TIBS(Threat IP Blocking System)

대용량 위협 IP 통합 관리 전략 소개

2018. 12. 13(목)

Keysight IXIA Group

김종우 부장(chris.kim@keysight.com)

1. 왜 수많은 위협 IP 차단 리스트가 존재 하는가?

위협 사이트의 증가로 인한 보안 강화 필요성 증가

활개치는 피싱사이트, 최근 5년간 2배 이상 늘었다

좋아요 4개 | 입력 : 2018-10-08 10:55

#피싱사이트 #사칭 #보이스피싱 #피싱범죄 #개인정보

최근 5년 간 금융기관 등 사칭하는 '피싱사이트' 탐지·차단 건수
정부기관, 금융기관, 포털 로그인 페이지, 가상화폐 이관 사이트
올 상반기 보이스피싱 피해액 1,800억에 달하는 등 피싱범죄로

[보안뉴스 원병철 기자] 가짜 포털 사이트 로그인 홈페이지가
운데, 실제 정부기관이나 금융기관 사이트를 사칭·모방하는 피
타났다. 바른미래당 신용현 의원(국회 과학기술정보방송통신위
은 자료에 따르면 2013년부터 올 7월까지 탐지·차단된 피싱사이

▲금융감독원을 사칭한 피싱사이트[자료

구체적으로 2013년 5,000여 건이었던 피싱사이트 탐지·차단
했으나, 2017년 전년 대비 2.4배 이상 늘어난 10,469건의 피

웹사이트 침해사고 주역 3인방, 예방법은?

좋아요 32개 | 입력 : 2018-07-05 10:49

#정보보호의 달 #홈페이지 변조 #웹사이트 침해사고 #악성코드 유포 #디페이스 해
취약점 #디도스 공격 #WebDAV #웹서버

홈페이지 주요 공격 이슈: 홈페이지 변조, 악성코드 유포, 디도스 공격
WebDAV·파일 업로드 취약점 이용 및 자바, IE 등 복합 취약점 이용해 악성 스크립트 실
WebDAV 서비스 중지, 파일 업로드 제한, 중요파일 백업, 웹서버 보안 강화해야

[보안뉴스 김경애 기자] 최근 웹사이트 침해사고가 끊이지 않고 발생하고 있다. 그중에
리로 사이트가 해킹당해 웹사이트 메인 화면이 변조되거나, 악성코드를 유포하는 사고
고 있다. 보안뉴스에서는 7월 둘째 주 수요일 '정보보호의 날'을 맞아 사용자들이 가장 주
사고의 종류와 예방법에 대해 살펴본다.

▲중국 해커조직의 홈페이지 변조 공격 화면[이미지=한국인터넷진흥원]

"국내 웹사이트 홈페이지 변조 해킹 피해 매년 증가"

조선비즈 | 김범수 기자

입력 2018.10.02 14:23

국내 웹사이트 홈페이지 변조 해킹 피

2일 국회 신용현 바른미래당 의원(과학
로부터 제출받은 자료에 따르면 국내
이상씩 증가해 3000건이 넘는 것으로

자료 출처 한국인터넷진흥원(KISA). /신

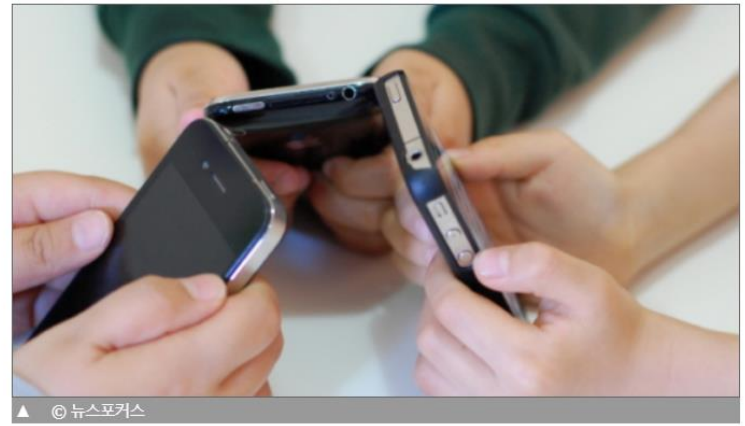
최근 3년간 홈페이지 변조 해킹 피해
건으로 72% 늘었다. 2017년에는 1724
건수는 390건이다.

홈페이지 변조는 KISA에서 전 세계 홈
니터링을 통해 국내 홈페이지 변조 확

청소년 27%, 모바일로 불법·유해사이트 방문

허승혜 | 기사입력 2018/01/12 [09:04]

트위터 페이스북 카카오톡 +가 -가



▲ © 뉴스포커스

국내 10대 청소년 10명 중 3명가량은 모바일 기기를 이용해 불법·유해정보 사이트에 접속하는 것으로 나타났다.

12일 방송통신심의위원회가 발간한 '2017년 인터넷 불법·유해정보 실태조사' 보고서에 따르면 조사 대상 10대 중 27%가 모바일 기기로 불법·유해 사이트에 접속했다.

이는 20대(12.1%), 30대(9.2%), 40대(6.4%), 50대 이상(8.2%) 등 성인보다 월등히 높은 비율이다. 10대 이하도 3.7%나 됐다.

불법·유해 앱을 모바일 기기로 이용한 비율도 10대(8.3%)와 10대 미만(4.5%)이 다른 연령대보다 가장 높았다. 보고서는 "불법·유해정보가 청소년 및 유·아동에게 미치는 악영향을 고려해보면 심각한 문제"라고 지

점차 늘어가는 Bot 트래픽

Malicious Bots by Type

Scrapers

The Damage

- Content theft and duplication.
- Theft of email addresses for spam purposes.
- Reverse engineering of pricing and business models.

The Target

Anyone.
Most commonly travel industry websites, classifieds, news sites, e-stores and forums.

Hacking Tools

The Damage

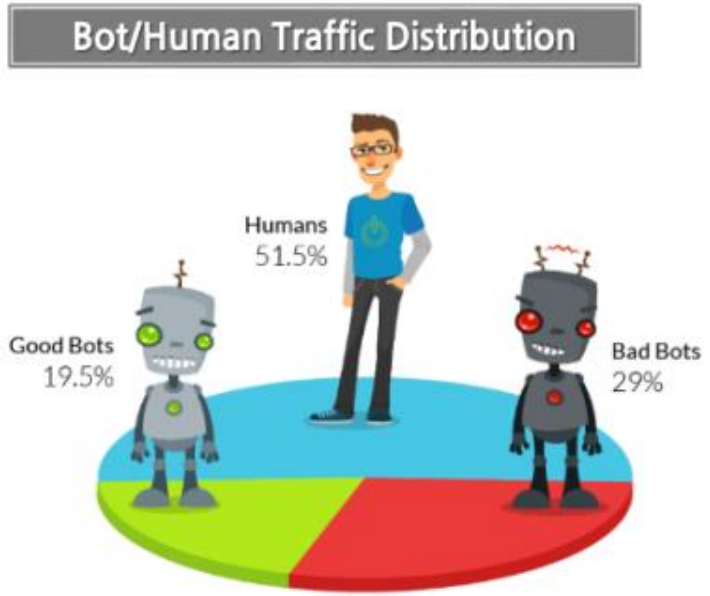
- Data (e.g. credit card) theft.
- Malware injection and distribution.
- Website/Server hijacking.
- Website defacement and content deletion.

