방화벽(Firewall)
교체 제안요청서

2015. 11.

목 차

1. 사업 개요

1.1. 사업명

1.1.1 방화벽(Firewall) 교체

1.2 사업기간

1.2.1 계약일 ~ 2015년 12월 31일

※ 현 방화벽 유지보수 계약 2015년 12월 31일 종료

1.3 추진배경

1.3.1 케이티파워텔㈜ (이하 ” 당사” 라 함)은 전국 무전통화 서비스를 기반으로 이동전화와 데이터 서비스를 함께 제공하고, 순수 국내기술을 활용해 독자적으로 개발한 자체 기술과 단말기로 3G• LTE망 상에서 세계 최초의 LTE 디지털 무전통신 서비스를 제공하고 있습니다.

1.3.2 당사 노후화 된 보안장비 교체작업의 일환으로 새로운 보안 위협이 증가함에 따라 장비 교체가 필요하게 되었으며, 이에 신규 방화벽 장비를 구축하여 안정적인 네트웍망 유지를 목적으로 추진하게 되었습니다.

2. 기술 사항

2.1 구성도

2.1.1 A1000 방화벽 구성도

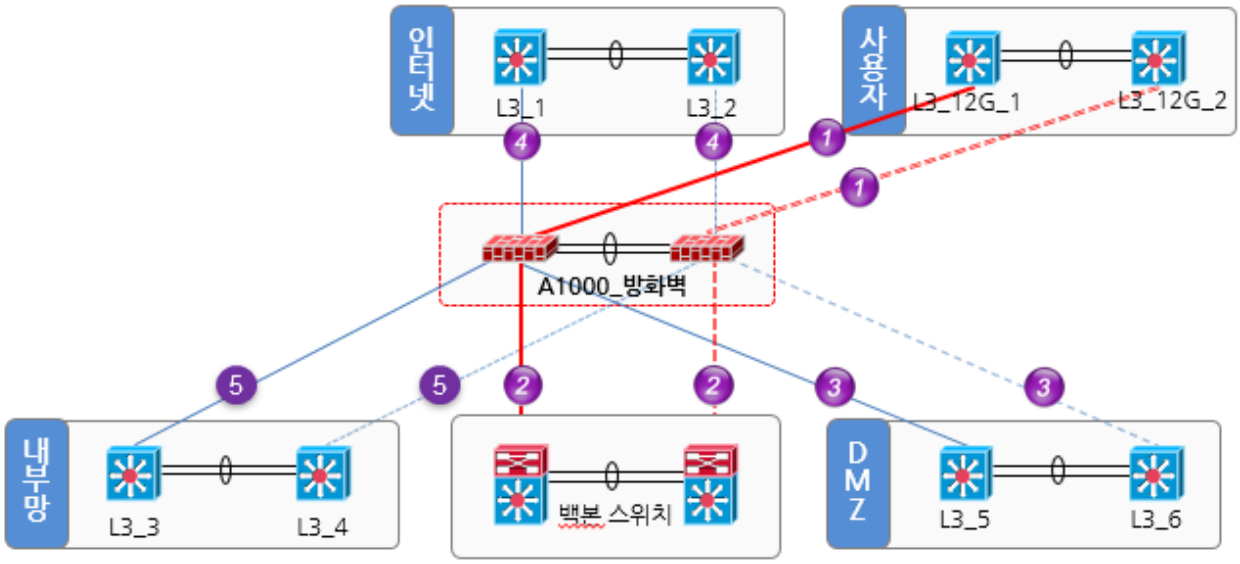
① **A1000 방화벽 – 사용자 구간**
- A1000, 사용자 구간 1G fiber 구성

