시스템 개요

유해트래픽차단시스템 (Attack Mitigator IPS)

Attack Mitigator IPS – Top Layer Networks

Top Layer Networks, Inc. 소개

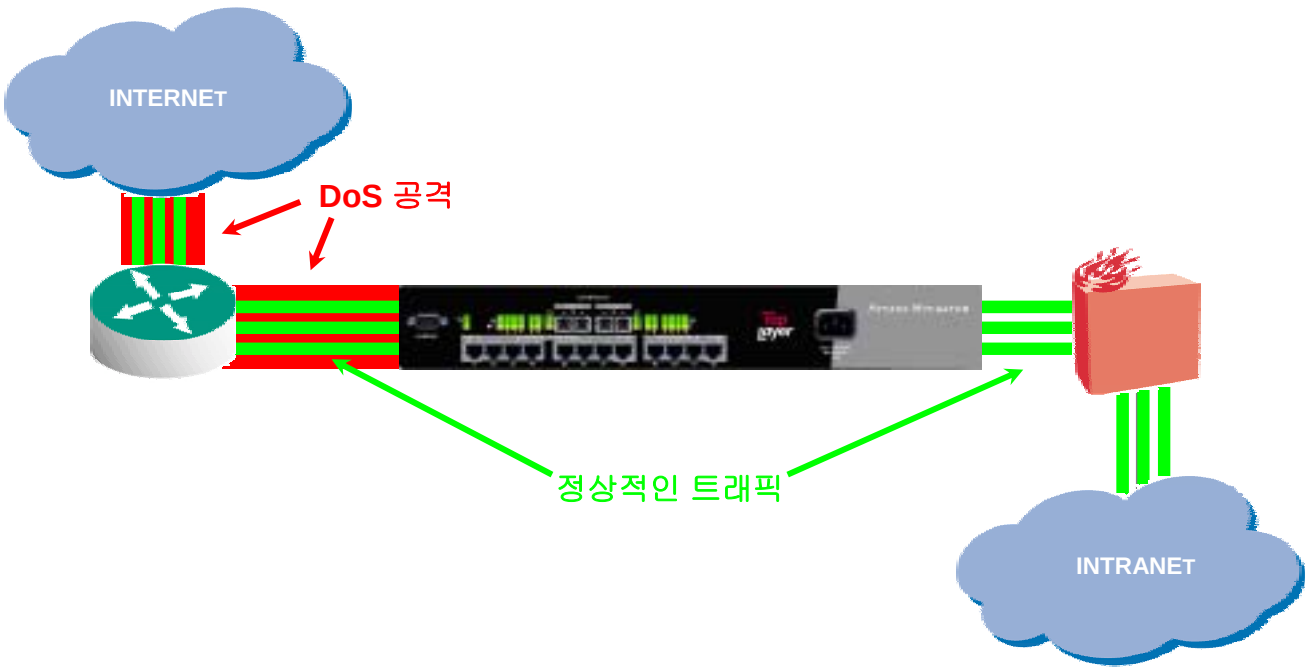
- 본　사 : 미국 보스톤
- 지　사 : 영국, 독일, 호주, 일본, 한국, 중국, 말레이시아 외 다수
- 직원수 : 전 세계적으로 약 200 + 여명의 직원이 근무
- 특　징 :
  - Layer 7 스위칭 기술 개념을 최초로 확립하여 이와 관련한 분야에서 선두 주자
  - 침입탐지시스템(IDS) 로드밸런싱 기술 및 시장의 선두 주자
  - 한국 금융권 보안 네트웍 납품 실적의 선두 주자

가. 시스템 개요

가) 유해트래픽차단시스템 (Attack Mitigator IPS)

Attack Mitigator IPS의 정의

- DoS/DDoS 및 HTTP Worm(Nimda/Codred) 공격이 네트웍 자원을 공격하여 네트웍 서비스가 무력화되기 이전에, 이를 효과적으로 차단하여 서버 및 네트웍 자원의 성능/효율이 떨어지지 않도록 하는 네트웍 보안 장비의 일종



가. 시스템 개요

가) 유해트래픽차단시스템 (Attack Mitigator IPS)

