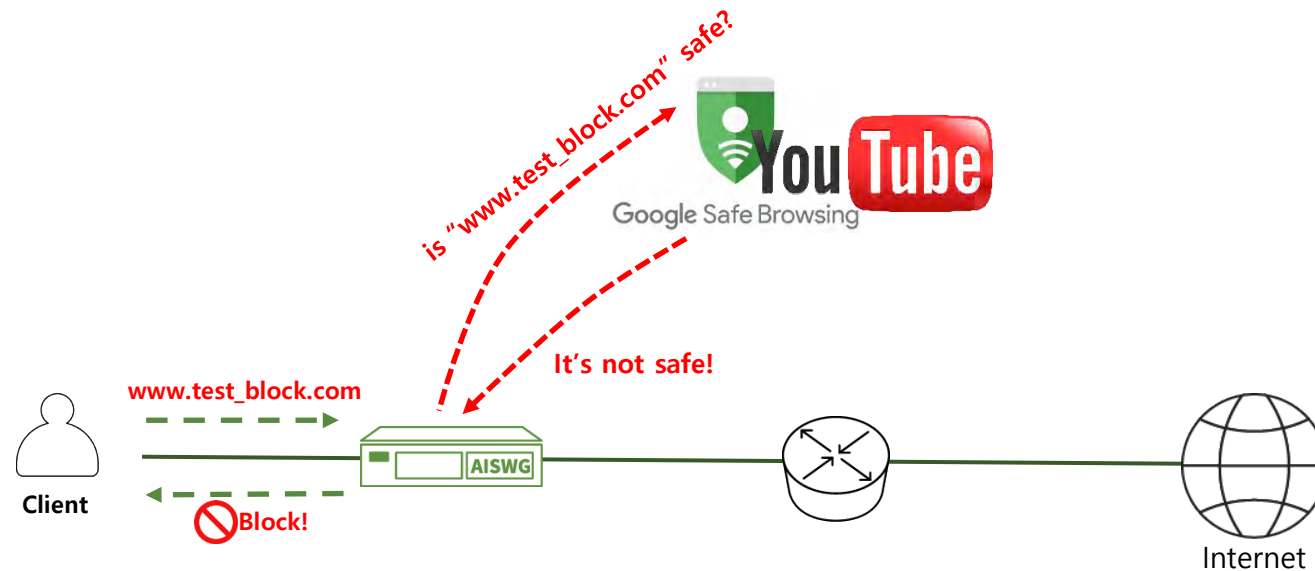


Nowadays, HTTP/2 is used by **50.8%** of all the websites.

02 AISWG 소개 및 특징점

◆ Google API 연동을 통하여 Safe Browsing, Youtube 카테고리 탐지/차단 연동 지원

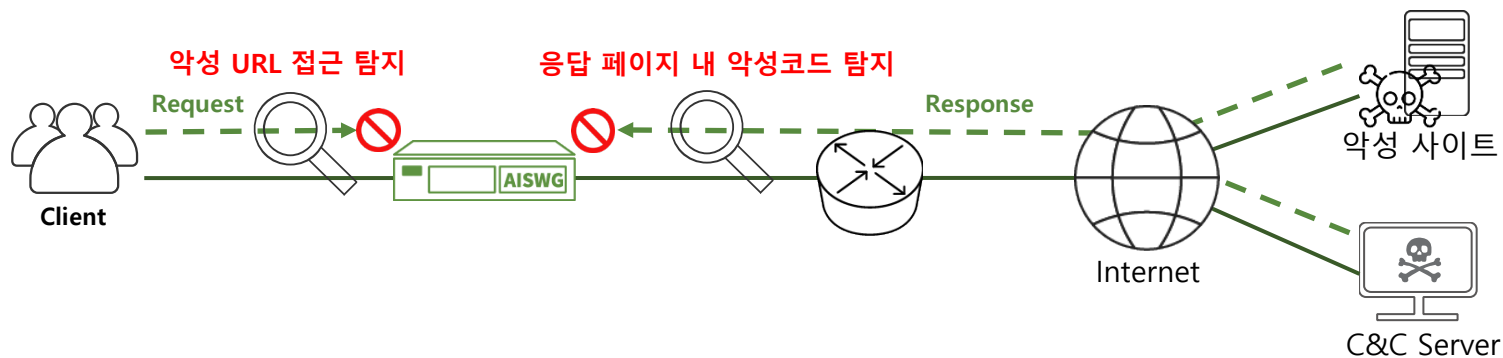
- Safe Browsing, Youtube 카테고리 분류에 사용될 API Key를 입력하여 카테고리 필터와 연동하는 가능
 - 알 수 없는 위험, 악성코드 위험, 사회 공학 위험, 원치 않는 소프트웨어 위험, 잠재적으로 유해한 응용 프로그램 위험의 5가지 Google Safe Browsing 카테고리 지원
 - 영화, 애니메이션, 자동차, 교통, 음악, 스포츠, 동물 등 다양한 Youtube 카테고리 지원



02 AISWG 소개 및 특징점

◆ 본문 데이터 내 악성코드 탐지

- URL 접근(요청) 차단 방식 외 시그니처 기반의 본문(응답) 데이터에 존재하는 악성코드 탐지 기능 제공
- 모든 웹 응답 트래픽을 검사하므로 unknown 악성사이트에 대한 효과적인 방어 수단
 - URL 접근 기반의 탐지는 known 악성사이트에 대한 제어만 가능