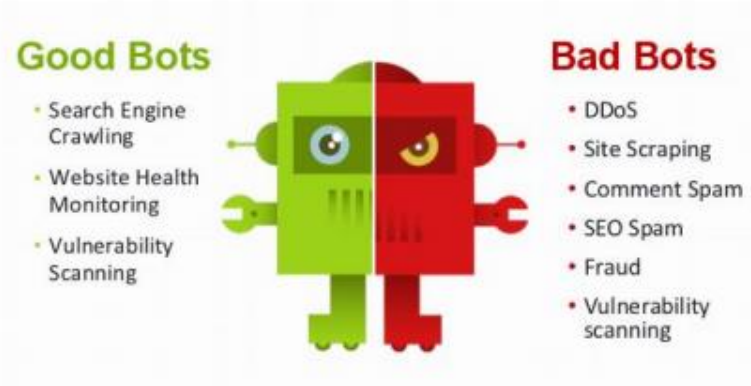
The Target

Anyone.
Most commonly CMS based websites (WP, Joomla, Vbulletin, Magento, etc.)

© Incapsula

전체 인터넷 트래픽 중 48% 이상이 Bot에 의한 트래픽*





* Bot traffic Report 2016 – Imerva
(Source : https://www.incapsula.com/blog/bot-traffic-report-2016.html)

ixia

유해 사이트/봇으로 인한 위협 IP의 증가

"지능적인 위협은 기하급수적으로 늘어나고 있다"

신규 기술 분석:

현재의 위협 지표를 기반으로 분석 한 결과, 위협을 주는 IP는 수십만개를 초과할 수 있다. 이 수치는 전통적인 보안 솔루션이 수용 가능한 성능을 훨씬 초과한다.

Gartner®

Source: Gartner Emerging Technology Analysis: Threat Intelligence Gateways - Nov, 2017

ixia

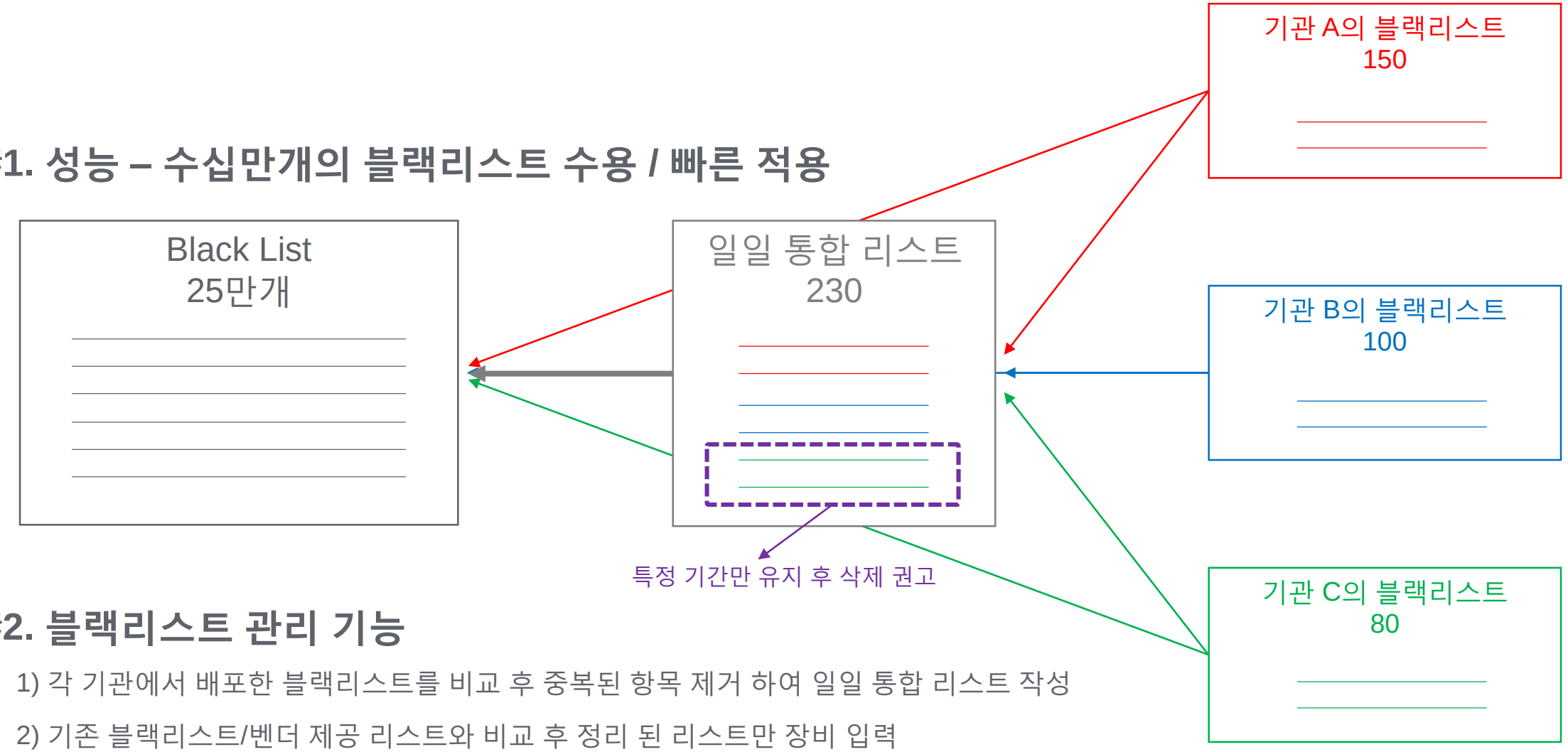
알려진 **위협 IP**에 대한 보안 기관들의 **차단 권고**

새로운 솔루션의 필요성 대두

Gartner

“위협 IP” 통합 관리를 위해 필요한 사항은 무엇인가?

