# TopLayer
# Attack Mitigator IPS

2003. 4.

FNET (주)에프넷트

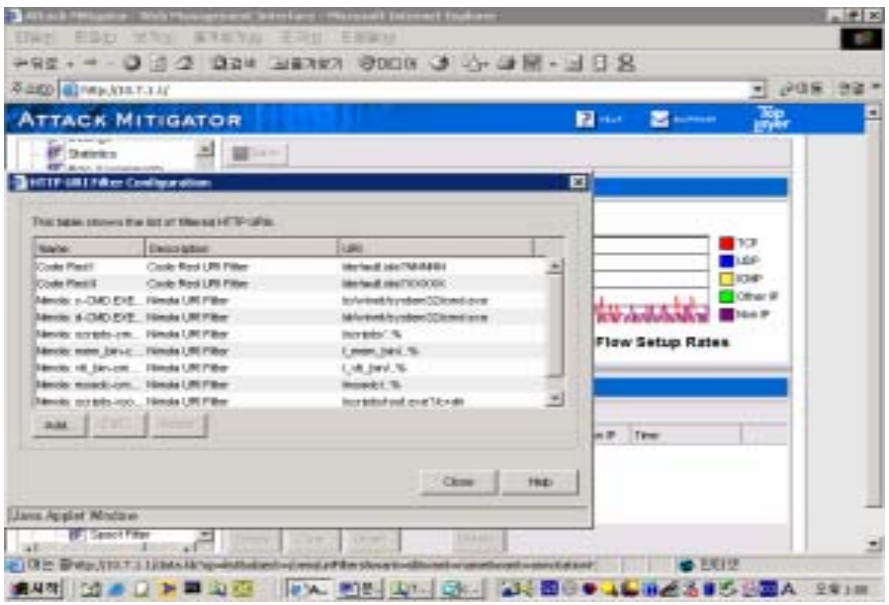
Free & Safe Networking

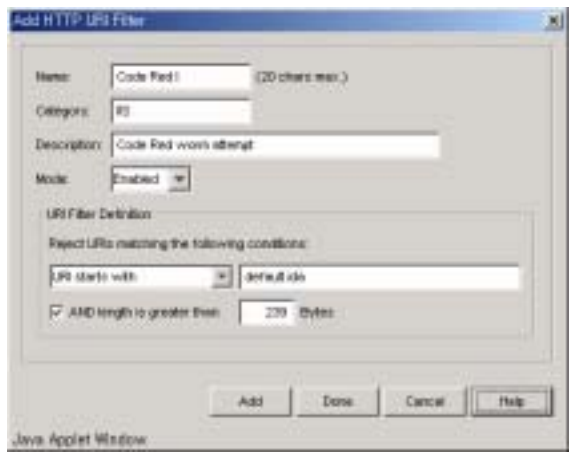
## 목 차

- 지속적으로 늘어나는 악성 바이러스 및 사이버 공격들
- 더욱 더 자동화되고 지능화되는 공격 유형들 출현
- 각종 HTTP 웜(Nimda, Code-Red)이나 DoS/DDoS 공격들이 네트워크 자원들을 무력화
- 피해가 해마다 지속적으로 증가

- 각종 HTTP 웜(Nimda, Code-Red)이나 DoS/DDoS 공격들이나 해킹 공격들을 차단
- 트래픽 흐름을 분석하고, 이러한 흐름들 중 공격을 검출, 악의적인 메커니즘을 가진 공격이 존재하면 자동적 차단
- 공격 인식 시 이를 경보하고, 이에 대한 통계를 수집 및 저장
- 기존 시스템 환경 변화 없이 투명하게 구성할 수 있는 인라인(In-Line) 장비로 적용
- 내부 시스템을 외부의 바이러스 및 해킹 공격으로부터 안전하게 보호하여, 서비스 가용성을 최대화