02 AISWG 소개 및 특징점

◆ 악성파일 분석 솔루션 연동

- 시큐레터(SecuLetter) 악성파일 분석 솔루션과 API 연동 기능 제공
- AISWG User Interface에서 WEB을 통해 오가는 모든 파일에 대한 분석 현황 및 악성 파일 탐지

SecuLetter 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

시간	클라이언트 IP	서버 IP	조직	사용자	파일명	URL	상태	결과
05-25 14:50:47	10.0.3.20	43.250.152.27	덕화조직	정덕화	006.png	https://s.pstatic.net/static/newsstand/2019/logo/00...	완료	정상
05-25 14:50:46	10.0.3.20	43.250.152.27	덕화조직	정덕화	076.png	https://s.pstatic.net/static/newsstand/2019/logo/07...	초기화	일수 없음
05-25 14:50:45	10.0.3.20	43.250.152.27	덕화조직	정덕화	croplmg_196x196_32273638602116210.jpeg	https://s.pstatic.net/static/www/mobile/edit/2020/0...	완료	정상
05-25 14:50:44	10.0.3.20	43.250.152.27	덕화조직	정덕화	croplmg_196x196_32273610600727289.jpeg	https://s.pstatic.net/static/www/mobile/edit/2020/0...	완료	정상
05-25 14:50:44	10.0.3.20	43.250.152.27	덕화조직	정덕화	312.png	https://s.pstatic.net/static/newsstand/2019/logo/31...	초기화	일수 없음
05-25 14:50:41	10.0.3.20	43.250.152.27	덕화조직	정덕화	croplmg_728x360_32273545986863300.jpeg	https://s.pstatic.net/static/www/mobile/edit/2020/0...	완료	정상
05-25 14:50:40	10.0.3.20	43.250.152.27	덕화조직	정덕화	024.png	https://s.pstatic.net/static/newsstand/2019/logo/02...	완료	정상
05-25 14:50:39	10.0.3.20	43.250.152.27	덕화조직	정덕화	nsd91458234.png	https://s.pstatic.net/static/newsstand/up/2020/0210...	완료	정상
05-25 14:50:38	10.0.3.20	43.250.152.27	덕화조직	정덕화	986.png	https://s.pstatic.net/static/newsstand/2019/logo/98...	완료	정상
05-25 14:50:22	10.0.3.20	43.250.152.27	덕화조직	정덕화	416.png	https://s.pstatic.net/static/newsstand/2019/logo/41...	초기화	일수 없음
05-25 14:50:21	10.0.3.20	43.250.152.27	덕화조직	정덕화	804.png	https://s.pstatic.net/static/newsstand/2019/logo/80...	초기화	일수 없음
05-25 14:50:20	10.0.3.20	43.250.152.27	덕화조직	정덕화	117.png	https://s.pstatic.net/static/newsstand/2019/logo/11...	완료	정상
05-25 14:50:19	10.0.3.20	43.250.152.27	덕화조직	정덕화	075.png	https://s.pstatic.net/static/newsstand/2019/logo/07...	완료	정상
05-25 14:50:18	10.0.3.20	43.250.152.27	덕화조직	정덕화	308.png	https://s.pstatic.net/static/newsstand/2019/logo/30...	초기화	일수 없음
05-25 14:50:10	10.0.3.20	43.250.152.27	덕화조직	정덕화	009.png	https://s.pstatic.net/static/newsstand/2019/logo/00...	완료	정상

02 AISWG 소개 및 특징점

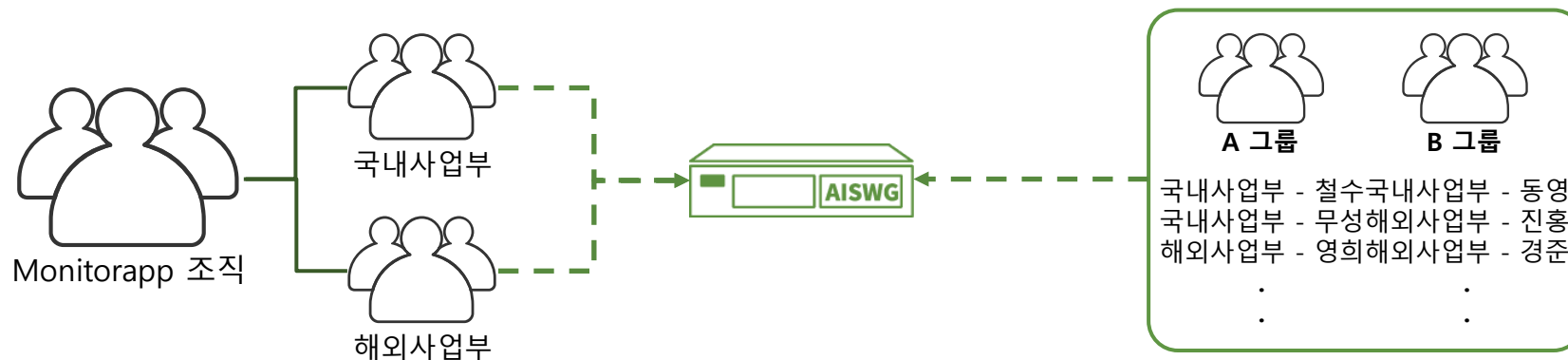
◆ 다중 사용자 그룹 관리

▶ 사용자 중심의 정책 설정

- 필요한 여러 규칙들을 조합(활성화/비활성화/예외처리 등)하여 보안 정책 생성
- 각각의 사용자 또는 그룹에 대해 생성된 보안 정책 적용

▶ 다중 사용자 그룹 관리

- 특정 조직에 대한 정책 설정 및 운영의 영향 범위가 해당 조직에 한 하도록 제한 하는 기능
- 기업의 규모가 크고 복잡하거나 관리 부서간 보안 담당자가 다른 경우 유연한 정책 설정을 위한 요소
- 다중 사용자 그룹 관리를 통해 각 조직 별 논리적으로 완전히 분리된 차등 정책 수립

