(주)리파인 신 사옥 IT시스템 장비 도입 및 이전 사업 제안 요청서



**제 안 요 청 서**

**신 사옥 IT시스템 장비 도입 및 이전 사업**

**㈜ 리 파 인**

목 차

1. 사업 내용
2. 개요
3. 추진배경 및 목적
4. 사업범위
5. 사업 관련 요구사항
6. 장비 구성 고려사항
7. 운영 및 유지보수 고려사항
8. 사업관리 및 기타 고려사항
9. 사업 세부 내용
10. 장비 세부 사양
11. 네트워크 공사 및 기타 장비
12. 프로젝트 관리
13. 제안 추진 일정
14. 제안서 접수
15. 제안 설명회
16. 사업자 선정 일정
17. 제안 평가항목
18. 유의사항
19. 제안 시 유의사항
20. 제안가격서 유의사항

[별첨1] 제안서 목차

[별첨2] 재무현황

[별첨3] 관련 사업 수행 실적

[별첨4] 참여 인력 현황

[별첨5] 평가 결과 승복 확인서

[별첨6] 제안서 평가 항목 및 배점(안)

※ 가격제안서(별도 제출)

I. 사업 내용

1. 개요

가. 사 업 명 : 『신 사옥 IT시스템 장비 도입 및 이전 사업』

나. 사업기간 : 사업개시일로부터 6개월 이내

다. 사업범위

• 유선 네트워크 구축

• 보안 장비 구축

• 유/무선 네트워크 공사 및 랙 설치

• 기존 장비 이전 및 구축

라. 사업예산 : 10.1억원(부가세 포함)

• 1차 : 30% (계약금)

• 2차 : 30% (장비 입고 및 장비 성능 테스트 완료 후)

• 3차 : 40% (사업완료 후)

마. 계약방식 및 공고 : 제안평가 및 가격입찰

바. 제안 대상 업체

• 소프트웨어산업진흥법에 의한 소프트웨어 사업자로 신고한 업체

• 최근 2년 이내 단일 계약 건 기준 2억원 이상 사업실적 보유 업체

2. 추진배경 및 목적

가. 본사와 지사의 통합으로 네트워크의 안정성과 보안성을 확보하면서, 사용자의 망 분리를 시행함에 불편함을 최소한으로 인프라 구축 목적

나. 대용량 데이터 처리를 위한 네트워크 인프라 고도화 (10G 회선 이중화 구성)

다. 안정적인 데이터 운영 및 네트워크 보안을 통한 보안관리 강화

3. 사업범위

가. 네트워크 고도화 구축 및 이전 사업

나. 네트워크 보안 사업

다. 도입장비 목록(간략)

|  |  |
| --- | --- |
| 구분 | 수량 |
| L3 스위치 24포트 | 4 |
| L3 스위치 48포트 | 4 |
| L2 스위치 48포트 | 30 |
| L2 POE 스위치 48포트 | 15 |
| 방화벽(UTM) | 4 |
| 망연계 | 8 |
| DLP | 2 |
| 서버(PTS) | 2 |
| 랙 | 20 |
| 케이블 | 1 |

라. 이전장비 목록(간략)

|  |  |
| --- | --- |
| 구분 | 수량 |
| 라우터 | 2 |
| L3 스위치 | 2 |
| L2 스위치 | 4 |
| 네트워크 보안장비(FW/UTM) | 2 |
| San 스위치 | 2 |
| VPN | 3 |
| NAC | 3 |
| 서버 | 10 |
| PC | 100 |
| 랙 | 1 |

마. 기 운영중인 네트워크/보안 장비 연동

1) 기 구축되어 운영중인 IDC센터 네트워크 장비와 완벽한 연동

2) AWS에서 운영중인 시스템과 완벽한 연동

II. 사업 관련 요구사항

1. 장비 구성 고려사항

가. 네트워크 장비의 경우 네트워크 연결 구간은 10G 기반으로 워크그룹 스위치와 클라이언트 구간은 1G 기반으로 인프라를 구성해야 한다.

나. 네트워크 장비는 단일 제조사 제품으로 제안하는 것을 원칙으로 한다.

다. 장비와 장비 연결 인터페이스는 광 모듈로 하며 연동을 위한 동일 제조사 모듈 및 Gbic 제공해야 한다.

라. 납품하는 모든 물품은 세부 규격 조건 이상을 만족하는 제조사의 정품 및 신품으로 공급하여야 한다.

마. 제안 업체는 장비 납품 후 네트워크장비 7년, 솔루션 3년 이내 제품이 단종 되지 않는 제품을 제안하여야 하며, 사업 기간 내에 제품 단종이 발생할 경우 기 납품한 장비를 신규 장비로 교체 설치하여야 한다.

바. 제안요청서에 명시되지 않은 사항 중 본 사업의 수행에 필요한 추가 제반 사항은 제안사와 리파인 협의하여야 한다.

사. 해당 제품 목록과 신규 구성도를 참조하여 장비 및 관련 부속품을 빠짐없이 제안하여야 하며 네트워크 장비당 여유 포트를 20%를 제공해야 한다.

아. 업무망/인터넷망 망분리 시 『국가정보원 국가 정보보안 기본지침』, 『국정원 공공기관 망분리 기술기준 권고』을 충족하는 방식으로 진행하여야 함.

2. 운영 및 유지보수 고려사항

가. 도입 설치되는 시스템 대한 무상 유지보수 기간은 최종 검수 완료 후 1년이며, 무상 유지보수기간 동안 매월 정기 점검을 실시하고 점검결과 보고서를 제출하여야 함.

나. 365일 24시간 안정적인 시스템을 운영할 수 있도록 구성해야 하며, 장애 시 주요 제안 제품에 대한 신속한 복구 방안을 제시하여야 한다.

다. 제안 업체는 설치된 장비에 대하여 최신의 펌웨어, 패치 등이 발생 시 담당자와 협의하여 최신의 상태를 유지하여야 한다.

