Here's your TIBS(Threat IP Blocking System)!

# 대용량 위협 IP 통합 관리 전략 소개

2019. 12. 11(수)


Keysight NSS(Network Solutions Sales)

김종우 부장(chris.kim@keysight.com)

# AGENDA

1. 왜 수많은 위협 IP 차단 리스트가 존재 하는가?
2. TIBS – 대용량 위협 IP 차단 솔루션 소개
3. TIBS 제품 구성

# 1. 왜 수많은 위협 IP 차단 리스트가 존재 하는가?

# 위협 사이트 급증으로 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 과학기술정보방송통신우
은 자료에 따르면 2013년부터 올 7월까지 탐지·차단된 피싱사


▲금융감독원을 사칭한 피싱사이트[자료

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

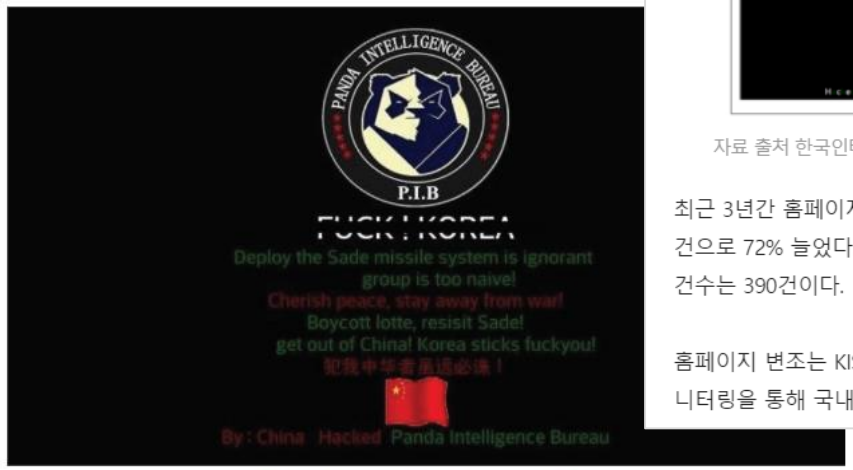
## 웹사이트 침해사고 주역 3인방, 예방법은?

좋아요 32개 | 입력 : 2018-07-05 10:49

#정보보호의 달 #홈페이지 변조 #웹사이트 침해사고 #악성코드 유포 #디페이스
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
WebDAV 서비스 중지, 파일 업로드 제한, 중요파일 백업, 웹서버 보안 강화해야

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

2일 국회 신용현 바른미래당 의원(
로부터 제출받은 자료에 따르면 국
이상씩 증가해 3000건이 넘는 것으

자료 출처 한국인터넷진흥원(KISA). /

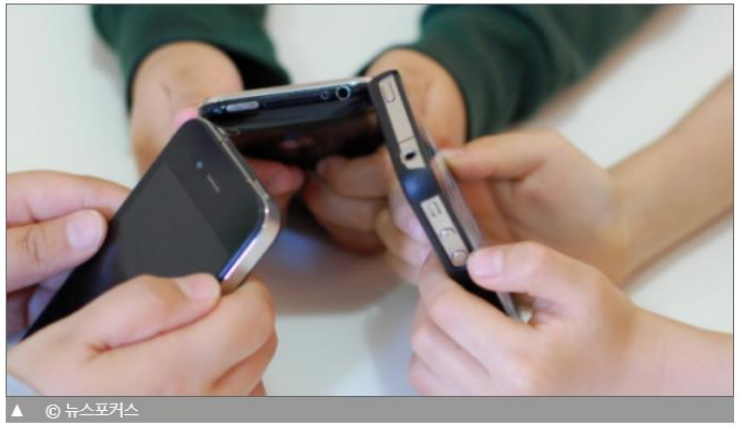
최근 3년간 홈페이지 변조 해킹 피
건으로 72% 늘었다. 2017년에는 17
건수는 390건이다.

홈페이지 변조는 KISA에서 전 세계
니터링을 통해 국내 홈페이지 변조

## 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



ixia

# 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**

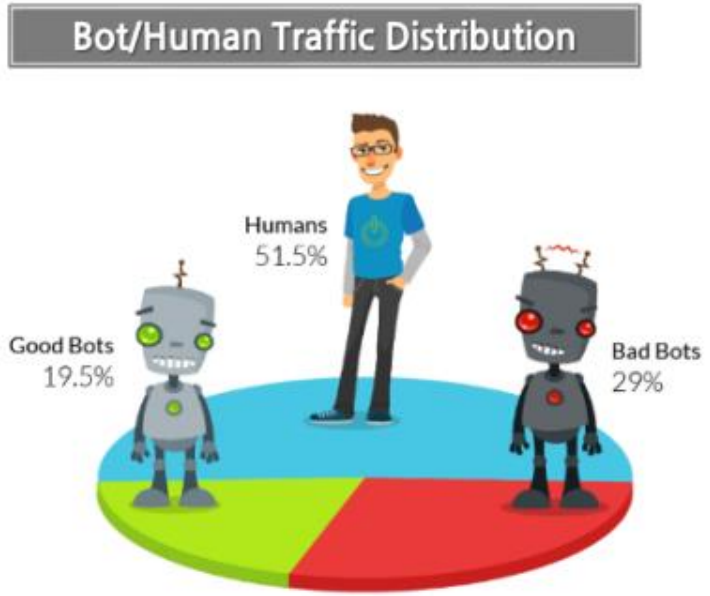
- Data (e.g. credit card ) theft.
- Malware injection and distribution.
- Website/Server hijacking.
- Website defacement and content deletion.

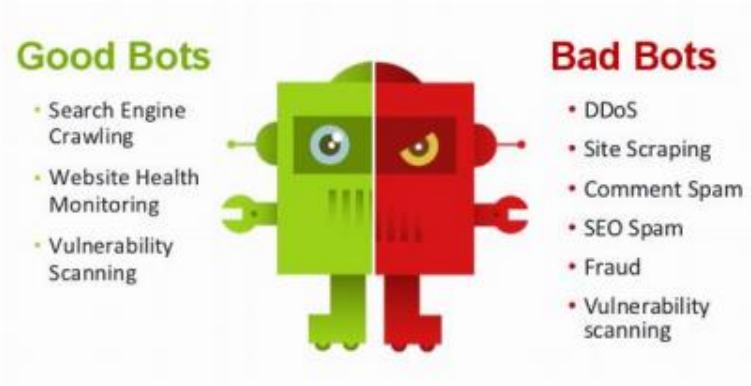
**The Target**

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 IP들의 기하급수적인 증가 추세

*"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 솔루션**의 필요성 대두

Gartner

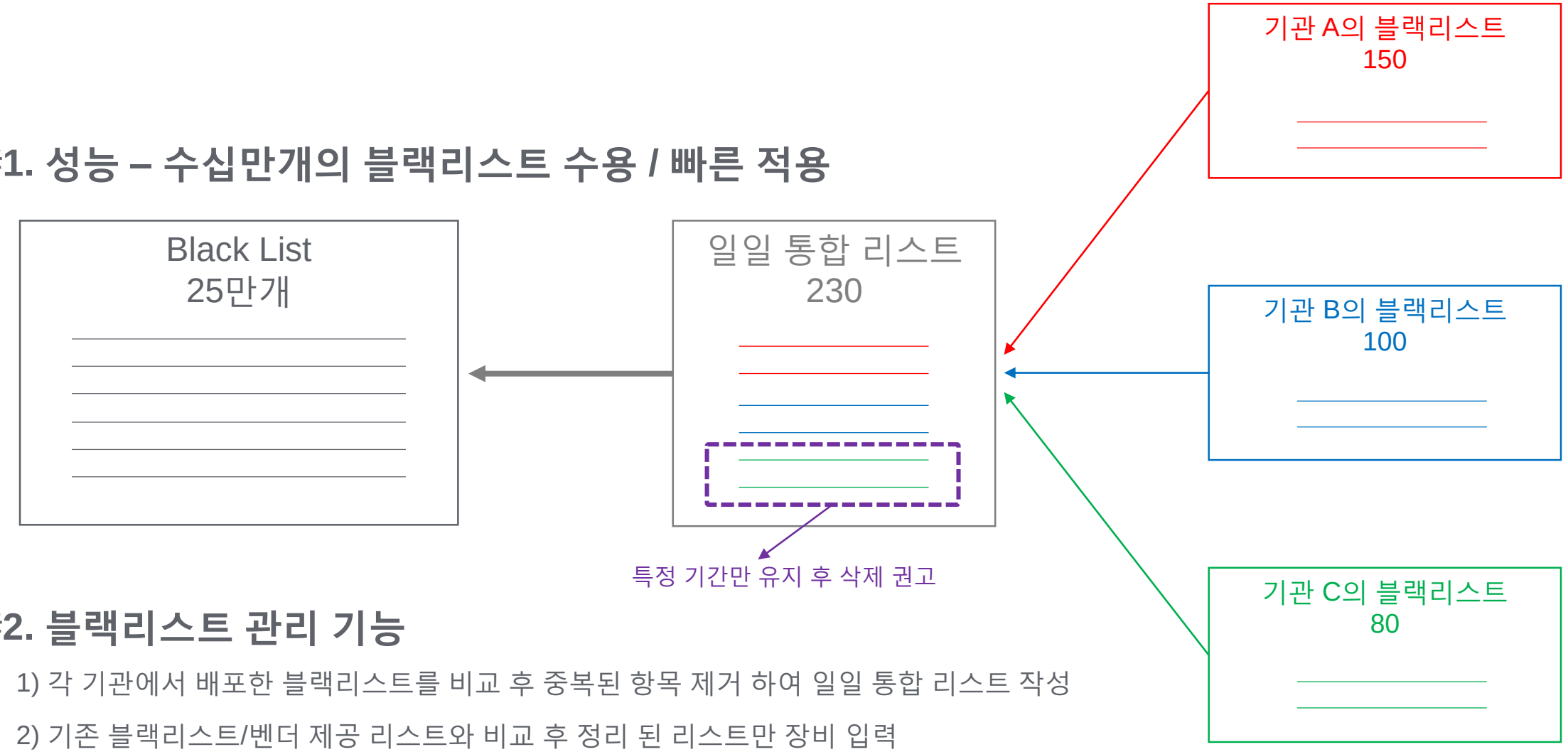
Here's your TIBS!