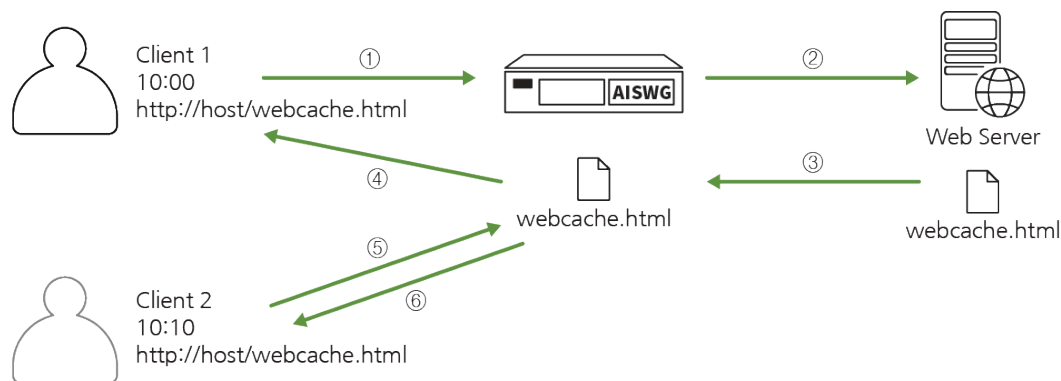


02 AISWG 소개 및 특징점

◆ 웹 캐시를 이용한 이점 제공

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

❖ 웹 캐시

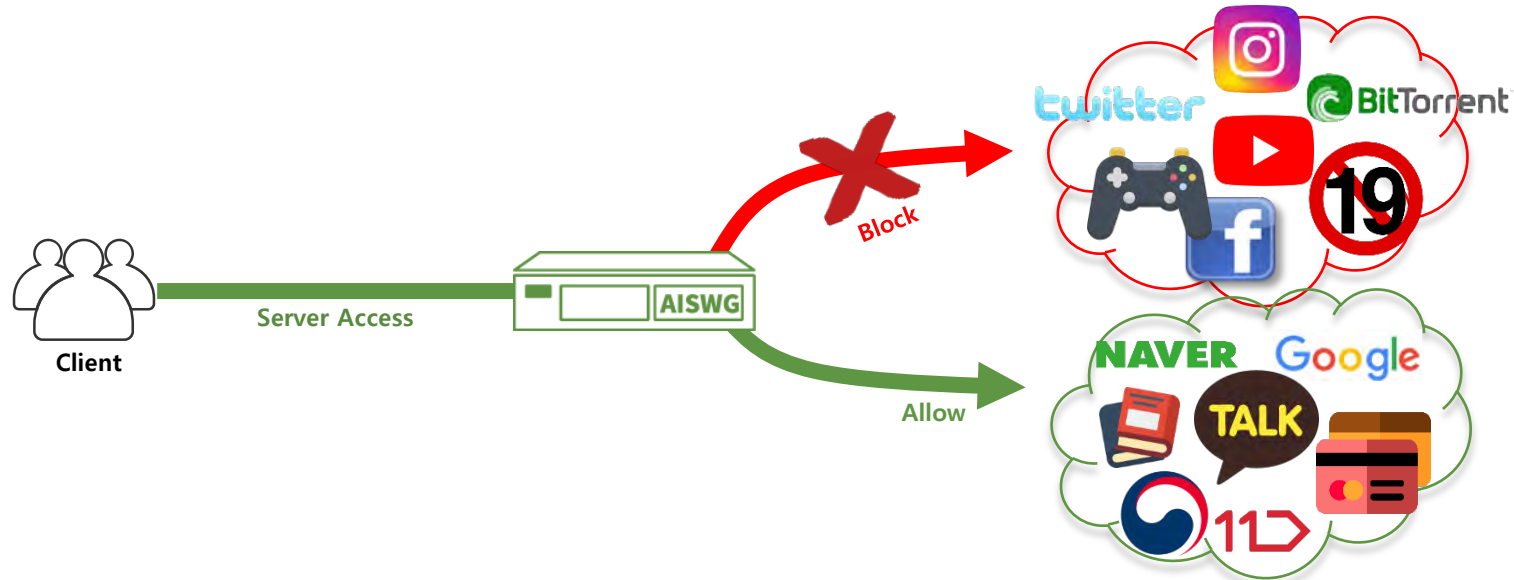


Host	Path	Cache size	Creation time	Expiration time	Request extension	Response content	Hit count
s0.2mdu.net	/590481510147020-220855495-RR-KCR_SB-01_0_160x60	112 KB	12-17 18:24:03	12-18 06:24:03	jpg	Image	0
s0.2mdu.net	/892468812072020-210431907-728x90.jpg	34 KB	12-17 18:23:58	12-18 06:23:58	jpg	Image	0
linuxconfig.org	/images/01-enable-firewall-ubuntu-18.04-gulfw.png	100 KB	12-17 18:23:58	12-18 06:23:58	png	Image	0
a802a9e378c54467a3808c391	/safe/frame1-0-37.html?container.html	4 KB	12-17 18:23:55	12-18 06:23:55	html	HTML	0
cdn.fuseplatform.net	/pub/fftags/222241prebid.js	77 KB	12-17 18:23:54	12-18 06:23:54	js	JavaScript	0
yimg.com	/v1_wetpl/linC-11VU2_0/images/default.webp	67 KB	12-17 18:23:52	12-18 06:23:52	webp	Image	0
linuxconfig.org	/images/linuxconfig_logo.png	3 KB	12-17 18:23:50	12-18 06:23:50	png	Image	0
linuxconfig.org	/images/banners/linuxcareers-get-alert_optim.png	12 KB	12-17 18:23:50	12-18 06:23:50	png	Image	0
cdn.fuseplatform.net	/pub/fftags/222241fuse.js	18 KB	12-17 18:23:48	12-18 06:23:48	js	JavaScript	0