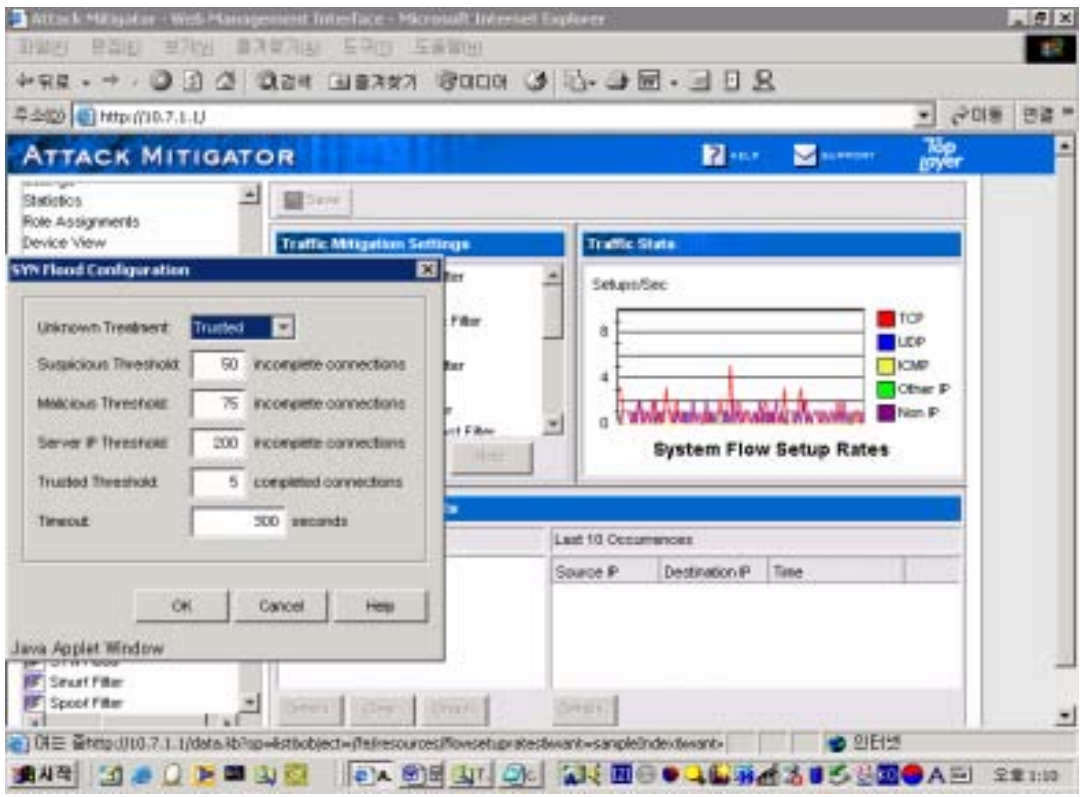
- 웜 바이러스란  컴퓨터 시스템을 파괴하거나 작업을 지연 또는 방해하는 악성프로그램을 말함
- URI 값이 특정한 사용자 정의 시그니처에 해당되는 HTTP 트래픽을 필터링
- HTTP를 통해 유입되는 Nimda / Code Red I, II 와 같은 웜 바이러스의 차단 설정
- 공격 시그니처의 이름, 분류, URI의 문자열 위치나 Wildcard의 사용으로 특정위치(시작, 중간, 끝) 및 정보를 정의



▪ SYN Flood Mitigation

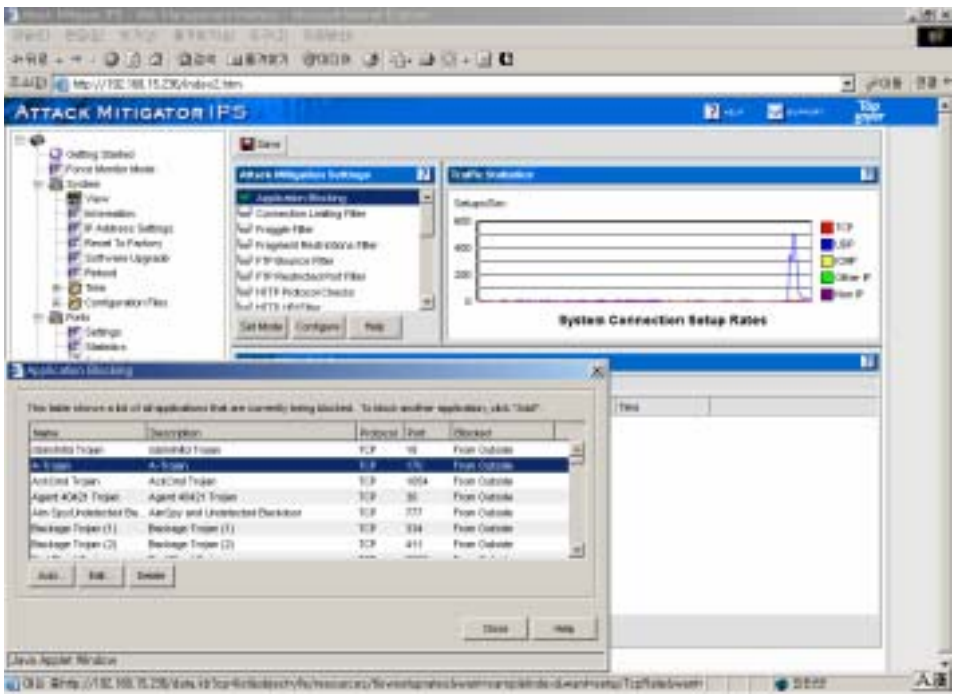
클라이언트로부터 서버에 오는 세션들 중 임계 치를 초과하여 TCP 핸드 쉐이킹이 맺어지지 않는 세션에 대해 사전에 정의된 위협 순위에 의해 IP 주소를 차단