라. 제안 업체는 사업기간 내에 장비의 장애 또는 성능 저하로 인하여 성능 개선 요구 발생 시 제안 업체가 동급 이상의 장비로 무상 교체하여야 한다.

마. 제안 업체는 각 제안시스템에 관리를 위하여 사업 종료 후 안정화 기간 제시하고 그 기간 동안 안정화 방안을 제안한다.

바. 기술지원 방법 및 체계를 제시하여야 한다. (기술지원 조직, 내용, 방법 등 구체적으로 제시)

사. 시스템 운영 및 유지보수에 필요한 지침서를 제공하여야 한다. (사용자 매뉴얼, 응급조치 매뉴얼 등)

아. 구축 완료 후 시스템 운영을 위한 관리자 교육을 실시하여야 함.

3. 사업관리 및 기타 고려사항

가. 계약 후 즉시 사업진행이 가능한 분야는 인력을 즉시 투입하여 내실 있는 사업이 될 수 있도록 한다.

나. 사업 추진일정은 세분화 하여 전체 추진일정을 제시한다.

다. 제안사는 기 운영중인 전산 업무에 영향을 끼쳐서는 안되며, 제안사는 시스템 구축에 필요한 모든 지원을 하여야 한다.

라. 사업자는 승인 없이 사업을 전부나 일부를 제 3자에게 하도급 할 수 없다.

마. 본 제안 요청서에 명시되어 있는 추진 계획 및 일정을 임의대로 변경할 수 없으며 리파인에 유리하다고 판단될 경우에라도 사전에 협의하여 승인 받아야 한다.

바. 제안사는 사업 수행기간 동안 안정적인 서비스 제공을 위해 구축 담당PM(경력 7년이상)은 사업기간 동안 상주 지원해야 하며, 아울러 PM은 제안사 자사 인력으로 증빙 가능하여야 한다.

사. 제안사는 본 사업을 수행할 추진조직, 투입인력 프로필과 단계별 인력투입계획을 제시하되, 참여인력이 사업 수행상 부적당하다고 판단되거나 자격미달인 경우 등 투입인력 변경이 필요한 경우에는 동일한 수준의 역량을 갖춘 인력으로 교체할 수 있다.

아. 제품 설치 완료 후 시험 및 시험운영, 테스트 방법 등을 구체적 제시하고 모두 제출하여야 한다.

자. 사업에 필요한 제안내용은 리파인에서 제시한 입찰참가 자격 조건에 충족한 사업자가 일괄 입찰해야 하며, 제안사는 총괄 공통 사항, 각 사업부문별 기본 요구 조건 및 상세 요구조건을 충족하도록 입찰해야 한다.

카. 제안사는 운영 목적 및 구성 목표를 정확히 파악하여 사업부문별 최적의 시스템 구축이 될 수 있도록 해야 한다.

타. 본 사업을 추진하는데 요구되는 조직체계 및 조직원 역할분담 등을 구체적으로 명시하여야 함.

파. 모든 제안 솔루션에 대한 제조사 공급 및 기술지원 확약서를 제출해야 함.

III. 사업 세부 내용

1. 장비 세부 사양

가. L3 스위치

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 물리적  사양 | • 최소 4포트 이상의 1/10G Interface를 제공해야 한다.  • 스위치는 24포트 4대, 48포트 4대 이상의 10/100/1000의 포트를 제공해야 한다.  • 최소 여유 포트를 20%를 제공해야 한다.  • 최소 두 개이상의 Power Supply 장착을 통해 네트워크 장비의 안정성을 제공해야 한다.  • 안정적인 장비 운영을 제공하기 위하여, 현장 교체가 가능한 FAN module을 제공해야 한다.  • 8GB 이상의 메모리(DRAM)과, 8GB 이상의 저장장치를 제공해야 한다.  • 효율적인 운영과 빠른 확장성을 위해, Stacking 구성 또는 MCLAG나 가상화 스위치 기술을 지원해야 하며 여러 대의 장비를 하나의 IP 통해 관리가 가능해야 한다.. |
| 성능 | • 최소 104Gbps 이상의 스위칭 성능을 제공해야 한다.  • 모든 포트 상에서 Line rate의 성능을 제공해야 한다. (IPv4: 64bytes, IPv6 : 78bytes 기준)  • 최소 77Mbps 이상의 forwarding rate을 제공해야 한다.  • 하드웨어 기반의 IPv6를 지원해야 한다.  • 최소 32K 이상의 Mac Address table 수를 제공해야 한다.  • 최소 4K 이상의 VLAN ID 수를 제공해야 한다. |
| 기능 | • 다음과 같은 기본 Switch 기능을 지원해야 한다.  - STP, RSTP, MSTP, PVRST+, 802.3ad, Routed Access  (OSPF Stub), PVLAN, LLDP, QoS  • QoS 기능 지원 시 다음과 같은 세부 기능을 지원해야 한다.  - CoS, DSCP, IP Precedence 기반의 트래픽 분류 및 마킹 지원  - 트래픽 폴리싱(Policing) 및 셰이핑(Shaping) 지원  - 물리적인 포트당 8 개의 전송(egress) Queue 제공  - Strict Priority Queuing, LLQ (Low Latency Queue) 지원  - Script를 이용한 QoS policy 자동 적용  - 2-level QoS 지원  • 네트워크 보안을 위하여 아래와 같은 보안 기능을 지원해야 한다.  -  802.1x 인증, RADIUS, ARP Snooping, DHCP Snooping  • 다음과 같은 Multicast 관련 기능을 지원해야 한다.  - PIM SM, PIM SSM, IGMP  • 네트워크 트래픽 모니터링을 위하여 아래와 같은 기능을 제공해야 한다.  - SPAN, RSPAN 등  • 네트워크 장비 관리를 위하여 아래와 같은 기능을 제공해야 한다.  - SNMP, Syslog, Telnet, SSHv2, WebUI |