# 2. TIBS – 대용량 위협 IP 차단 솔루션 소개

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

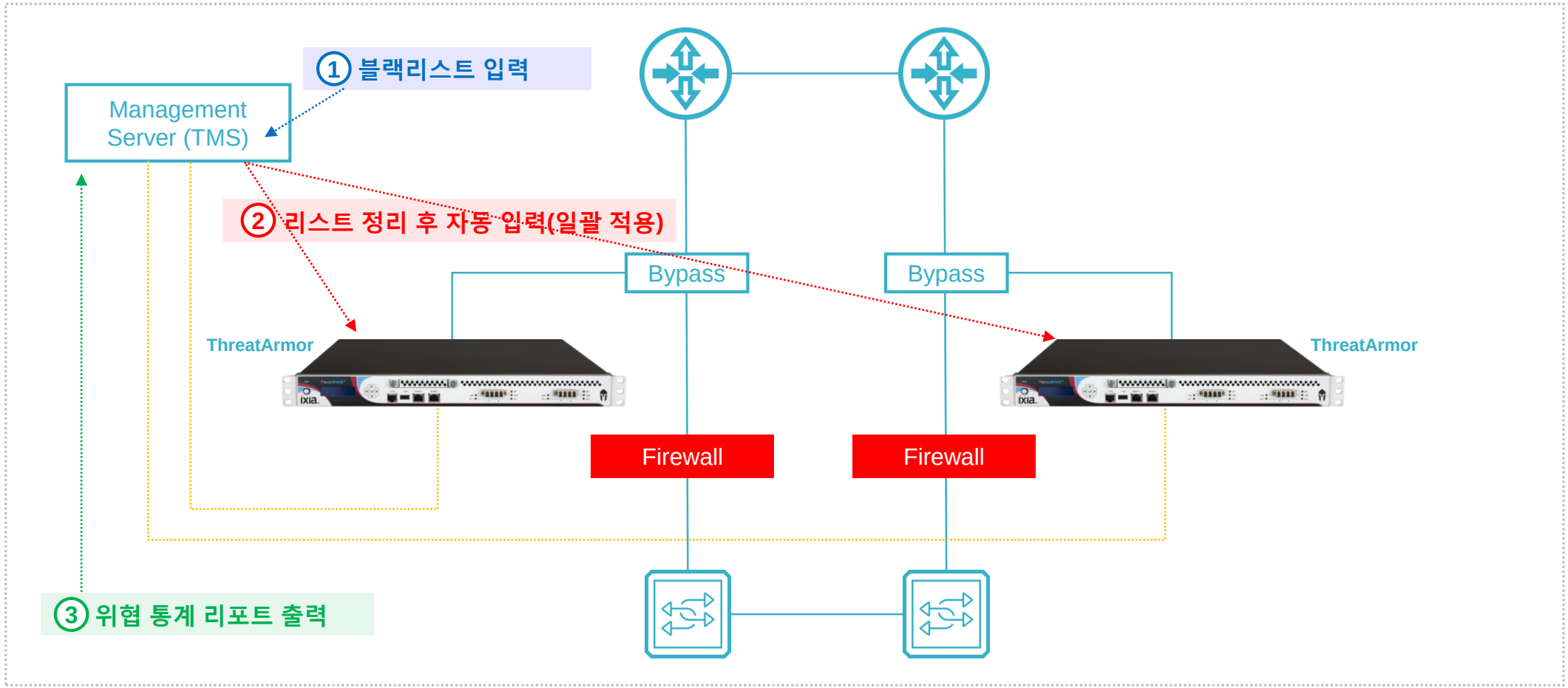
1) 원하는 기간의 차단/로그 통계 수치 리포트 작성
2) 자체 로그 분석 후, 필요한 블랙리스트 생성 후 적용
3) 일정 기간 사용되지 않는 블랙리스트는 확인 후 삭제