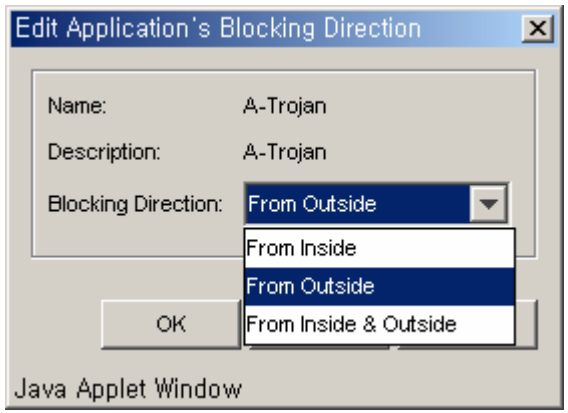


▪ Application Blocking Filter

TCP/UDP 포트 번호 기반으로 정의된 네트워크 어플리케이션을 차단

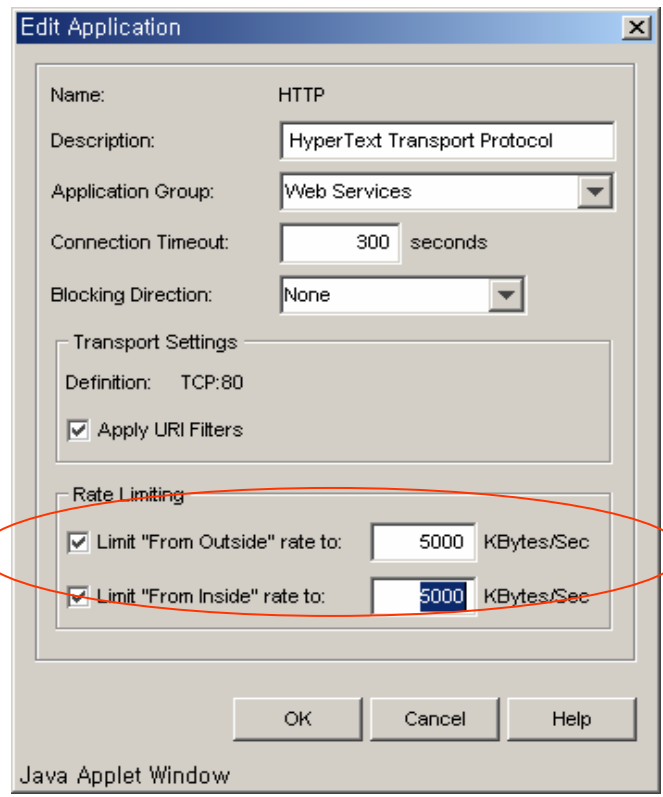
각 어플리케이션별로 From Inside, From Outside, From Inside&Outside 방향으로 차단 가능