나. L2 스위치

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 물리적  사양 | • 최소 4포트 이상의 1/10G Interface를 제공해야 한다.  • 스위치는 최소 48포트 이상의 10/100/1000의 포트를 제공해야 한다.  • 최소 여유 포트를 20%를 제공해야 한다.  • 안정적인 장비 운영을 제공하기 위하여, 현장 교체가 가능한 FAN module을 제공해야 한다.  • 1GB 이상의 메모리(DRAM)과, 128MB 이상의 저장장치를 제공해야 한다.  • 효율적인 운영과 빠른 확장성을 위해, Stacking 구성 또는 MCLAG나 가상화 스위치 기술을 지원해야 하며 여러 대의 장비를 하나의 IP 통해 관리가 가능해야 한다. |
| 성능 | • 최소 56Gbps 이상의 스위칭 성능을 제공해야 한다.  • 모든 포트 상에서 Line rate의 성능을 제공해야 한다. (IPv4: 64bytes, IPv6 : 78bytes 기준)  • 최소 41Mbps 이상의 forwarding rate을 제공해야 한다.  • 하드웨어 기반의 IPv6를 지원해야 한다.  • 최소 16K 이상의 Mac Address table 수를 제공해야 한다.  • 최소 11K 이상의 IPv4 routing table 수를 제공해야 한다.  • 최소 1.5K 이상의 IPv6 routing table 수를 제공해야 한다.  • 최소 1K 이상의 VLAN ID 수를 제공해야 한다. |
| 기능 | • 다음과 같은 기본 Switch 기능을 지원해야 한다.  - STP, RSTP, MSTP, PVRST+, 802.3ad, (OSPF Stub), PVLAN, LLDP, QoS  • QoS 기능 지원 시 다음과 같은 세부 기능을 지원해야 한다.  - CoS, DSCP, IP Precedence 기반의 트래픽 분류 및 마킹 지원  - 트래픽 폴리싱(Policing) 및 셰이핑(Shaping) 지원  - 물리적인 포트당 8 개의 전송(egress) Queue 제공  - Strict Priority Queuing, LLQ (Low Latency Queue) 지원  - 2-level QoS 지원  • 네트워크 보안을 위하여 아래와 같은 보안 기능을 지원해야 한다.  - 802.1x 인증, RADIUS, ARP Snooping, DHCP Snooping  • 다음과 같은 Multicast 관련 기능을 지원해야 한다.  - PIM SM, PIM SSM, IGMP  • 네트워크 트래픽 모니터링을 위하여 아래와 같은 기능을 제공해야 한다.  - SPAN, RSPAN  • 네트워크 장비 관리를 위하여 아래와 같은 기능을 제공해야 한다.  - SNMP, Syslog, Telnet, SSHv2, WebUI |

다. L2 POE 스위치

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 물리적  사양 | • 최소 4포트 이상의 1/10G Interface를 제공해야 한다.  • 스위치는 최소 48포트 이상의 10/100/1000의 포트를 제공해야 한다.  • 최소 여유 포트를 20%를 제공해야 한다.  • 안정적인 장비 운영을 제공하기 위하여, 현장 교체가 가능한 FAN module을 제공해야 한다.  • 2GB 이상의 메모리(DRAM)과, 128MB 이상의 저장장치를 제공해야 한다.  • 효율적인 운영과 빠른 확장성을 위해, Stacking 구성 또는 MCLAG나 가상화스위치 기술을 지원해야 하며 여러 대의 장비를 하나의 IP를 통해 관리가 가능해야 한다. |
| 성능 | • 최소 104Gbps 이상의 스위칭 성능을 제공해야 한다.  • 모든 포트 상에서 Line rate의 성능을 제공해야 한다. (IPv4: 64bytes, IPv6 : 78bytes 기준)  • 최소 41Mbps 이상의 forwarding rate을 제공해야 한다.  • 하드웨어 기반의 IPv6를 지원해야 한다.  • 최소 16K 이상의 Mac Address table 수를 제공해야 한다.  • 최소 11K 이상의 IPv4 routing table 수를 제공해야 한다  • 최소 1.5K 이상의 IPv6 routing table 수를 제공해야 한다.  • 최소 1.5K 이상의 ACL table수를 제공해야 한다.  • 최소 6MB 이상의 buffer size를 제공해야 한다.  • 최소 1K 이상의 VLAN ID 수를 제공해야 한다. |
| 기능 | • 다음과 같은 기본 Switch 기능을 지원해야 한다.  - STP, RSTP, MSTP, PVRST+, 802.3ad, (OSPF Stub), PVLAN, LLDP, QoS  • QoS 기능 지원 시 다음과 같은 세부 기능을 지원해야 한다.  - CoS, DSCP, IP Precedence 기반의 트래픽 분류 및 마킹 지원  - 트래픽 폴리싱(Policing) 및 셰이핑(Shaping) 지원  - 물리적인 포트당 8 개의 전송(egress) Queue 제공  - Script를 이용한 QoS policy 자동 적용  - 2-level QoS 지원  • 네트워크 보안을 위하여 아래와 같은 보안 기능을 지원해야 한다.  - 802.1x 인증, RADIUS, ARP Snooping, DHCP Snooping  • 다음과 같은 Multicast 관련 기능을 지원해야 한다.  - PIM SM, PIM SSM, IGMP  • 네트워크 트래픽 모니터링을 위하여 아래와 같은 기능을 제공해야 한다.  - SPAN, RSPAN, EEM  • 네트워크 장비 관리를 위하여 아래와 같은 기능을 제공해야 한다.  - SNMP, Syslog, Telnet, SSHv2, WebUI |

라. 방화벽(UTM)

