물 품 규 격 서

구 분	세 부 규 격	수 량
제품명	차세대방화벽	2식
지원 인터페이스	<ul style="list-style-type: none"> - 40GE QSFP+ 2슬롯 이상 제공 - 25GE SFP28 / 10GE SFP+ 4슬롯 이상 제공 - 10GE SFP+ 4슬롯 이상 제공 - 1GE SFP 8슬롯 이상 제공 - 1GE RJ45 16포트 이상 제공 - 1GE Mgmt RJ45 1포트, 1GE HA RJ45 1포트 제공 	
시스템성능	<ul style="list-style-type: none"> - 방화벽 성능 : 1518바이트 기준 80Gbps, 64바이트 기준 45Gbps 이상 제공 - 방화벽 성능(PPS) : 67.5Mpps 이상 제공 - IPS 성능 : 12Gbps 이상 제공 - NGFW 성능 : 9Gbps 이상 제공 (FW, IPS, App-Control enable) - Treat Protection 성능 : 7Gbps 이상 제공 (FW, IPS, App-Control, Malware enable) - SSL Inspection 성능 : 10Gbps 이상 제공 - 8,000,000개 이상 동시 접속 세션 처리 성능 제공 - 500,000개 이상 초당 접속 세션 처리 성능 제공 - SSL VPN 성능 : 8Gbps 이상 제공 - IPSec VPN 성능 (AES256-SHA256) : 512바이트 기준 48Gbps 이상 제공 - Firewall Latency : 2.8μs 이하 성능 제공 - 방화벽 정책 : 100,000개 이상 수립 가능 	
세부 기능	<p>▶ 네트워크 기능</p> <ul style="list-style-type: none"> - Static 및 다양한 Dynamic Routing 프로토콜을 지원해야 한다 - LLCF(혹은 유사한 인터페이스 감시) 기능을 제공해야 한다. - ECMP (Equal Cost Multi Path)를 지원해야 한다. - Policy Based 라우팅 기능을 제공해야 한다 - IPv6 주소 체계를 지원해야 한다 - Active-Standby HA 기능을 제공해야 한다. - Active-Active HA 기능을 제공해야 한다. - 인터페이스 별 Secondary IP 를 지원해야 한다. - 인터넷 회선의 효율적인 사용을 위하여 NLB (Network Load Balancing) 기능 제공 - SSL pinning 을 사용하는 client 통신을 가능하게 할 수 있도록 ssl inspection 제외 기능을 제공해야 한다. (ip 별, 서비스 별, fqdn 별, url 별 제외 기능 필요) - 내부 서버의 ssl 통신을 검토하기 위하여 private key 를 사용한 inspection 기능을 제공해야 한다.(ssl proxy) - 다수의 ssl 인터넷 연결의 암호화를 복호화 하기 위한 ssl forward proxy 기능을 제공하여야 한다. - SSL Traffic 을 복호화하여 주변 보안장치에 전달할 수 있도록 ssl mirror 기능을 제공하여야 한다. - 사용자 인터넷 회선의 효율적인 사용을 위하여 Web Cache 기능 제공 - VPN 회선의 효율적인 사용을 위하여 WAN Accelerator 기능 제공 	

- 무선 보안을 위하여 Wireless Controller 기능 제공 (동일제조사)
- AP를 포함한 무선 와이파이 맵을 제공하여야 한다.
- 불법 SSID 탐지 및 차단 기능을 제공하여야 한다.
- 주위 환경 변경 없이 방화벽 적용을 위하여 virtual wire 기능을 제공 하여야 한다.
- WAN 구간 이중회선의 지원시 회선의 패킷손실, 지터, 트래픽 증가 등 품질에 따라 업무용 애플리케이션이 회선 선택을 자동화 할 수 있어야 한다