- Application Rate Limiting

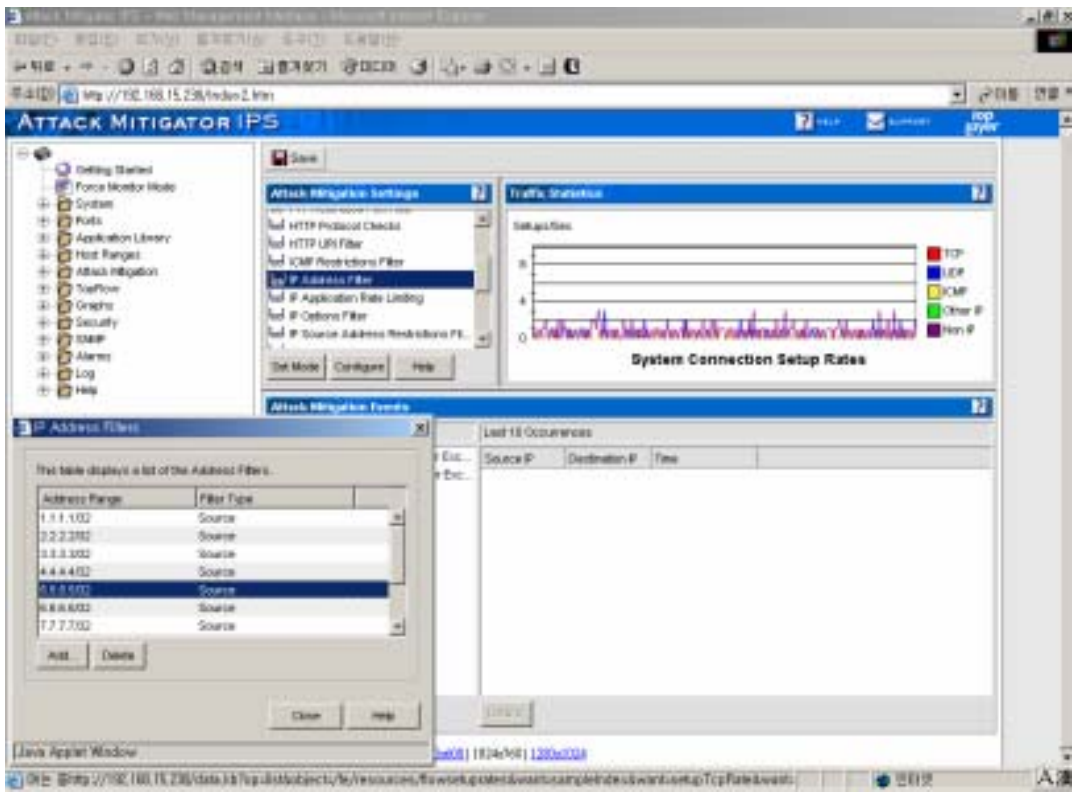
대역폭 제한 임계치(Threshold) 값에 기반하여, 내부/외부 네트웍으로의 어플리케이션 트래픽을 필터링

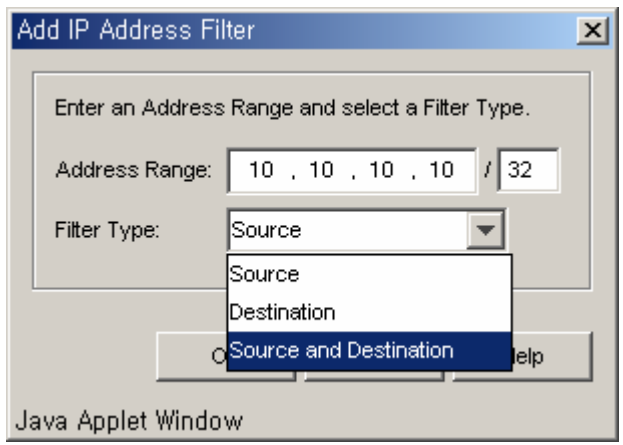



▪ Address Filters

출발지 또는 목적지 주소 모두가 정당하지 않은 주소 값을 가진 경우 필터링

(예 : 10.0.0.0/8 to 10.255.255.255와 같은 RFC 1918 주소값들)



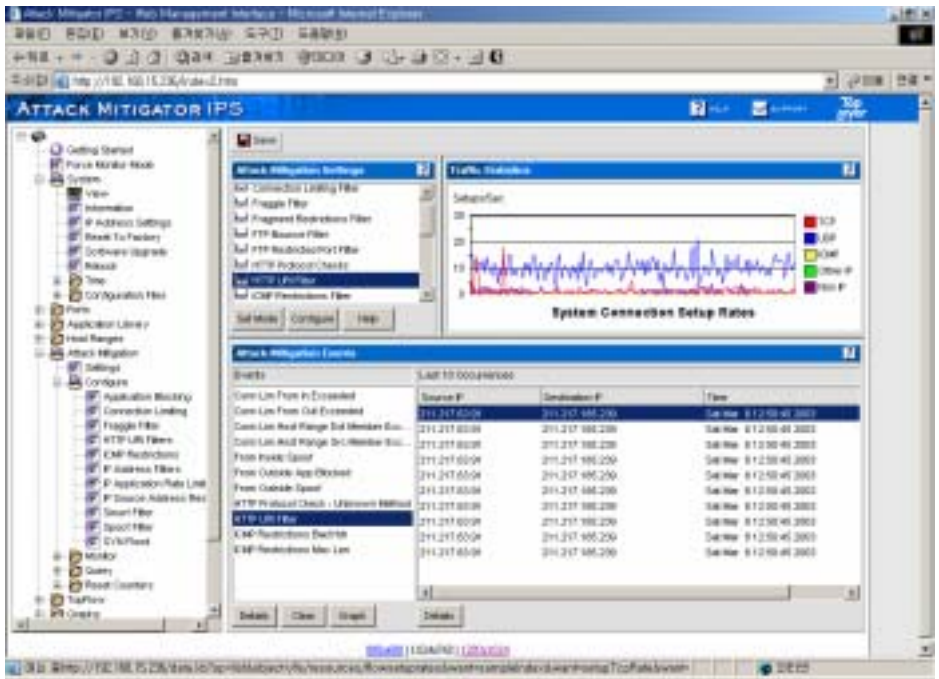
- Connection Limiting
- ICMP Restriction 차단
- IP Source Address Spoof 필터링
- Smurf 필터링
- Fraggle 필터링
- Fragmentation Restrictions
- FTP Bounce
- FTP Restricted Port
- IP Options
- IP Source Route
- Lan.D
- UDP Bomb 등

