통합위협관리시스템(UTM) 구축 사업

시방서

2013. 12.

금강대학교

Ⅰ 일반사항

1. 개요

가. 계 약 명 : 통합위협관리시스템(UTM) 구축 사업

나. 사업목적 : 다양한 최신 해킹공격으로부터 교내 전산 인프라를 안정적으로 보호하기 위해 여러 가지 보안솔루션 기능이 하나로 통합된 통합위협관리시스템을 구축함

다. 주요 사업 내용

1) 통합위협관리시스템(UTM) 시스템 S/W, H/W 납품 및 설치

2) 보안정책 적용 및 서비스 정상 가동

3) 시스템 운영자 교육 및 기술지원

※ 세부규격은 「Ⅲ. 제품 규격서」 참조

라. 설치장소 : 금강대학교 정보지원센터

마. 납품기한 : 계약일로부터 4주 이내

바. 검　　수 : 제품기능 검사서 제출 후 1주 이내

2. 계약조건 및 자격

가. “국가를당사자로하는계약”에 관한 법에 정한 결격 사유가 없는 자

나. 소프트웨어산업진흥법 제24조의 규정에 의한 소프트웨어 사업자로 등록된 업체

다. 계약일 이전부터 대전광역시 또는 충청남도가 주된 사업장 소재지인 업체

라. 아래의 서류를 제출할 수 있는 자

1) 계약 시 제출

- 사업자등록증 사본 1부.
- 법인등기부등본(해당자에 한함) 1부.
- 인감증명서 및 사용인감계(해당자에 한함) 1부.
- 국세, 지방세 완납증명서 1부.
- 소프트웨어사업자 사본 1부.
- 제조사의 제품공급확약서 및 기술지원확약서 1부
- 국가정보원 CC인증 증빙서류 1부

2) 계약 후 제출

- 제품 설치계획서 1부
- 금강대학교 정보지원센터 출입자 명단 및 보안각서 각 1부

3) 설치 완료 및 검수 요청 시 제출

- 정품 라이선스 1부
- 설치확인서 1부
- 제품 기능검사서 1부
- 사업완료보고서 1부
- 시스템 운영자 매뉴얼 2부
- 기타 검수에 필요한 서류

II 계약수행 사항

1. 기본사항

가. 금강대학교대학교 “통합위협관리시스템(UTM) 구축사업”을 수행함에 있어, 금강대학교(이하 “갑”이라 한다)와 계약업체(이하 “을”이라 한다)간에 원활한 계약 이행을 위한 기본 조건을 규정함에 있다.

나. “을”은 계약사항에 명시된 물품 일체를 납품하고 “갑”과 협의하여 설치하되, 구축된 시스템의 성능과 기능이 기준에 미달되는 경우에는 계약해지 사유가 된다.

다. 납품하는 물품의 모든 구성품은 물품의 세부규격을 100% 만족시키는 제조사의 정품, 완제품으로 공급되어야 하며, 품목별 구성 물품 또한 해당 제조사가 공급하는 동일 제품이어야 한다. 단, 성능 및 안정성이 우수하다고 인정되거나 제조사가 해당 물품을 제조하지 않을 경우 동일 성능 이상의 물품으로 “갑”의 승인 후 대체할 수 있다.

라. 시스템 설치 및 개통에 필요한 각종 설치환경 조성에 있어서 계약사항에 명시된 물품 이외에 추가 물품이 소요될 시에는 “을”이 무상으로 제공하여야 한다.

마. “을”이 납품한 H/W 및 S/W는 “갑”이 현재 운용하고 있는 각 서버 및 응용프로그램들의 운영에 지장을 초래하지 않아야 한다.

바. 모든 과업은 “갑”의 업무에 지장을 초래하지 않는 시간에 진행한다.

사. 납품 및 설치하는 전산장비에 대하여 H/W 구성, 통신망(LAN) 연결, 전원 공급 등은 “갑”의 목적 수행에 전혀 지장이 없도록 하여야 하며 품질의 신뢰성, 제품의 안정성에 아무런 문제가 없어야 한다. 본 사업을 수행함에 있어서 운영 중인 전산시스템 및 도입 장비 등 제반 시스템에 손상이 있을 경우 “을”의 비용으로 즉각 원상 복구하여야 한다.

아. “을”이 납품하는 물품은 계약일을 기준으로 공급이 단종이거나 단종 예정인 기종이어서는 안 된다. 또한 기술 및 기능 향상에 의거 변경된 사양은 제조업체와 합의하에 추가 또는 대체하며, 이 경우 추가 발생되는 장비 및 기능은 “갑”의 요구가 우선하며 계약금액의 한도 내에서 “을”이 책임지고 공급한다.