#1. 성능 – 수십만개의 블랙리스트 수용 / 빠른 적용



#2. 블랙리스트 관리 기능

1) 각 기관에서 배포한 블랙리스트를 비교 후 중복된 항목 제거 하여 일일 통합 리스트 작성

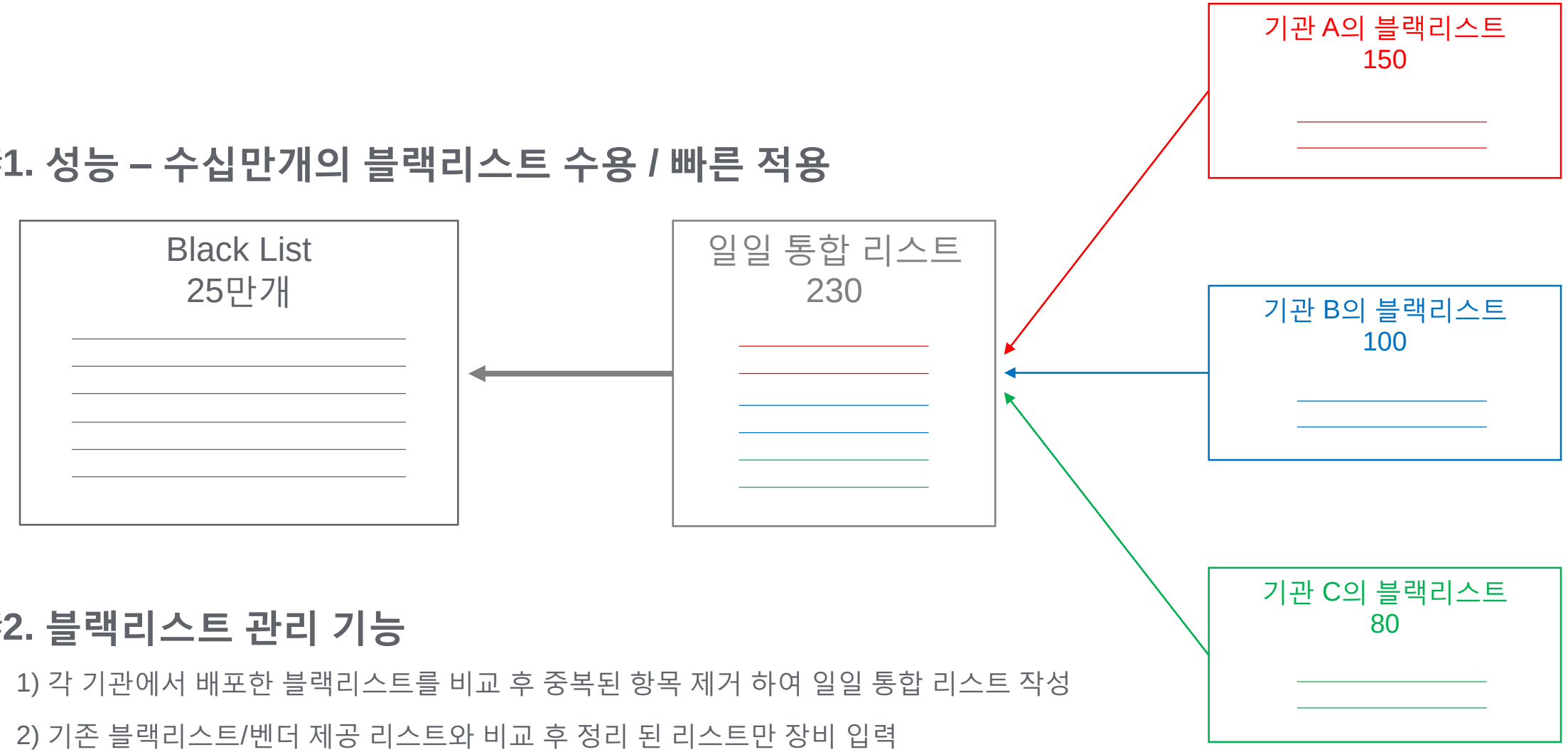
2) 기존 블랙리스트/벤더 제공 리스트와 비교 후 정리 된 리스트만 장비 입력

3) 경우에 따라서 특정 기관의 블랙리스트는 일정 기간 적용 후 삭제 권고

ixia

“위협 IP” 통합 관리를 위해 필요한 사항은 무엇인가?

#1. 성능 – 수십만개의 블랙리스트 수용 / 빠른 적용



#2. 블랙리스트 관리 기능

1) 각 기관에서 배포한 블랙리스트를 비교 후 중복된 항목 제거 하여 일일 통합 리스트 작성

2) 기존 블랙리스트/벤더 제공 리스트와 비교 후 정리 된 리스트만 장비 입력

3) 경우에 따라서 특정 기관의 블랙리스트는 일정 기간 적용 후 삭제 권고

ixia

“위협 IP” 통합 관리를 위해 필요한 사항은 무엇인가?

#1. 성능 – 수십만개의 블랙리스트 수용 / 빠른 적용

#2. 블랙리스트 관리 기능

1) 각 기관에서 배포한 블랙리스트를 비교 후 중복된 항목 제거 하여 일일 통합 리스트 작성
2) 기존 블랙리스트/벤더 제공 리스트와 비교 후 정리 된 리스트만 장비 입력
3) 경우에 따라서 특정 기관의 블랙리스트는 일정 기간 적용 후 삭제 권고