- Web Management Interface

  Navigation Tree, Traffic Statistics, Event Area로 구성

- Device View

시스템 정보, 포트 설정, 포트 통계, 포트 역할, 포트연결상태 등을 GUI 기반으로 확인




[Web Management Interface]

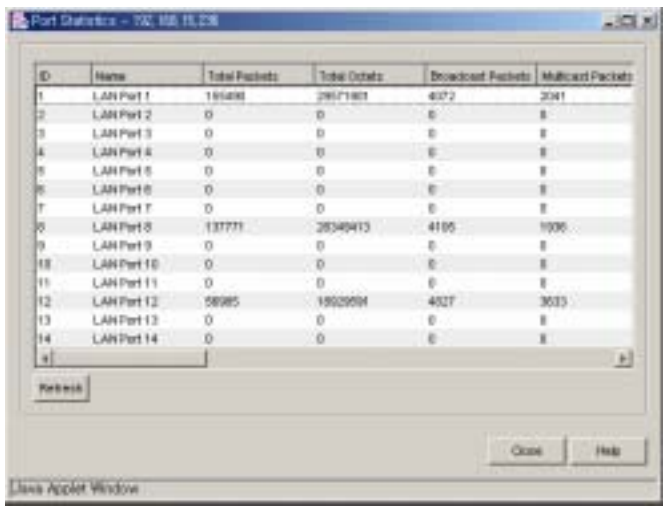
[Device View]

▪ 다양한 보고 기능을 내장하고 있을 뿐만 아니라, 원격지 외부 서버로도 다양한 형태의 보고 메시지를 전송 가능

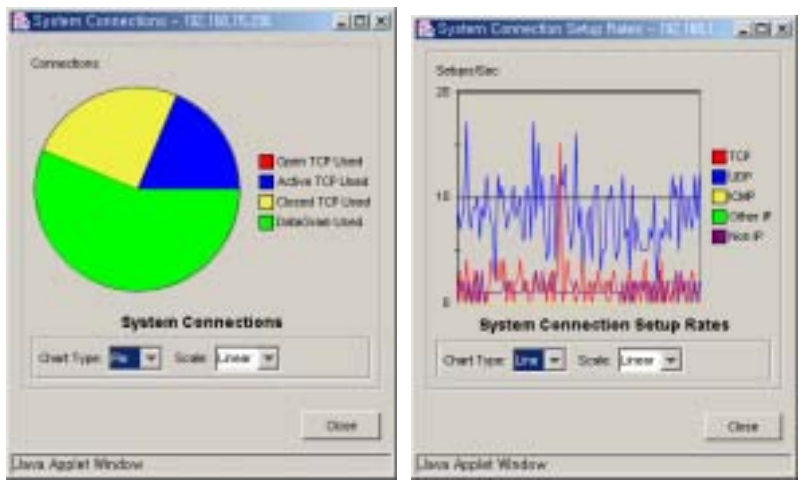
▪ **포트 통계(Port Statistics)**

▪ **실시간 그래프 (Real-Time Graph)**

시스템의 정보, SYN Flood 공격 정보, Connection Limiting 정보를 제공



[Port Statistics]




[Real-Time Graph]

- Alarm Manager 기능

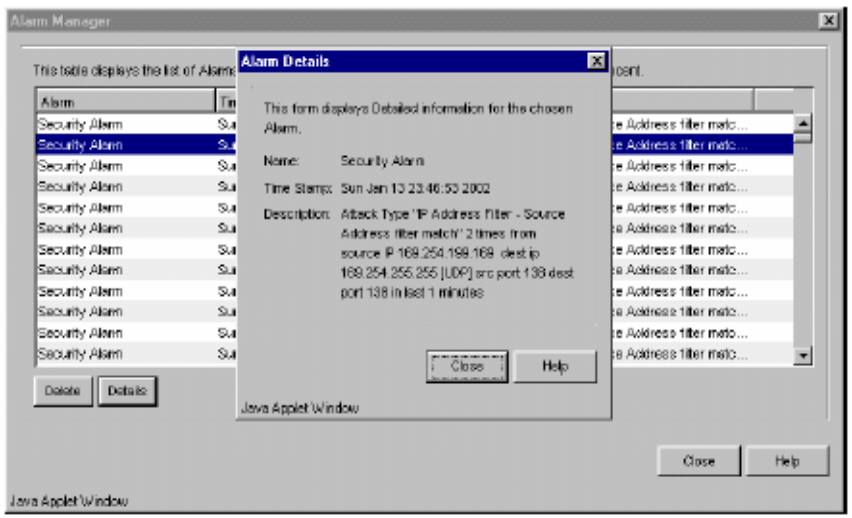
각종 경보들은 특별한 상황에 경고를 관리자에게 보내기 위해 알람 매니저를 사용한다.