Attack Mitigator IPS 개요

- 트랜스페어런트(Transparent) 모드의 공격 차단/억제 기능으로 논리적인 네트웍의 분리/추가가 필요없음

- 보호하고자 하는 네트웍 자원의 전단에 위치하여 각종 DoS/DDoS, HTTP Worm 공격들을 효과적으로 차단하는 시스템

- Full ASIC 기반의 아키텍쳐로 효율적인 트래픽 처리가 가능

- 하드웨어와 소프트웨어가 일체화된 원박스 타입의 장비로 동작을 위해서 별도의 부가적인 소프트웨어 추가가 필요없음

- 기존에 사용되고 있는 네트웍 및 보안 시스템을 제거하지 않고도 그대로 사용 가능함으로써 기존 투자 자원을 그대로 보전

- 웹 기반의 손쉬운 사용자 인터페이스를 제공하며, 마법사(wizard) 형식으로 장비 설정이 가능하여 손쉽게 설치/운영이 가능

나. 시스템 특징 및 장단점

가) 유해트래픽차단시스템 (Attack Mitigator IPS)

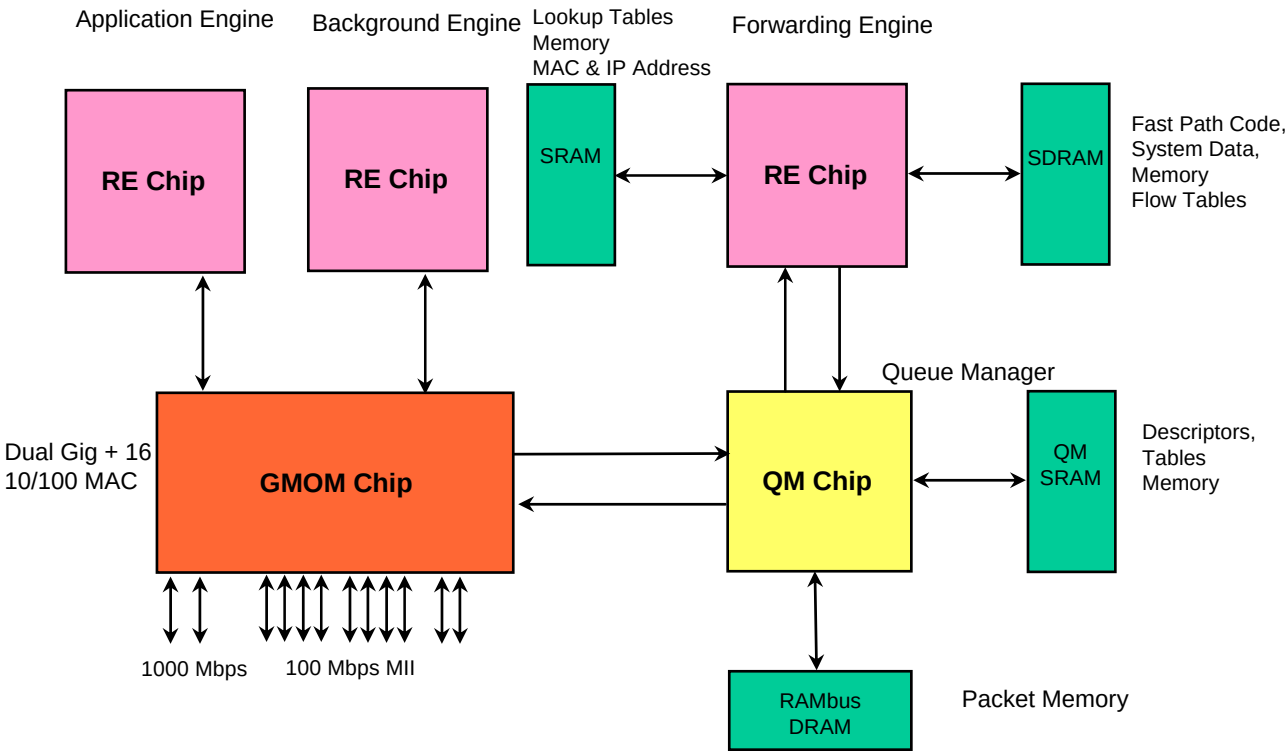
Attack Mitigator IPS의 특징과 장점

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

다. 시스템 사양

가) 유해트래픽차단시스템 (Attack Mitigator IPS)