② **A1000 방화벽 – 백본 스위치 구간**
- A1000방화벽, 백본 구간 1G fiber 구성

③ **A1000 방화벽 – DMZ 구간**
- A1000방화벽, DMZ 구간 10/100 Coper 구성

④ **A1000 방화벽 – 인터넷 구간**
- A1000방화벽, 인터넷 구간 10/100 Coper 구성

⑤ **A1000 방화벽 – 내부망 구간**
- A1000방화벽, 내부망 구간 10/100 Coper 구성



※ 각 존 구간 보안 장비(IPS, 웹방화벽등) 운영 중

※ 10/100 Coper 구간은 1G fiber 로 교체할 예정이므로 광 케이블 포설을 해야 하며, 보안장비(방화벽, IPS등)와 연결된 네트워크 장비에 Gbic 모듈이 필요한 경우 제안사가 제공해야 함

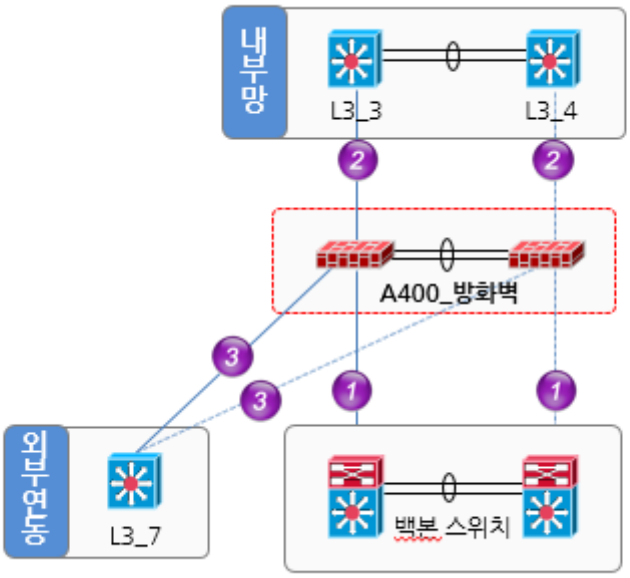
※ 장비 설치에 필요한 소요자재(케이블, Gbic 등)에 필요한 부대비용은 제안사가 부담 함

2.1.2 A400 방화벽 구성도

① A400 방화벽 – 백본 스위치 구간
- A400방화벽, 백본 구간 10/100 Coper 구성

② A400 방화벽 – 내부망 구간
- A400방화벽, 내부망 구간 10/100 Coper 구성

③ A400 방화벽 – 외부 연동 구간
- A400방화벽, 외부 연동 구간 10/100 Coper 구성



※ 각 존 구간 보안 장비(IPS, 웹방화벽등) 운영 중

※ 10/100 Coper 구간은 1G fiber 로 교체할 예정이므로 광 케이블 포설을 해야 하며, 보안장비(방화벽, IPS등)와 연결된 네트워크 장비에 Gbic 모듈이 필요한 경우 제안사가 제공해야 함

※ 장비 설치에 필요한 소요자재(케이블, Gbic 등)에 필요한 부대비용은 제안사가 부담 함

2.2 시스템 구성

○ 제안사는 납품 시스템에 대하여 당사가 운영중인 기존 장비(네트워크 및 보안장비 등)와 연동함에 있어서 완벽히 호환이 가능한 장비여야 합니다. (장비 추가 및 구조 변경 없이 기존 장비를 신규 장비로 교체하여 교체 전후 구성이 동일해야 합니다.)

2.3 물품 내역 및 상세규격

① Ahnlab Absolute 1000 장비 교체용 2대

품명	구분	세 부 규 격	수량
방화벽 (Firewall)	보안 인증	▶ 국가정보원 CC 인증 EAL4 이상 인증 획득 ▶ 국가 공인기관으로부터 Ipv6 인증 획득	2대
	H/W 사양	▶ 하드웨어 일체형 장비 ▶ OS : 전용 운영체제 ▶ CPU : 2.4Ghz(4core) 이상 ▶ Main Memory : 8G 이상 ▶ CF Memory : 2G 이상 ▶ HDD : 2TB 이상 ▶ NIC : 10/100/1000 Base-T * 최소 6port 이상 1G Base-X * 최소 8port 이상 (* NIC 구성은 당사 구성에 따라 포트 개수 및 타입 변경이 가능해야 하며[단, 추가비용 발생 시 제안사 부담], 제안사는 사업담당자와 최종 구성 협의 후 발주를 진행해야 함) ▶ 전원 이중화 및 Hot-Swap 제공	
	성능	▶ 방화벽 Throughput 8Gbps (최대 12Gbps) 이상 ▶ 동시세션 4,000,000 이상	
	네트워크 기능	▶ Route 모드 및 Bridge 모드 구성 제공 ▶ 이중화 구성시 L4 스위치 없이 구성(Active-Active, Active-Standby) 제공 ▶ 회선 장애 시 자동 우회 및 LLCF(Link Loss Carry Forward) 통한	