알람 경고 시 알람 종류, 시간, 설명 필드를 관리자에게 전송한다.

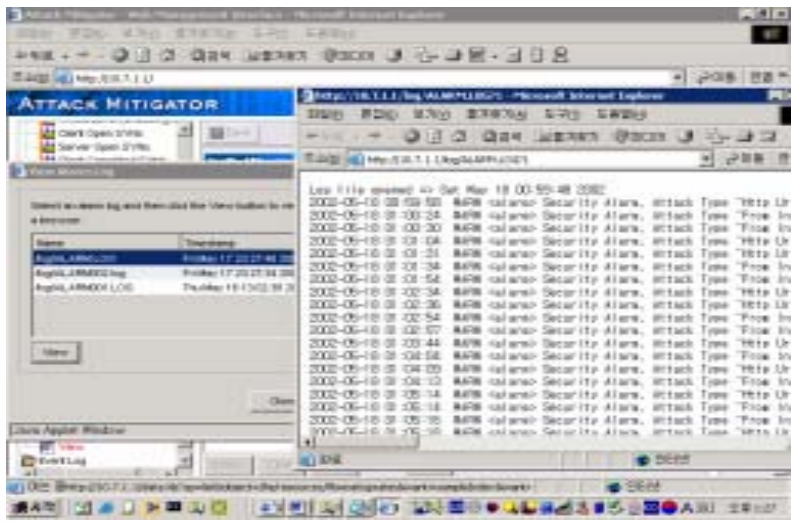
- 알람 로그 (Alarm Log) 기능

모든 알람 로그는 텍스트 포맷으로 자동으로 저장

MS-Excel 매크로 기능을 이용하며, 그래프와 보고서 형태의 포맷으로 변환 가능




[Alarm Manager]



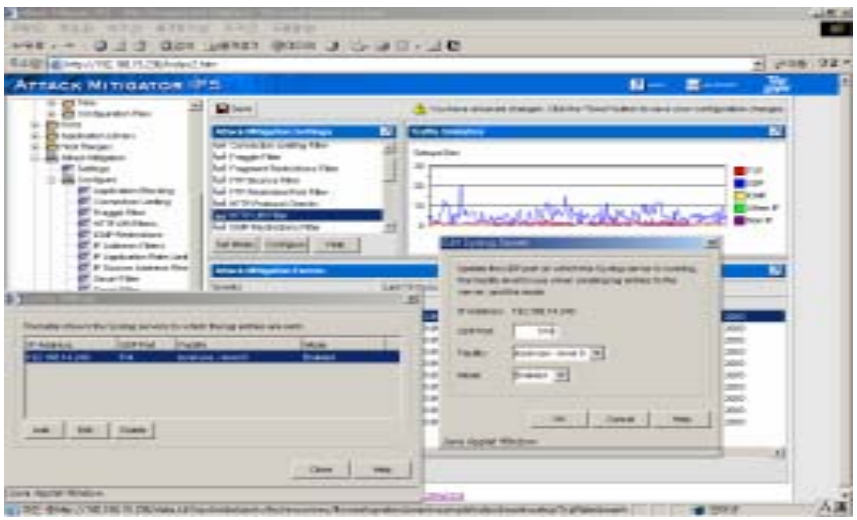

[Alarm Log]