#3. 리포트 기능

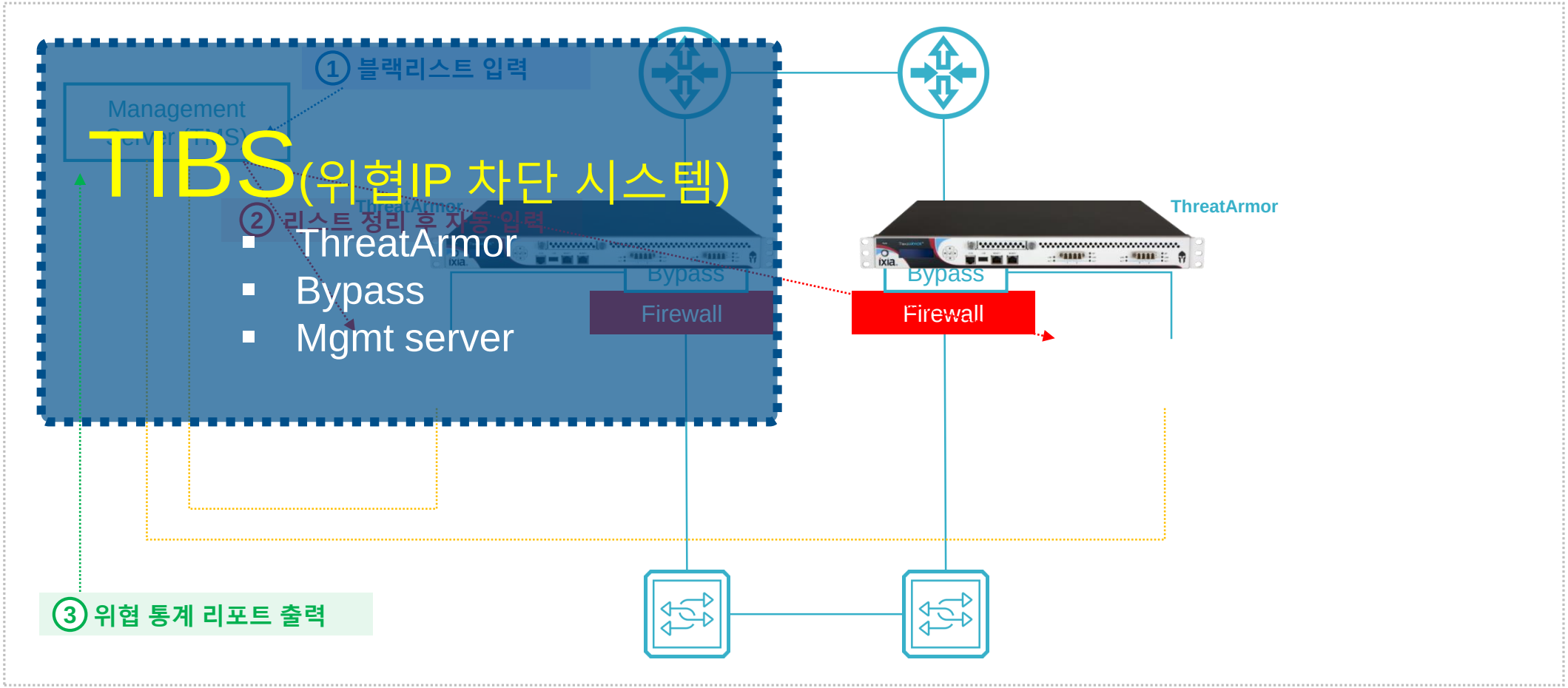
1) 원하는 기간의 차단/로그 통계 수치 리포트 작성
2) 자체 로그 분석 후, 필요한 블랙리스트 생성 후 적용
3) 일정 기간 사용되지 않는 블랙리스트는 확인 후 삭제

2. 대용량 위협 IP 차단 솔루션 소개

ixia

대용량 위협 IP 차단 시스템 : TIBS(Threat IP Blocking System)

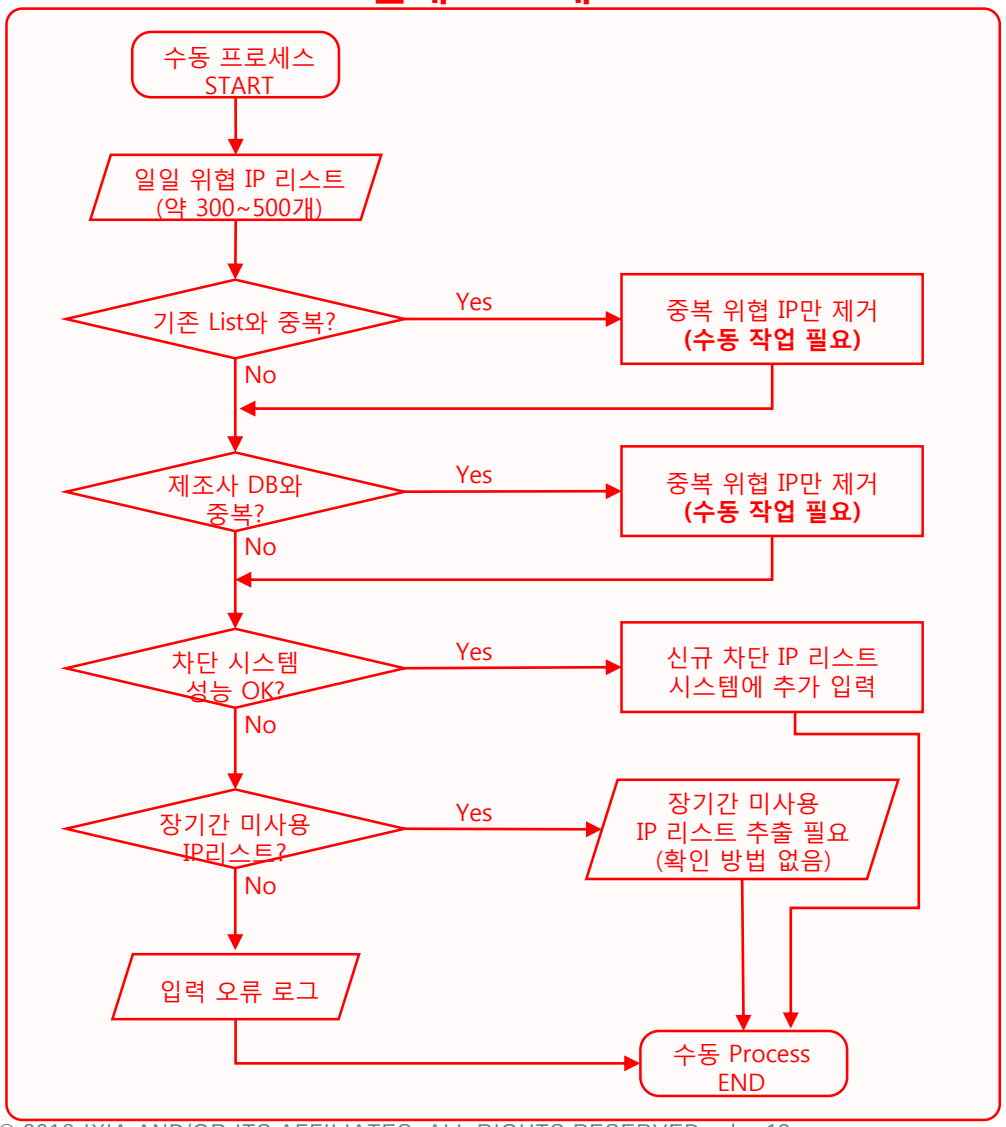
- 매일 수백 개씩 늘어나는 유해 IP 리스트를 통합 관리하기 위한 원-클릭 자동화 시스템 도입