자. “을”은 도입시스템의 설치 및 기타 공사와 관련한 각종 폐기물을 반출·처리하여야 한다.

차. “을”은 “갑”의 전산기계실 출입 등에 “갑”이 요구하는 제반 보안사항을 충실히 이행하여야 하며, 제품납품 중 취득한 모든 자료는 보안사항으로서 보안을 유지하여야 하며 이에 따른 문제발생시 “을”이 모든 민·형사상의 책임을 진다.

카. “을”은 각종 위험으로부터 자기책임으로 생명과 신체를 보호하여야 하며, 이의 불이행으로 재해가 발생되는 경우 “갑”에게 민·형사상 책임을 물을 수 없다.

2. 설치사항

가. “을”은 계약일 기준으로 최신 사양의 제품을 납품하여야 한다.

나. 신규장비도입에 따른 “갑”의 전산기계실 내 장비 설치 및 재배치가 필요한 경우 “을”의 주관 하에 필요한 자재 등을 부담하여 재배치 작업을 하여야 한다.

다. “을”은 신규 도입된 제품에 대하여 “갑”이 지정하는 위치에 설치, 정상작동 여부를 점검하여 그 결과를 “갑”에게 제출한다.

라. 본 물품세부규격에 명시되지 아니한 사항은 반드시 "갑"과 협의 후 시행하여야 한다.

마. 장비납품 시 파손이나 시험운영 중에 장애가 발생하였을 경우, A/S를 불허하며 동일사양 이상의 신규제품으로 교체하여야 한다.

3. 물품 검수 및 시험 운영

가. 물품검수는 본 시방서 및 세부 규격서의 내역에 따르며, 규격 확인이 어렵거나 미흡한 경우에는 “을”이 관련 증빙서류 제출 및 기타 확인과정을 통하여 이를 입증하여야 한다.

나. “을”은 검수 요청 전 “갑”의 담당자 입회하에 각종 시험을 실시하여 시스템의 정상 작동여부를 입증하고, 그 결과 문제가 없을 경우 “제품 기능검사서” 제출과 함께 검수 요청을 하여야 하며, 시험 가동시 발견되는 에러나 불합리한 문제점, 시스템 보완요구 등에 대해서는 즉각 조치하여야 한다.

다. 시험운영 중 발견되는 에러나 불합리한 문제점에 대하여 “을”은 정상가동될 수 있도록 즉시 조치하여야 하며, 수정 및 보완 요구 사항이 제기되면 이를 전면 수용하여야 한다.

라. “을”은 검수에 필요한 시스템 개요와 운영관련 기술을 “갑”에게 충분히 제공하여야 하며 시험가동과 검수에 필요한 물품 및 S/W는 검수기간 동안 “갑”에게 무상으로 설치·제공하여야 한다.

마. 최종 검수결과 시스템 운영이 불가하다고 판단되거나 기기의 하자 발생으로 계약조건을 이행하지 못하는 것으로 판단될 시 “갑”의 요구에 따라 “을”은 납품·설치한 모든 장비를 철거 및 회수해야 하며 그 비용은 “을”의 부담으로 한다.

바. “을”은 “검수 요청 전 유지보수계획(처리절차, 지원범위, 지원방법 등), 장애발생에 대한 대책(예상장애별 조치사항, 비상복구 방안 등)이 포함된 ”사업완료보고서“를 3부 제출한다.

4. 유지보수 및 기술지원 사항

가. “을”은 “갑”의 검수 후 납품 및 설치시스템에 대하여 검수 완료일로부터 1년 간 무상으로 하자보증 및 유지보수를 실시하여야 한다.

나. 구입 장비의 하자보증기간 및 무상유지보수 기간 동안 장비의 하자가 발견될 경우 “을”은 해당 장비를 무상으로 수리하거나 동일 신품으로 무상 교환하여야 한다.

다. “을”은 자체 기술 인력을 보유하여 장애 발생 시 반드시 12시간 이내에 정상 복구를 위한 적절한 조치 및 원인 규명을 해야 한다.

라. 하자보증기간 동안은 시스템 설치에 참여한 “을” 중 “갑”이 지정하는 인력으로 하여금 기능개선, 오류사항 등 지속적인 성능개선을 지원하여야 한다.

마. “갑”이 추후 무상 유지보수기간동안 시스템을 확장하거나 이설, 타 기종으로 교체가 발생할 경우 “을”은 이에 적극 지원하여야 한다.

