구매사양서

Ⅰ. 구매품목

품 명	모델명	수량(식)	설치장소
DDoS 방어장비	SNIPER ONE-d 2200	1	서울캠퍼스 제1공학관 101-1호
DNS 장비	TE-1415	1	〃
무선랜사용자 인증시스템	PPX-ANYLINK 8000	1	〃

Ⅱ. 세부사양

1. DDoS 방어장비_SNIPER ONE-d 2200

구 분	세 부 규 격
제품사양	CPU : 2.2GHz(10core) RAM : 32GB(DDR3) HDD : 2TB, SSD : 64GB NIC : 1G *4port (max 8port) 전원 이중화 제공 Throughput : 4Gbps (Max 8Gbps) Concurrent Session : 5,000,000 CC인증(EAL4) 이상을 획득한 제품
일반기능	MAPP 파트너십을 통한 MS 취약점에 대한 선정보 취득 및 대응 능력 보유 공격발생 시 신속한 대처를 위해 최신 해킹패턴 및 공격에 대한 시그니처 업데이트 제공 자체 CERT 보유를 통한 취약성 DB 구축 및 지속적 업데이트 지원 암호화 검증모듈 탑재 LLCF(Link Loss Carry Forward) 지원 In-Line Bridge(Transparent) 모드 구성 지원 기존 네트워크의 구성 및 설정값(Routing 정보등) 변경 없이 구축 및 적용 가능 기본 서비스 및 네트워크 구성변경 없이 자체 장비로 HA기능 지원 HA구성시, Active/Active 및 Active/Standby 구성 지원 Fail-Over, 설정 동기화 지원 내장형 Bypass 기능을 통해 시스템 장애발생 시 통신망 유지기능 및 장애원인 분석을 위한 IDS기능 지원(SPAN 모드) Segment 별 상이한 침입차단 정책을 적용 가능해야 함 Virtual Zone별 멀티라이선스 선택 기능 및 Virtual Rule-set 기능 제공
탐지/차단 기능	전용 DDoS 방어 엔진을 통해 정상/비정상 사용자에 대한 구분 제공 전용 DDoS 방어 엔진을 통해 인가된 사용자에 대한 대역폭 보장 기능 제공 IP대역 학습기능을 통해 정상적인 사용자의 트래픽과 비 인가된 사용자의 트래픽을 분류할 수 있어야 하며, 비 인가된 사용자 트래픽에 대한 QoS 기능 제공 네트워크 영역을 구분하여 이벤트, 통계, 정책설정 등 영역별 관리가 가능한 IP Pool 기능 제공 DDoS 공격에 대한 실시간 수집 및 분석 기능 지원 IP 변조/ 변조되지 않은 Fragment 공격 대응 지원

	정상사용자와 동일한 Source IP로부터의 공격에 대해 유해트래픽만 차단 학습을 통한 시그니처 추출/생성 기능 제공 (Zero-day 공격 대응 가능) SYN,FIN,DHCP,ICMP,TCP,UDP 등 각종 Flooding 공격 탐지/차단 지원 패킷차단 및 트래픽 대역폭 제어기능 제공 IP/Port/Protocol/Flag 별 트래픽 제어가 가능해야 하며, SYN/ACK, SYN-ETC등으로 세분화 대응 기능 제공 국가/IP/URL/URI별 유형에 따라 탐지/차단 및 시간별 정책 설정 기능 제공 평판(IP, 국가IP, URL, DNS쿼리, HTTP 호스트, full URL) 기반의 탐지/차단 제공 및 확장된 외부평판정보 연계지원 탐지 임계치와 차단 임계치 별도 관리기능 제공
관리기능	원격 접속 시 암호화 통신(SSH, HTTPS 등) 기능 제공 보안정책 및 장비상태, 장애감지, 보안감사 등 관리환경(GUI) 제공 실시간 탐지/차단 현황 및 트래픽, 패턴 업데이트, 시스템정보를 확인하는 상황판 제공 실시간 네트워크 트래픽의 정보 모니터링 및 시스템 자체의 부하량 정보 제공 IP Pool기능에 의한 네트워크 분할관리 및 이벤트 통계, 정책설정, 보고서 출력 등 각 영역별 관리기능 제공 각종 트래픽 및 이벤트에 대한 통계, 분석, 리포트 기능을 지원 관리자용 도움말의 한글화를 제공하여 보안정책 적용에 용이한 접근성 제공 시스템 자체 저장장치(HDD) 보유 Log 저장 및 백업, 복구 가능, 별도 서버 없이 운영 가능 SNMP, Syslog 정보 전송기능 제공 내부/외부를 구분하여 탐지, 차단하는 세분화된 모니터링 기능 제공