ixia

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

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

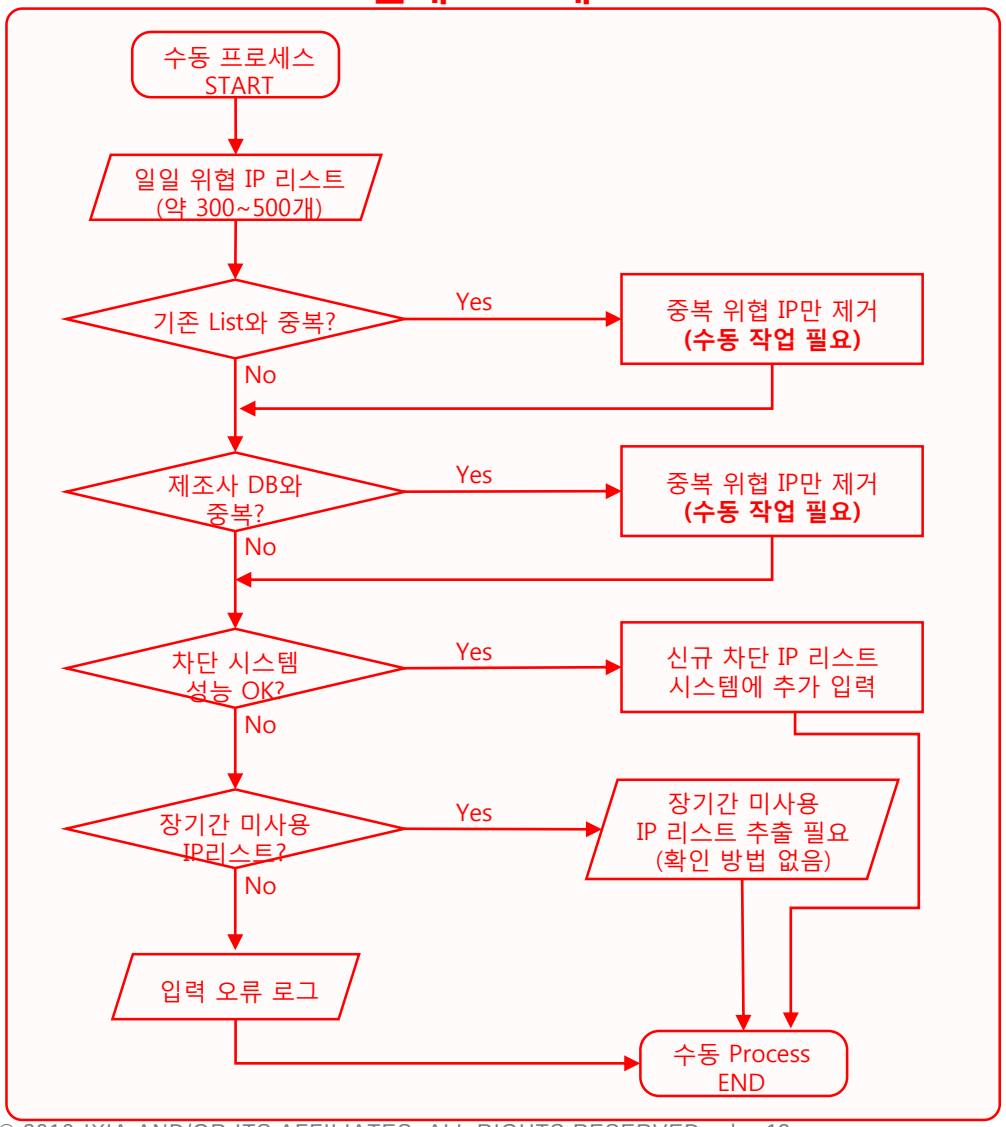


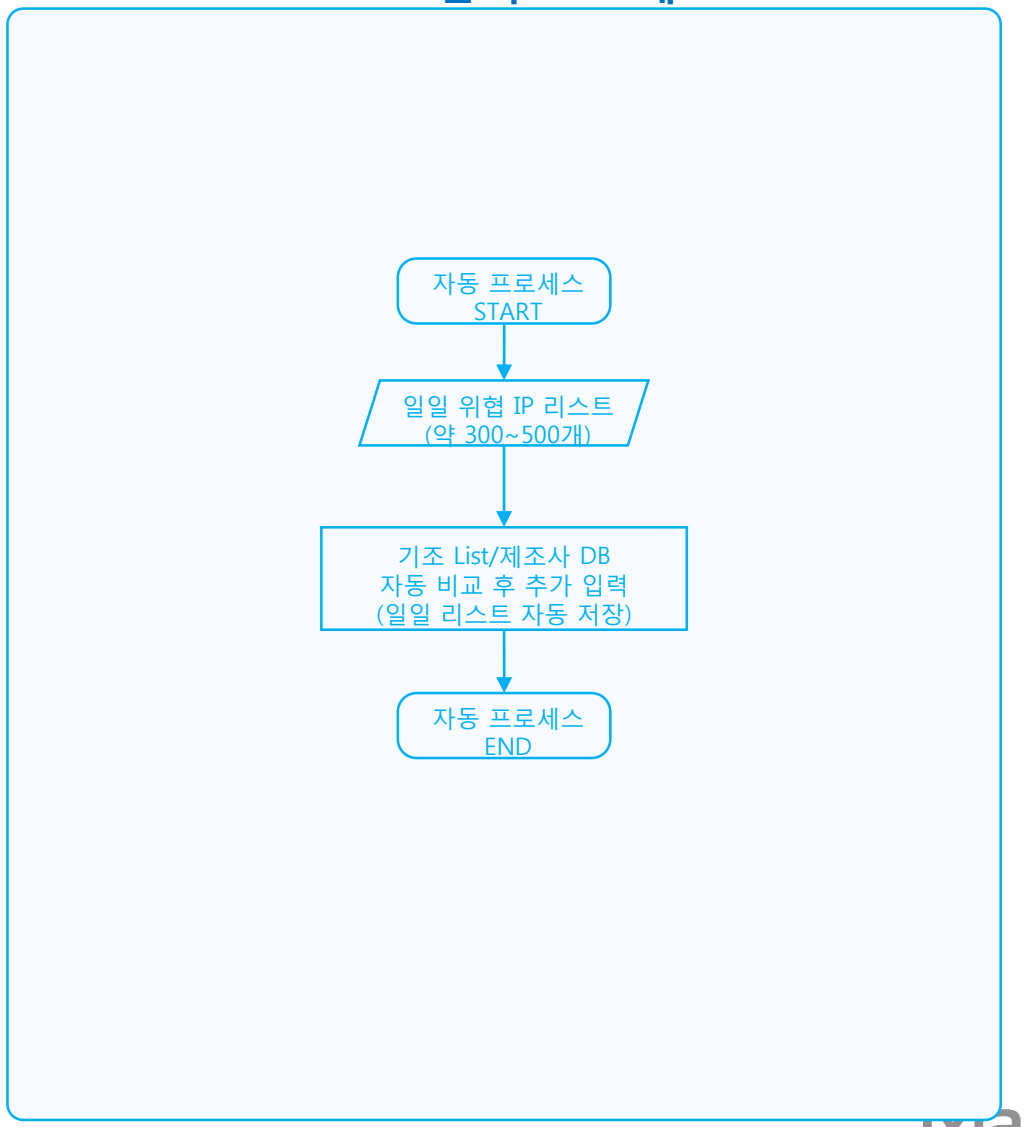
ixia

# 위협 IP 차단 리스트 적용 프로세스

## 현재 프로세스




## TIBS 도입 후 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**

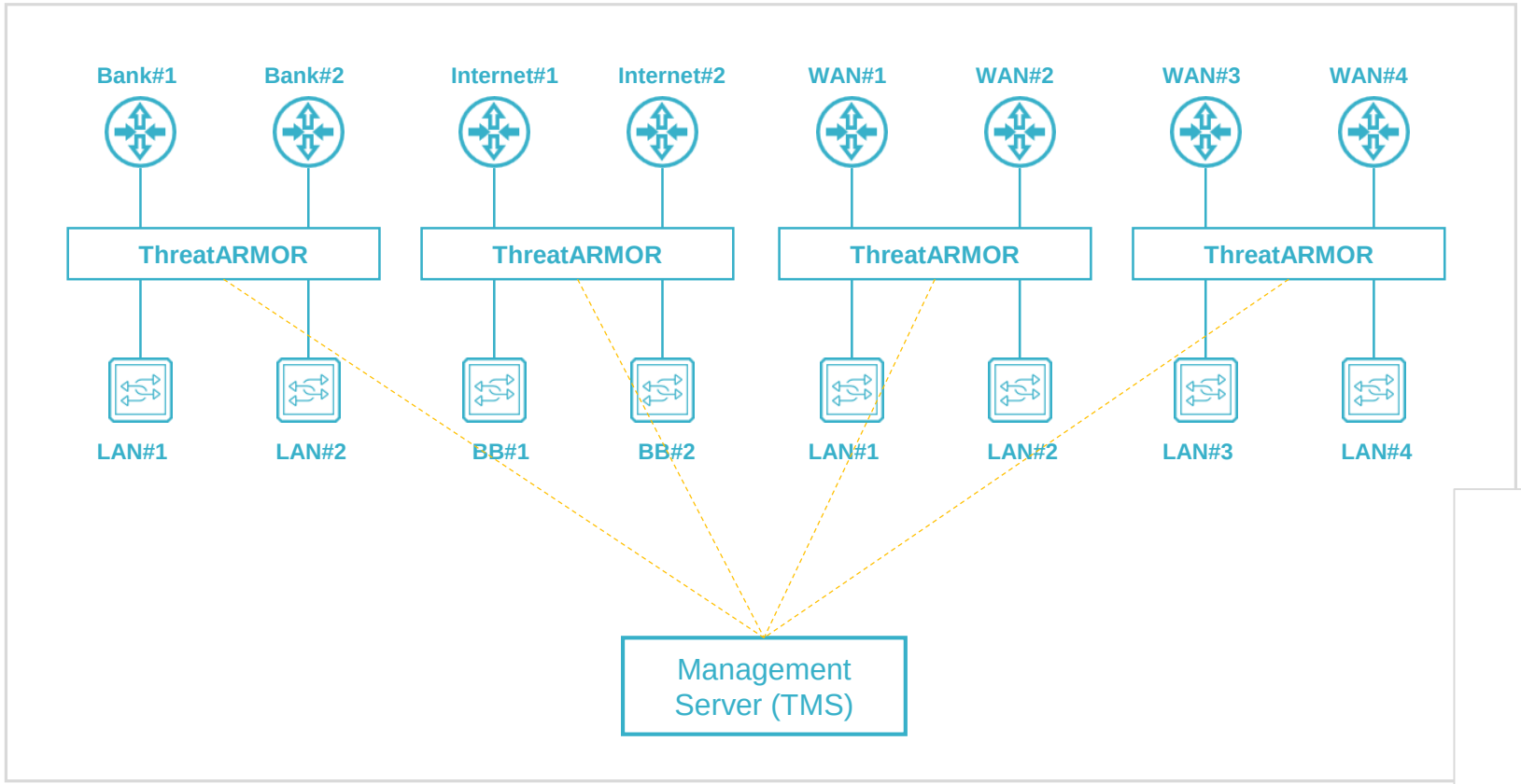
| 일반 방화벽 | VS | IXIA TIBS |
|---|---|---|
| 약 100,000 | **확장성** (최대 IP차단 개수) | 약 4,300,000,000 |
| 신규 적용 리스트 수동 비교 후 관리 필요<br>기간별 관리를 위해 수동 | **효율성** (위협 IP 관리 관점) | 원-클릭 자동 처리 및 모든 차단 리스트 개별 저장<br>기간별 차단 리스트 관리(예. 3개월 후 자동 삭제) |
| 외부 모니터링 장비 필요<br>(예. 바이패스 스위치) | **안정성** (장애 발생 관점) | 자체 바이패스 지원 |
|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

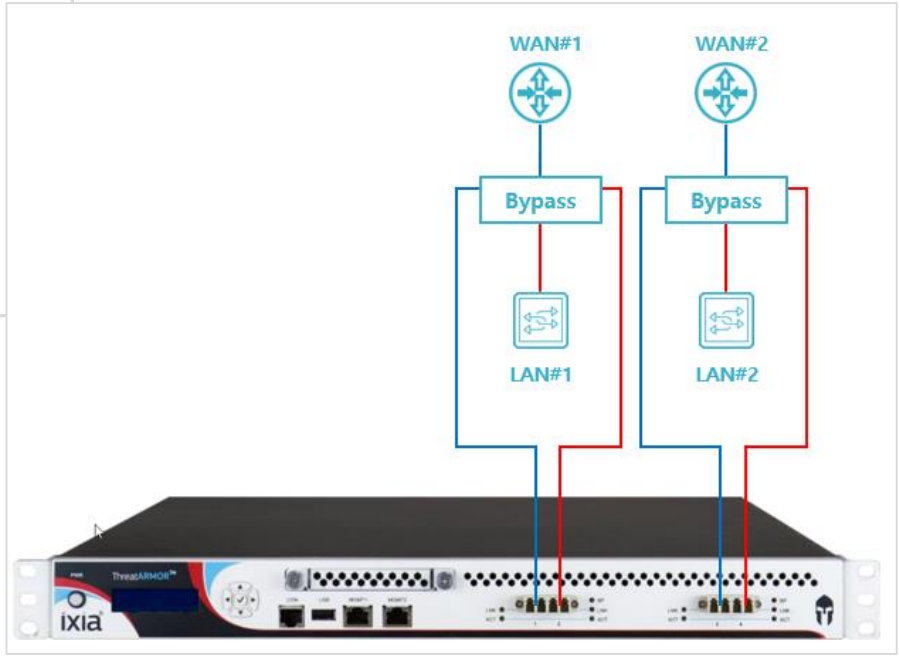
* Working hour : 기존 시스템 – 2hour/day, TIBS – 5min/day
** 일반 방화벽 : 40,000개, TIBS : 2,000,000