cdn-17800.kocdn.com	/templates/ll_headlines/images/bgreset5.png	4 KB	12-17 18:23:48	12-18 06:23:48	png	Image	0
2e3edcd8a8de590291f8e3892	/safe/frame1-0-37.html?container.html	4 KB	12-17 17:57:33	12-18 05:57:33	html	HTML	0
cdn.mos.cms.futurecdn.net	/PmBudsms/PwGfR5vlpG4PU-970-80.jpg.webp	23 KB	12-17 17:53:10	12-18 05:53:10	webp	Image	0
s.wildapricot.net	/Static/images/v2/FontAwesomeIcon/gethelp/favicon.ico	15 KB	12-17 17:32:50	12-18 05:32:50	ico	Image	0
s.wildapricot.net	/Scripts/v1/00/Combined.js	71 KB	12-17 17:32:48	12-18 05:32:48	js	JavaScript	0
cdn.elevio	/file/uploads/2a29235c9aydw8KGTML1DUg7H0h1K0Y19q3	78 KB	12-17 17:32:47	12-18 05:32:47	jpg	Image	0

3. 비업무사이트 차단과 웹 어플리케이션 제어

03 비업무사이트 차단과 웹 어플리케이션 제어

◆ 비 업무 사이트 및 악성 사이트 제어



- ### ➡ 악성 사이트 접속 차단
- 14개의 악성카테고리 분류(Google Safe Browsing 포함)
 - 실시간 악성 URL정보 업데이트
 - 악성 URL 접근 차단 및 악성 URL 포함 첨부파일 차단

- ### ➡ 업무 및 비 업무 사이트 통제
- 57개 카테고리 분류에 따른 금융, 포탈, 블로그 등의 비 업무 트래픽 통제
 - 조직/사용자별 차등 정책 적용을 통한 유연한 정책 수립

03 비업무사이트 차단과 웹 어플리케이션 제어

◆ 다양한 비 업무 및 우회 어플리케이션 제어

- ▶ 파일 전송, 원격접속, VPN, Game, SNS, Mail, Messenger 등 22개 그룹으로 분류된 약 1,000 여개 어플리케이션 제어
- ▶ 기본 제공 어플리케이션 목록 외 사용자 정의 어플리케이션 등록 지원
- ▶ 매월 1회 온라인 어플리케이션 DB 업데이트 제공



메신저, SNS



파일전송, 웹 하드



우회(VPN)/원격 프로그램



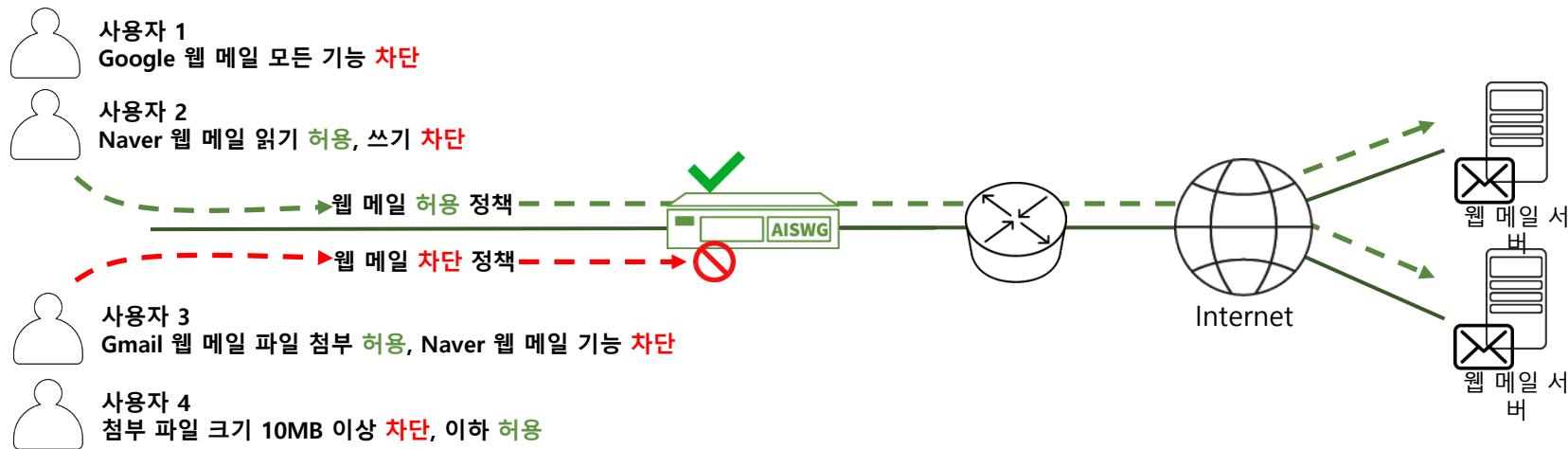
Cloud APPs

...