Attack Mitigator IPS의 아키텍쳐



- 기능별로 분리된 ASIC 기반의 아키텍쳐
  - Attack Mitigator 장비는 ASIC 기반의 엔진들을 장착한 소프트웨어/하드웨어 통합 모듈로 구성되어 있음
  - 전체 아키텍쳐는 Forwarding Engine, Background Engine, Application Engine, QM이라는 ASIC 프로세서와 물리적인 포트를 관장하는 GMOM 칩 및 이에 부속된 메모리로 구성되어 있음

- 최적화된 구조 설계로 회선속도(wire-speed) 제공

- 확장이 용이

다. 시스템 사양

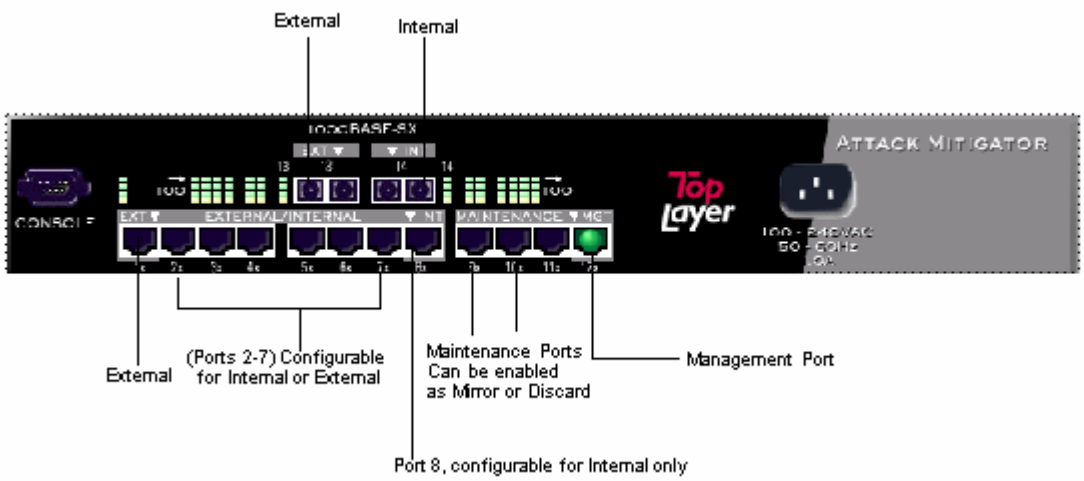
가) 유해트래픽차단시스템 (Attack Mitigator IPS)

Attack Mitigator IPS의 시스템 사양

- 전체 포트 수 (**IPS 1000**) : **2 x 1Gbps + 12 x 10/100Mbps**
- 전체 포트수 **(IPS 100)** : **12 x 10/100Mbps**
- 포트당 최대 대역폭 : **1Gbps**
- 백플레인**(backplane)** 속도 : **4.4Gbps**
- 최대 처리율 **(throughput)** : **2.2Gbps FDX**
- 최대 초당 패킷 처리율 **(pps)** : **2.6Mpps**
- 메모리 용량 : **320MByte**
- 최대 플로우 **(Flow)** 테이블 : **256K (262,143)**개
- 최대 세션 **(session)** 테이블 : **128K (131,071)**개
- 최대 동시 사용자 수 : **16,000**명
- 최대 초당 **SYN Flood** 차단률 : **80K ~ 90K**개
- 최대 **Applications** : **16,000**개
- 최대 **Applications Groups** : **8**개
- 최대 브리지 **(Bridge)** 테이블 : **8,192**개
- 최대 **ARP** 테이블 : **8,192**개
- 최대 멀티캐스트 **(Multicast)** 테이블 : **1,024**개
- 최대 **IP Address Filters** : **996**개
- 최대 **URIs** : **256**개