ixia

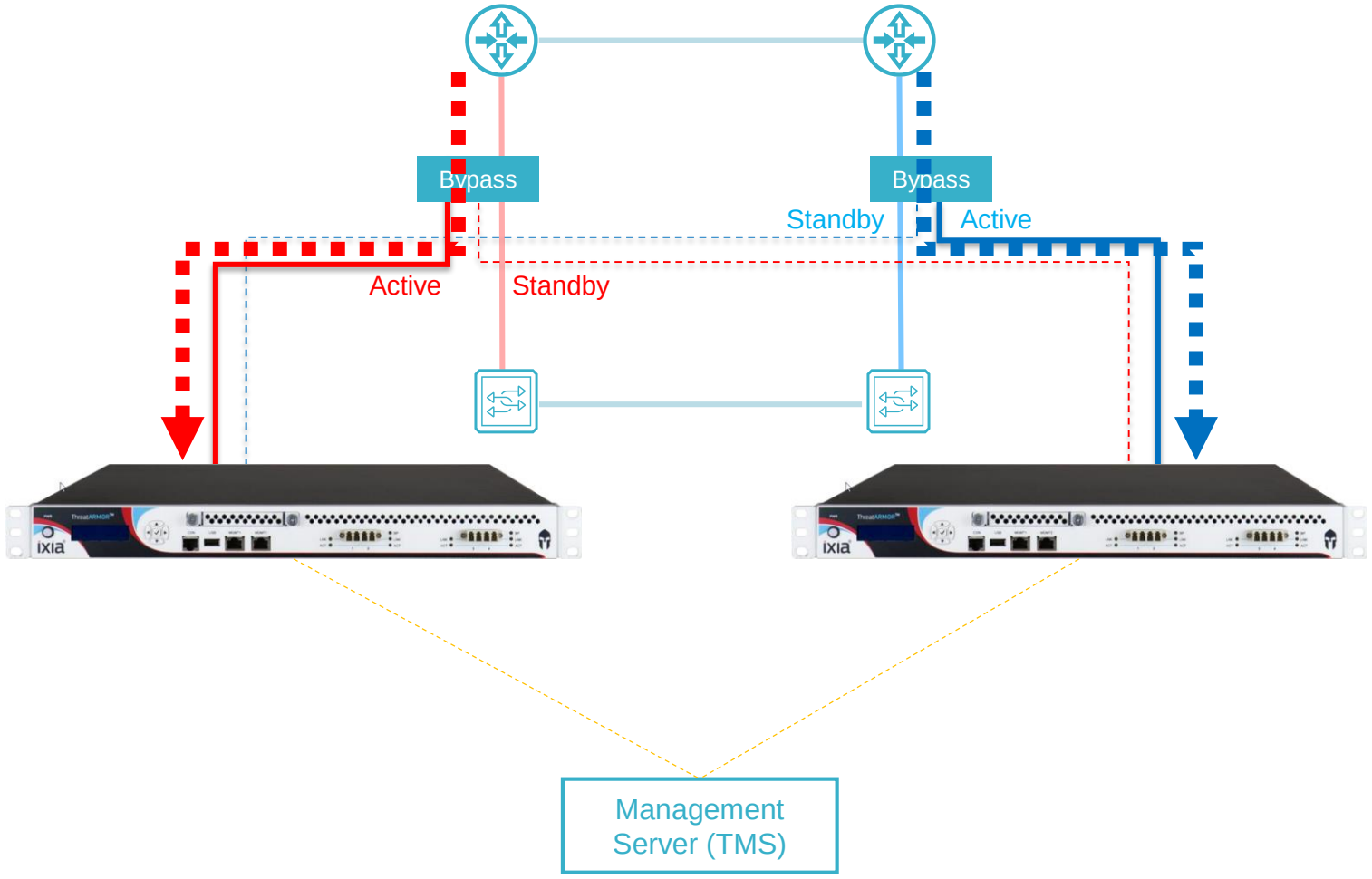
# 시스템 구축 예제 #1 – 다중 회선 동시 관리



# 시스템 구축 예제 #2 – 이중화를 통한 빈틈없는 안정적 구조



# 3. TIBS 제품 구성

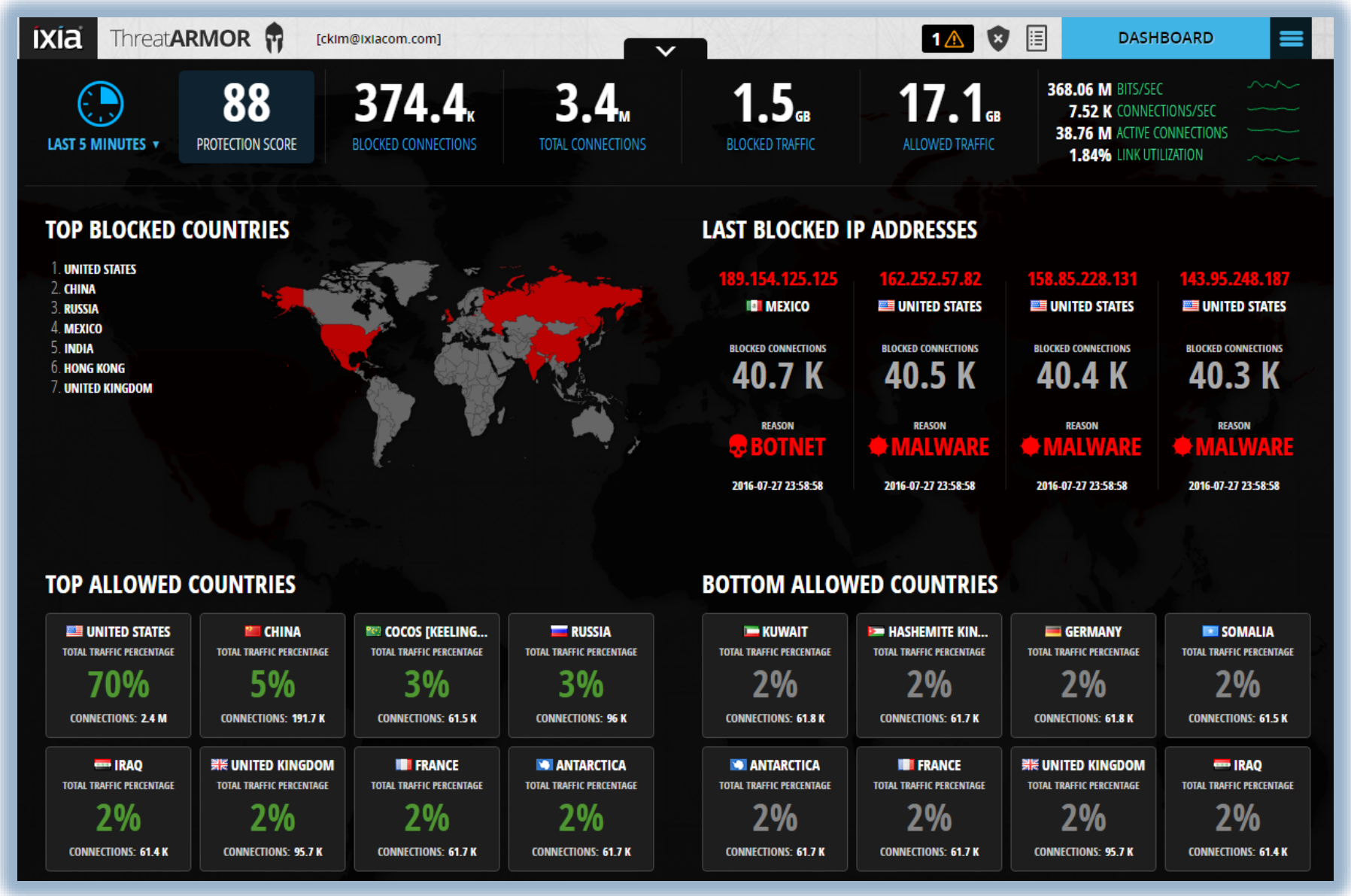
# 대용량 위협 IP 차단 시스템 구성요소

| 구 분 | IXIA ThreatARMOR<br>(차단 장비) | IXIA iBypass<br>(바이패스 스위치) | TIBS 관리 서버 |
|---|---|---|---|
| 장비 외형 |  |  |  |
| | 실제 위협 IP 리스트 적용 및 차단 장비 | 운영 안정성을 위한 바이패스 스위치 | 위협 IP 리스트 통합 관리 서버 |
| H/W Spec | ▪ 1RU / 10G x 4 포트<br>▪ 전원 이중화 / Mgmt 2포트 | ▪ 1RU (2개 장비 설치 가능)<br>▪ 4 x 10G SFP+ ports, 2 x 10G내장<br>▪ 전원 이중화 / Mgmt 2포트 | ▪ 2RU<br>▪ 전원 이중화 / Mgmt 4포트 |
| 주요 기능 | ▪ 위협 IP 차단 리스트 적용 후 실제 트래픽 차단 및 모니터링 역할<br>▪ 최대 4.3B 차단 리스트 적용 가능<br>▪ 현재 동시 적용 최대 200만개 가능<br>▪ 제조사 권고DB 서버 접속을 통한 5분 단위 업데이트<br>▪ 차단된 IP들의 차단 근거를 상세한 리포트로 제공(Rapsheet)<br>▪ 자체 무전원 바이패스기능 지원<br>▪ WebUI에서 강제 Bypass 설정 기능 지원 | ▪ 차단 장비 실시간 모니터링 역할<br>▪ Fail-open, Fail-close 모드 지원<br>▪ 1G / 10G 모드 지원<br>▪ 1:2 (네트워크:툴) 이중화 바이패스<br>▪ Active/Active, Active/Standby 지원<br>▪ 직관적인 손쉬운 GUI를 통한 관리<br>▪ CLI, SSH, WebUI(HTTPS) 지원<br>▪ Syslog, SNMP(v2, v3) 지원<br>▪ Cost effective solution for with and without NPBs | ▪ 전체 차단 장비를 통합 관리 역할<br>▪ 위협 IP 리스트를 자동화를 통해 원-클릭 일괄 등록/수정/관리/적용<br>▪ 차단장비 정보를 통해 기간별 차단 트래픽 및 근거에 대한 리포트 작성<br>▪ CLI/WebUI 지원<br>▪ 탐지/차단 내역에 대한 신뢰성 검증 기능<br>▪ IP / Domain to IP Blocklist 입력 지원<br>▪ 기간별 블랙리스트 자동 관리<br>▪ 기간별 리포트 작성 가능 |