03 비업무사이트 차단과 웹 어플리케이션 제어

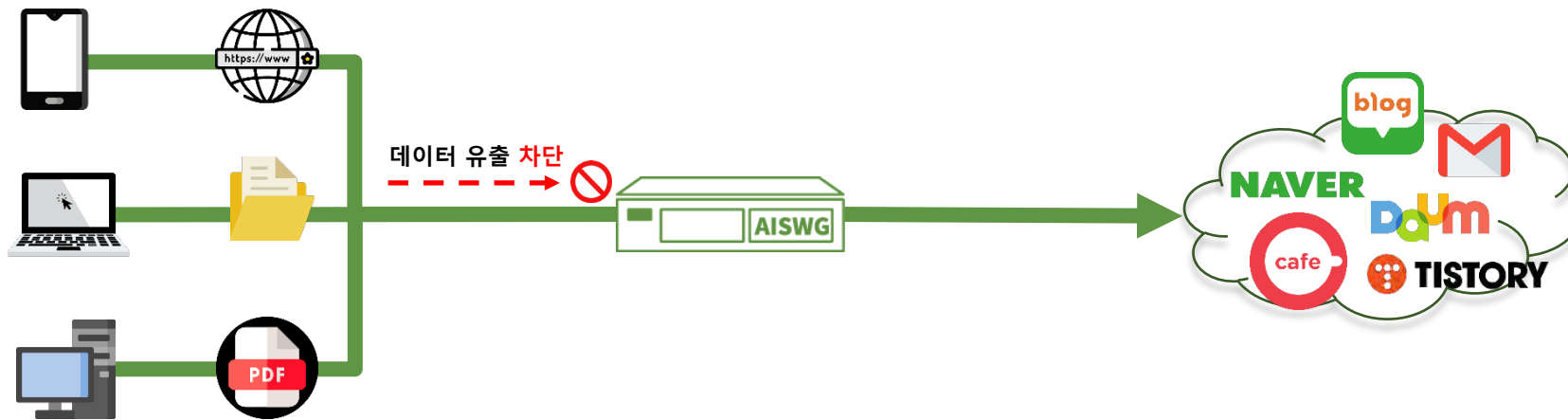
◆ 상용 웹 메일 서비스 로깅 및 기능 별 통제

- ▶ Naver, Daum, Nate, Gmail, Hotmail 5대 상용 웹 메일 서비스 로깅 및 기능 별 통제 완벽 지원
- ▶ 단순 웹 메일 사이트 접근 차단 방식이 아닌, "송/수신 웹 메일 로깅" 및 "읽기", "쓰기", "첨부파일 제한", "키워드 제한" 등 내부 사규에 따른 웹 메일 기능 별 통제



03 비업무사이트 차단과 웹 어플리케이션 제어

◆ WEB을 이용한 데이터 유출 방지



➤ 유출 경로 예방

- 웹 메일을 통한 데이터 유출 방지
- 게시판이나 웹 하드 등 웹을 통한 파일 업로드 탐지
- 키워드, 파일 사이즈 제어 등을 통한 데이터 유출 방지
- 악성코드 감염에 의한 PC 내 데이터 유출 방지

➤ DLP 보안 규칙 수립

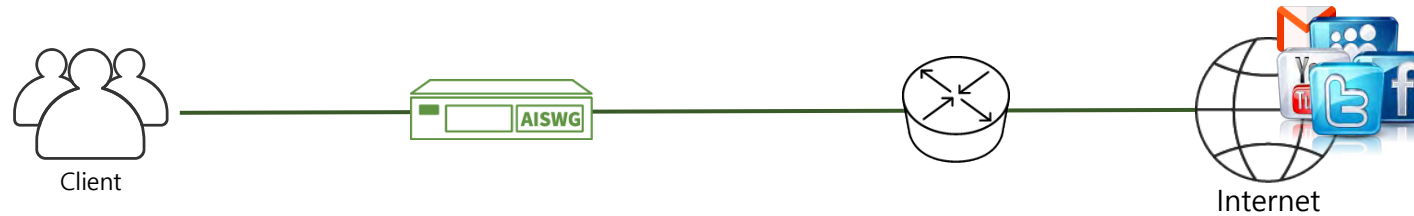
- SSL 트래픽 탐지 및 제어 가능
- 주민등록번호, 운전면허번호, 휴대폰 번호 등 8개 기본 템플릿 제공
- 첨부파일 및 압축파일을 이용한 개인정보 업로드 시에도 제어 가능
- 사용자 정의 키워드 및 정규 표현식 등록 지원