▶ 방화벽 기능

- Layer 2 Transparent 및 Layer 3 Route 모드를 지원해야 한다 (L2/L3동시사용가능)
- Active-Active 및 Active-Standby구성이 가능해야 한다
- HA 구성 간에는 Configuration 및 Session Stateful Failover를 지원해야 한다
- 정책 별 QoS기능을 지원 (IP, Port, Application 별 QoS 기능 지원)
- Per-IP별 QoS 정책 적용
- 회선별 rate limit 기능 적용
- 특정 서비스 포트 또는 프로토콜에 대한 세션 Timeout 값 설정 기능을 지원
- 시간대 및 날짜 별 Schedule 정책 설정이 가능해야 한다
- Source 및 Destination Address에 대해 NAT 및 PAT 기능을 제공 (1:1, N:N, N:M)
- IPv4 <-> IPv6 NAT 기능을 제공해야 한다(NAT 6to4 터널)
NAT44, NAT46, NAT64, NAT66 기능을 제공할 수 있어야 한다.
- 실시간 Packet Sniffing 기능을 지원해야 한다
- ALG(FTP) 기능, 포트 변경 기능을 제공해야 한다
- 국가별 트래픽 통계를 확인 할 수 있어야 한다.
- 외부에서 가져온 IP목록을 방화벽 정책에서 사용 가능해야 한다.
- 외부에서 가져온 멜웨어 Hash, Domain Name, Web Filter 카테고리 등을 보안정책에서 사용할 수 있어야 한다.
- Public/Private Cloud SDN과 연동하여 Daynamic 주소 객체 사용 지원
Public Cloud SDN : AWS, Azure, GCP, OCI, Alicloud 등 지원
Private Cloud SDN: Kubernetes, ESXi, NXS, OpenStack, Cisco ACI, Nuage/Nutanix Platform 등 지원
- MAC 주소 기반의 방화벽 정책 생성을 지원해야 한다.

▶ Application Control 기능

- 어플리케이션 및 어플리케이션 Group별 정책 설정이 가능해야 한다
- 4,200개 이상의 어플리케이션 Signature를 지원해야 한다
- 어플리케이션별로 식별 및 차단이 가능해야 한다 (Gmail등)
- 클라우드 App 카테고리별 (business, storage, video, cloud, email, social 등) 분류 기능
- 사용자정의 어플리케이션 시그니처 지원

▶ 가상화 기능

- 가상 방화벽 기능 지원
- 가상 방화벽 구성 시 기본 구성 가능한 가상 방화벽 수는 10개를 제공해야 한다.
- 가상 방화벽 구성 시 Transparent 및 Route 모드를 혼합구성이 가능하여야 하며, 가상 방화벽 별 Configuration backup 및 restore 가 가능해야 한다
- 가상 방화벽 별 관리를 위한 관리자 계정이 별도로 존재해야 하며 생성된 관리자는 지정된 가상 방화벽만 관리가 가능해야 한다
- 가상 방화벽 별 방화벽 세션, 오브젝트, 정책 등 리소스 할당 기능을 제공해야 한다

▶ IPS 기능

- Syn Attack, ICMP 및 UDP Flooding, IP Spoofing, Port Scan, DoS, DDoS Attack 등에 대한 탐지/방어 기능을 제공 해야 한다
- Scanning 공격 탐지/차단 기능을 제공해야 한다
- IPS 패턴기반 공격 탐지/차단 기능을 제공해야 한다
- IPS 사용자 정의 패턴에 대한 탐지/차단 기능을 제공해야 한다
- IPS 패턴 DB에 대한 주기적/긴급 업데이트를 지원해야 한다
- IPS 룰 차단, 모니터링 시 공격이 발견되면 공격 패킷에 대하여 pcap 형태로 저장할 수 있어야 한다.
- 10,000 개 이상의 signature 를 제공 하여야 한다.
- 취약점 정보 CVE-ID를 제공해야 한다.
- 실시간 차단 정보 모니터링 및 로그 전송 기능을 제공해야 한다
- (Breaking Point 최신 업데이트 기준) Strike Test 시 95% 이상의 방어율을 제공
- 공격에 대한 정확도가 95% 이상 이어야 한다.
- 각종 evasion attack 에 대한 탐지율이 90% 이상이어야 한다.
- Botnet Servers 차단 기능을 제공해야 한다