ixia

# ThreatARMOR Main Dashboard

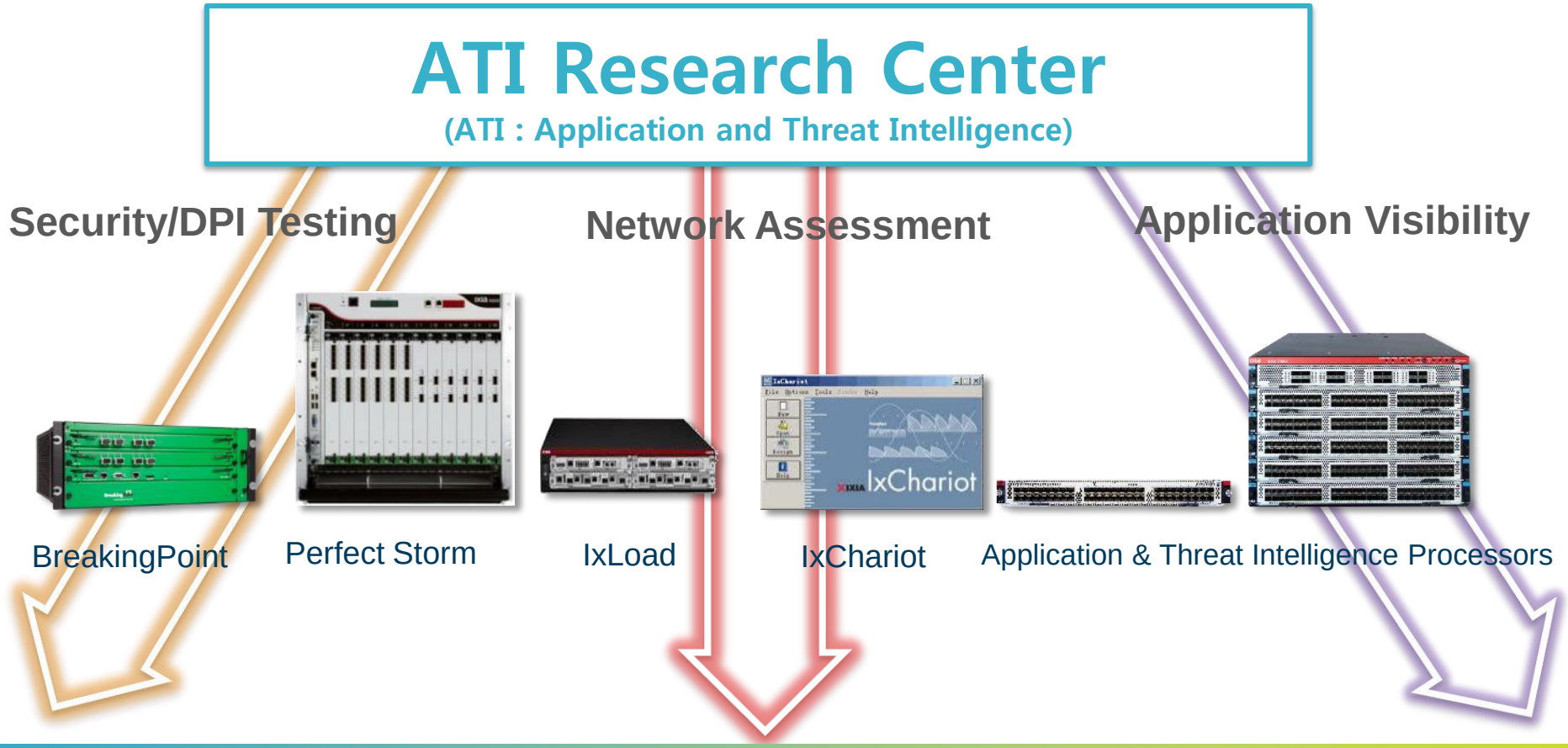


ixia

# 왜 IXIA만 가능한 기술인가?

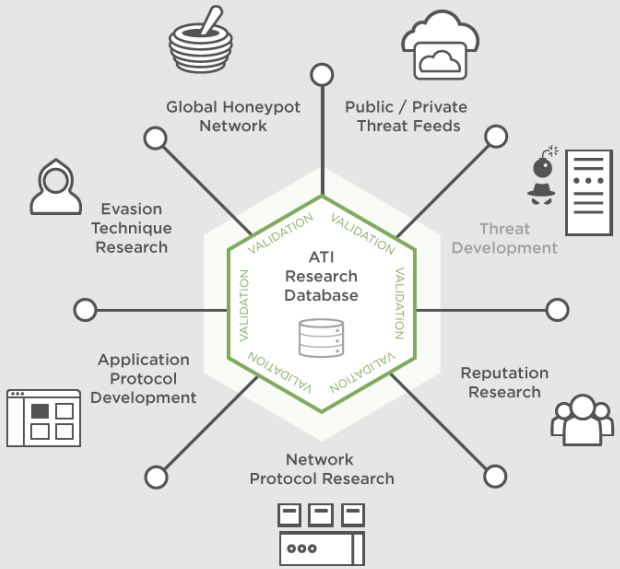
- 독점적인 애플리케이션/보안 트래픽 생성 원천 기술 보유



# ThreatARMOR 내부 차단 리스트 관리 - 5분 간격 Rapsheet Update

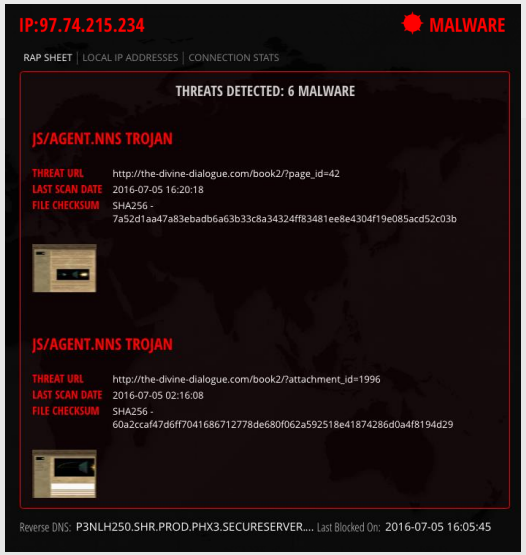
## IXIA ATI Research Center

**업계 선도하는 검증 된 보안(위협 인지) 기술을 활용한 기술 보유**




## ThreatARMOR Rap Sheets

**모든 Block 행위에 대한 분명한 증거 제시**




## ThreatARMOR Appliance

Set, Select and Forget.

Maximum reliability.

**5분 간격 Update**

ixia

# Rapsheet(위협 IP 근거 리포트) – 100% 차단 근거 제시 [1/2]

IP:185.68.16.161

RAP SHEET | LOCAL IP ADDRESSES

THREATS DETECTED: 5 MALWARI

JS:IFRAME-BND [TRJ]

THREAT URL http://chuguevnews.info/index.php?view=article&ca
02&id=935:2014-02-14-08-49-37&tmpl=component&

LAST SCAN DATE 2016-01-10 15:46:51

FILE CHECKSUM SHA256 -
fecdbcc77c324650fb10645b4dd535a131edccf9b85f

PAGE TITLE Home | chuguevnews

JS:IFRAME-BND [TRJ]

THREAT URL http://chuguevnews.info/index.php/2012-12-16-21-
17-35?tmpl=component

LAST SCAN DATE 2016-01-10 15:39:20

FILE CHECKSUM SHA256 -
9b470f11291dcb18a8b72fe62d441f2b8e661379b59
9

Reverse DNS: 185.68.16.161 Last Blo

MALWARE

IP:202.97.174.82

RAP SHEET | LOCAL IP ADDRESSES

THREATS DETECTED: 2 BOTNE

COMMUNICATED WITH
WIN32/TROJANDOWNLOADER.AGENT.RRR TROJAN

LAST SCAN DATE 2016-01-06 00:53:40

FILE CHECKSUM SHA256 -
79938cad61289bca6f35ac3c496fa57aa5412b70edc

COMMUNICATED WITH A VARIANT OF
WIN32/TROJANDOWNLOADER.AGENT.RRR TROJAN

LAST SCAN DATE 2015-12-07 07:36:03

FILE CHECKSUM SHA256 -
a15e9de35a616186ee27a6142d790a8610c55e54a

Reverse DNS: 202.97.174.82 Last B

BOTNET

IP:205.203.0.1

HIJACKED

RAP SHEET | LOCAL IP ADDRESSES

THIS IP IS HIJACKED

HIJACKED INFO

This particular network range has been hijacked. A hijacked range is a netblock brought back from the dead, often by a spammer. The original owner of the block may have left it derelict for any number of reasons. For more information about these types of IP ranges please visit http://www.spamhaus.org/faq/section/DROP%20FAQ#258