	라우팅 우회 기능 제공 ▶ 다양한 라우팅 프로토콜 (Static / Multicast / RIPv1 / RIPv2 / OSPF/ BGP/ VRRP / Proxy ARP 등) 지원 ▶ 다양한 IPv6 라우팅 프로토콜(Static / RIPv6/ OSPFv6 / BGPv6 등) 지원 ▶ IPv6 변환 메카니즘 (IPv4/IPv6 Dual Stack, IPv6-in-IPv4 Tunneling, NAT-PT, 6 to 4 등) 지원
방화벽 기능	▶ 양방향 정책 적용 기능 제공 ▶ 정책 수에 관계없이 일정한 독립적인 성능 지원 ▶ 미 사용 정책 및 객체 검색 기능 제공 ▶ 정책 또는 객체 생성 시, 중복 항목 입력을 실시간으로 탐지 및 필터링 기능 제공 ▶ IPv4, IPv6별 방화벽 QoS 기능 지원 ▶ 트래픽 조절 (QoS) 및 정책 별 과도하게 발생한 세션을 탐지 / 차단 기능 제공 ▶ 다양한 네트워크 주소 변환(Static NAT / Dynamic NAT / Excluded NAT / NAT Traversal / Load-Sharing NAT 등) 지원 ▶ IPv6 패킷 방화벽 필터링 지원 ▶ HA 정책 동기화 시, 동기화 정책/ 설정 목록 선택 세분화 ▶ 정책 일괄 설정 및 관리를 위한 Export, Import 기능 제공 ▶ 정책/ 시스템 설정 롤백 및 펌웨어 업그레이드 롤백 기능을 지원
모니터링 및 관리	▶ 3단계 이상의 사용자 권한 유형 제공(슈퍼관리자/일반관리자/모니터링 등 권한 별 기능 세분화) ▶ 로그인 실패 횟수 잠금 및 세션 타임아웃 설정 기능 제공 ▶ 별도의 관리 콘솔 서버 없이 Web GUI를 통한 관리 기능 및 실시간 상세 로그(출발지IP, 목적지IP, 프로토콜등) 정보 제공 ▶ 원격 접속 시 암호화 통신(SSH, HTTPS등) 및 IP 기반 접근제한 기능 제공 ▶ 실시간 시스템 상태, 네트워크 트래픽, 장애 및 각종 이벤트 현황 정보 제공 ▶ 시스템 자체 저장장치(HDD) 보유 Log 저장 및 백업, 복구 가능

		▶ 설정 데이터 백업/복구 기능 제공 ▶ Syslog 기능 등을 통한 외부 통합 로그 수집. 분석 시스템과 연동 ▶ RADIUS, LDAP, AD등과 연동하여 사용자 인증 지원 ▶ 시스템 및 링크 상태 확인을 위한 외부 LCD Display Panel 제공	
	보고서	▶ 각종 트래픽 및 이벤트에 대한 통계, 분석, 리포트 기능 제공 ▶ 각종 기간별(일/주/월) 보고서 기능 제공	
	기타	▶ 최소 3개월 이상의 로그 분석 후 정책 이관 적용	