2. DNS 장비_TE-1415

구 분	세 부 규 격
제품사양	CPU: Intel Xeon Quad-Core 1.2 GHz 이상 2 X 1G Base-T LAN ports, 1 X 1G Base-T Ethernet(HA port) 1 X 1G Base-T MGMT port, Option: 4 x 1GE Option or Copper SFP Interface 전원 이중화 제공, 19인치 렉마운트 Memory: 32Gb DDR4 HDD: 900GB 이상 초당 DNS 쿼리수: 45,000QPS 이상 제공 초당 DHCP 리스수: 300LPS 이상 제공 CC인증(EAL2) 이상을 획득한 제품 기존 운영제품(Infoblox TE-1410)과 호환운영 가능한 제품
DNS기능	DNS 로드 밸런싱, 빠른 응답, 안정된 서비스를 위해 BGP기반의 DNS Anycast기능을 지원 DNS64 기능을 지원 실시간으로 Authoritative, Non-Authortative도메인에 대한 DNS 쿼리량 측정 기능이 지원 DNSSEC기능을 지원 미사용 도메인,레코드 정보제공을 지원 설정작업의 관리자 승인을 위한 Workflow를 제공 확장속성 Field 제공으로 속성값별로 관리기능 제공 DNS Hijacking 공격 방어를 위한 Integirty check 기능을 지원 DNS Phantom Domain 공격 방어기능을 제공
DHCP기능	서비스 가용성 극대화를 위해 Active-Active 방식의 DHCP Failover를 지원 단일 장비에서 현재 DHCP 서비스와 유동/고정 IP주소 사용량 모니터 링이 용이하도록 IP주소 관리 기능을제공 IP주소와 DHCP IP주소 풀의 사용량이 관리자가 지정한 임계치에 다다르면 email과 SNMP를 통해 관리자에게 통보하여 장애방지 DHCP Finger Print기능이 지원 전체 네트워크 구조와 IP주소의 상태를 한눈에 확인할 수 있는 그래픽 View(Network container와 IP MAP)를 제공 API를 통해 커스텀 CSV 파일의 DHCP 설정과 고정 IP주소를 일괄 입력기능 제공

	MAC, vendor option, DHCP option 필터를 지원하여 다양한 환경과 요건에 맞게 정책을 정의 웹 UI에서 CSV 파일을 통해 대량의 DHCP/IPAM 정보를 업데이트제공 IPv6 Ready 기능 (IPv6 Anycast)기능이 지원 DNS패킷의 출발지와 목적지 주소에 기반한 정책에 따라 DNS응답결과를 선택적으로 제공
관리기능	다수의 장비와 데이터를 통합적으로 모니터링 및 관리할 수 있는 모듈을 지원 (선택옵션) 장비의 가용성 극대화 및 서비스 안정을 위하여 이중화를 지원해야하며 별도의 추가적인 설비 없이도 HA구성 DNS/DHCP/IPAM 데이터 설정과 장비관리기능에 대한 관리콘솔이 별도의 추가 장비 없이, 어플라이언스 자체적으로 지원 root계정을 통한 장비의 OS에 대한 접근이 불가하여야 함. 서버해킹/바이러스 감염 등 외부 위험요소로부터 피해를 방지하기 위해 보안기능이 강화된 자체OS 사용 빠른 장애 대응을 위해 서비스 시작/중지, 구성상의 변경 발생시 관리자에게 전자메일로 통보기능 지원 감사를 위해 시간/관리자/변경 내역 등에 대한 로그를 지원 신속한 서비스 제공과 관리를 쉽게 하기 위하여 내부에 데이터베이스를 함께 제공 원격관리의 보안성을 강화하기 위해 모든 원격세션은 Secure Layer를 통해 암호화 서비스와 관련된 모든 리소스 및 데이터 입력 및 구성정보의 설정을 원격에서 손쉽게 지원하기 위해 https 기반의 GUI인터페이스를 제공 네트워크별, 서비스별, 장비별 관리자 권한 위임 기능을 제공하며, Role기반으로 접근제어기능을 지원 내부 database는 이중화구성시, 장애발생시 원활한 서비스 보장을 위해 Pair간 실시간 동기화제공 기존 NMS에 의한 관리가 가능하도록 SNMP, Syslog 기능을 함께 제공해야 한다. 관리자가 상황을 알아보기 쉽도록 그래픽 기반의 상황판 기능을 제공