LAST SCAN DATE 2015-12-30 06:28:54

MORE INFO AT http://www.spamhaus.org/sbl/sbl.lasso?query=SBL104616

ASN 9737 TOTNET-TH-AS-AP TOT Public Company Limited,TH

ASN REGISTRAR apnic

ASN DESCRIPTION TOTNET-TH-AS-AP TOT Public Company Limited,TH

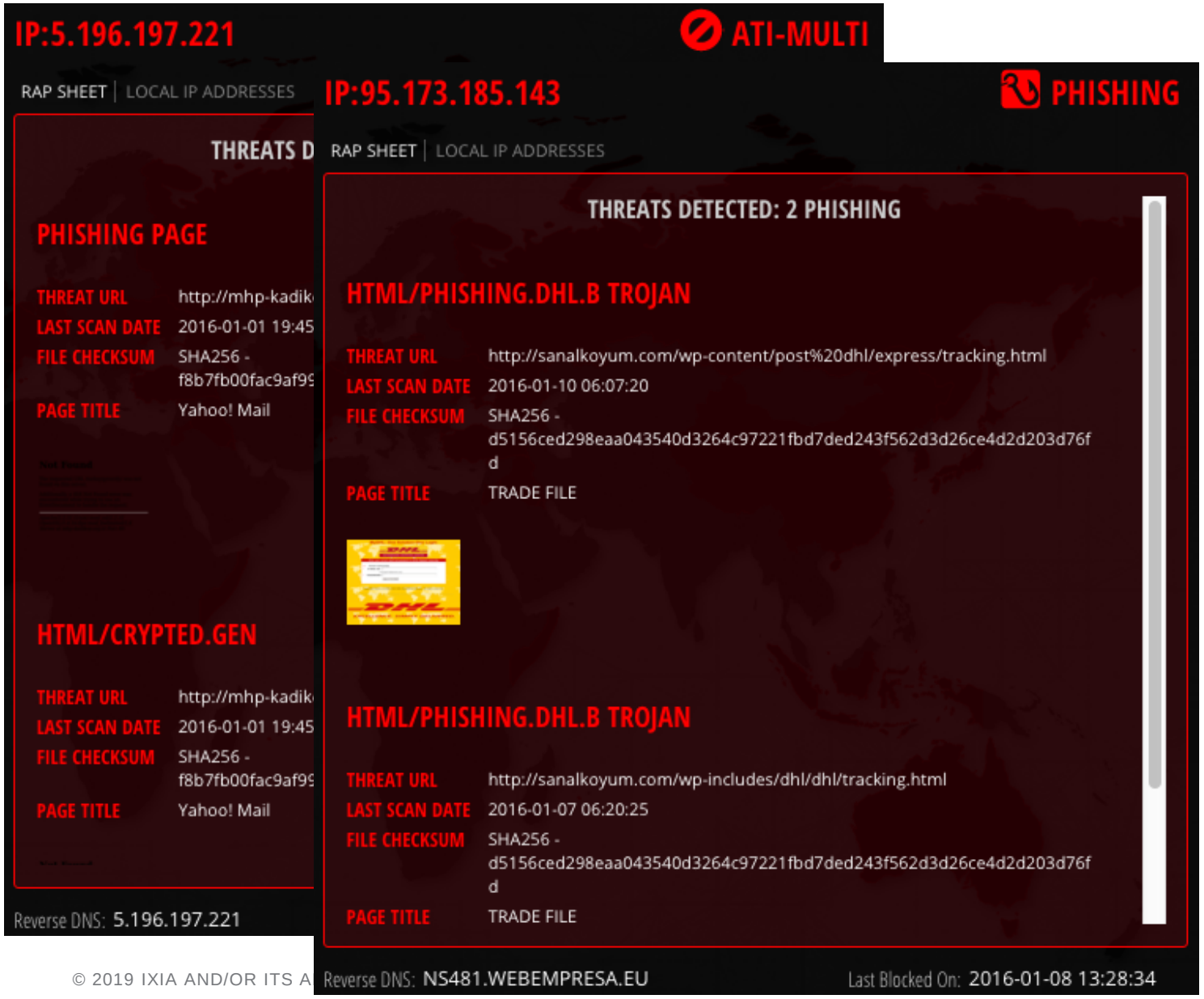
ASN REGISTRATION DATE 2011-04-08

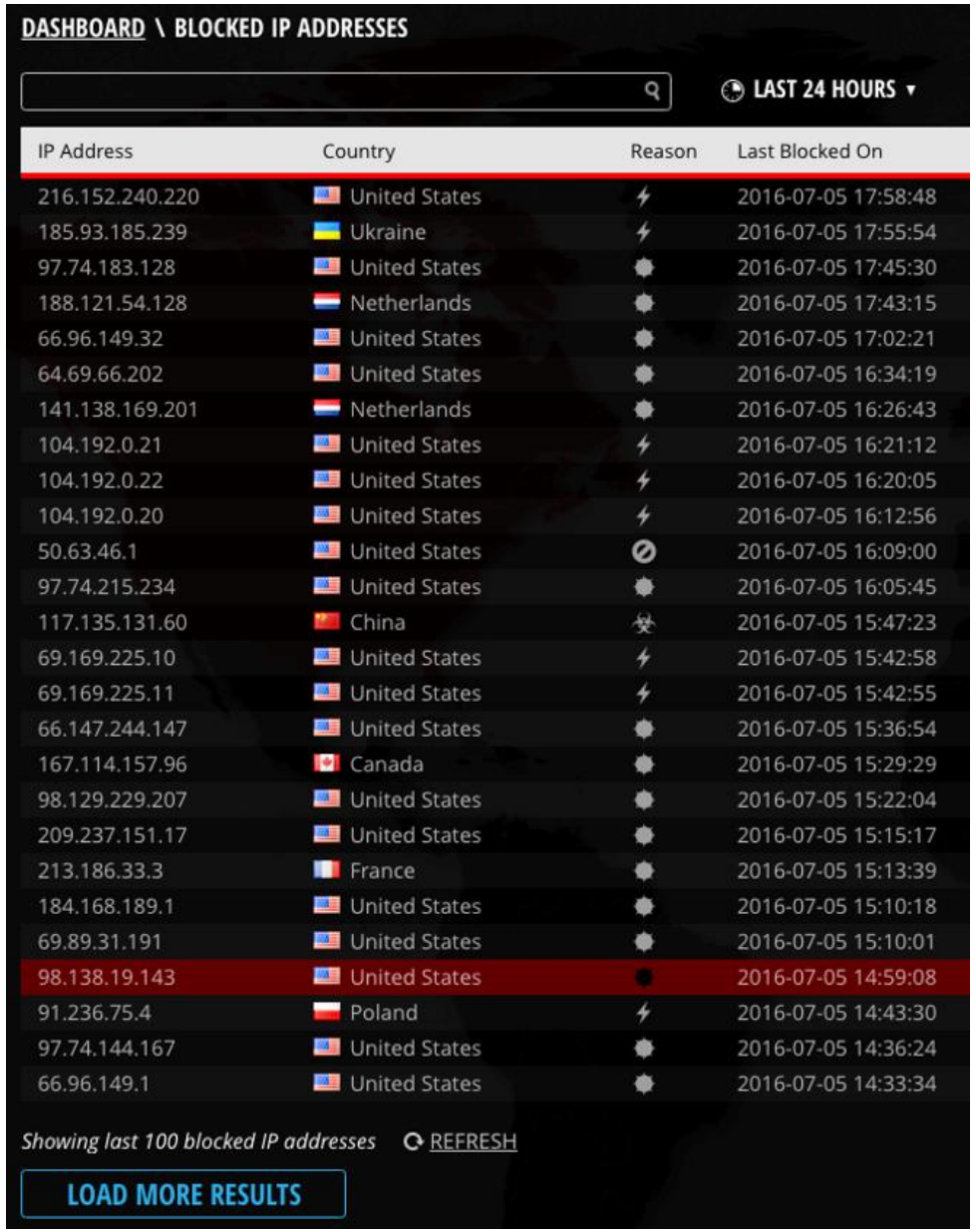
ASN (AUTONOMOUS SYSTEM NUMBER) 9737

Reverse DNS: 205.203.0.1 Last Blocked On: 2016-01-08 13:28:34

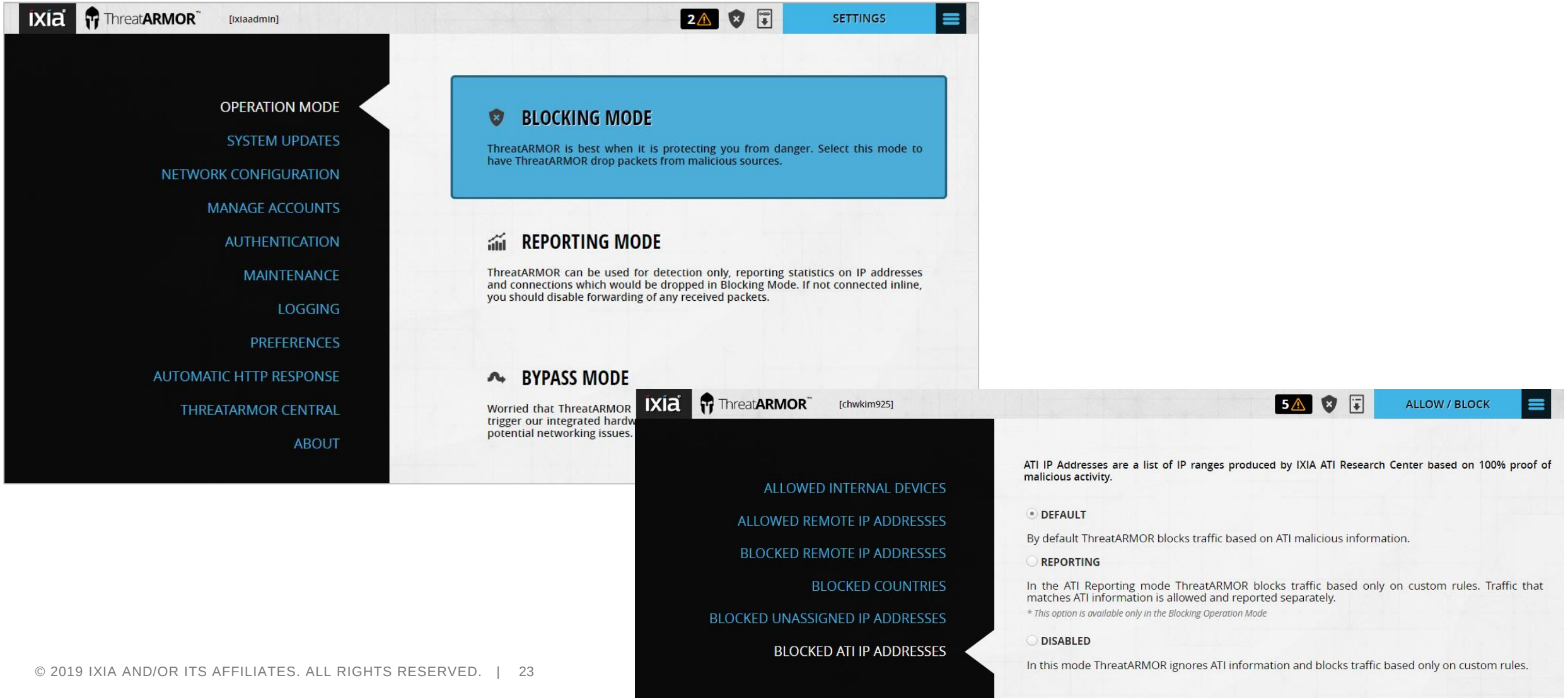
# Rapsheet(위협 IP 근거 리포트) – 100% 차단 근거 제시 [2/2]