② Ahnlab Absolute 400 장비 교체용 2대

품명	구분	세 부 규 격	수량
방화벽 (Firewall)	보안 인증	▶ 국가정보원 CC 인증 EAL4 이상 인증 획득 ▶ 국가 공인기관으로부터 Ipv6 인증 획득	2대
	H/W 사양	▶ 하드웨어 일체형 장비 ▶ OS : 전용 운영체제 ▶ CPU : 3.1Ghz(2core) 이상 ▶ Main Memory : 4G 이상 ▶ CF Memory : 4G 이상 ▶ HDD : 1TB 이상 ▶ NIC : 10/100/1000 Base-T * 최소 6port 이상 1G Base-X * 최소 4port 이상 ▶ 전원 이중화 및 Hot-Swap 제공	
	성능	▶ 방화벽 Throughput 3Gbps (최대 6Gbps) 이상 ▶ 동시세션 2,000,000 이상	
	네트워크 기능	▶ Route 모드 및 Bridge 모드 구성 제공 ▶ 이중화 구성시 L4 스위치 없이 구성(Active-Active, Active-Standby) 제공 ▶ 회선 장애 시 자동 우회 및 LLCF(Link Loss Carry Forward) 통한	

	라우팅 우회 기능 제공 ▶ 다양한 라우팅 프로토콜 (Static / Multicast / RIPv1 / RIPv2 / OSPF/ BGP/ VRRP / Proxy ARP 등) 지원 ▶ 다양한 IPv6 라우팅 프로토콜(Static / RIPv6/ OSPFv6 / BGPv6 등) 지원 ▶ IPv6 변환 메카니즘 (IPv4/IPv6 Dual Stack, IPv6-in-IPv4 Tunneling, NAT-PT, 6 to 4 등) 지원
방화벽 기능	▶ 양방향 정책 적용 기능 제공 ▶ 정책 수에 관계없이 일정한 독립적인 성능 지원 ▶ 미 사용 정책 및 객체 검색 기능 제공 ▶ 정책 또는 객체 생성 시, 중복 항목 입력을 실시간으로 탐지 및 필터링 기능 제공 ▶ IPv4, IPv6별 방화벽 QoS 기능 지원 ▶ 트래픽 조절 (QoS) 및 정책 별 과도하게 발생한 세션을 탐지 / 차단 기능 제공 ▶ 다양한 네트워크 주소 변환(Static NAT / Dynamic NAT / Excluded NAT / NAT Traversal / Load-Sharing NAT 등) 지원 ▶ IPv6 패킷 방화벽 필터링 지원 ▶ HA 정책 동기화 시, 동기화 정책/ 설정 목록 선택 세분화 ▶ 정책 일괄 설정 및 관리를 위한 Export, Import 기능 제공 ▶ 정책/ 시스템 설정 롤백 및 펌웨어 업그레이드 롤백 기능을 지원
모니터링 및 관리	▶ 3단계 이상의 사용자 권한 유형 제공(슈퍼관리자/일반관리자/모니터링 등 권한 별 기능 세분화) ▶ 로그인 실패 횟수 잠금 및 세션 타임아웃 설정 기능 제공 ▶ 별도의 관리 콘솔 서버 없이 Web GUI를 통한 관리 기능 및 실시간 상세 로그(출발지IP, 목적지IP, 프로토콜등) 정보 제공 ▶ 원격 접속 시 암호화 통신(SSH, HTTPS등) 및 IP 기반 접근제한 기능 제공 ▶ 실시간 시스템 상태, 네트워크 트래픽, 장애 및 각종 이벤트 현황 정보 제공 ▶ 시스템 자체 저장장치(HDD) 보유 Log 저장 및 백업, 복구 가능

		▶ 설정 데이터 백업/복구 기능 제공 ▶ Syslog 기능 등을 통한 외부 통합 로그 수집. 분석 시스템과 연동 ▶ RADIUS, LDAP, AD 등과 연동하여 사용자 인증 지원 ▶ 시스템 및 링크 상태 확인을 위한 외부 LCD Display Panel 제공	
	보고서	▶ 각종 트래픽 및 이벤트에 대한 통계, 분석, 리포트 기능 제공 ▶ 각종 기간별(일/주/월) 보고서 기능 제공	
	기타	▶ 최소 3개월 이상의 로그 분석 후 정책 이관 적용	

3. 제안 안내

3.1 제안 일반사항

3.1.1 모든 일정은 당사 입찰공고를 참조 바랍니다.