3. 무선랜사용자 인증시스템_PPX-ANYLINK 8000

구 분	세 부 규 격
제품사양	CPU : Intel Quad 3.1Ghz 이상 메모리: 8GByte(MAX 16GByte) 향후 추가적인 확장을 위한 6개 이상의 포트 기본 지원 10/100/1000M * 6 EA, SFP * 4 포트 CF: 2GByte 이상, LOG HDD : 1TByte 이상 전원 이중화 제공 CC인증(EAL4) 이상을 획득한 제품
인증기능	802.1x, 802.11i EAP/WPA/WPA2 RADIUS 표준 인증서버 기능지원 RFC 1492 TACACS+ 표준 인증서버 기능지원 내장 RFC 6238 OTP(Time-Based One-Time Password Algorithm) 표준 인증 기능지원 단말의 MAC 및 EAP 인증방식을 이용한 인증 지원 MAC+ID+PW+IP 조합인증 지원 MAC 인증, 자체 WEB 인증(WEB Portal), 자체 WEB Redirection 지원 무선, 유선접속 사용자에 대한 자체 웹인증 유도 및 인증 지원 무선, 유선접속 이후 지정된 URL로 강제 접속 지원 외부 방문객을 위한 라우팅 및 VLAN을 통한 자체 웹인증 지원 OTP 기반 계정 발급, 자체 SMS를 통한 계정 발급 및 인증 기능 지원
일반 및 관리기능	향후 인증서버의 다양한 확장을 위하여 자체 DB 보유 SSID 그룹화를 이용한 그룹 정책제어 지원 모든 인증(Authenticator), 권한(Accounting) 동작상태 실시간 모니터링 지원 관리자별 관리권한 제어 및 사용자별 인증권한 제어 지원 TACACS+ 사용자 비밀번호 일괄변경/만료일/갱신일 설정 지원 사용자 ID, NAS, 사용자/NAS별 명령어/서비스 정책설정 지원 TACACS+ 사용 명령어(성공/실패) 수집기능 제공

	외부 DB 지원(Oracle, Mysql, MSSQL 및 ODBC 지원, AD, LDAP지원) 사용자 인증/사용 현황 Log 관리 지원 사용자의 사용시간, 사용량, 인증 실패 유무 Log 관리 지원 외부와 시간 동기화를 위한 NTP 서버 내장 device별 인증통계 및 사용 트래픽 현황 제공 다양한 표준 인증 방식 지원(EAP-MD5,EAP-TLS,TTLS,PEAP,EAP-MSCHAPv2등) 이중화 지원: Active-Active, Active-Standby, 자체 VRRP 이중화 지원 접속 세션별 사용내역(시간/사용자/사용량) 실시간 조회 기능 및 Excel, Word 변환 지원 사용내역에 대한 사용자별 장비별 조회 기능 및 Excel 변환 지원 Vendor Specific Attribute를 포함한 accounting 정보에 대한 사용 내역조회 지원 사용자 개별 GUI(웹)화면 제공(암호변경, EAP 키 생성, OTP키 변경) 무선, 유선 그룹에 대한 유해 트래픽 차단 정책 생성 및 로그 지원 사용자(MAC, IP)별 실시간 사용량 및 트래픽 접속 확인기능 지원 정책에 의한 그룹별 접속 IP/URL 차단 지원 자체 시스템 보호를 위한 관리자 GUI(웹) 기반의 자체 방화벽 설정 기능 제공 SNMP 프로토콜을 통한 RADIUS/TACACS+ 인증 성공 실패량 및 시스템 리소스 정보 제공