< 웹 방화벽 규격서 – AIWAF-1000_Y20 >

구분	기술기준 세부 항목
H/W	- CPU : 16core 2.1GHz - Memory : 32GB 이상 (최대2TB) - HDD : 2TB 이상 - Throughput : 11G - Power : 800W Redundant Power Supply - Optional NIC: 4P UTP / 4P Fiber / 2P 10G
세부기능	In-Line, One-Armed, Sniffing, Mirroring 의 다양한 구성모드 지원 - 인터페이스에 IP 가 부여되지 않는 투명 프록시 게이트웨이 모드 지원 - 장비 자체적인 HA(Active-Active / Active-Standby) 구성 기능 제공 - 별도의 장비 없이 이중화 시스템 간 비동기 트래픽 처리 기능 제공 - 다중 네트워크 수용을 위한 멀티 세그먼트 환경에서의 비동기 트래픽 처리 기능 제공 - 네트워크 인터페이스 본딩 기능 제공 - Ipv6 트래픽에 대해 Ipv4 트래픽과 동일한 보안 기능 및 구성 제공 - 별도의 라이센스 및 H/W 없이 기본 SSL 트래픽의 암복호화 처리 기능 제공 - 3rd party 솔루션으로 복호화 된 HTTPS 트래픽 전송 기능 제공 - SSL 미지원 웹서버의 SSL 서비스 대행을 위한 SSL Termination 기능 제공 - 웹 서버 SSL 트래픽 부하 감소를 위한 SSL Offload 기능 제공 - 서버 로드밸런싱(Hash, Round-robin, Latency, Least connection) 기능 제공
	- 양 방향 세션(클라이언트/서버)에 대한 SSL 버전 및 암호화 알고리즘(Cipher) 차등 설정 기능 제공 - 히든 필드의 파라미터 조작 탐지 기능 제공 - 미 허용 SSL 버전에 대한 상위 프로토콜 사용 권고 안내 페이지 제공 기능 - 미러링모드 구성시에도 SSL 트래픽에 대한 암복호화 및 탐지 기능 제공 - 국정원 8 대취약점 및 OWASP Top10 탐지 기능제공

	- URL, HEX, Unicode, Base64 등 우회 목적의 더블(또는 다중) 인코딩 트래픽에 대한 실시간 디코딩 및 보안 기능 탐지 제공 - 도메인별 정책 설정 및 도메인별 관리자 설정 지원 - 별도의 도메인 등록없이 웹서버 IP/Port 정보만으로 URL 탐지 기능제공 - 각 정책 별 개별 패턴에 대한 Enable / Disable 기능 - 각 정책 별 적용 클라이언트 IP, 예외 클라이언트 IP 설정 및 적용 URL, 예외 URL 설정 기능 제공 - HTTP 본문 외 헤더(User-Agent, Origin, Cookie 등)에 삽입된 공격 탐지 기능 제공 - 웹 소켓(Web Socket) 트래픽에 삽입된 공격 탐지 기능 제공 - 웹 서버 응답페이지 본문에 삽입된 악성코드(Exploit Kit, 리다이렉트, js 난독화 등) 검출을 통한 경유지/유포지 악용 탐지 기능 제공 - 인가된 사용자만 계정 기반으로 지정된 서비스(URL)에 접속할 수 있도록 제한 하는 기능 제공 - HTTP 기반 DoS 공격(HTTP Flood, Slowloris, RUDY, Hash DoS, Range DoS, 과다 세션 발생)에 대한 방어 기능 제공 - CAPTCHA 를 통한 일반 사용자 또는 컴퓨터 프로그램 여부 검증 기능 제공 - 크롤러, 스크래퍼 등 컴퓨터 프로그램(Bot) 탐지 가능한 Honey Pot TRAP, JS Injection 기능 제공 - HTTP 요청 파라미터 유형에 대한 프로파일링 기능 및 자동 정책 반영 기능 제공 - 자동 및 수동 패턴 업데이트 및 업데이트시 네트워크에 영향이 없는 무 중단 서비스 제공 - 구 정책의 일괄적인 복원 시 리부팅 없는 무 중단 서비스 제공 - 정책 별 차단페이지 설정 기능 제공 - HTTP 프로토콜에 위배되는 비정상적인 요청 탐지 기능 제공 - Proxy 서버를 경유하는 클라이언트의 실제 IP(X-Forwarded-For, True-Client-IP 등) 헤더 지정 및 지정 헤더(IP) 기준 정책 탐지 기능 제공 - 외부에 오픈 되어 있는 Proxy 서버 IP 정보 자동 업데이트 및 Proxy 서버 경유 IP 탐지 기능 제공