3.1.2 제안서 작성 요령

○ 제안서목차 및 작성지침을 준용하여 제안서를 작성합니다.

※ ‘ 3. 제안 안내 – 3.3 제안서 목차 및 작성지침’ 참조

3.1.3 제안서 규격

○ 제안서는 A4용지 3 Hole 바인더를 사용하며, Page 번호를 부여하여야 합니다. (제본 불가)

○ 제안서는 MS PowerPoint로 작성하여야 하며, 분량은 30page(단면인쇄) 이내이어야 합니다.

3.1.4 제출서류

○ 제출서류

- 제안서 원본 1부, 사본 1부, 전자사본(USB) 2부
- 입찰참가신청서(당사 소정양식) 1부
- 입찰서(당사 소정양식, 견적서 첨부, 기명날인 후 2중밀봉) 1부
- 입찰보증금(보증보험증권, 입찰금액의 100분의 5이상) 1부
- 각서(당사 소정양식) 1부
- 법인등기부등본 및 사업자등록증사본 각 1부
- 법인인감증명서 및 사용인감계 각 1부
- 재무제표 증명원(국세청 발급) 1부
- 구축(또는 납품) 또는 유지보수 실적증명서(제안서에 첨부)
- 위임장(대리인 참가시, 대리인 신분증 사본) 및 재직증명서
- 기타 입찰에 필요한 서류(제안요청서 별지 양식의 서류 등)
- 해당물품 제조사의 “ 제품공급 및 기술지원 확약서” 원본 각 1부
  ※ 제안요청서 물품 상세규격을 모두 만족하는 제조사의 확인서 포함
- 국가정보원 정보보호제품 인증서(국가정보원 CC인증 EAL4) 1부

○ 검수 완료 후 제출서류

- 관리자/사용자 매뉴얼 (CD 및 USB) 각 2부
- 구축 산출물 (CD 및 USB) 각 2부

3.1.5 제출방법

○ 제안서 접수장소는 당사“ 서울시 양천구 목동서로 201(목동) KT정보전산센터 19층 케이티파워텔㈜ 경영지원팀 계약업무 담당자”에게 제출하여야 합니다.

- 계약업무 담당자 박호진(Hp. 010-7469-5376)

○ 제안서는 접수마감일까지 제안사가 접수 장소에 직접 제출하여야 하며, 우편(fax)이나 택배등의 접수는 인정하지 않습니다.

3.1.6 제안 관련 문의처

○ 소 속 : 케이티파워텔㈜ 경영지원팀

○ 담 당 자 및 전화번호:

- 김성진 대리(Hp. 010-7469-5185)

3.2 유의사항

○ 제안서에 제시된 내용 및 발주자의 요구에 의하여 수정 또는 보완 변경된 제안내용은 계약서에 명시되어 있지 않더라도 계약서와 동일한 효력을 가집니다. 다만, 계약서에 명시된 내용과 배치될 시에는 계약서가 우선합니다.

○ 제안서 검토 후 필요시 추가자료 요청 또는 사실관계 증명요청 및 제안사의 추가 설명을 요청할 시 제안사는 이에 성실히 임하여야 하며 자료 미제출 및 불응에 대한 불이익은 제안사가 책임을 집니다.

○ 제출된 제안서의 내용은 당사가 요청하지 않는 한 변경, 추가, 수정할 수 없으며, 기재내용은 실제 제공되는 서비스와 일치하여야 합니다.

○ 제안요청서에서 요구조건으로 제시하고 있는 사항에 대하여 언급이 안되어 있는 부분은 해당 서비스제공 기능이 없거나, 해당 서비스 제공의사가 없는 것으로 간주 합니다.

○ 제안요청서에서 요구한 내용이 포함되어 있지 않거나, 규정된 사항을 준수하지 않았을 경우 제출된 제안서는 거절될 수 있습니다.