4. 다양한 구축 방안과 연동 사례

04 다양한 구축 방안과 연동 사례

◆ Proxy base Full Transparent 모드

- ▶ APPLICATION INSIGHT SWG는 별도의 IP 부여 없이 Stealth-mode로 운영
 - 기존 네트워크 구성 환경 변화 없음
- ▶ 하드웨어 자체 바이패스 기능 모듈 장착하여, 시스템 이상 발생 시 물리적 바이패스 기능 제공
 - Fail-Open / Fail-Close 선택 가능



04 다양한 구축 방안과 연동 사례

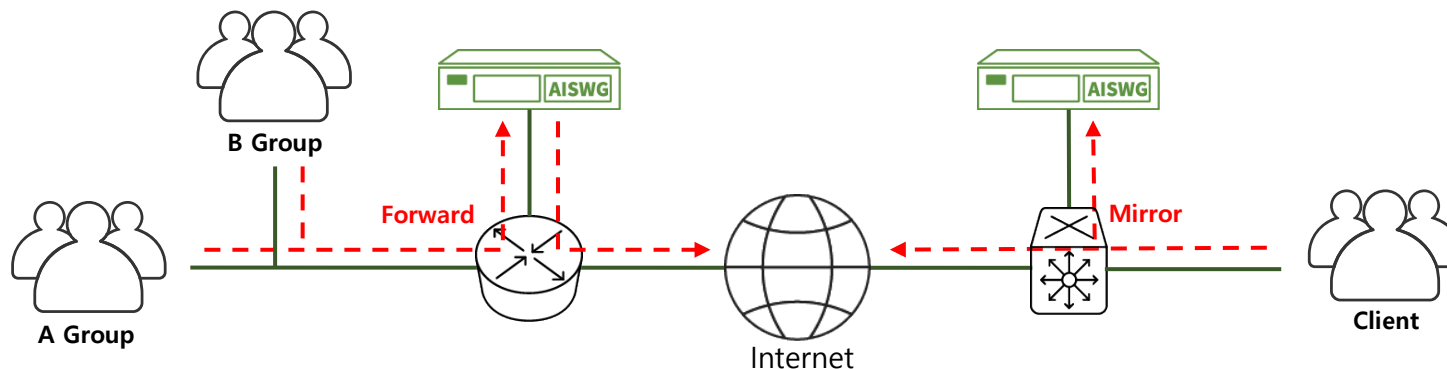
◆ 다양한 네트워크 구성 환경 지원

▶ 포워드 프록시 모드 구성 지원

- 프록시 서버의 중간 서버 역할로, 시스템 위치와 무관하게 AISWG 경유를 유도할 수 있도록 분산 패치 되어 있는 다양한 클라이언트들에 대하여 광범위한 보호 제공
- PAC(Proxy Auto Config) 기능 제공

▶ 미러링(Mirroring), 스니핑(Sniffing) 모드 제공

- 복사된 패킷을 받거나(Mirroring), 스니핑을 통하여 Proxy 특성으로 발생 가능한 이슈를 최소화 하며, SSL 트래픽 복호화는 불가하나, SNI(Server Name Indication)를 통하여 https 접근 탐지 혹은 차단 가능

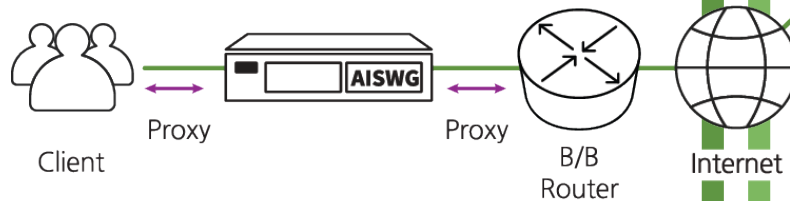


04 다양한 구축 방안과 연동 사례

◆ 다양한 네트워크 구성 방식[1/2]

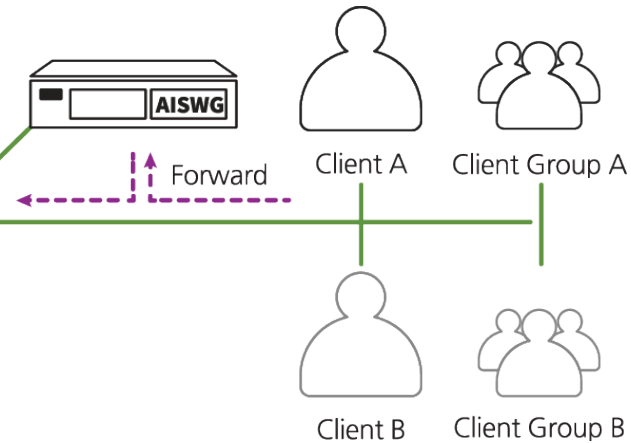
Transparent Proxy(IN-Line)

- 운영 모드: Transparent Proxy
- 물리적 구성: IN-Line
- 네트워크 경로상에 Bridge 형태로 In-line 구성
- IP가 없는 Transparent Proxy Mode로 작동
- SSL 트래픽 제어 완벽 지원
- 구축 레퍼런스 중 70% 구성 방식



