




DDoS Attack Defense List

| TCP 공격 방어 | HTTP 공격 방어 | UDP 공격 방어 |
|---------------------------------------|---|--|
| TCP SYN Flooding | HTTP Flooding | UDP Flooding |
| TCP SYN-ACK Flooding | HTTP Post Attack (Session, IP) | UDP Invalid Header Length Attack |
| TCP RST Flooding | HTTP Caching Behavior Anomaly (CC, Circle Attack) | UDP Land2 Attack |
| TCP FIN Flooding | HTTP Slow loris Attack | UDP BPS, PPS Rate-Limit |
| TCP ACK Flooding | HTTP Request Anomaly Attack | UDP Invalid Port Attack |
| TCP URG Flooding | HTTP XFF Field Based Defense | |
| TCP PSH Flooding | HTTP Invalid URI Length Attack | DNS 공격 방어 |
| TCP XMAS Flooding | HTTP Slow Read Attack (Session, IP) | DNS Request Flooding |
| TCP MISC Flooding | HTTP Repeated Pattern Flooding Attack | DNS Response Flooding |
| TCP Land2 Attack | Server Behavior Anomaly Attack | |
| TCP CPS, Session, BPS, PPS Rate-Limit | Slow Read Attack | VoIP 공격 방어 |
| TCP Open Connection | SSL Renegotiation Attack | Request Flooding |
| TCP No Data Connection | SQL Query Flooding Attack | Response Flooding |
| TCP Invalid Port Attack | | Malformed Message |
| TCP Invalid Flag Attack | ICMP 공격 방어 | |
| | ICMP Flooding | 비정상 패킷 공격 방어 |
| FTP 공격 방어 | ICMP Echo Request Flooding | 시그니처 기반 방어 |
| FTP Direction Traversal Attack | ICMP Echo Replay Flooding | Anti-Botnet |
| FTP Bounce Attack | ICMP Unreachable Flooding | |
| FTP User Name Overflow | ICMP BPS, PPS Rate-Limit | 지역 기반 방어 |
| FTP/Telnet Escape Sequence Detect | ICMP Ping of Death Attack | Zero-Day Attack & Unknown Attack 방어 |

Hardware Specification

| SECUI MFD | 2100 | 4100 | 21000 |
|------------------------------|---|--|---|
| Chassis |  |  |  |
| CPU | 4 Core | 10 Core | 18 Core x 2EA |
| Memory | 16 GB | 32 GB | 64 GB |
| HDD | 1 TB | 2 TB | 2 TB |
| DDoS 방어 성능 | 2 Gbps(max 10Gbps) | 4 Gbps(max 40Gbps) | 20 Gbps(max 100Gbps) |
| Network Interface | 1G Copper | 8(max 32) | 8(max 32) |
| | 1G Fiber | 8(max 16) | 8(max 16) |
| | 10G Fiber | - | -(max 8) |
| Power Supply | Redundant (500 Watts) | Redundant (500 Watts) | Redundant (800 Watts) |
| Dimension (W x D x H) | 2U (431 x 577 x 88) | 2U (431 x 577 x 88) | 2U (437 x 671 x 88) |

SECUI (주)시큐아이

서울특별시 중구 소공로 48 5~7F
tel 02 3783 6600 fax 02 3783 6499 www.secui.com

대표전화 080 331 6600

침해대응센터 02 3783 6500
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)

Copyright © SECUI All Rights Reserved. 본 카탈로그에 게재된 회사명, 상품명은 당사의 등록 상표입니다. 사양과 외관은 개량을 위해 예고 없이 변경되는 경우가 있습니다.