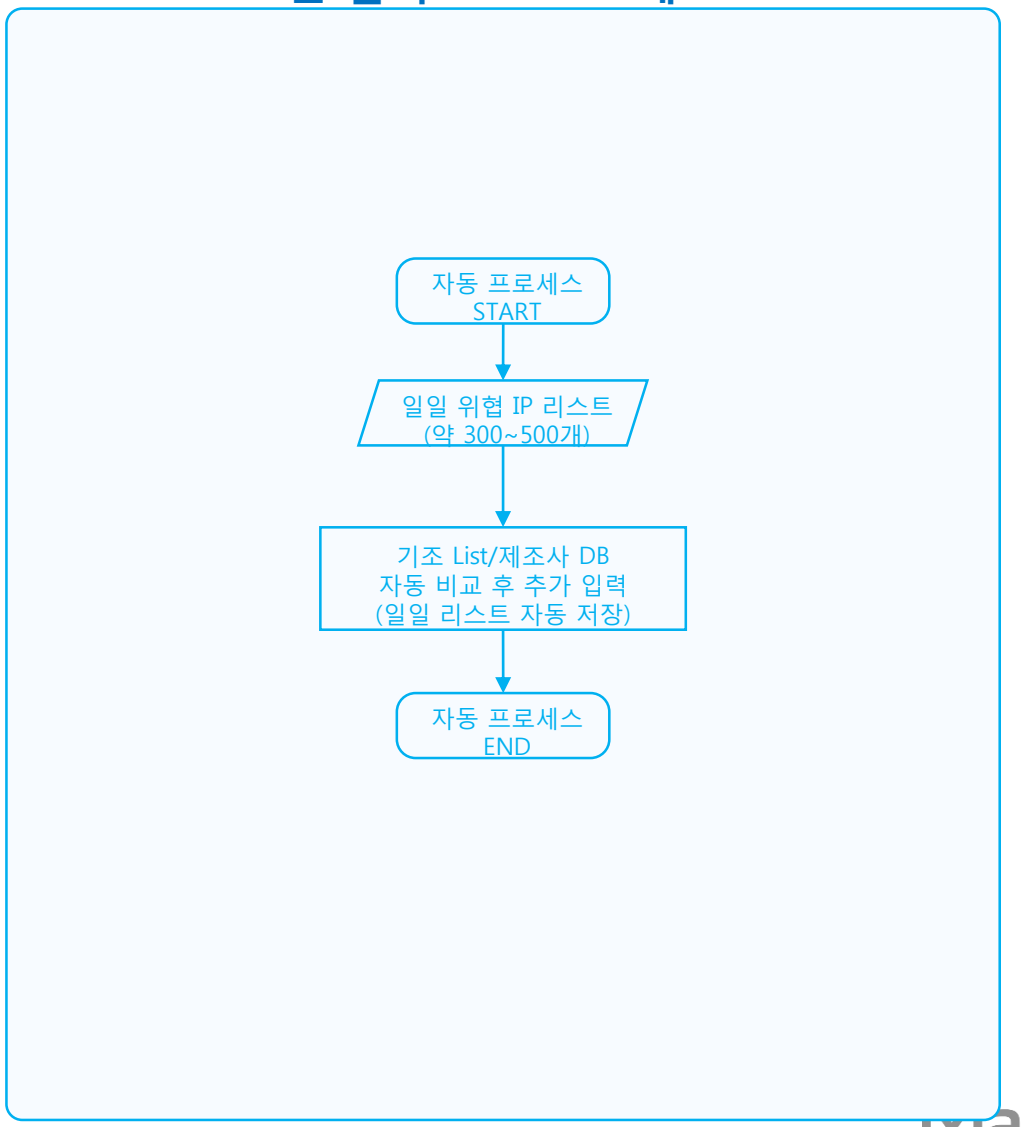
ixia

위협 IP 차단 리스트 적용 프로세스

현재 프로세스



원-클릭 TIBS 프로세스



TIBS (Threat IP Blocking System) – 대용량 위협 IP 차단 시스템

▪ 위협 IP 차단 전용 장비를 통한 업무 효율성 극대화

업무시간
최대 20* 배 감소

일회 적용 가능 IP
최대 50 배 적용**

수용 가능 IP
최대 4.3B 적용

일반 방화벽	VS	IXIA MIBS
약 100,000	**확장성** (최대 IP차단 개수)	약 4,300,000,000
신규 적용 리스트 수동 비교 후 관리 필요 기간별 관리를 위해 수동	**효율성** (위협 IP 관리 관점)	원-클릭 자동 처리 및 모든 차단 리스트 개별 저장 기간별 차단 리스트 관리(예. 3개월 후 자동 삭제)
외부 모니터링 장비 필요 (예. 바이패스 스위치)	**안정성** (장애 발생 관점)	자체 바이패스 지원
개별 장비에서 위협 IP 리스트 관리	**운영 편리성**	관리 서버로 통합 원-클릭 자동 관리

* Working hour : 기존 시스템 – 2hour/day, MIBS – 5min/day
** 일반 방화벽 : 40,000개, MIBS : 2,000,000