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 물리적  사양 | • 제안시스템은 하드웨어 일체형의 어플라이언스 타입 장비이어야 한다.  • 방화벽과 VPN, IPS, Application Control, Anti-Virus, Anti-Spam, Web-Filtering, 가상화 등의 기능을 제공하여야 한다.  • 제안시스템은 보안 모듈이 ASIC 처리가 되어야 한다.  • 인터페이스는 기본적으로 10/100/1000 UTP 16포트, 1G SFP 8포트, 10G SFP+ 8 포트 이상 지원해야 한다.  • 방화벽 트래픽 용량에 따라 최대 79.5/78.5/70 Gbps까지 지원해야 한다.  • IPsec VPN 트래픽 용량은 최대 55 Gbps까지 지원해야 한다.  • IPS 트래픽 용량은 최대 12 Gbps까지 지원해야 한다.  • Threat Protection Throughput 용량은 최대 9 Gbps까지 한다.  • 동시세션은 최대 7.8 Million을 지원해야 한다.  • 초당 세션 수는 최대 500,000을 지원해야 한다.  • 한 장비에서 가상화 기능을 지원해야 하며, 최소 10개 이상의 가상화 라이선스를 기본 제공하여야 한다.  • 가상 방화벽 당 Configuration restore 및 backup이 가능해야 한다.  • IPsec과 SSL VPN을 단일장비에서 동시 지원해야 하며, 장비의 최대 수용 용량을 수용할 수 있는 라이선스를 기본 제공해야 한다.  • IPsec VPN Tunnel 수는 2,000개를 지원해야 하며, SSL VPN 동시접속 사용자 수는 1,000명을 지원해야 한다.  • 가상 방화벽별 리소스 할당 기능을 지원 해야 한다. (방화벽 세션 수, 방화벽 정책 수, 방화벽 오브젝트 수 등) |
| 기능 | • 다음과 같은 침입차단 기능을 제공하여야 한다.  - 출발지 IP별 접근 통제  - 목적지 IP별 접근 통제  - Protocol별 접근 통제  - Service Port별 접근 통제  • AWS와 VPN 통신 기능을 제공하여야 한다.  • 출발지, 목적지 IP별 세션 제한 기능을 제공하여야 한다.  • DLP(Data Loss Prevention) 기능을 지원해야 한다.  • 장비 장애 시 서비스 연속성을 보장하기 위한 장비 이중화 구성이 가능하여야 하며, 이중화 구성 시 세션이 동기화 되어야 한다.  • 장비의 안정성을 위하여 관리 모듈과 트래픽 처리 모듈이 분리되어 있어야 하며, 관리 모듈은 트래픽 처리에 영향을 주어서는 안된다.  • L4 Switch 없이 자체적으로 HA 구성이 가능해야 하며, stateful failover를 지원해야 한다.  • 암호화 통신(SSL, SSH 등)을 통한 방화벽의 관리가 가능하여야 한다.  • Layer-3 방식의 NAT, Route 모드가 지원되어야 한다.  • Source Address와 destionation address에 대해서도 NAT 및 PAT 기능을 제공하여야 한다.  • Static, OSPF, RIP, BGP v4 등의 라우팅 프로토콜을 지원함으로써 대규모 네트워크 구성 변경 없이 적용이 가능하여야 하며, MTU 사이즈와 무관하게 적용 가능하여야 한다.  • IPv4와 IPv6를 지원하여야 한다.  • 우회접속 어플리케이션 차단 기능을 지원한다.  • URL 필터를 위해 DB를 통한 탐지/차단 기능을 지원한다.  • 어플리테이션별 QoS 기능을 지원한다.  • CPU, Memory 사용량, CPS, 동시세션 등 Firewall 리소스 상태에 대하여 실시간 확인 및 모니터링이 가능하여야 한다.  • 제안시스템의 문제상황(CPU 및 Memory 과다사용, 과다 세션 발생 등)에 대해 경고기능이 제공되어야 한다.  • 네트워크 실시간 차단기능을 제공하며, 4가지 바이러스 악성코드 탐지기능을 제공한다. (Proxy/Flow/Local Sandbox, Cloud Sandbox)  • Anti-Virus 및 IPS 등 UTM 기능은 단일 벤더의 솔루션으로 제공되어야 한다.  • Standalone과 동일하게 모든 보안기능을 가상화로 제공하여야 하며, VDOM-link를 통해 VDOM 간 직접 통신 및 가속기능을 지원하여야 한다.  • IP 기반 + ID 기반 + Device 기반 정책 적용 기능을 제공한다. (BYOD)  • 클라이언트의 위험스런 행위를 판별할 수 있는 평판 모니터링 기능을 지원해야 한다. (Client Requtation)  • SSL/SSH Inspection 기능을 제공한다. (Client side : transparent scanning HTTPS, FTPS, SMTPS, IMAP3, POP3S, SSH)  • Log에 국가별 표시 기능을 지원해야 한다. |
| Attack  방어기능 | • 다양한 종류의 네트웍 공격들에 대한 방어 능력이 있어야 한다. (SYN Attack, ICMP/UDP Flooding Attack, Ping of Death a Attack, IP Spoofing Attack, Port Scan Attack, Dos, DDoS 공격 등등) |
| 운영 및 관리  요구사항 | • Syslog, SNMP V1/V2를 지원하여야 하며, 통합보안관리시스템과 연동이 가능하여야 한다.  • 여러명의 관리자 설정이 가능하여야 하며, 각 관리자 마다 별도의 권한 부여가 가능하여야 한다.  • 기능상의 버그 및 추가 패치가 있을 경우, 원격 지원 및 On –Site 지원이 동시에 가능하여야 한다.  • 설정파일에 대한 관리 및 백업이 가능하여야 한다.  • 방화벽 매니지먼트 통신은 암호화되어야 한다.  • Rest API를 통해 수행한 명령어 내역을 Log로 남길 수 있어야 한다.  • 관리자가 CLI에서 수행한 명령어 내역을 Log로 남길 수 있어야 한다.  • 본 시스템은 Rebooting 된 후에도 정보가 Syslog를 통해 저장되거나, 저장할 수 있는 방법이 제공되어야 한다. (log 저장은 6개월 이상)  • 제안시스템의 문제상황(CPU, Memory 과다사용, 과다 세션 발생 등)에 대해 경고기능이 제공되어야 한다.  • 초기 설정을 위한 콘솔 포트 및 모뎀 포트를 제공하여야 한다.  • 관리상의 편의를 위하여 한글 GUI 및 한글 매뉴얼을 제공하여야 한다. |