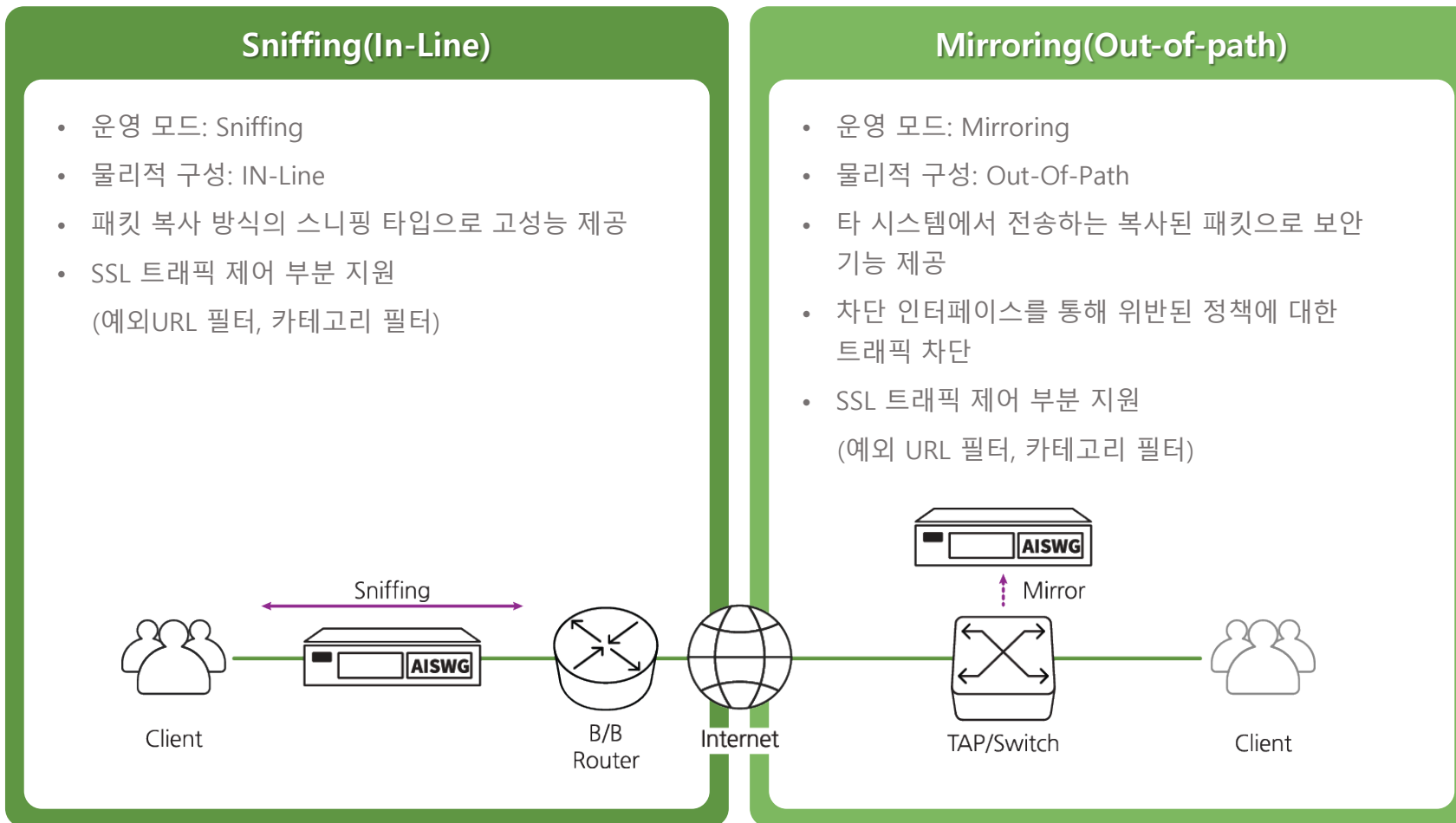
Port Redirection(Out-of-path)

- 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)
- SSL 트래픽 제어 완벽 지원



04 다양한 구축 방안과 연동 사례

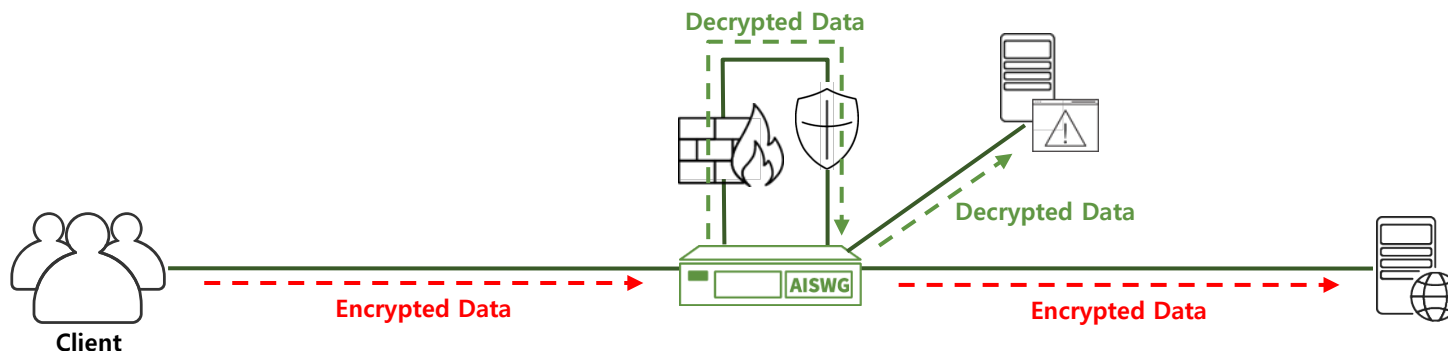
◆ 다양한 네트워크 구성 방식[2/2]