다. 시스템 사양

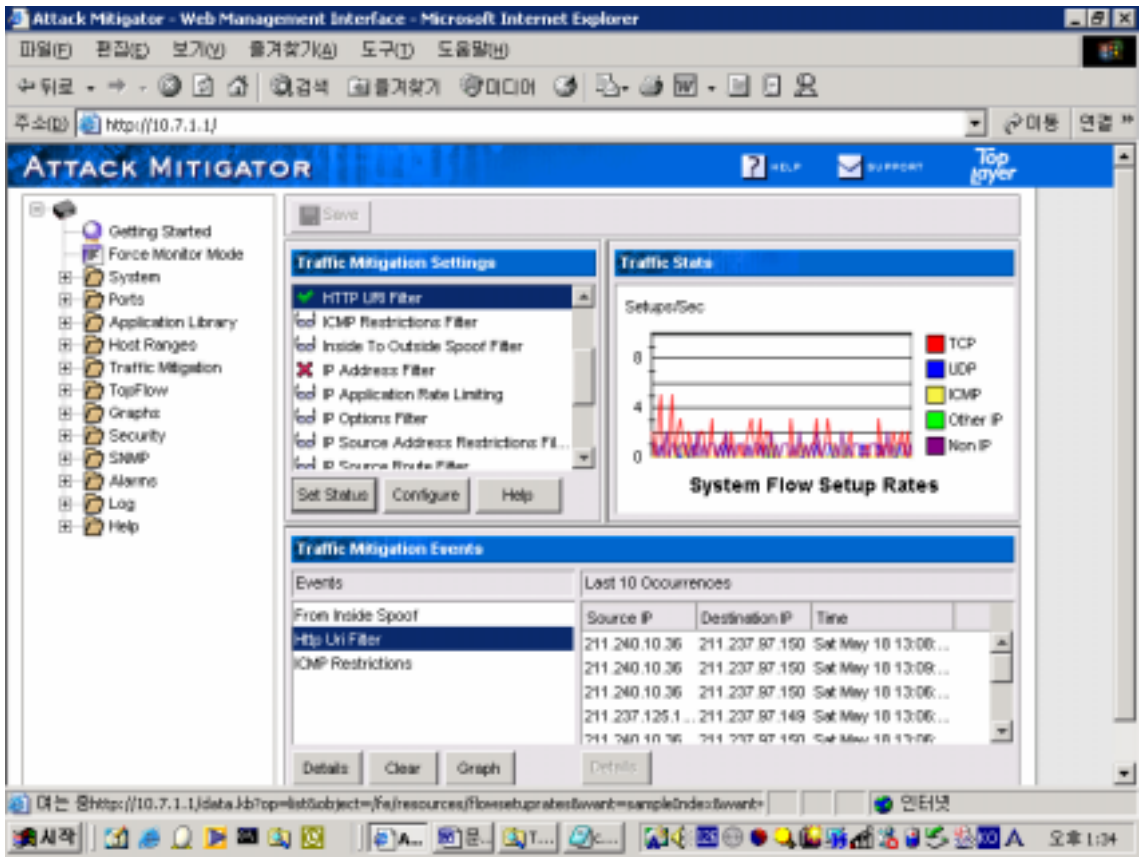
Attack Mitigator IPS 1000 전면 구성



- 전면 구성
  - 커멘드 방식의 인터페이스(CLI)를 지원하기 위한 RS-232c 포트 제공
  - 총 2개의 1000Mbps SX포트와 12개의 10/100Mbps 네트웍 인터페이스로 구성
  - 각각의 인터페이스 포트는 External, Internal, Monitor, Discard, Management 포트들로 구성
- 외부 네트웍과의 열결을 위한 external 포트 제공
- 내부 네트웍과의 연결을 위한 internal 포트 제공
- 시스템을 통과하는 모든 트래픽을 수집하기 위한 monitor 포트와 설정된 룰(rule)에 의해 드롭된 패킷을 수집하기 위한 Forensic 포트 제공
- 시스템 자신이 공격 대상이 되는 것을 방지하기 위해서 별도의 운영(management) 포트 제공