마. 망간자료전송(스트림연계)

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 사양 및 기능 | [HW – 요구사항]  • CPU : Intel Xeon 3.4GHz 4Core 이상  • Memory : 16GB 이상  • HDD : 2TB 이상  • NIC : 10/100/1000 \* 2EA, 10G \* 2EA 이상  • Power : Dual Power (이중화)  [SW – 요구사항]  • 보안기능확인서 인증 제품.  • 10G 기준 공인 성적서 제출.  - 720,000 TPS 이상 / 5,500,000 CC이상  • 차세대 IP 주소체계 대응을 위한 IPv6 인증 제품. (인증성 제출)  • 망간통신은 일반적인 TCP/IP가 아닌 안전한 전용프로토콜을 통한 기밀성 보장.  • 정책에 대한 객체 정의, IP, Port 및 정책그룹 설정 기능을 제공.  • 이중화(HA) 구성으로 최소한 다운타임 서비스 제공  • 원활한 Session 관리를 위한 Garbage Session Timeout 기능 제공  • 망연계 정책에 따른 서비스 현황 모니터링 기능을 제공.  • 과도한 패킷 유입 시, 패킷 차단기능 제공  • White-list 기반의 망간자료 연계 정책을 제공.  • 정책 적용 시 장비 재기동 없이 적용 가능하도록 정책 적용 기능 제공  • URL 정책 연계 기능 제공 |

바. 망간자료전송(파일연계)

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 사양 및 기능 | [HW – 요구사항]  • CPU : Intel Xeon 3.4GHz 4Core 이상  • Memory : 16GB 이상  • HDD : 2TB 이상  • NIC : 10/100/1000 \* 2EA, 10G \* 2EA 이상  • Power : Dual Power (이중화)  [SW – 요구사항]  • 보안기능확인서 인증 제품.  • 10G 기준 공인 성적서 제출.  - 720,000 TPS 이상 / 5,000,000 CC이상  • 차세대 IP 주소체계 대응을 위한 IPv6 인증 제품. (인증성 제출)  • 운영체제(OS)는 안정적 서비스를 위해 5년 이상 제공해야 한다.  • 한글, 파워포인트, 워드 등 OLE 확장자 검사 기능 제공  • 신규 File MIME Type 관리자 추가 기능 제공  • 결제자의 전송파일에 대한 미리 보기 기능 지원  • 일괄 결재 기능 제공  • 망간통신은 일반적인 TCP/IP가 아닌 안전한 전용프로토콜을 통한 기밀성 보장.  • 확장자 위변조 검사 및 차단 기능 제공  • 클라우드 환경 변화에 따른 솔루션 전환 가능 제품으로 제안 할 것  • 이중화(HA) 구성으로 최소한 다운타임 서비스 제공.  • 업무상 필수적으로 연계가 필요한 외부기관 연계 기능 제공  • 특정 URL을 허된 사용자별 접속 정책설정 기능 제공  • URL 연계 후 외부기관 URL 변경시 변경 URL을 확인할 수 있어야 함  • URL 연계 시 포트로 제어할 수 있는 기능 제공  • URL 또는 도메인의 서브도메인 및 하위 URL까지 연계 지원 |

사. DLP(내부정보유출방지 및 개인정보검색솔루션)