CERTIFICATIONS



SECUI
MFD



SECUI MFD IS DESIGNATED FOR DDoS ATTACK
PREVENTION SYSTEM

Anti-DDoS

SECUI

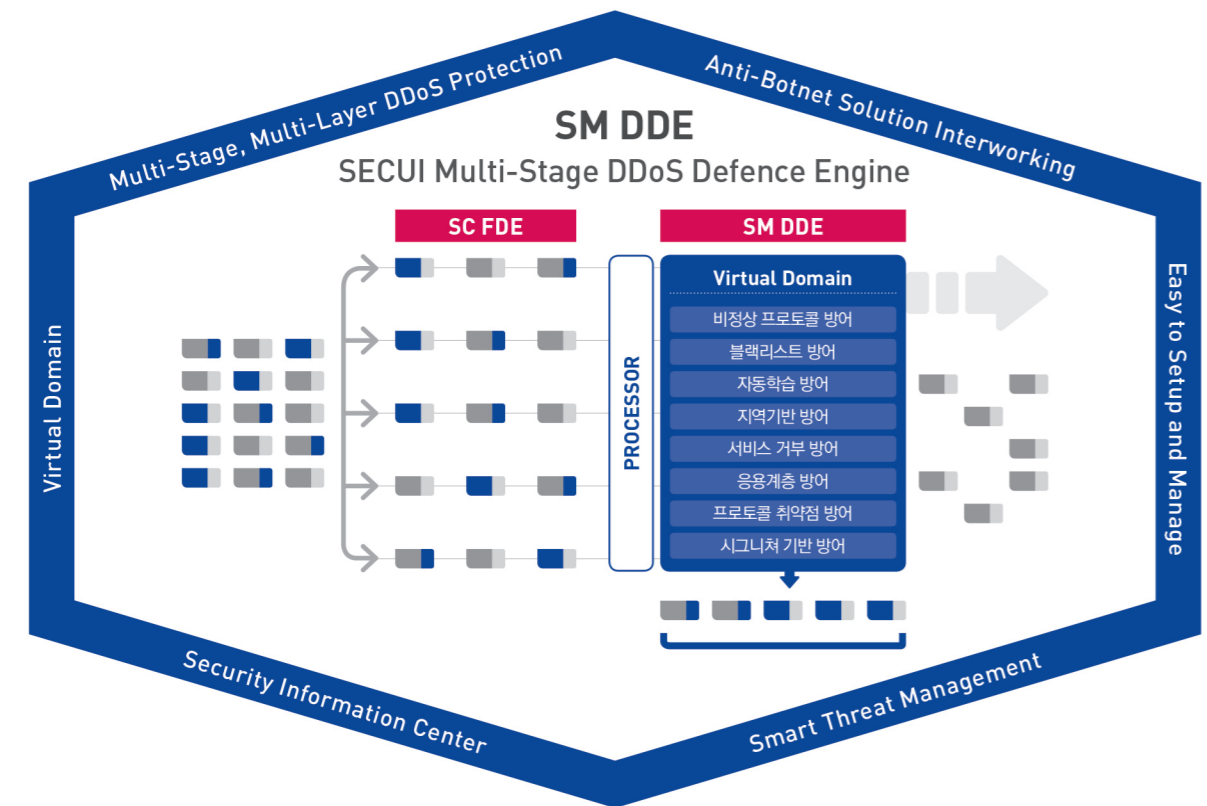
SECUI MFD

SECUI MFD는
변화하고 있는 DDoS 공격에 대응하는
차세대 Anti-DDoS 장비입니다.



Key Features

| | | | |
|--|---|---|--|
| <p>고성능</p> <ul style="list-style-type: none"> 64비트 OS, 멀티코어 지원 트래픽 분산 처리 및 멀티코어 최적화 기술 (SC FDE) Wired-Speed 제공 | <p>정밀성</p> <ul style="list-style-type: none"> 다단계/다계층 DDoS 공격 탐지 및 차단(SM DDE) Snort, PCRE 지원 Anti-Botnet 솔루션 연동 | <p>유연성</p> <ul style="list-style-type: none"> 보호 도메인, 보호 프로파일 In-Line 및 Out-of-Path 구성 | <p>가시성</p> <ul style="list-style-type: none"> 통합 모니터링 실시간 대쉬보드 보안 정책 검색 상세 로그 및 리포트 |
|--|---|---|--|



Key Functions

Multi-Stage, Multi-Layer DDoS Protection

IP 계층부터 애플리케이션 계층까지 다양한 DDoS 공격을 정밀하게 탐지 및 차단

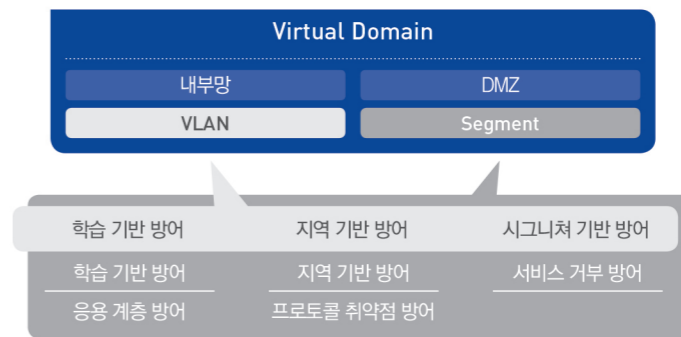
- Flooding 공격부터 다양한 응용 계층 공격까지 완벽한 방어
- 자동 학습을 통한 차단 및 국가별 DDoS 공격 방어

| | |
|--|-------------|
| 비정상 프로토콜 방어 | 서비스 거부 방어 |
| Multi-Stage, Multi-Layer DDoS Protection | 응용 계층 방어 |
| 자동 학습 방어 | 프로토콜 취약점 방어 |
| 지역 기반 방어 | 시그니처 기반 방어 |

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