○ 제안서는 허위 또는 단순예상으로 작성하지 않아야 하며. 모든 기재사항은 객관적으로 입증할 수 있어야 하며, 허위로 작성한 사실이 발견될 경우 심사대상에서 제외되며 계약 후 제안 내용이 충족되지 못할 경우에는 계약무효로 하거나 손해배상의 책임을 져야 합니다.

○ 제안서는 제안서 작성 요령에서 정한 목차에 따라 간결하고 명확하게 기술하여야 합니다.(“ ~할 수도 있다.”,“ ~이 가능하다”, 등과 같은 모호한 표현은 불가능한 것으로 간주함)

○ 제안사의 투입인력은 프로젝트 수행에 적절한 인력 수준(경력, 자격증 등)이어야 하며, 이를 객관적으로 증명할 수 있는 자료를 추후 제출해야 합니다.
○ 당사가 기술자의 용역수행능력이 부족하다고 판단하는 경우 기술자의 교체를 요구할 수 있으며 제안사는 이에 따라야 합니다.
○ 제안서의 내용을 객관적으로 입증할 수 있는 관련자료는 제안서의 별첨으로 제출하여야 합니다.
○ 교육훈련 계획 등 유상으로 제공되는 서비스일 경우에는 제공항목, 금액 등 관련내용을 명확히 제시하여야 합니다.
○ 시스템 납품 및 설치 중 제반 안전사고 및 납품 과정에서 발생하는 행정적, 기술적 제반 비용은 제안사가 부담하며, 상세규격에 명시된 품목 외에 추가적인 품목(기타장비, 케이블, 커넥터등)과 비용이 요구될 경우 본 사업범위에 포함하여 무상 공급하여야 합니다.
○ 제안사는 장비납품 시 파손이나 시험운영 중 하드웨어 장애가 발생하였을 경우 A/S를 불허하며 동일 사양 이상의 신규제품으로 교체해야 합니다.
○ 납품하는 물품의 모든 구성품은 제품 상세규격에서 기술한 규격 이상의 성능을 지원하는 상위 규격 이어야 합니다. 또한, 정품 완제품으로 공급하여야 하며, 반드시 해당 물품 제조사의 정품을 사용하여야 합니다.
○ 납품하는 모든 소프트웨어는 정품 및 최신 버전이어야 하고 각 제품 별로 라이선스(저작권)를 제공하여야 하며, 원 소유자의 저작권을 침해하지 않는 제품이어야 합니다.
○ 본 사업의 무상 유지보수기간은 구축 완료 후 검수일로부터 2년으로 합니다. 무상 유지보수기간에 납품 시스템에 동일 장애가 3회 이상(30일 이내) 발생하는 경우 교체 요청시 제안사는 동급 이상의 신 시스템(또는 장비)으로 교환 조치하여야 합니다. 또한, 장애로 인하여 장시간 당사의 시스템 가동 운영서비스가 어렵다고 판단 될 경우에는 제안사는 해당 시스템(또는 장비)을 동급 이상의 시스템 기종으로 대체 설치하여 당사의 운영서비스에 지장이 없도록 하여야 합니다.
○ 모든 제안업체는 하도급거래공정화에관한법률(이하 “ 하도급법”이라 한다.) 등 관련 법령의 제 규정을 준수해야 합니다.
○ 당사의 조치나 기타의 불가항력 환경변화로 본 제안요청의 일부 또는 전부가 변경되거나 취소되는 경우라도 제안사는 이의를 제기하지 못합니다.
○ 본 사업은 당사의 내부사정에 의거 변경 또는 취소될 수 있습니다.
○ 제출된 서류는 일체 반환하지 않습니다.