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 사양 및 기능 | [Off-Line]  • 이동식 저장소를 통한 유출 모니터링 통제기능  • 이동식 저장소에 대한 기간 별 및 장치 별 예외 기능 (결제/승인 기능)  • 스마트폰(MTP/PTP)을 통한 유출 모니터링 및 통제 기능  • 테더링 사용 차단 기능 (블루투스 및 USB)  • 블루투스 연결 차단 및 파일 전송 차단 기능  • USB 장치 연결 기록 및 차단 기능(BAD USB 방지)  • 매체 제어 및 장치 연결 차단 기능 (CD/DVD,FDD,시리얼,패러럴, 적외선 등)  • 모뎀 및 무선 랜 차단 기능  • 무선 AP(핫스팟)에 대하여 MAC 값 별로 차단 기능  • HDD / NIC 추가 장치 차단 기능  • 프린터를 통한 출력물 워터마킹 및 사본 저장 기능  • 비업무 프로그램 실행 기록 및 모니터링  • 내부 중요 파일(확장자)에 대한 프로그램 별 접근 제어 기능  • 내부 중요 프로그램 사용에 대한 화면 녹화 기능  • PC내 개인정보가 있는 파일들에 대한 기록/암호화/격리/삭제 처리 기능  [On-Line]  • MS-Outlook 메일 발송 및 첨부파일에 대한 모니터링 및 통제 기능  • Web-Mail(SSL) 전송에 대한 모니터링 및 통제 기능(Gmail, Naver, Nate 등)  • Web-Mail(SSL) 전송에 대한 URL별 예외 적용 기능  • Http/Https(SSL)을 통한 웹 첨부 파일 유출 방지 기능(IE/Chrome/Firefox 지원)  • 비업무 사이트 Http/Https(SSL)사이트 접속 방지 기능(IE/Chrome/Firefox 지원)  • FTP, P2P 등을 통한 파일 유출 모니터링 및 통제 기능  • 네트워크 공유 사용 로깅 및 네트워크 공유폴더 접근 / 생성 차단 기능  • 네트워크 드라이브 연결 차단 기능  • 네트워크 Port 통제 기능  • 특정 사이트에 대한 별도의 접속 기록 및 통제 기능  • 웹 브라우저 확장 앱에 대한 별도 실행 통제 기능(Chrome, MS Edge)  • 메신저 대화 모니터링 및 이미지 붙여넣기 차단 기능(카카오톡, 네이트온 등)  • 메신저 파일 업로드 통제 기능 (카카오톡, 네이트온, 스카이프, 라인 등)  [보안관리]  • 정보 유출에 대한 제어를 정책 별로 통제 기능  • 개인정보 및 중요 키워드 유출에 대한 정책 설정 및 통제 기능  • 정보 유출 시 실시간으로 서버에 기록 저장 기능(유출내용, 원본파일, 동영상 등)  • 파일 유출 시 탐색기에서 파일생성/변견/유출 등의 이력들을 도식화한 원본 추적 기능  • 화면보호기 강제 설정 기능 (이미지/동영상)  • PC 취약점 보안 감사/리포팅 기능 (윈도우 보안 설정 모니터링 등)  • 화면 캡쳐 기능 사용시 경고 및 차단 기능  • 파일 확장자 변경 금지 기능  • On/Off-line을 통한 정보 유출에 대한 원본저장 기능  • 정책에 위배되는 유출 행위 시 해당 사용자에게 경고 알림 기능  • 클립보드 사용시 개인정보 및 키워드에 대한 제안 기능  • Off-Line시 기존정책 유지 후 On-line시 유출에 대한 전송 기능  • PC 모니터 워터마크 적용 기능  • 보안정책 적용의 예외사항에 대한 신청/승인 프로세스 기능  • 보안정책 예외사항에 대한 다양한 승인권한 제공 기능  • 그룹별 보안감사 권한 상속 기능  [관리자 기능]  • 내부 정보 유출에 대한 각종 로그 관리 및 보고서 기능  • 유출현황에 대한 실시간 조회 기능  • 생성되는 리포트 및 보고자료는 편집 가능한 형태로 제공(엑셀)  • 대쉬보드에서 유출행위에 대해 별도의 조회 없이 상세내역 확인 가능  • 유출내역에 대한 이상징후 모니터링 및 관리자 알림 기능  • 메일을 통한 주기적 정기 보고서 기능  • 특정 사용자에 대한 지정 일자 별 사용/유출 이력 조회 기능  • 특정 클라이언트별 어플리케이션 사용 이력 및 웹사이트 접속 이력 기능  • 사용자별, 그룹별, 어플리케이션별 설치 목록 조회 기능  • 보안 정책을 개인별, 그룹별 단위로 적용 기능  • 보안관리자 계정 권한 분리를 통한 보안관리 사고 최소화 지원  • 관리자용 접근 IP 또는 대역 제한 기능  • 유출 유형별 위험도에 따른 중요도 설정 기능  • 보안 정책 변경 이력 및 감사 조회 기록 기능  • 다양한 오프라인 정책 적요 기능  • Agent 무력화 방지 (Process Kill, 서비스 정지, 안정모드 구동 등)  • Agent 이상동작 모니터링 기능  • 주민번호, 카드번호에 대한 과탐을 최소화한 알고리즘 제공  • 정책관리자 이중 인증 기능  • PC의 S/W, H/W 구성 현황 확인  • 일반USB에 S/W방식의 보안USB 기능 제공  • Server와 Agent 간의 시간동기화 기능  • Agent 메시지 전송 기능  [기타]  • 내부정보유출 / 개인정보 검색 시스템에 관한 기초 정책 제시 및 발주기관 합의하에 정책 변경  • 제안 솔루션은 Agent 방식의 PC에 직접 설치/운영 할 수 있는 솔루션  • 각 클라이언트에 대한 로그를 일정기간(12개월) 보관할 수 있는 운영서버 Spec 선정 |

2. 네트워크 공사 및 기타 장비

가. 네트워크 공사

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 사양 | [설치 범위]  • 신사옥 B2 ~ 7F  [포설 범위]  • 2층 전산실  [설치 범위]  • 각층 UTP CABLE CAT.6  • 각 장비 업링크 10G 광케이블  • 전산실 시스템 장비 UTP CABLE CAT.6 혹은 광케이블 |

나. RACK 도입 및 구축

|  |  |
| --- | --- |
| 구분 | 기능 및 규격 |
| 사양 | [설치 장소]  • 전산실 및 각층 EPS/TPS  [네트워크 랙]  • 전산실 : 41U / D 800 \* W 600  • 각층 EPS/TPS : 37U / D 800 \* W 600  [서버 랙]  • 전산실 : 42U / D 1200 \* W 600  [기타사항]  • 랙 구성과 관련된 사항은 사전 협의 후 진행  • 기타 엑세서리 및 옵션 무상 제공 |

3. 프로젝트 관리

가. 사업 추진과정에서 생산되는 제반 작업 단위 별 산출물에 대해서 산출물의 종류, 주요 내용 등 제반 사항에 대해 제출해야 한다.

나. 프로젝트를 성공적으로 수행하기 위해서 위험관리를 해야 한다.

다. 사업자 선정 후 일정 지연, 품질 저하 등 위험 발생을 사전에 예방하고 위험요소 발생 시 사후 조치 방안을 구체적이고 상세히 제출하여 계획된 대처 방안에 따라 신속히 대응해야 한다.

라. 각 항목별 수치화나 단계화 된 위험도를 정하여 단계별로 의사 결정 등에 의한 실행 계획을 작성해야 한다.

마. 프로젝트 추진과정에서 요구되는 진척, 위험, 변경사항의 관리방안 및 지속적인 문제점을 파악 관리할 수 있는 방안을 작성해야 한다.

바. 장애 발생시 대책 및 지원 방안 등 상세한 하자보수 계획을 작성해야 한다.

사. 프로젝트 완료 단계에서 기술이전 및 교육훈련 방안을 작성해야 한다.