바. “을”은 고장수리 보장 시간 내에 정상 가동시키지 못했을 경우 “갑”에게 3일 이내에 그 원인을 통보하여야 한다. 단, 정확한 원인규명에 많은 시일을 요할 경우 그 사유를 7일 이내에 문서로써 통보하여야 한다.

사. 구매된 제품의 무상유지보수 기간 내에 제품의 버전(S/W)이 업데이트 되는 경우 무상 업데이트를 수행한다.

아. “을”은 시스템 장애가 월 3회 이상 발생할 경우 “갑”의 요구 시 신규장비로 교체하여야 한다. 단, 3회란 최초발생일 기준 30일 이내 3회를 의미한다.

5. 보안유지

가. “을”은 본 사업과 관련하여 취득한 “갑”의 보안사항과 시스템 운영 환경(내부자료 구성, 구현기법, 통신망구성, 데이터베이스정보, 시스템정보 등) 및 시설 등에 관한 정보를 외부에 누설하여서는 안된다.

나. “을”은 전산실 출입 등 필요한 제반 보안사항을 충실히 이행하여야 하며, 장비 구입·설치를 위한 인력 및 유지보수인력은 신원 상 결격사유가 없는 자이어야 한다.

다. “을”은 계약체결 후 7일 이내에 정보보안 준수 및 의무 사항(소정 양식)”을 작성받아 제출하여야 한다.

라. 본 장비의 보안상 문제점이 발견될 시 “을”은 즉시 그 대책을 수립하여 해결 하여야 하며, 모든 민·형사상의 책임을 지고 보상하여야 한다.

6. 교육지원

가. “을”은 교육훈련에 의한 기술이전을 철저히 시행하여 “갑”의 인수 후 업무에 지장을 초래하지 않도록 한다.

나. “갑”에게 인계 후 운용 미숙으로 인한 재교육 요청 시 이를 실시하여야 하며 경비 부담은 “을”이 부담한다.

다. “을”은 납품한 시스템과 관련된 제조사의 정규교육(On-site 또는 외부 집합교육)을 무상으로 지원한다.

라. 교육훈련에 소요되는 모든 경비는 “을”의 부담으로 하되 일정은 상호 협의하여 결정한다.

마. 기타 운용 등에 관련된 자료 요구 시 “을”은 “갑”에게 제공하여야 한다.

7. 기타사항

가. 본 계약서에 명시된 모든 조항은 최소한의 사양만으로 규정하였으므로 상세히 기술되지 않았거나 누락된 사항에 대하여 “을”은 관리상 문제가 발생하지 않도록 조치하여야 한다.

나. 구매사양에 명기되지 않은 사항은 “갑”에게 별도의 사양서를 제출하여야 하며 사양서의 내용을 수정할 필요가 있을 경우 별도의 합의서를 작성할 수 있다.(단, “갑”의 추가비용이 없어야 함)

다. 계약서 내용에 대하여 “갑”과 “을”의 해석간 차이가 있을 때에는 관계법령과 일반관례에 따르며 소송관할법원은 “갑”의 주소지를 관할하는 법원으로 한다.

III 제품 규격서

구분	세 부 규 격	수량
공통	- 국정원 EAL 4등급 이상의 CC인증 획득 제품(방화벽 PP로 CC인증 획득)	1식
H/W	- Main Processor 4 Core 3.2Ghz 이상 - Main Memory 8GB 이상 - Compact Flash 4GB 이상 - HDD 1TB 이상 - Type 19“ Rack Mount, 2U - Redundant Power Yes - 10/100/1000 Base-T (Copper) 6이상 - 1G Base-X (Fiber - SFP) 6이상 - Firewall Throughput (Max) 8G이상 - IPS Throughput (Max) 3G이상 - VPN Throughput 900M이상 - SSL VPN 동시접속 사용자 1,000이상	
S/W	- Operating System : 전용 OS 탑재 - Route, Transparent, NAT Mode 지원 - H/W, S/W 장애 시 Fail-Open(Bypass)기능 지원 (S/W HANG 발생 시 Bypass 시연 가능) - Route/Bridge 구성에서 LSNAT(Load Sharing NAT), Twice(Twist/Both) NAT, PAT(M:N, N:1), Static(1:1), Excluded 등 다양한 NAT 지원 - L2/L3 스위치기반 Route/Transparent Mode A-A, A-S HA 기능 지원 - VLAN Interface HA 기능 지원 - L2없이 Full Mesh 구성을 위한 A-S Link Aggregation 지원 - VRRP(Virtual Router Redundancy Protocol) 지원 - 대역폭 확장을 위한 A-A Link Aggregation(802.3ad 등) 지원 - DB Instance에 대한 상태 및 DB 보안 서버의 자원상태 정보를 제공할 수 있는 제품 - 802.3ad 구현 시 Load-Balancing 알고리즘(L2/L3/L4기반) 설정 지원 - IPv6 네트워킹 및 방화벽 기능 지원 - IPv6 - IPv4 간 Transition 지원 (6to4/ ISATAP/ NAT-PT) - IPv6 Dynamic Routing 지원 (RIPv6/ OSPFv6/ BGPv6) - IPv6 TTA Verified 인증 획득 및 실 구축 레퍼런스 보유 - 최대 4개 Load Balancing/Fail-Over제공 Multiple Default Gateway 지원 - 최대 4개 xDSL Interface 지원 - DHCP Server/Client/Relay 지원 - Interface별 Secondary IP지원 - 802.1Q VLAN지원xcel형식) 기능 - LLCF(Link Loss Carry Forward) 지원	