3.3 제안서 목차 및 작성지침

작성항목	작성방법	비고
Ⅰ. 제안개요	● 제안사는 해당사업의 제안요청 내용을 명확하게 이해하고 본 제안의 목적, 범위, 전제조건 및 제안의 특징 및 장점을 요약하여 기술	
Ⅱ. 일반부문		
1. 일반현황	● 제안사의 일반현황 및 주요 연혁, 최근 3년간의 자본금, 매출액, 당기순이익 등을 명료하게 기술	별지 제1호
2. 조직 및 인원	● 제안사의 조직 및 인원현황을 제시	
3. 주요사업내용	● 제안사의 주요 사업내용을 분야별로 구분하여 기술	
4. 주요사업실적	● 본 사업과 관련이 있는 유사 사업실적, 기술 경험 등을 기술 ※ ‘ 4.입찰 안내’ 의 ‘ 4.1.1항’ 과 관련된 내용 기술	별지 제2호
Ⅲ. 사업수행부문		
1. 사업수행 및 수행조직	● 사업의 이해도 - 사업수행 목표 기술 - 사업수행 시 필요업무 내역 및 구축작업 추진 계획 등 기술 ● 사업 투입 및 유지보수 인력 기술	별지 제3호
2. 예방점검방안	● 예방점검 방안 - 무상 유지보수 기간동안 장애예방을 위한 점검활동 방안 기술 ※ 무상 유지보수 기간에 월, 분기, 반기등 당사 점검 지원 방안 기술	
3. 장애처리체계	● 장애발생시 기술지원 조직 및 프로세스 - 기술지원조직, 장애조치 프로세스, 사후관리 등을 구체적으로 명시 - 평시 및 취약시기(야간, 공휴일 등) 시점별 장애대응 체계 기술 - 장애의 원인 분석 방법론 및 장애이력 관리 방안	
Ⅳ. 지원부문		
1. 교육훈련 및 기술이전 등 지원사항	● 본 사업 관련 교육훈련, 기술이전 등 지원 가능한 사항을 기술	

※ 4. 입찰 안내 – 4.1 입찰 참가자격’ 의 관련 서류는 제안서 첨부

4. 입찰 안내

4.1 입찰 참가자격(아래 사항을 모두 충족해야 입찰 자격 인정)

4.1.1 최근 3년(2012년~2014년) 계약금액 2억 이상(부가세 별도) 사업에 보안시스템 구축(또는 납품) 5건 이상 또는 보안시스템 유지보수 실적 1억 이상(단일건 기준, 부가세 별도) 5건 이상인 업체

※ 구축 또는 유지보수 실적 증명서 제출 (계약서 사본으로 대체 가능)

※ 보안시스템 : 방화벽(웹방화벽) 포함 유사시스템인 UTM, IPS(WIPS), VPN, DDos 등 보안 관련 시스템으로 한정

(단, 위 기재된 보안시스템 외 제안사가 실적 증명 제출한 건에 대해서는 해당 사업부서에서 적절한지 판단하며 본 사업과 부적절하다고 판단 되는 건은 제외함)

4.1.2 전년(2014년) 매출액 200억 이상인 업체

4.1.3 아래 서류가 제출 가능한 업체

○ 해당물품 제조사의 " 제품공급 및 기술지원 확약서" 원본 각 1부
- 제안요청서 물품 상세규격을 모두 만족하는 제조사의 확인서 포함

○ 국가정보원 정보보호제품 인증서(국가정보원 CC인증 EAL4) 1부

※ 제안사는 H/W 및 S/W 납품, 설치, 유지보수등에 대한 원제조사의 제품 공급증명서와 기술지원확약서를 제출하셔야 합니다. 미제출시 제안사의 입찰은 낙찰 무효 처리됩니다. 입찰보증금은 회수 처리되며, 기타 불이익을 당할 수 있습니다.

4.2 유의사항

○ 본 입찰과 관련된 소요비용은 제안사의 부담으로 합니다.

○ 계약은 낙찰업체인 제안사(주사업자)와 계약을 합니다.

○ 본 입찰과 관련하여 당사에 기 제출된 모든 문서와 당사가 제공한 자료 및 정보에 대해서는 외부 타 기관에 공개 및 유출하지 않습니다.

○ 제안서 제출은 당사의 보안 요구에 동의하는 것으로 간주되며 위반 시 당사의 적법한 조치에 대하여 이의를 제기할 수 없습니다.

○ 제안사는 평가결과에 대해 일체의 이의를 제기할 수 없으며, 평가결과는 공개하지 않습니다.