아. 교육 훈련은 시스템 관리자, 일반 사용자 등으로 분류하여 교육 내용, 교재작성을 해야 한다.

자. 집체 교육이 어려울 시 각 파트 및 업무 담당 파트를 방문해서 집합 및 개별 교육을 해야 하며, 시스템 오픈 전에 사용자의 이해도 및 시스템 사용 능력을 향상시켜야 한다.

차. 교육기간, 인원 조건 등을 명시하여 제출해야 한다.

카. 교육에 따른 교재 및 소요 경비는 계약 업체가 지원한다.

타. 시스템 운영 및 유지관리 등을 리파인에서 수행할 수 있도록 충분히 기술전수 및 교육을 실시하여야 한다.

파. 구축 시스템의 기술 발전방향 및 신제품에 대한 정보가 정기적으로 전달되도록 하고, 시스템 구축 이후에도 관련 분야의 정보에 대한 기술 자문에 응해야 한다.

Ⅳ. 제안 추진 일정

1. 제안서 접수

가. 접수 마감 : 2024년 4월 23일 (화) 17:00

나. 제출 방법 : 방문 또는 이메일 제출

다. 제출 자료 : 제안서 포함 기타 서류 일체 및 파일

라. 주 소 : 서울시 강남구 삼성동 테헤란로625, 덕명빌딩5층 ㈜리파인

마. 접 수 처 : IT전략본부

사. 담 당 자 : 장성진파트장 (Tel : 02.2189.8714(333), [rf1592@refine.co.kr](mailto:rf1592@refine.co.kr))

2. 제안서 발표

가. 일 시 : 2024년 4월 25일 (목) 13:00

나. 장 소 : ㈜리파인 4층 1회의실

다. 방 법 : 제안 접수 역순 (발표 및 질의응답)

라. 발 표 자 : 사업 수행 PM

마. 제안서 발표자료는 별도 작성 가능하나 제안서 내용과의 일관성을 반드시 유지해야 함.

사. 상기 일정은 당사 사정에 의해 변경 가능

3. 사업자 선정 일정

|  |  |
| --- | --- |
| 항 목 | 일 정 |
| 제안요청서 발송 | 2024년 4월 12일 (금) |
| 제안서 Q&A | 2024년 4월 15 ~ 17일 |
| 제안서 마감 | 2024년 4월 23일 (화) 17:00 |
| 제안서 발표 | 2024년 4월 25일 (목) 13:00 |
| 우선협상대상자 선정 | 2024년 5월 02일 (목) |

4. 제안 평가항목

가. 제안일반

나. 제안사 부문

다. 사업수행 기술부문

라. 관리 및 지원부문

마. 비용

Ⅴ. 유의사항

1. 제안 시 유의사항

가. 제안자 및 제안요청자는 상호 습득한 모든 정보에 대하여 그 비밀 보호를 보장하여야 하며, 상호 협의 없이는 무단 전재, 재전달 및 복사 등을 통한 정보 유출 금지 함.

나. 본 제안은 당사의 사정에 의해 쥐소 가능하며, 이에 대한 이의 제기 불가

다. 본 제안서에 의해 제안업체가 작성한 각종 보고서 및 산출물 등의 모든 권한은 당사에 귀속함.

라. 제안서 내용의 객관성과 타당성을 인정할 수 있도록 계량화된 자료명시

2. 제안가격서 유의사항

가. 가격제안서는 별도 밀봉하여 제출

나. 가격단위는 원화로 하고, 부가세 포함 금액 제시

다. 장비 이전에 대한 비용은 가격제안서에 포함하지 않고 별도 견적서로 분리 제출할 것

<별첨 1> 제안서 목차

|  |  |
| --- | --- |
| **작성 항목** | **작성 방법** |
| Ⅰ. 제안개요  1. 제안 배경 및 목적  2. 제안 범위  3. 기대효과 | ❍ 제안사는 해당사업의 제안요청 내용을 명확하게 이해하고 본 제안의 배경 및 목적, 범위, 추진방향 및 주요내용, 구축 전략, 제안의 특징 및 장점, 기대효과를 요약하여 기술 |
| Ⅱ. 제안업체 일반  1. 일반현황  2. 조직 및 인력  3. 주요사업내용  4. 주요사업실적 | ❍ 제안사의 일반현황 및 주요 연혁, 최근 3년간의 자본금 및 부문별 매출액을 명료하게 제시  ❍ 조직 및 인원현황, 주요사업내용을 제시  ❍ 해당사업과 관련이 있는 주요 사업실적을 제시 |
| Ⅲ. 기술부문  1. 세부 구축 일정 및 방법  2. N/W/보안 설계 및 장비 구축 방안  3. 테스트 및 시험운영 안정화 방안  4. 비상대책 방안 | ❍ 현재 네트워크 구성 및 전송 구간별 속도에 대한 현황 분석 및 문제점 파악 방법 제시  ❍ 구축시 각 구성요소별로 차질 없는 업무수행을 위한 설치 절차와 정책 수립 방법 제시  ❍ 복잡한 구성에 따른 장애위험을 감소하고, 무중단의 안정적인 운영을 위한 방안 제시  ❍ 향후 주요 네트워크 장비 구축를 위한 단계적 설치 및 전송속도 개선을 위한 방안 제시  ❍ 기존 네트워크 호환성 분석 및 연계방안과 네트워크 구성요소별 구성장치의 사양 및 기능을 제시 |
| Ⅳ. 사업관리부문  1. 추진전략  2. 전체사업 추진일정 계획  3. 보고 및 검토 계획  4. 사업수행조직 및 인력투입계획 | ❍ 추진일정을 도표로 기술  ❍ 단계별 보고일정 수립 및 보고양식 제시  ❍ 투입인력을 장비/솔루션 단위별로 제시하고, 이력사항을 붙임양식을 이용하여 작성 |
| Ⅴ. 지원부문  1. 교육훈련계획  2. 유지보수계획  3. 기술이전계획  4. 기타 지원사항 | ❍ 이용대상자별로 교육내용, 교육기간, 인원 등을 상세히 제시  ❍ 유지보수를 위한 종합적인 방안이 제시  ❍ 유지보수 요원에 대한 기술이전계획을 분야별로 상세하게 제시 (단, 산출물로 제시할 수 없는 원천기술부문이 있는 경우 이를 제안서상에 명시)  ❍ 지원 가능한 사항에 대한 기타 내용을 기술 |
| Ⅵ. 기타  \* 추가제안 등 | ❍ 위 항목에서 제시되지 않은 기타 내용을 기술 |