# 3가지 운영 모드 지원

- 차단 모드, 리포트 모드, 바이패스 모드 지원 – 제조사 제공 Block IP 리스트만 리포트 모드로 사용 가능



# 유해 IP 리스트 TIBS 시스템으로 전달 경로

**IXIA ATI Research Center**

5분 자동 Update

**유해 IP 차단 시스템 (TIBS)**

1G ThreatARMOR

**KISA**

KISA 인터넷보호나라&KrCERT

C-TAS

Request

Export API

**TIBS 관리서버**

C-TAS 및 Admin 관리 솔루션

API

10G ThreatARMOR

**Admin**

Web Console

수동 Update

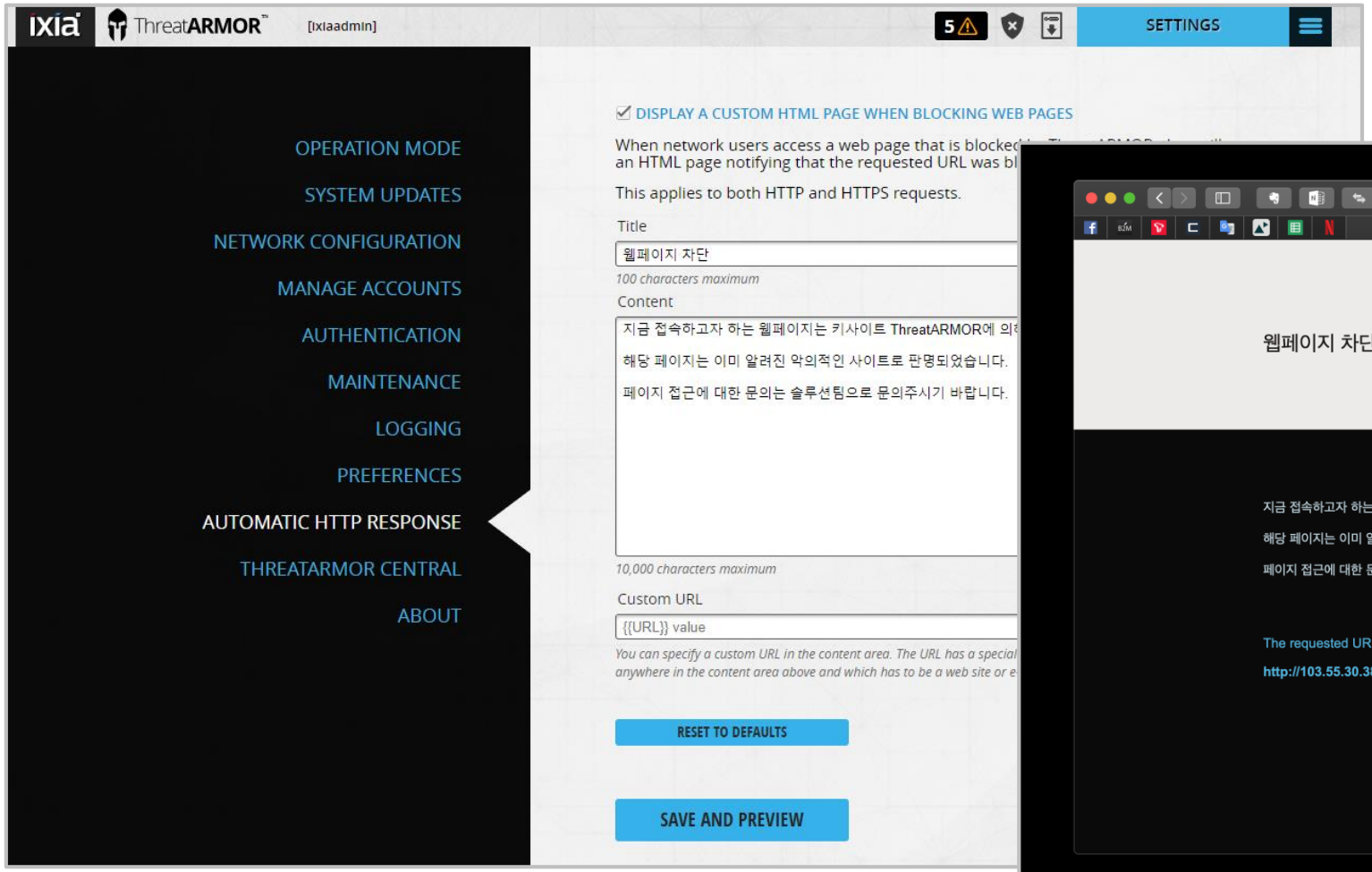
실제 유해 IP 차단 시스템

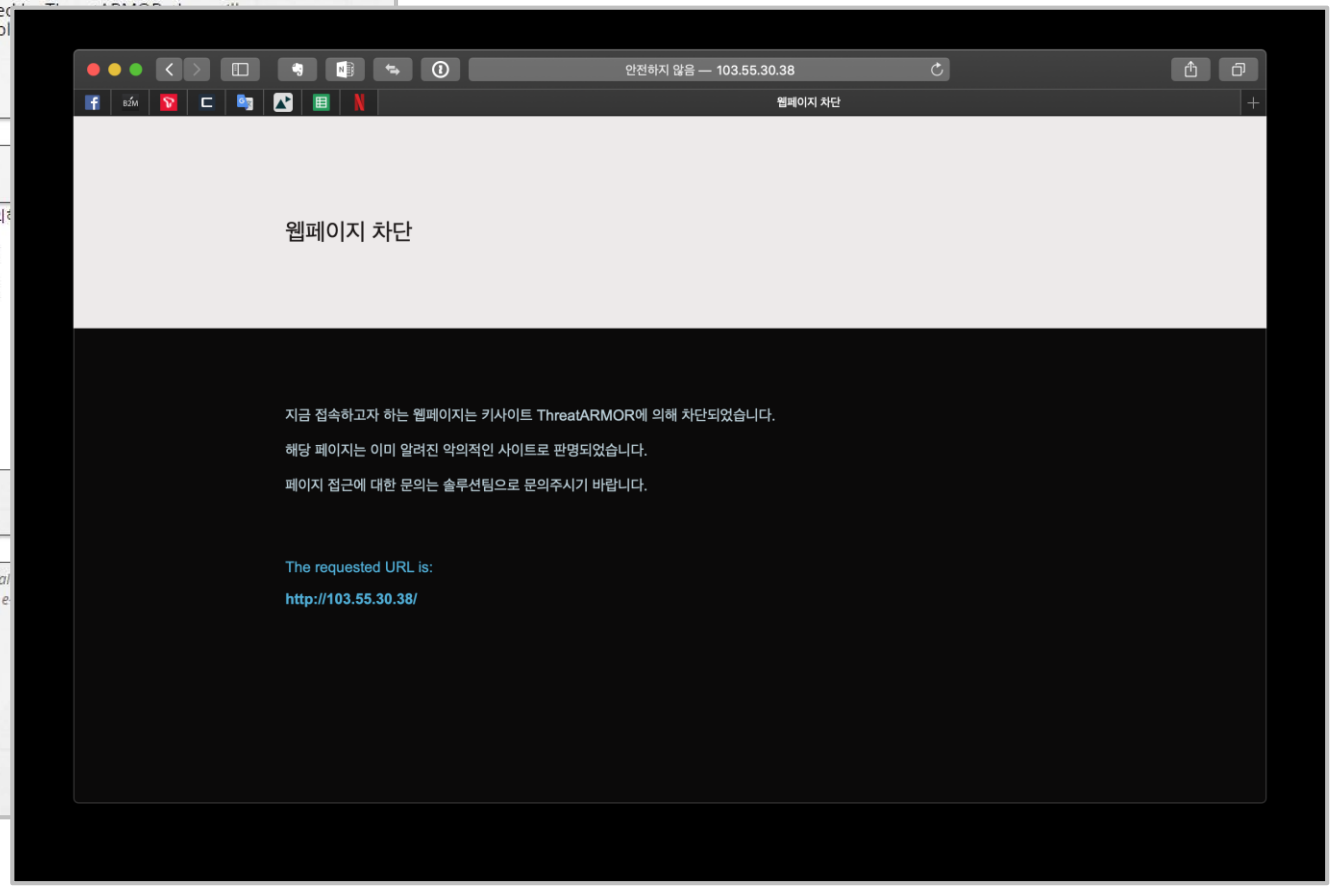
ixia

# 차단 후 안내 페이지 전달

- 차단 안내 페이지 설정 – 차단 된 사용자 수신 화면




- 브라우저에서의 실제 안내 페이지

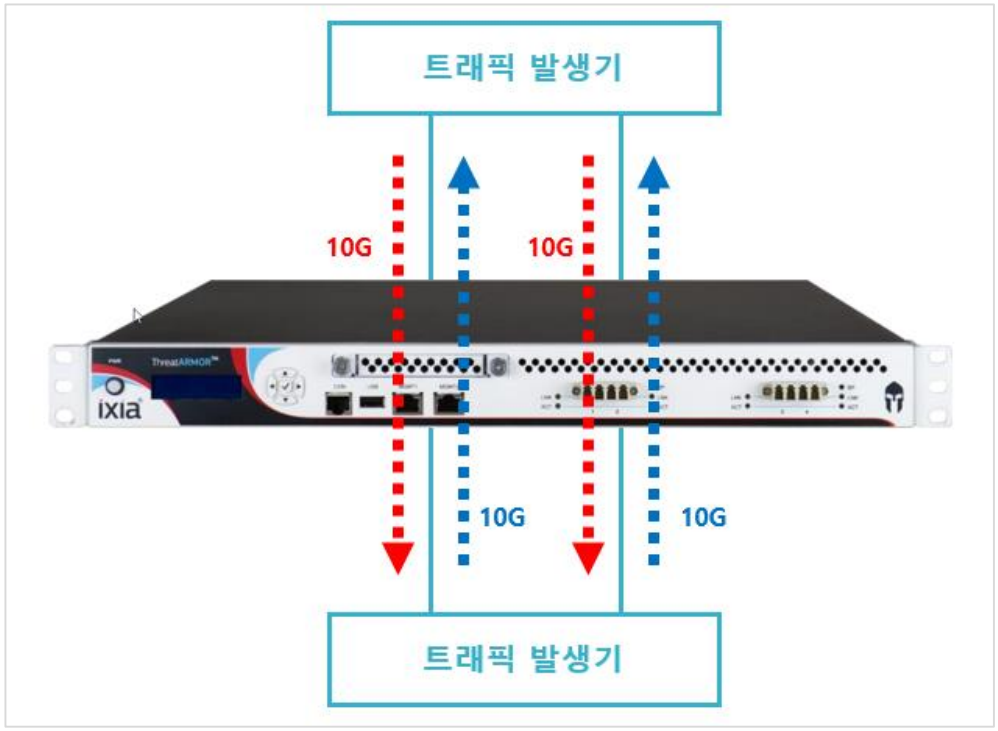


ixia

# ThreatARMOR 성능 측정 [1/3] – Throughput

- 테스트 구성도




- 테스트 트래픽 내역
  - Throughput : 총 40G bps
    ➔ 2개 회선 각각 양방향 20Gbps
  - 트래픽 종류 : TCP 80
  - 패킷 사이즈 : 1024Byte
  - 테스트 시간 : 총 3시간 15분

- 트래픽 발생기 설정 화면

**7.7.3. Settings**

| Parameter | Value |
|---|---|
| Test Duration/Test Duration Measured by a Time Interval | 03:15:00 |
| Test Duration/Test Duration Measured in Frames | 0 |
| Delay Start | 00:00:00 |
| Packet Templates/Type | TCP |
| Data Rate/Data Rate Unit | Megabits / Second |
| Data Rate/Data Rate Type | Constant |
| Data Rate/Minimum Data Rate | 10000 |
| Data Rate/Maximum Data Rate | 500 |
| Data Rate/Increment N Units/Period | 0 |
| Data Rate/Every N Seconds | 1 |
| Data Rate/Data Rate Ramp | Limit |

# ThreatARMOR 성능 측정 [2/3] – 100% Line-rate throughput

- 테스트 결과
  - 100% 트래픽 수신
  - 40Gbps의 Throughput 지원

## 7.3. Component Summary

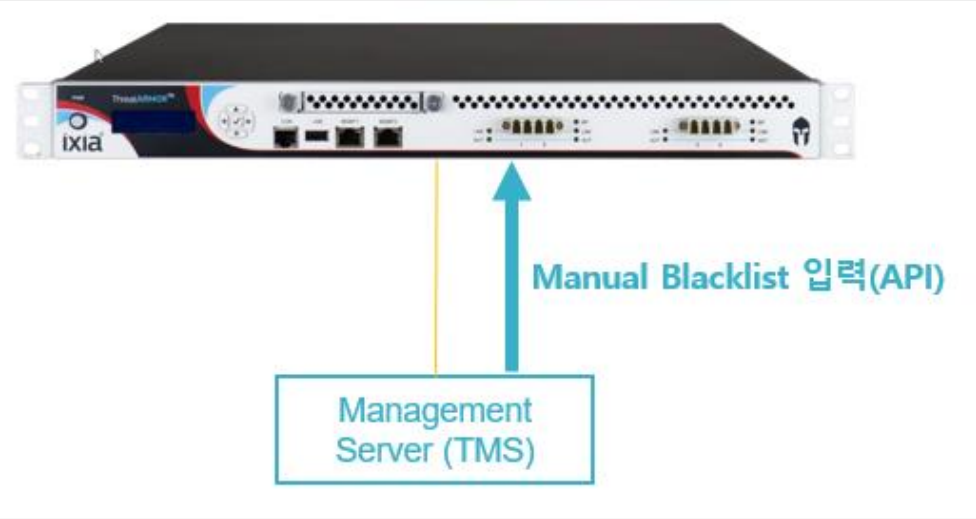
| Measurement | Value |
|---|---|
| Frames transmitted | 38,036,372,400 |