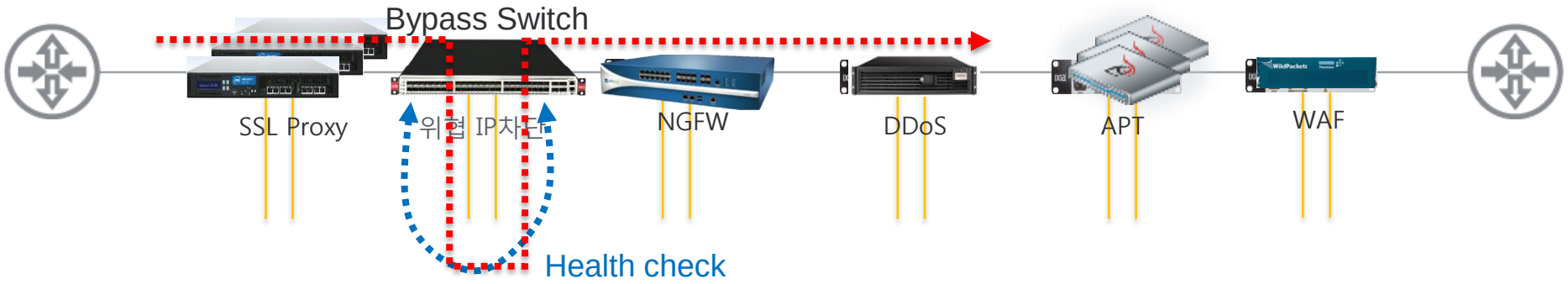
ixia

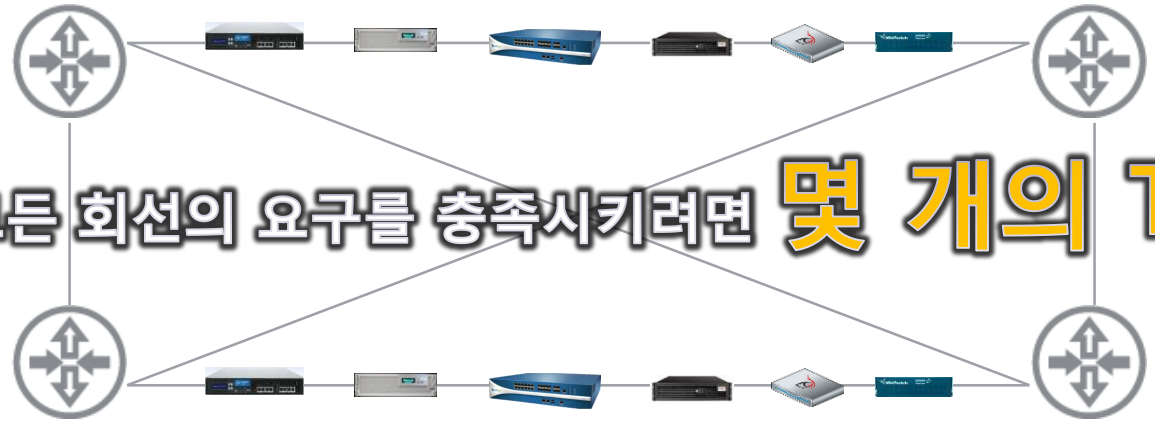
3. TIBS 도입을 위한 통합 보안 인프라 구축

ixia

CHALLENGE #1 : 너무 다양한 종류의 보안/모니터링 장비들

- Security/monitoring tool을 **Inline으로 운영**하고자 하는 요구가 증가
- 안정적인 운영을 위해서는 **외장 Bypass 장비** 요구사항이 많아짐(10G upgrade)
- **시리얼 연결**(다수의 보안 장비)에 대한 요구가 많아 짐 + **Load balancing** 필요

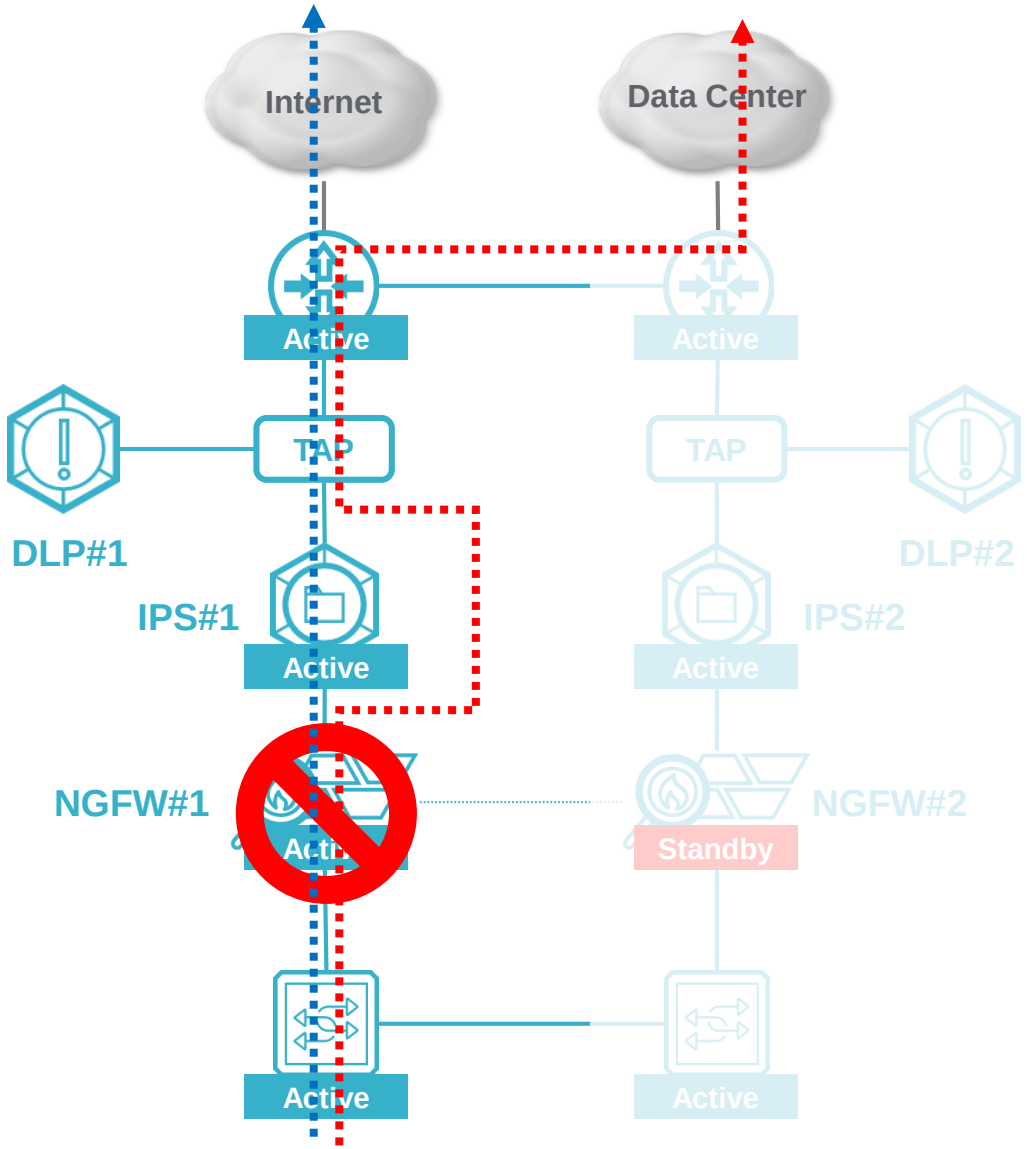




모든 회선의 요구를 충족시키려면 몇 개의 Tool이 필요한가?

ixia

CHALLENGE #2 : 네트워크 및 보안 장비의 비효율적 운영



- 하나의 보안 장비만 Active-Standby 구조여도 고가용의 Network 전체 회선이 Standby로 사용 됨
- 장비 장애 및 재부팅이 필요한 유지보수 시, 회선 전체를 Failover 필요
- 트래픽 종류 별로 별도 보안 장비를 통과하게 하는 등의 정책 적용 불가 – 성능 극대화 불가 (예. Data Center로 가는 트래픽은 IPS 우회)
- 네트워크 회선의 증설 (질적/양적 증설)
- 네트워크 프로토콜 헤더로 인한 보안장비 인지 불가 (VLAN, MPLS, TRILL, VxLAN)

ixia

ixia Security Fabric

- 차세대 보안 인프라 솔루션
- 안정성
- 확장성
- 운영편리성
- 효율성(보안장비)