▪ Syslog 서버를 이용한 Syslog 열람기능

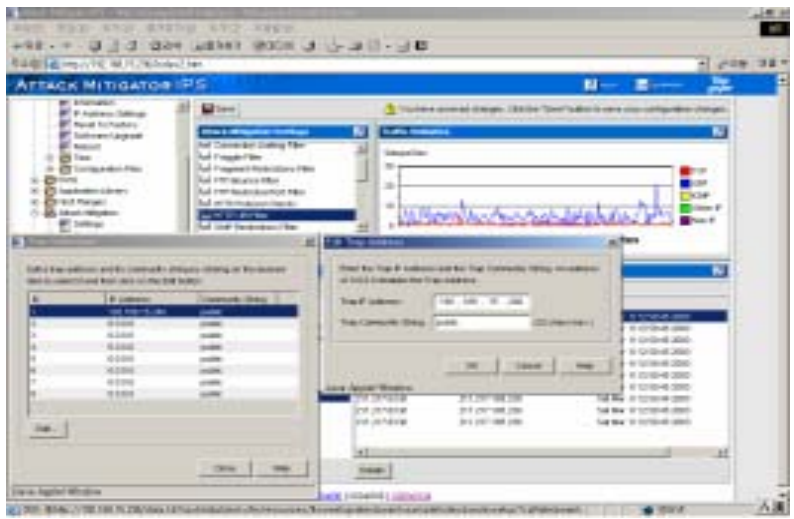
원격지에 위치한 별도의 Syslog 시스템에 통보/저장

▪ SNMP Trap 기능

각종 시스템 관련 정보를 SNMP Trap을 통해 원격지에 있는 시스템에 통보



[Sys Log]



[Alarm Log]

# AM IPS100 & 1000

❑ TopFire® 아키텍쳐

- 분산 ASIC 디자인
- 어플리케이션 인식 소프트웨어
- 최적화된 다중 공격 검출 Method
- Deep Packet/Multi-Packet inspection

❑ Patented Mitigation 알고리즘

## ❑ 주요 특징

- 12개의 FE 포트(IPS100)
- 12개의 FE 포트 + 2GE (IPS1000)
- 네트워크 구성의 변화가 없는 In-Line 장비
- HTTP worm, protocol anomaly, Traffic anomaly, DDoS/DoS 검출
- Patented SYN flood 차단
- 커넥션 & 어플리케이션 대역폭 제한
- 진보된 IP spoof 차단
- By-Pass 포트 지원으로 장애 시에도 통신 보장
- 쉬운 사용 및 적용
- 통합 관리 용이 : Syslog, SNMP, Checkpoint ELA, TLN

## ❑ 적용 환경

- 방화벽 전후단
- DMZ
- 내부 서버 팜
- 부서간 보호
- Extranet과의 연결 보호

# AM IPS 성능 개요

1. ASIC 기반의 프로세싱 엔진들로 구성되어 있어 높은 성능을 지원
2. 트랜스페어런트(Transparent) 모드의 공격 차단/억제 기능을 지원하여, 별도의 논리적인 네트웍 추가나 설정이 필요없이 손쉽게 네트웍 구성이 가능
3. DoS/DDoS 차단으로 네트웍 자원을 보호하고 네트웍 성능을 향상
4. Nimda/Codered I, II와 같은 HTTP Worm 공격을 사전 정의된 URI 필터링을 통해 차단
5. 알려진 DoS/DDoS 공격에 대한 사전 정의가 되어 있어 별도의 튜닝작업이 거의 없음
6. 알려지지 않은 DoS/DDoS 공격에 대해서는 커넥션 제어를 통해 네트웍 자원에 대한 부하를 최소화하여 공격의 효용성을 무력화시키는 것이 가능
7. 특정 어플리케이션에 대해 송수신 대역폭 제한 기능을 제공하여 특정 네트웍 자원을 보호할 수 있음
8. 직관적이고 통합적인 Web 기반의 GUI와 사용이 간편한 wizard 타입의 설정 기능을 제공하므로 설정과 모니터링이 용이
9. 다양한 보고 기능 및 로그 기능 제공
10. 장비를 통과하는 트래픽을 수집, 분석하기 위한 monitor port와 설정된 룰(rule)에 의해 drop되는 패킷만을 수집하기 위한 discard port 제공
11. 장비 자체가 공격 대상이 되는 것을 방지하기 위해 네트웍 운영을 하기 위한 별도의 운영포트 제공

# AM IPS의 바이러스 및 공격 차단 항목

1.전형적인 DoS/DDoS 공격들

- LanD
- Teardrop
- Bonk/Boink/NewTeardrop
- jolt/sping
- TCP sequence Number
- TCP connection hijacking
- UDP Bomb
- FTP Bounce
- ICMP Violations
- Trinoo
- TFN(Tribed Flood Network)
- IP Fragmentation Restrictions 등

2. Flood 공격들

SYN Floods
ICMP Floods, UDP Floods
UDP137,UDP138,TCP139를 이용한 오파 바이러스

3. Spoof 공격

Source IP Address spoofing

4. HTTP Worm 공격 (사용자 정의가 가능)

- Nimda
- Code-Red I, II
- RAT/Orion/KAOS 등 각종 백 도어 프로그램들
- SQL Overflow/ANYwhere/AW-DBSYNC 등의 SQL 취약점을 이용한 각종 공격들
- Doly/NETmonitor Trojan 및 각종 트로이 목마
- 이외의 여러 종류의 HTTP Worm 공격들

