DDoS Attack Defense List

TCP 공격 방어
TCP SYN Flooding
TCP SYN-ACK Flooding
TCP RST Flooding
TCP FIN Flooding
TCP ACK Flooding
TCP URG Flooding
TCP PSH Flooding
TCP XMAS Flooding
TCP MISC Flooding
TCP Land2 Attack
TCP CPS, Session, BPS, PPS Rate-Limit
TCP Open Connection
TCP No Data Connection
TCP Invalid Port Attack
TCP Invalid Flag Attack
TCP Invalid Header Length Attack

FTP 공격 방어
FTP Direction Traversal Attack
FTP Bounce Attack
FTP User Name Overflow
FTP/Telnet Escape Sequence Detect

HTTP 공격 방어
HTTP Flooding
HTTP Post Attack (Session, IP)
HTTP Caching Behavior Anomaly (CC, Circle Attack)
HTTP Slow loris Attack
HTTP Request Anomaly Attack
HTTP XFF Field Based Defense
HTTP Invalid URI Length Attack
HTTP Slow Read Attack (Session, IP)
HTTP Repeated Pattern Flooding Attack
Server Behavior Anomaly Attack
Slow Read Attack
SSL Renegotiation Attack
SQL Query Flooding Attack

ICMP 공격 방어
ICMP Flooding
ICMP Echo Request Flooding
ICMP Echo Replay Flooding
ICMP Unreachable Flooding
ICMP BPS, PPS Rate-Limit
ICMP Ping of Death Attack

UDP 공격 방어
UDP Flooding
UDP Invalid Header Length Attack
UDP Land2 Attack
UDP BPS, PPS Rate-Limit
UDP Invalid Port Attack

DNS 공격 방어
DNS Request Flooding
DNS Response Flooding

VoIP 공격 방어
Request Flooding
Response Flooding
Malformed Message

비정상 패킷 공격 방어

시그니쳐 기반 방어

지역 기반 방어

Zero-Day Attack& Unknown Attack 방어

Hardware Specification

Title		MFD 2000	MFD 4000	MFD 20000
Chassis				
CPU		4 Core	10 Core	8 Core x 2EA
Memory		16 GB	32 GB	32 GB
HDD		1 TB	2 TB	2 TB
DDoS 방어 성능		2 Gbps	4 Gbps (MAX 20 Gbps)	20 Gbps (MAX 100 Gbps)
Network Interface	1G Copper	8 (max 32)	8 (max 32)	- (max 32)
	1G Fiber	8 (max 16)	8 (max 16)	- (max 24)
	10G Fiber	-	- (max 8)	8 (max 24)
Power Supply		Redundant (460 Watts)	Redundant (600 Watts)	Redundant (1010 Watts)
Dimension (W x D x H)		2U (431 x 600 x 88)	2U (431 x 600 x 88)	3U (431 x 664 x 132)

* CC 인증 평가 기준의 성능 및 기능 시험을 모두 통과한 DDoS 전용 제품

CERTIFICATIONS

SECUI (주)시큐아이
서울특별시 중구 소공로 48 5-7F
tel 02 3783 6600 fax 02 3783 6499 www.secui.com
대표전화 080 331 6600
평일 am 8:00 - pm 5:00 (토, 일, 공휴일 제외)

SECUI MFD is Designated for DDoS Attack Prevention System
* DDoS_ Distributed Denial of Service

SECUI MFD

SECUI MFD IS
DESIGNATED FOR DDoS ATTACK PREVENTION SYSTEM

SECUI

Introduction

SECUI MFD는
네트워크 보안 **국내 1위**인 **시큐아이**의 오랜 노하우를
바탕으로 개발한, 변화하는 보안 위협에 능동적으로 대응하는
차세대 **네트워크 보안 솔루션**입니다.

Designated for DDoS(Distributed Denial of Service) Attack Prevention System

최근 DDoS 공격은 사회 전반에 걸쳐 빈번하게 발생하고 있으며, 목적이 명확하고 조직적인 형태를 띠고 공격 방법도 진화하여 기존의 단순한 임계치 기반으로는 효과적인 대처가 어렵습니다. 변화하고 있는 DDoS 공격에 대응하기 위해서는 진보된 Anti-DDoS 장비가 필요합니다.