다. 시스템 사양

Attack Mitigator IPS GUI 메뉴(Web 기반) 구성

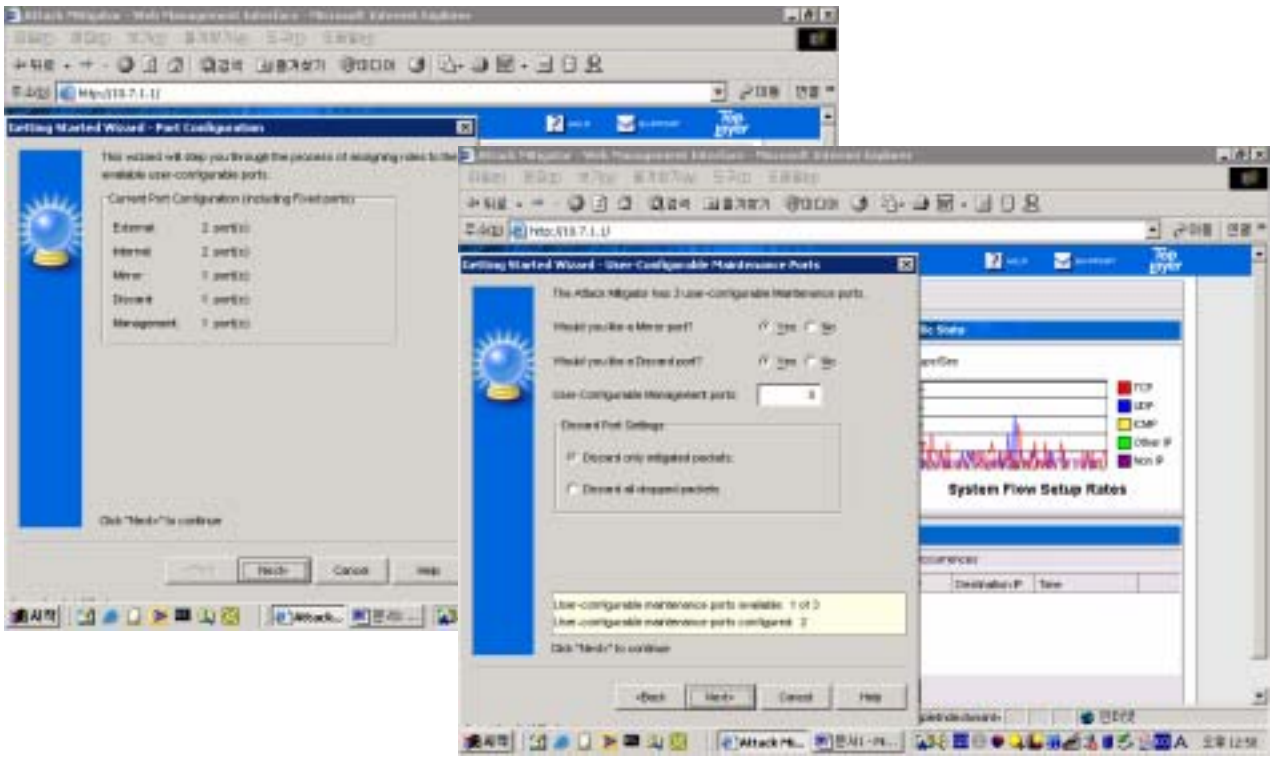


- 인터페이스 구성

  - 설정 메뉴 디렉토리 (좌측면 윈도우)
  - 공격에 대한 룰 설정 메뉴 (중앙 상단 윈도우)
  - 실시간 트래픽 그래프 (우측 상단 윈도우)
  - 인식된 공격의 종류 (중앙 하단 윈도우)
  - 해당 공격의 source/destination 주소값 과 발생 시각 (우측 하단 윈도우)

다. 시스템 사양

Attack Mitigator IPS 의 설정



- Wizard 형태의 설정

  - 친숙한 PC 프로그램 설치 과정과 유사한 구성
  - 정해진 과정을 따라서 진행하기만 하면 실시간 적으로 설정이 가능
  - 직관적이고 논리적인 설정 인터페이스를 제공