| Frames received | 38,036,372,400 *100.000%* |
| Frame bytes transmitted | 57,739,213,303,200 |
| Frame bytes received | 57,739,213,303,200 *100.000%* |
| Maximum frame transmit rate | ~3251000 |
| Maximum frame receive rate | ~3251000 |
| Maximum frame data transmit rate | ~40000 |
| Maximum frame data receive rate | ~40000 |
| Corrupted frames received | 0 |
| Out-of-sequence frames received | 708,779,797 |
| Frames not received on the correct port | 0 |
| Frames received more than once | 0 |
| Frames received that were not test-generated | 0 |
| Slow start frames sent | 0 |
| Dropped frames | 0 |
| Frames received with bad IP checksum | 0 |
| Frames received with bad UDP checksum | 0 |

ixia

# ThreatARMOR 성능 측정 [3/3] – Manual Blacklist 입력 성능

- 테스트 구성도




- 테스트 결과

| Blacklist 적용 개수 | 적용 시간 |
|---|---|
| 100K (10만) | 700 ~ 800 ms |
| 200K (20만) | 800 ~ 1,050 ms |
| 500K (50만) | 1,800 ~ 1,900 ms |
| 1M (100만) | 3,200 ~ 3,300 ms |
| 2M (200만) | 6,300 ~ 6,500 ms |

# 급격히 늘어가는 위협 IP 리스트를 가장 효율적으로 처리하는 방안

위협 IP 차단 리스트가 20만개가 넘어서 방화벽이 너무 느려요

대량의 위협 IP 리스트를 수동 관리하는 데에 인력 낭비가 심하고 오류가 많아요.

오후 3:24

TIBS는 최대 43억 개 차단 리스트를 적용할 수 있어 성능 저하가 없습니다.

자동화 관리 시스템이라 TCO 절감은 기본이고, 오류가 없습니다.

오후 3:24

제조사 보유 위협 IP 리스트 포함 기존 리스트와의 중복도 자동으로 관리 되나요?

차단 통계 로그를 확인함으로써 위협 IP 차단 시스템의 효과를 파악하고 싶어요.

오후 3:28

제조사 보유 위협 IP 리스트 포함하여 기존 리스트와 신규 리스트를 비교하여 필요한 IP 리스트만 적용합니다.

통계 보고서(기간/IP내역 별)를 통해 그 효과를 명확히 파악할 수 있으며, 제조사 DB 업데이트를 통한 최신 보안 트렌드 또한 확인이 가능합니다.

오후 3:28

특정 시점으로 롤백이 가능한가요?

오후 3:29

일자 별로 위협 IP 차단 리스트가 저장되므로, 원하는 시점 어디로든 되돌릴 수 있습니다.

오후 3:29


ixia