▶ Anti-Virus / Malware Protection 기능

- HTTP, SMTP,POP3, IMAP, MAPI, FTP, IM 프로토콜에 대한 Anti-virus scan을 지원
- 다양한 형태의 AntiVirus 탐지 방법을 제공하여야 한다.
 - 단순 signature 매치 방식 탐지
 - 휴리스틱 엔진이 적용된 방식
 - 모든 패킷을 조합하여 탐지하는 방식 (proxy based)
- 변종 Virus 를 탐지하기 위한 독자 기술을 보유, 적용 하여야 한다.
- 100,000 이상의 Anti-Virus Signature를 제공해야 한다
- 다양한 압축 파일 포맷 (zip,tar,cab 등) 별 AV 탐지 기능을 지원
- 다중 압축된 악성코드를 탐지할 수 있어야 한다
- AV 탐지를 위한 파일 사이즈 설정 기능을 제공해야 한다
- 알려지지 않은 Zero-Day 공격에 대응할 수 있는 기능을 제공
- Mobile Malware 에 대하여 방어, 모니터링이 가능하여야 한다.
- APT 공격 방어를 위하여 자체 Sandbox 연동과 Cloud Sandbox 기능을 제공
- 문서내에 포함될 수 있는 악성코드를 사전에 제거할 수 있는 CDR (Content Disarmed and Reconstruction) 기능을 오피스, PDF, 압축파일에 지원하여야 한다
- Proxy, Tunneling 등 보안장비 우회 방식에 대하여 차단이 가능하여야 한다.

▶ URL Filtering 기능

- 사용자 정의 URL 모니터링 및 차단 기능을 제공해야 한다
- 차단 시 안내 웹 페이지를 제공해야 하며, 수정이 가능해야 한다
- 카테고리별 웹 URL DB 에 대한 허용 또는 차단 기능 제공해야 한다
- 정규식 표현, 와일드 카드, 키워드 설정 기능을 제공해야 한다
- 웹사이트 변경에 대응하기 위하여 실시간 query 기반의 URL 필터 기능을 제공하여야 한다.
- 사용자 정의 카테고리를 이용하여 URL 필터 기능을 제공하여야 한다.
- 동일 사이트이더라도 특정 하부 URL, 특정 링크, 특정 파일에 대하여 다른 위협을 파악 할 수 있어야 한다.