구축 예제 – 다수의 보안장비에 “위협 IP” 차단 솔루션 추가 도입

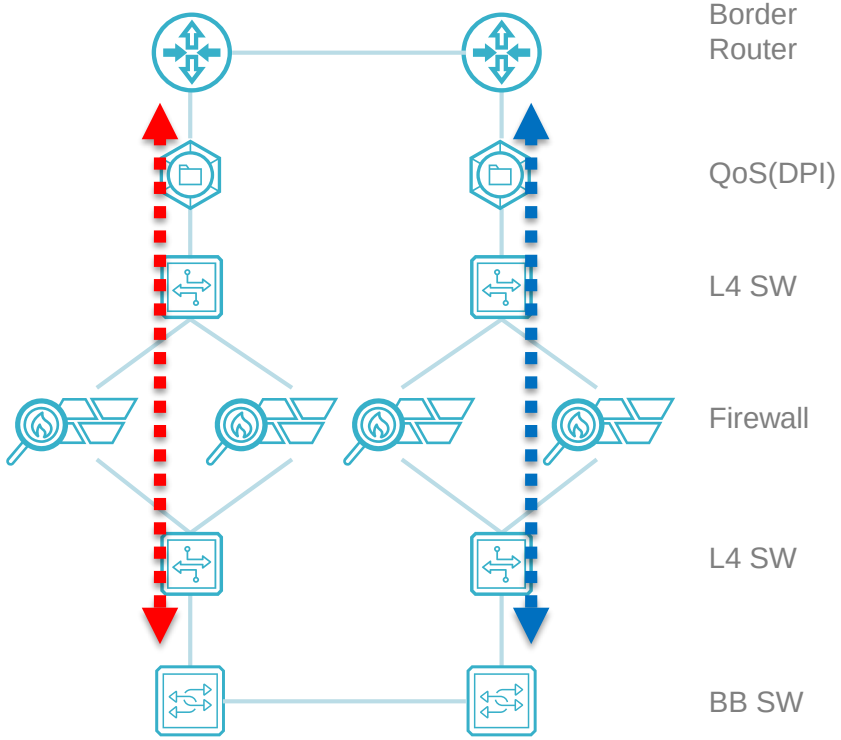
- 현재는 DPI장비, 방화벽(x2)이 Inline으로 구성 중인 상태 - **복잡한 구성**이고, **성능 저하**의 문제
- TIBS(유해IP차단), IPS, WAF 등의 **보안 솔루션 추가 계획**

추가 도입 검토 시스템들

TIBS

IPS (x2)