5. 커넥션 기반의 공격들 (사용자 정의가 가능)

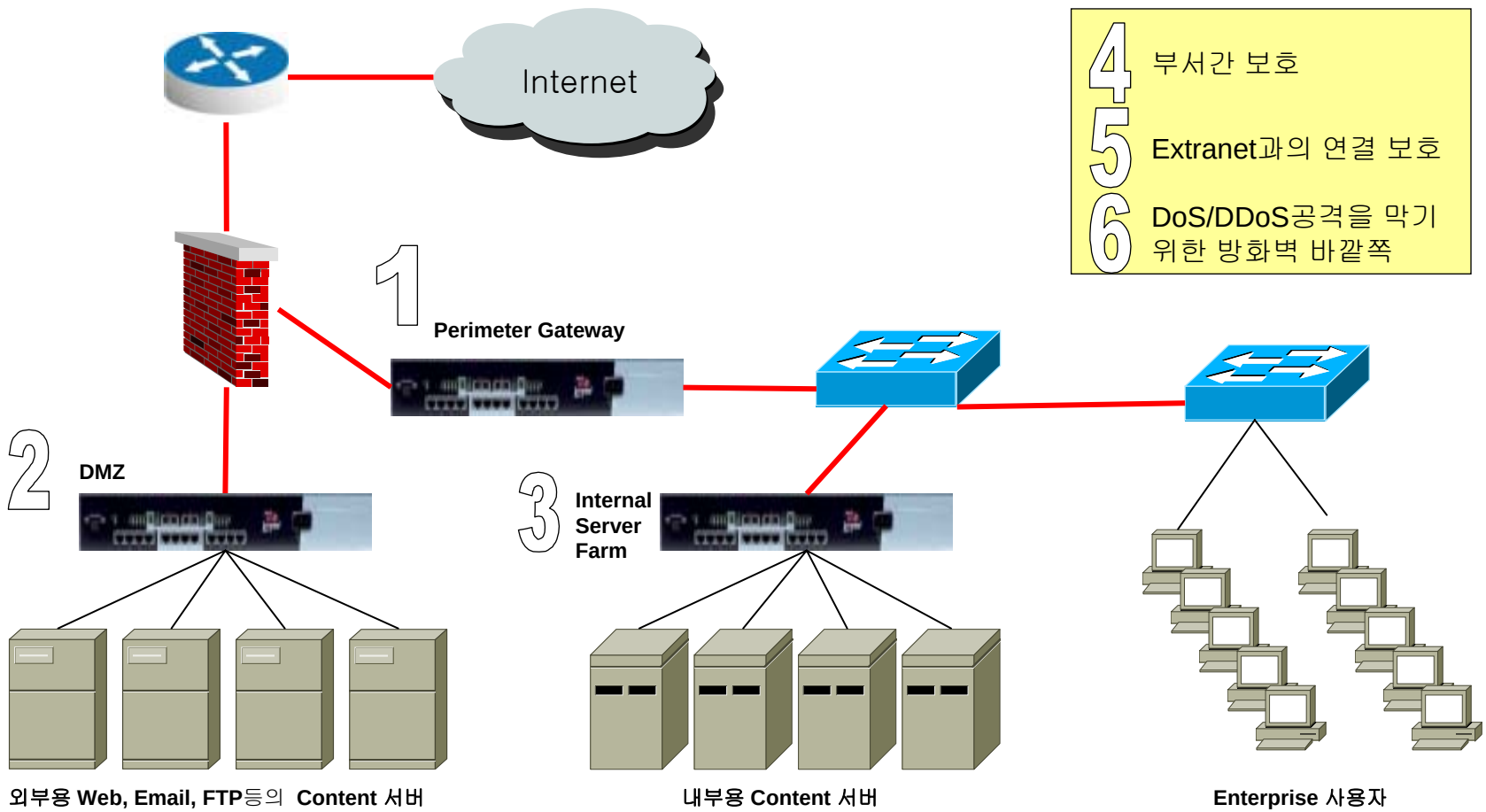
- 대량의 합법을 가장한 HTTP GETs 공격 (어플리케이션 대역폭 제한을 사용하여 차단)

6. Broadcast 공격들 (사용자 정의가 가능)

- Smurf
- Fraggle

# AM IPS 장비 배치 구성

- 아래 그림에서처럼 네트워크 안에 다양한 설치 옵션을 가집니다



# 감사합니다.

㈜에프네트 SS팀

김임성 T. 02-2167-2953, 018-262-0820, iskim@f-net.co.kr

김형태 T. 02-2167-2844, 016-231-9926, htkim@f-net.co.kr