04 다양한 구축 방안과 연동 사례

◆ 암호화 된 SSL/TLS 트래픽 복호화를 통한 타 보안 시스템 보안 능력 극대화

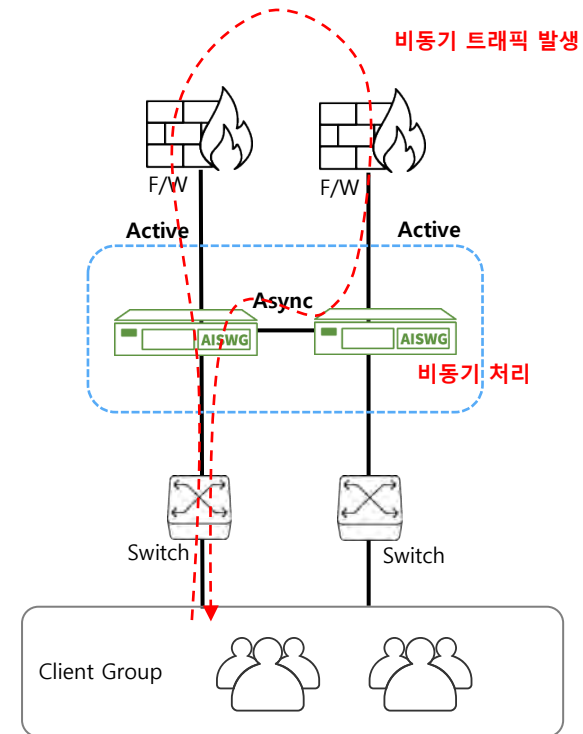
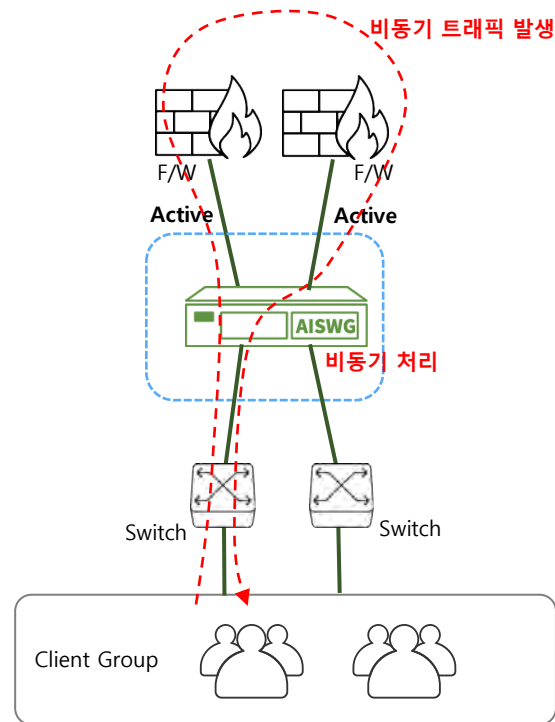
- 별도의 추가 시스템 없이 AISWG에서 SSL/TLS 트래픽 복호화 지원하며 복호화 트래픽을 3rd party 솔루션(들)로 전송
- Active Inline 모드로 Inline 복호화 구간 형성
 - SSL/TLS 복호화가 불가능한 보안 시스템 군을 AISWG의 Active 포트와 인라인으로 연결하여 복호화 된 트래픽을 송수신 하기 위한 구성
 - 암호화 된 트래픽에 대해 보안 정책을 적용하지 못하는 보안 시스템과 연동하여 보안 능력 극대화
- Passive Mirroring 기능
 - 복호화 한 트래픽을 Mirroring 하여 다양한 형태의 시스템과 연동 지원
 - Active Inline 모드와 동시 사용 가능



04 다양한 구축 방안과 연동 사례

◆ 비동기 트래픽 환경 지원

- ▶ 단일 장비 멀티세그먼트 구성에서 발생하는 비동기 트래픽 처리
- ▶ 이중화 구성에서 발생하는 비동기 트래픽 처리



04 다양한 구축 방안과 연동 사례

◆ AISWG 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	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port	8 Slot - 1G UTP 4Port - 1G Fiber 4Port - 10G Fiber 2Port
Recommended users base on web traffic	100M 200	500M 1,000	1G 5,000	1G 10,000	1G 20,000	1G 40,000
Recommended web Traffic based on users	200M 100	750M 700	1G 5,000	2G 7,000	3G 10,000	4G 10,000
Max WEB Bandwidth	1G	2G	5G	7G	8.5G	10G
Max RPS(TPS)	30,000	50,000	100,000	150,000	200,000	300,000

• 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.

THANK YOU & Q/A

(주)모니터랩

서울시 구로구 디지털로 27가길 27 아남빌딩 9층 (우) 08375

Tel : 02-749-0799 | Email : tech_support@monitorapp.com

Website : <https://www.monitorapp.com>

Partner Portal : <https://partner.monitorapp.com>

(주) 동훈아이텍

서울시 강남구 역삼로 225 동훈빌딩 3F / 6F

Tel : 580 6300 | Email : support@dhitech.co.kr

FAX : 538-3241

Website : <https://www.dhitech.co.kr>

MONITORAPP

dh DONGHOON
동훈아이텍