<p style="text-align: center;">관리기능</p>	<ul style="list-style-type: none"> ▶ 관리자 운영 <ul style="list-style-type: none"> - 관리자 계정별 Level 제한 기능을 제공해야 한다 - 관리자 페이지 (웹 또는 콘솔) 접속 시 암호화 통신을 제공해야 한다 (https, ssh 등) - 특정 IP또는 계정에 대하여 로그인 접근 제어가 되어야 한다 - 관리자 계정 인증 시 다양한 외부 인증 장비와 (Token, Radius, TACACS) 연동 기능을 제공해야 한다 - 관리자 계정의 자동 로그아웃 기능을 제공해야 한다 (time 설정) - 메모리, CPU 과도 사용 시 장비를 보호할 수 있는 기능을 제공해야 한다. - 다수의 동일 제조사 방화벽을 운용할 경우 관리의 편의성을 위해 SAML(Security Assertion Markup Language) 기능을 지원해야 한다 ▶ 시스템 소프트웨어 <ul style="list-style-type: none"> - remote로 OS upgrade 기능을 제공해야 한다 (upgrade시 기존 config, 기능 유지) - ftp, tftp, web, telnet을 통한 Config 설정 및 백업 기능이 가능해야 한다 - Process list 및 Process별 CPU 점유율을 확인 및 제어가 가능해야 한다 - Password 분실시 복구 방안 제공해야 한다 - 모델별 동일한 기능(UTM 기능, OS, GUI, CLI 등)을 제공해야 한다 ▶ 기타 <ul style="list-style-type: none"> - Dashboard 기능을 제공 - telemetry 기능을 제공하여 주변 동일제조사 장치 및 client 에 대한 topology를 확인할 수 있어야 한다. - device 에 대한 os, 장치 별로 방화벽 정책을 수립할 수 있어야 한다. - 침해 사고를 쉽게 파악하기 위하여 여러가지 조건식을 이용한 로그 서치 기능 제공 - client ip, server ip, url, application 종류, 통신량 등의 조건을 조합하여 로그 서치 - REST 기반의 API 를 제공하여 외부 시스템에서 자동으로 모니터링, 명령어 입력이 가능하여야 한다. - 자동 트래픽 학습을 통한 내부 정보를 수집하고 인식 할 수 있어야 한다. - compliance 를 체크할 수 있는 기능을 제공하여야 한다. - 보안 취약점을 자체 점검할 수 있는 기능을 제공하여야 한다. - Automation Engine에 의해서 자동화된 조치 (Alarm, CLI 명령어 실행, 호스트격리 /접속금지 등) 가능 - 이벤트에 대한 빠른 대응을 위하여 Dashborad, 로그 모니터링, 통계 화면에서 즉시 격리 또는 접속 차단 가능해야 한다.
<p style="text-align: center;">로그관리 및 리포팅</p>	<ul style="list-style-type: none"> ▶ 리포팅 기능 <ul style="list-style-type: none"> - Graphical 리포팅 기능 제공(Top user, Application, 목적지, 웹사이트, 위협 정보 등) - 다양한 Built-in 리포트 템플릿 제공 - NGFW, 트래픽, 이벤트 요약 리포트 - JSON & XML (Web 서비스) API 제공 - 사전 정의된 리포트 템플릿 및 커스텀 템플릿을 생성할 수 있음 ▶ 로그관리 기능 <ul style="list-style-type: none"> - 100GB/Day, 24TB Storage Capacity에 대한 VM License 제공 - 안전한 로그 전송을 위해 방화벽과 암호화된 로그 전송 제공

	<ul style="list-style-type: none"> - 실시간 및 Historical 로그 뷰 기능 제공 - 트래픽, 이벤트, 보안 로그별, 정해진 기간별로 선택하여 로그 검색 가능 - 장비별 검색 또는 전체 장비에 대한 통합 로그 검색 - 관리자 권한에 따라 특정 로그 필드는 Masking 된 정보를 보여줄 수 있는 기능 - 로그 항목별로 선택적 필터링 기능 <p>▶ 이벤트 관리</p> <ul style="list-style-type: none"> - 전체 트래픽 로깅 및 이벤트를 한눈에 확인 할수 있는 다양한 위젯 제공 - 보안 level, 특정 이벤트, 행위에 따른 Trigger 기능 - 사전 정의된 다양한 이벤트 발생 조건 및 관리자가 이벤트 발생 조건 설정 가능 - 다양한 방식으로 임계치 설정 - E-mail/SMS 알림 및 syslog 전송 기능 <p>▶ 기타</p> <ul style="list-style-type: none"> - 최대 10,000대의 방화벽 연동 지원 - 기타 Syslog 호환 device 지원 - 제안 방화벽과 로그/리포팅 관리툴은 동일 제조사 제품이어야 함
<p style="text-align: center;">기타 (유의사항)</p>	<ul style="list-style-type: none"> - CC인증 제품이어야 함 (국내 또는 국제) - SFP-10G (SR) 8ea 제공 - SFP-1G (SX) 8ea 제공 - 이중전원장치 제공 - 방화벽 라이선스 3년 제공 : 방화벽 RMA + IPS + Anti-Virus/SPAM/Malware + Application Control + URL Filtering - 제조사 공급 협약 및 기술지원 협약서 제출(제조사 양식) - 설치 및 무상 유지보수 3년 제공(월 정기점검 및 점검보고서 제출) - 무상 유지보수 종료 후 라이선스 갱신을 포함한 유지보수 금액은 총 계약금액의 15% 이내로 한다.