**<별첨 2> 재무현황**

**재무구조 및 최근 3년간 매출액**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **구 분** | | **20 년** | **20 년** | **20 년** | **합 계** | **평 균** |
| 1. 총자본 | |  |  |  |  |  |
| 2. 자기자본 | |  |  |  |  |  |
| 3. 유동부채 | |  |  |  |  |  |
| 4. 고정부채 | |  |  |  |  |  |
| 5. 유동자산 | |  |  |  |  |  |
| 6. 당기순이익 | |  |  |  |  |  |
| 7. 매출원가 | |  |  |  |  |  |
| 8. 부문별  매출액 | H/W |  |  |  |  |  |
| S/W(솔루션 등) |  |  |  |  |  |
| 시스템개발(SI) |  |  |  |  |  |
| 컨설팅 |  |  |  |  |  |
| 기타( ) |  |  |  |  |  |
| 합 계 |  |  |  |  |  |
| 9. 자기자본이익율  (당기순이익/자기자본) | |  |  |  |  |  |
| 10. 부채율  ((유동부채+고정부채)/자기자본) | |  |  |  |  |  |

주) 1. 신용평가기관(한신평, 한기평 등) 발행 신용분석보고서 첨부

주) 2. 결산공고 되었거나 자체 보고된 대차대조표, 손익계산서, 이익잉여금처분계산서, 현금흐름표 등 재무구조 및 매출액을 확인할 수 있는 회계자료 첨부

**<별첨 3> 관련 사업 수행 실적**

(단위: 백만 원, VAT포함)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 사업명 | 사업개요 | 사업기간 | 발주처 | 금액 | 비 고 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 계 | | | |  |  |

주) 1. 현재 수행 중인 사업도 포함하여 연도순으로 기재하며, 제안과제와 유관한 것만 기재한다

2. 하도급은 발주처가 승인한 경우에 한하여 작성하며 비고란에 원 도급 회사를 기재한다

3. 사업기간에는 해당사업 전체기간과 해당회사의 참여기간을 구분하여 기재한다

4. 비고란에는 공공기관, 일반기업, 기타로 구분하여 기재한다

**<별첨 4> 참여 인력 현황**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 소속 |  | 성명 | 직위 | 기술 등급 | 담당업무 | 해당분야 자격증 | 프로그래밍 경력 | RPA  경력 | 참여기간 | 참여공수 (M/M) |
| 소속사 |  | 홍길동 | 부장 (PM) | 특급 | 총괄 | 정보기술사 | 15.6년 | 2년 | 14.04-14.03 |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | 소 계 | | | | | | | | |  |

주) 1. 근무경력은 제안일 현재를 기준으로 기재

2. 1인이 자격증을 여러 개 소지한 경우 상위 1개만 작성

**<별첨 5> 평가결과 승복 확인서**

**평가결과 승복 확인서**

귀사가 추진 중인 “신 사옥 IT시스템 장비 도입 및 이전 사업” 제안에 참여한 당사는 ㈜리파인의 공정한 심사와 객관적인 내부절차를 존중하여 제반 결정에 아무런 이의를 제기하지 않을 것임을 확약합니다.

2024년 월 일

주식회사 대표이사 (인)

**㈜리파인 귀하**

**<별첨 6> 제안서 평가 항목 및 배점(안)**

**제안서 평가 항목 및 배점(안)**

|  |  |  |  |
| --- | --- | --- | --- |
| 평가부문 | 평가항목 | 세부평가항목 | 배점기준 |
| 제안 일반  (5) | 1. 제안요청 내용 이해 | - 제안요청 사항에 대한 명확한 이해  - 제안서 작성의 충실도  - 추진전략, 제안의 특 • 장점  - 제안내용의 정확성 | 5 |
| 제안사 부문  (25) | 1. 수행조직 및 인력 | - 조직체계 구성의 적절성  - 전문인력 보유 현황 | 10 |
| 2. 유사용역 실적 | - 유사용역에 대한 수행실적  (컨설팅, 유/무선 네트워크 구축)  - 유사용역 수행경험 인력 수 | 10 |
| 3. 재무건전성 | - 부채비율, 매출규모, 신용도 등 | 5 |
| 사업수행  기술부문  (30) | 1. 사업수행 방안의 적정성 | - 사업수행 방법론  - 사업수행 절차의 적정성 및 타당성 | 5 |
| 2. 수행계획의 적합성 및 우수성 | - 세부 과제별 제안내용의 우수성  - 세부 업무 구성의 적절성  - 추진방안의 실현 가능성  - 참여인력의 적정성(외부인력 포함) | 25 |
| 관리 및  지원부문  (30) | 1. 사업 관리 방안 | - 과제 수행 방법론의 우수성  - 체계적 관리 방안의 적절성 | 10 |
| 2. 일정계획 및 산출물 | - 일정계획의 타당성  - 단계별 산출물의 적정성 | 10 |
| 3. 품질보증 | - 품질보증계획의 적정성 | 5 |
| 4. 보안관리 등 | - 기술지원 계획의 적정성  - 유지보수 지원방안의 적정성  - 보안관리 체계의 적정성 | 5 |
| 비용  (10) | 1. 비용 방안 | - 도입 비용의 적정성 | 10 |
| 기술 및 비용 평가점수 계 | | | 100 |