구분	세 부 규 격	수량
S/W	- 보안정책/세션 수와 상관없이 균등한 성능 지원 - 최대 65,500개 보안정책 지원 - 대용량 정책 사용 시 실시간 신규정책 적용기능 - 방화벽 정책 유효성 검증 기능(룰 Hit Counting 기능/ Last Hit 기능) - 중복정책 검색기능 - 정책 별 세션 제어 기능/ 소스 IP 별 세션 제어 기능 - 보안정책 Export(Excel형식) 기능 - TCP, UDP, ICMP, IP Protocol별/서비스별 세션 유지시간 설정기능 지원 - SIMS에 대한 연동 규격 지원 - 방화벽 Policy/IP/Port/Schedule별 7단계 우선순위 QoS기능 지원 - 최대 대역폭 및 최소 대역폭 보장 QoS기능 지원(7단계 Leveling) - H.323, SIP등 VoIP 트래픽 처리 지원 - H.323/SIP기반 VoIP ALG(Application Layer Gateway) 기능 지원 - Dynamic Routing 지원 (OSPF, RIP v1/v2,BGP 등) - ECMP 라우팅 지원 - 멀티캐스트 지원(IGMPv2, PIM-SM 등) - STP 지원 - OTP및 RADIUS/LDAP/Active Directory 연동 User Authentication 지원 - CPU/Memory/Disk/HA상태 이상 발생 시 이메일/SMS를 통한 경보 지원 - HTTPS (SSL)를 통한 Web 기반 및 SSH를 통한 관리용 암호화 통신 지원 - HTTPS/SSH 관리용 UI의 Session Idle time 설정 기능 지원 - 다수 장비에 대한 다중 레벨 관리자 계정 지원 - 한국어/영어/중국어 기반 Web UI 지원 - 다수의 장비에 대해서 통합보안정책 설정 및 One-Click 일괄 배포기능 지원 - 통합 보안정책 및 통합로그 검색 시 계정별 권한 부여 기능 지원 - 다수의 장비의 주요 데몬상태에 대한 실시간 모니터링 기능 지원 - 다수의 장비에 대한 통합 보고서 생성 기능 지원 - 24시간/주간 시스템/네트워크/보안위협 추이분석 보고서 기능 지원 - 실시간 모니터링 정보에서 Drill-Down방식의 편리한 정보검색 기능 지원 - SNMP/Syslog/SIMS를 통한 ESM(통합관리시스템)과 연동 지원 - 로그 간소화 선택 기능을 통해 로그저장량 설정기능(Connection/Expire Log, BlockLog Counting 등) - 상용 DB(MS-SQL,DB2 등) 기반 로그저장 구조를 통해 대용량 로그에 대한 빠른 검색 지원 - SMTP,POP3,FTP,HTTP,SQL-Net,DNS,TCP,UDP 전용 Proxy 지원 - 1000만 센서 자체 DB기반 악성코드 유포사이트 차단기능 - 패킷기반 고속 탐지모듈 적용을 통해 성능저하 없이 유해사이트 URL 차단	