- 64비트 SecuiOS™와 멀티코어 플랫폼에 최적화된 아키텍처로 Wired-Speed 제공
- 보호 도메인, 보호 프로파일로 네트워크 환경에 적합한 유연한 보안 정책 적용
- 다계층, 다단계 방어 엔진으로 정밀한 DDoS 공격 탐지 및 차단
- 위협관리시스템 및 정보보안센터와 연계하여 효과적인 방어 체계 구축

Key Features

- **고성능**
  - 64비트 OS, 멀티코어 지원
  - 트래픽 분산 처리 및 멀티코어 최적화 기술 (SC FDE)
  - Wired-Speed 제공
- **정밀성**
  - 다단계/다계층 DDoS 공격 탐지 및 차단(SM DDE)
  - Snort, PCRE 지원
  - Anti-Botnet 솔루션 연동
- **유연성**
  - 보호 도메인, 보호 프로파일
  - In-Line 및 Out-of-Path 구성
- **가시성**
  - 통합 모니터링
  - 실시간 대쉬보드
  - 보안 정책 검색
  - 상세 로그 및 리포트

Key Functions

- 비정상 프로토콜 방어
- 서비스 거부 방어
- 블랙리스트 방어
- 응용 계층 방어
- 자동 학습 방어
- 프로토콜 취약점 방어
- 지역 기반 방어
- 시그니쳐 기반 방어

Multi-Stage, Multi-Layer DDoS Protection

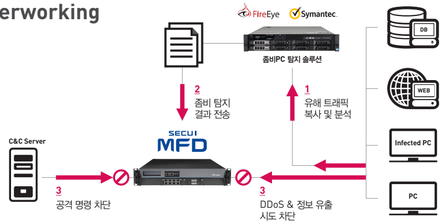
IP 계층부터 애플리케이션 계층까지
다양한 DDoS 공격을 정밀하게 탐지 및 차단

- Flooding 공격부터 다양한 응용 계층 공격까지 완벽한 방어
- 자동 학습을 통한 차단 및 국가별 DDoS 공격 방어

Anti-Botnet Solution Interworking

좀비 PC 탐지 차단 솔루션 연동으로
침해 사고 예방

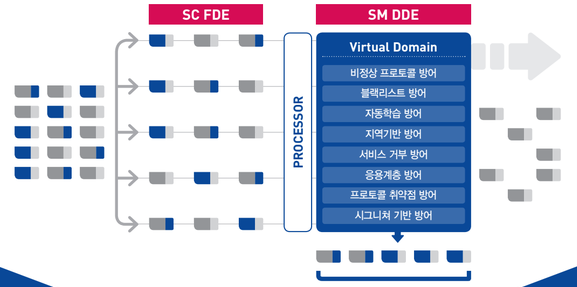
- 봇(Bot) 감염 PC 탐지 솔루션과 연동
- DDoS 공격 시도 차단 및 내부 정보 유출 방지



SM DDE

SECUI Multi-Stage DDoS Defence Engine

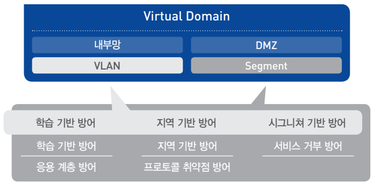
Multi-Stage, Multi-Layer DDoS Protection / Anti-Botnet Solution Interworking / Easy to Setup and Manage / Smart Threat Management / Security Information Center / Virtual Domain



Virtual Domain

가상 도메인으로 네트워크 환경에 적합한
유연한 DDoS 방어 정책 적용

- 네트워크를 물리적 및 논리적인 가상 도메인 설정
- 도메인별 별도 보호 프로파일 지정으로 유연한 보안 정책 적용



Easy to Setup and Manage

편리한 설정 및 관리 기능으로 관리자 개입 최소화

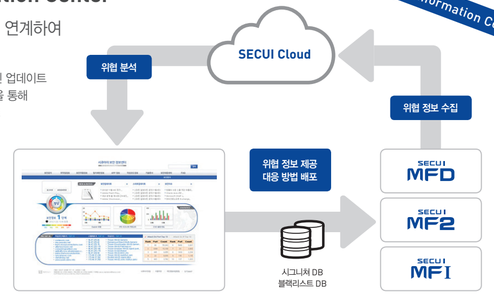
- 통합 대시보드 및 실시간 모니터링으로 직관적인 공격 현황 파악
- 보안 정책 검색 및 로그 기반의 간편 보안 정책 설정 제공

통합 대쉬보드 / 글로벌 공격현황

Security Information Center

시큐아이 보안정보센터와 연계하여
효과적인 방어 체계 구축

- DDoS 전용 시그니쳐의 지속적인 업데이트
- 클라우드 기반의 악성코드 분석을 통해 악성코드를 배포하는 블랙리스트 정보로 사고 예방



Smart Threat Management

위협관리시스템인 STMS(SECUI TMS)와 연동을 통해
보안 위협에 대한 조기 예경보 체계 구축

- 통합 설정, 모니터링, 로그 관리 등 통합 설정 기능 연동
- SECUI MFD, SECUI MF2, SECUI MFI 제품의 정보 분석 및 위협 관리