	- 악성 파일 업로드 탐지 기능 (확장자 제어 및 컨텐츠 미일치 탐지기능 등) - 웹쉘 파일 업로드 및 업로드 된 웹쉘의 접근 탐지 기능 제공 - 단순 로그인 페이지의 접속이 아닌 다량의 로그인 시도 탐지 기능 제공 - 웹 서버 응답페이지의 DBMS 메시지 클로킹 기능 제공 - 웹 캐싱 기능을 통한 웹 가속 및 캐싱 정보/현황 디스플레이 기능 제공 - 이중화 된 장비간 정책 동기화 기능 제공 - 원격 접속 시 암호화 통신(SSH, HTTPS) 기능 제공 - 관리자별 권한 설정 및 접근 제어 IP 기능 제공 - 다양한 EMS 연동을 위해 탐지로그 및 감사로그, 시스템 로그의 포맷 사용자 지정기능 제공 - 별도의 설치프로그램 및 Active-X 설치가 필요 없는 웹 기반 GUI 관리 콘솔페이지 제공 - 다양한 항목의 통계보고서 및 자동 보고서 생성 및 이메일 발송 기능 제공 - SNMP GET 및 SNMP TRAP 기능 제공 - 반복적인 공격을 수행하는 클라이언트 IP 를 효율적으로 차단하기 위한 탐지 대상 정책 설정(제공되는 정책 중 필요 정책만 선택) 및 자동 탐지 기능 제공 - 3rd party 솔루션과 연동을 위한 웹 방화벽 운영 및 정책 설정에 대한 REST API 제공 - 웹 서버 응답페이지 내 존재하는 주석 문 제거 후 클라이언트에게 전송하는 기능 제공 - 보호대상 서버에 해당되는 수신 트래픽 중, 웹이 아닌 경우 자동으로 바이패스 하여 서비스 가용성을 확보할 수 있는 옵션 제공 - 개인정보가 삽입된 임베디드 타입 파일(파일 내 또 다른 파일 존재)에 대한 업로드/다운로드 탐지 기능 제공 - HTTPS 서버에 대한 인증서 및 개인키 관리 시, 보호대상 웹 서버에 등록/설정된 SSL 인증서를 비롯 프로토콜 및 알고리즘 동기화 기능 제공 - 탐지로그에서 해당 탐지 정책의 예외 URL 로 즉시 등록 가능한 원 클릭 편의 기능 제공

	- 탐지로그에서 해당 클라이언트 IP 를 화이트리스트 또는 블랙리스트로 즉시 등록 가능한 원 클릭 편의 기능 제공 - 도메인별 개별 대시보드 제공 및 HTTP/HTTPS 트래픽 처리(MBPS, CPS, TPS 등) 정보 분리 제공 - 도메인별 HTTP, HTTPS, 전체에 대한 각 각의 트래픽 임계치를 설정하여 과다 트래픽이 발생하는 도메인에 대한 자동 경고 메일 발송 기능 제공 - 탐지 데이터에 대해 사용자 정의 형태로 차트 생성가능한 피벗 차트 기능 제공 - 보호대상 웹 서버의 서비스 퀄리티(응답 코드, 응답속도, 가용률 등)에 대한 실시간 모니터링 제공 - 웹 서비스 가용성 확보를 위한 도메인별 대역폭 QoS 설정(Bandwidth Limit) 기능 제공 - 공격 트래픽의 탐지 여부 확인을 위한 셀프 테스트 기능 제공 - CVE 취약점 코드 별 대응 패턴 검색 기능 제공 - Cyber Threat Intelligence Platform 연동을 통한 다양한 웹 공격 위협(Black Client IP, C&C IP 등)에 대한 실시간 대응 - 머신 러닝 연동을 통한 Unknown 공격 탐지 기능 제공 - HTTP/2 프로토콜 지원(HTTP/1.1 과 동일한 보안 기능 및 탐지로그 제공) - HTTPS TLS 1.3 지원 - HTTPS 인증서 만료 시 서비스 가용성 확보를 위한 자동 바이패스 기능 제공 - HTTPS 인증서 만료 전 사전 알림(경고 팝업, E-mail) 기능 제공 - User Interface 기반 TCPDUMP, Debug log, 시스템 복구 모드 등 다양한 트러블슈팅 기능 제공