구분	세 부 규 격	수량
S/W	- 방송통신위원회 DB기반 유해사이트 차단기능 - 정규식/Wildcard기반 사용자 정의 URL 지원 - Anti-Virus, Anti-Spam - SMTP, POP3, FTP, HTTP 서비스의 바이러스 차단 기능 지원 - 100명 이상의 자체 악성코드 엔진제작 조직 보유 - Spam발송 SMTP서버기반 SPAM DB엔진 보유(글로벌 스팸 전문엔진 탑재) - RBL(Real-Time Black List) 지원 - Keyword,정규식/Wildcard타입 사용자 정의 문자열 지원 - Split DNS 지원 - DNS 응답메시지의 사설IP 차단 기능 지원 - 1대의 장비로 복수개의 세그먼트 구성 지원 - 32개 네트워크 Zone 별 상이한 IPS 정책/ Signature 적용 가능 - 100명 이상의 자체 악성코드 분석 및 시그니처 제작 조직 보유 - Microsoft 보안패치공지 이전 취약점 정보공유(MAPP 계약)를 통한 Zero-Day Attack 차단 - 1일 2회 이상의 악성코드 탐지패턴 자동 업데이트 - 실제 적용 가능한 5,000개 이상의 시그니쳐 보유 - 악성코드 행위제어 시그니처 3,000개 이상 보유 - Bot 행위제어 시그니처 보유 (C&C서버 접속제어/ IRC 채널통신제어/ HTTP채널 통신제어) - OWASP 10대 취약점 기반의 Web Attack 시그니쳐 보유 - 클라우드 컴퓨팅 기반 좀비악성코드 활동 탐지 및 대응체제 보유 - 폐쇄망에서의 시그니처 자동 업데이트 지원 - 인터넷이 불가능한 완전 폐쇄망 업데이트 지원 - Protocol Analyzing, Pattern Matching, Anomaly Detection 지원 - 150여 개 P2P/ IM/ 웹하드 등 Application Control 기능 지원 - IPS 탐지 정보 전송 기능 - 사용자 정의 패턴 정의 지원 - 우회공격(TCP Segment분리,IP Layer Fragmentation 공격 등)탐지 지원 - DDoS 방어 전문엔진 탑재(특허취득 기술 포함) 지원 - TCP 대리 응답 방식을 통한 IP Spoofing DDoS공격 차단 지원 - HTTP 대리 응답 방식을 통한 HTTP Flooding공격 차단 지원 - 행위 기반의 HTTP/TCP/UDP/ICMP별 DoS/DDoS 공격 차단 기능지원 - MSN, NateOn, Yahoo 등의 메신저 제어(채팅,파일전송,원격제어 등)기능 - e-Donkey,소리바다 등 P2P에 대한 제어(검색,파일전송 등)기능 - IDS/Stealth mode 지원 - PC용 Anti-Virus 제품과 유기적 연동을 통해서 악성코드에 감염된 PC의 악성패킷 기반 격리 (Quarantine) 및 자동 치료 지원	

구분	세 부 규 격	수량
S/W	- PC용 Anti-Virus 제품과 유기적 연동을 통한 NAC(Network Admission Control) 기능 지원 - SSL VPN - 단일 장비에서 IPSec과 SSL VPN을 동시에 기능 지원 - 32/64bit기반 Windows 2000/XP/Vista/7 OS 지원 - SSL VPN 검증필 암호화 모듈 탑재 - SEED/ARIA/3DES/AES 표준 암호화 알고리즘 탑재 - SHA-1/SHA-2/HAS160 표준 해시 알고리즘 지원 - User Level Access Control 지원 - SSL VPN 접속 시 가상IP 할당기능 지원 - SSL VPN 접속 시 초기 홈페이지 리다이렉션 지원 - SSL VPN 연결시간 제한 기능지원 - 인터넷 장애 등으로 인한 비정상 접속 장애 시 자동 재연결 기능 지원 - SSL VPN사용 시 Client보안(개인방화벽,Anti-KeyLogger,Cookie/Cache 자동삭제) 기능 지원 - SSL VPN과 IPS 연동기능을 통한 VPN구간의 악성코드 전파차단 지원 - 사용자 그룹화 및 그룹별 정책 지원 - 접속한 실시간 사용자 정보제공 지원 - 접속 사용자 강제 접속 차단 기능 지원 - SSL 사용자가 초기 접속 시 자신의 Password 설정 기능 지원 - 일정기간동안 SSL VPN 미사용자에 대한 조회 및 잠금 기능 - 관리자의 SSL 사용자 Password 초기화 기능 지원 - RADIUS/LDAP/Active Directory 연동을 통한 10,000명 이상의 User 등록 지원 - L2/L3스위치 기반 A-S VPN-HA 지원 - L4스위치와 연동하여 VPN Load-Balancing 지원 - 내부 DNS/WINS 연동 기능 지원 - 사용자 그룹화 및 그룹별 정책 지원	