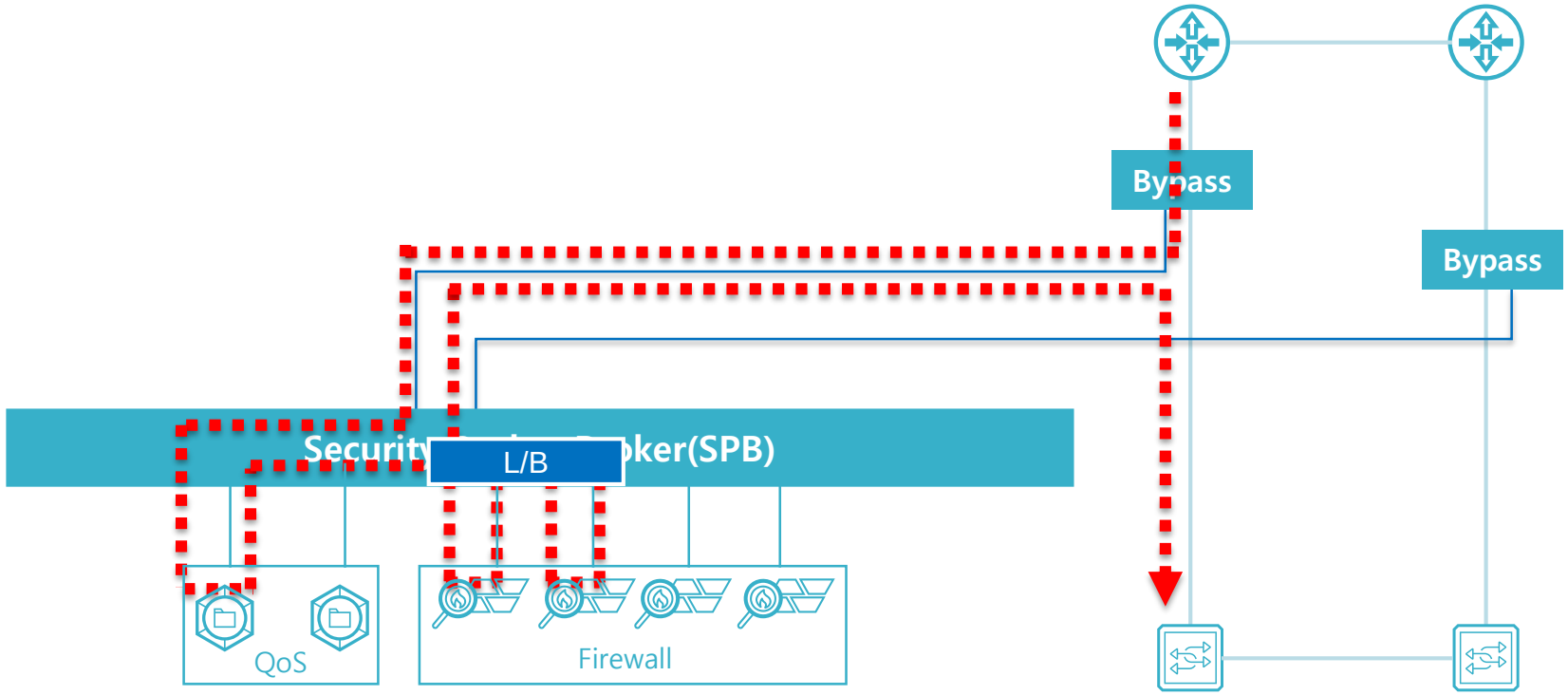
WAF



ixia

구축 예제 – 다수의 보안장비에 “위협 IP” 차단 솔루션 추가 도입

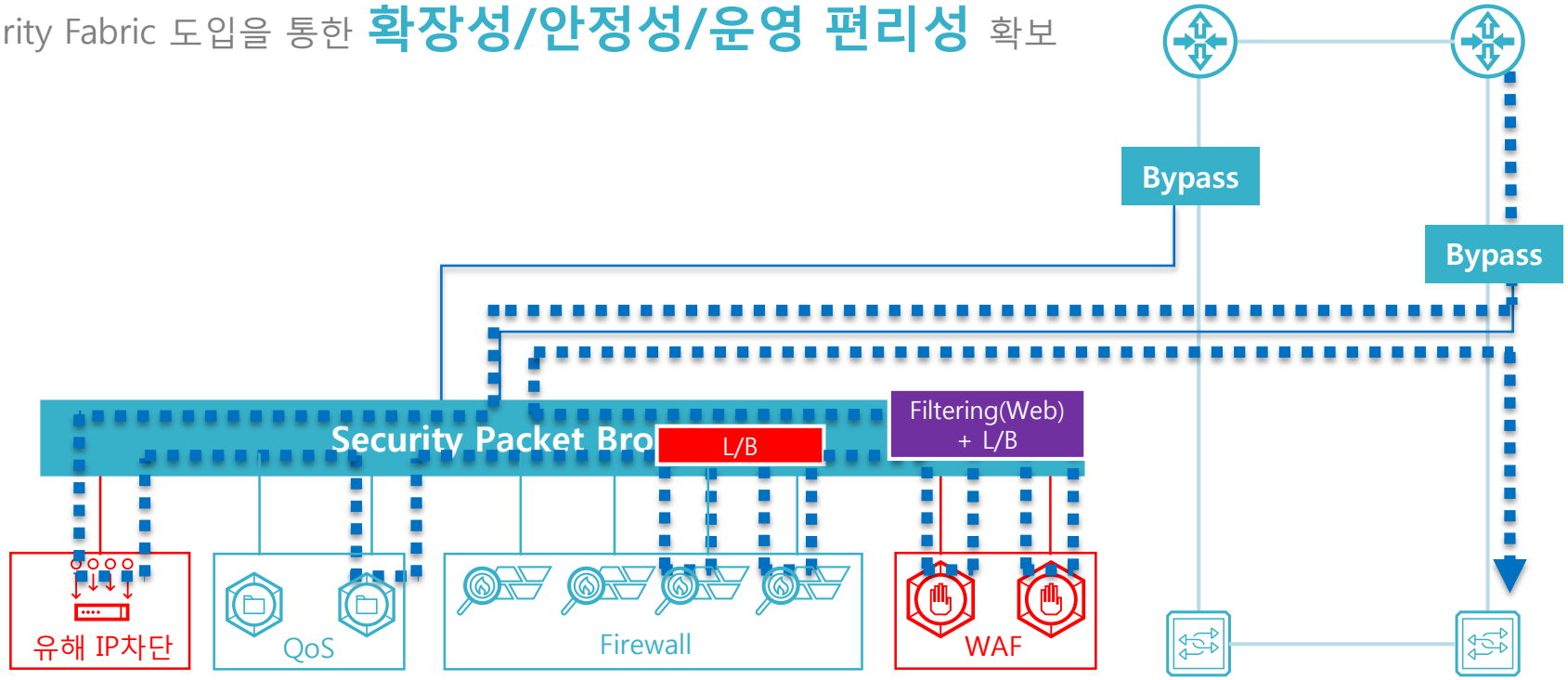
- 현재는 DPI장비, 방화벽(x2)이 Inline으로 구성 중인 상태 - **복잡한 구성**이고, **성능 저하**의 문제
- TIBS(유해IP차단), IPS, WAF 등의 **보안 솔루션 추가 계획**



ixia

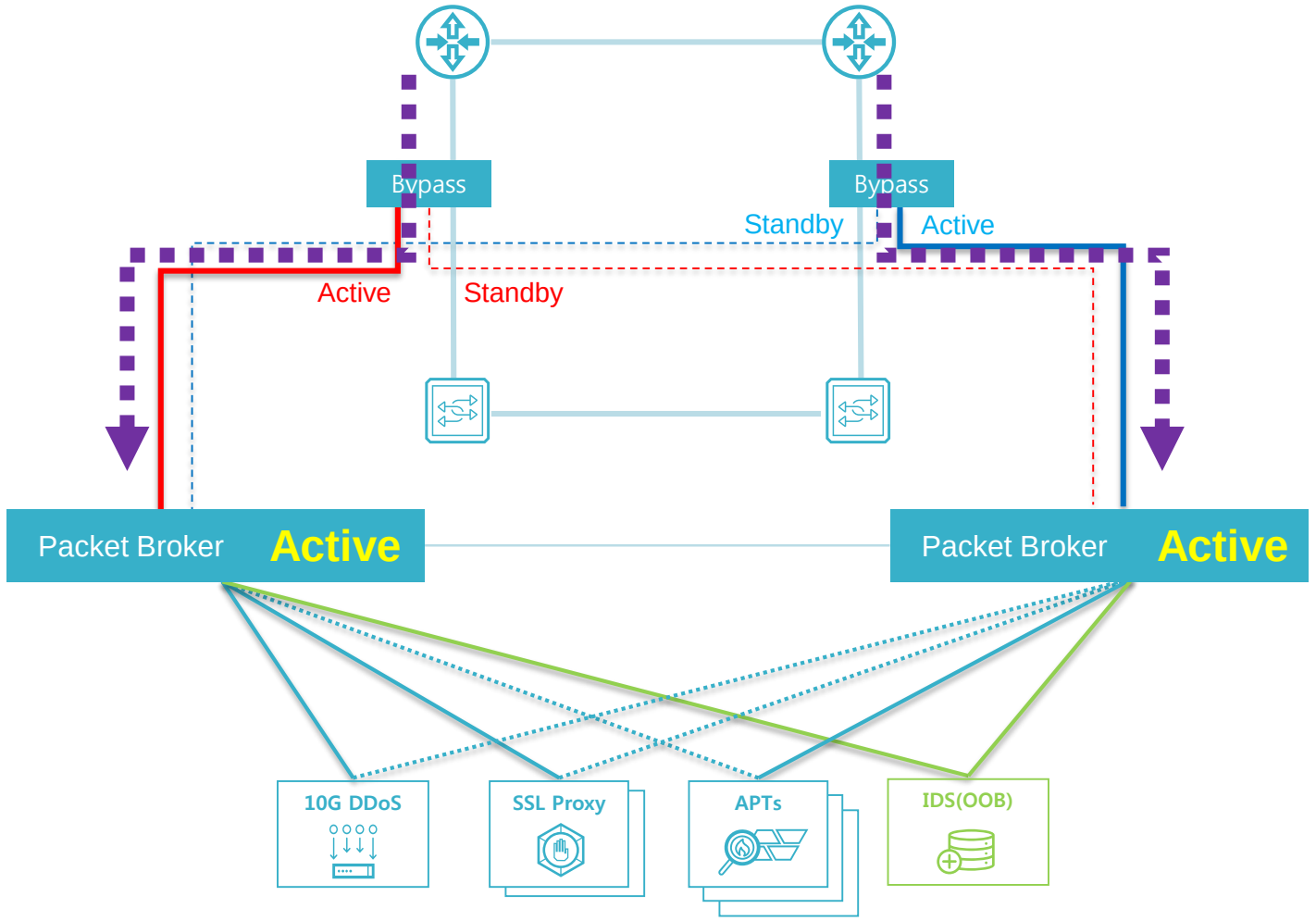
구축 예제 – 다수의 보안장비에 “위협 IP” 차단 솔루션 추가 도입

- 현재는 DPI장비, 방화벽(x2)이 Inline으로 구성 중인 상태 - **복잡한 구성**이고, **성능 저하**의 문제
- TIBS(유해IP차단), IPS, WAF 등의 **보안 솔루션 추가 계획**
- IXIA Security Fabric 도입을 통한 **확장성/안정성/운영 편리성** 확보



ixia

안정적인 인라인 구성을 위한 HA(High Availability) 구성 제안



- 업계 **유일**의 HA **Active-Active** 및 모든 Inline 통합 기능 포함

ixia


ixia