삼육대학교
방화벽(NGFW)장비 이중화 구성
제안요청서

2021. 7.

삼육대학교
SAHMYOOK UNIVERSITY

목 차

Ⅰ. 사업개요

1. 사업명 : 삼육대학교 방화벽(NGFW) 장비 이중화 구성

2. 사업 기간 : 계약일로 2개월 이내

3. 사업 추진 배경 및 목적

1) 기존 방화벽 구성은 단일화로 운영 중
2) 코로나19로 인한 비대면 영상회의 및 온라인 교육 등의 업무환경 변화
3) 급변하는 IT 기술로 인해 대용량 멀티미디어 서비스에 대응할 수 있는 기반 조성 필요
4) 이중화 구성을 통해 안정화 추구

4. 주요 사업 내용

1) 기설치된 방화벽 이중화 구성 (모델명 : Palo Alto PA-3260)

구 분	수량
차세대 방화벽(NGFW)	1대
방화벽 이중화 구성 환경설정	1식

Ⅱ. 사업자 선정 제안 요구 사항

삼육대학교에서 제시한 목표구성에 적합한 방화벽을 제안하고 안정성, 효율성 및 추후 확장성을 고려하여 운영상 문제가 발생하지 않도록 필요한 모든 제품을 제안하여야 한다.

1. 운영 및 유지보수 고려사항

1) 모든 시스템(H/W)의 무상유지보수 기간은 사업종료 후 12개월까지로 한다.
2) 제안업체는 방화벽 설치 장비가 1년 365일 24시간 안정적으로 운영될 수 있도록 운영 및 유지보수 방안을 제시하여야 한다.
3) 제안업체는 설치된 H/W 장애 및 하자 발생 시 신속한 장애복구 방안을 구체적으로 제시하여야 한다.(6시간 이내 장애 복구 완료)
4) 제안업체는 설치된 장비에 대해서 최신의 펌웨어, 패치 등이 발생 시 삼육대

학교 담당자와 협의하여 최신의 상태를 유지하여야 한다.

5) 제안업체는 각 제안시스템에 관리를 위하여 사업 종료 후 안정화 기간 제시하고 그 기간 동안 안정화 방안을 제안한다.

7) 제안업체는 월 1회 현장 정기점검을 통해 장비의 원활한 동작을 위한 필요한 모든 조치를 수행하며, 그 결과를 삼육대학교 담당자에게 보고한다.

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

9) 시스템 운용 및 유지보수에 필요한 지침서를 제공하여야 한다.
(사용자 매뉴얼, 응급조치 매뉴얼등)

2. 사업관리 및 기타 고려사항

1) 계약 후 즉시 사업진행이 가능한 분야는 인력을 즉시 투입하여 내실 있는 사업이 될 수 있도록 한다

2) 사업 추진일정은 세분화 하여 전체 추진일정을 제시한다.

3) 기존 시스템 및 운영 중인 타 시스템에 운영에 미칠 영향을 최소화한 수행방법을 제안한다.

4) 사업자는 삼육대학교의 승인 없이 사업을 전부나 일부를 제 3자에게 하도급할 수 없다.

5) 본 제안 요청서에 명시되어 있는 추진 계획 및 추진 내용, 일정은 임의대로 변경할 수 없으며 삼육대학교에 유리하다고 판단될 경우에라도 사전에 삼육대학교와 협의하여 승인받아야 한다.

6) 제안서 또는 계약서에 대한 해석상의 이견이 발생할 경우 삼육대학교의 해석을 우선으로 한다.

7) 본 사업의 업무범위는 제안요청서에 누락된 업무 또는 제안서에 제시하지 않는 업무도 상호협의에 의해 본 용역에 포함할 수 있다.

8) 사업자는 계약진행 및 사업완료 후 하자보수기간 동안 삼육대학교에서 감사 등의 사유로 본 사업 이행에 관한 자료제출, 서류열람 등을 요구할 경우 이에 적극 협력하여야 한다.

9) 제품 설치 완료후 시험 및 시험운영, 테스트 방법 등을 구체적을 제시하여야 한다.

10) 낙찰된 업체는 Black Market을 경유한 제품 또는 Service Fee 가 포함되지 않은 제품의 반입으로 제조사 차원의 기술지원 및 유지보수를 원활하게 받을 수 없을 경우를 방지하기 위해 제조사공급증명 및 기술지원 확약서를 제출하여야 한다.

Ⅲ 제안요청 장비 규격

1. 차세대 방화벽 요건

구분		기능 및 규격	비고
성능 및 제원	성능	• 최대 10Gbps의 방화벽성능을 제공해야 한다. • IPS/Anti-Virus/Anti-Spyware등의 기능 enable시 최대 4.4Gbps의 성능을 제공해야 한다. • 3,000,000 최대 동시 세션(CCS)을 지원해야 한다. • 114,000 초당 처리 세션(CPS)을 지원해야 한다. • 최대 4.8 Gbps IPSec VPN 성능을 지원해야 한다. • 최대 6,000개 IPSec VPN Tunnel을 지원해야 한다. • SSL VPN 최대 2,048 동시 사용자 접속을 지원해야 한다. • 최대 10,000개 이상 정책 설정을 지원해야 한다. • 최대 처리 Concurrent Session 은 모든 보안 기능 사용 시에도 유지되어야 한다.	
	인터페이스	• 12포트 10/100/1000 UTP, 8포트 1/10Gbps SFP/SFP+, 4포트 40Gbps QSFP 이상 제공해야 한다.	
	이중화	• 방화벽 이중화 및 전원 이중화를 지원해야 한다. • High-Availability 구성을 지원해야 한다.	
주요기능	정책 설정	• 정책 설정시 IP, Port, 사용자, Application 4가지를 and 조건이 가능해야 한다. • IP/Port(service) 이외에 사용자/Application/URL 에 대한 and 조건의 추가적인 정책 설정이 가능해야 한다. • 정책의 출발지/목적지에 그룹 오브젝트(ip address) 설정 없이 외부와 연동하여 자동으로 오브젝트 적용이 가능해야 한다. • 정책의 출발지/목적지의 IP 를 나라별로 설정이 가능해야 한다. • 정책별 hit count 기능을 제공해야하며, 재부팅 후에도 유지되어야 한다. • 방화벽 정책별 URL 허용/차단 기능을 설정할 수 있어야 한다. • 시간/날짜별 설정으로 스케줄 정책 설정이 가능해야 한다. • URL 기반의 정책 설정이 가능해야 한다.	
	NAT	• 1:1 NAT, 1:N NAT, N:N NAT을 지원해야 한다. • Static/Dynamic NAT를 지원해야 한다. • 인터페이스 및 정책 기반의 NAT를 지원해야 한다.	
	어플리케이션 통제	• GUI기반의 사용자 정의(Custom) Application 시그니처 생성이 가능해야 한다. • Unknown Application 에 대한 구분과 제어가 가능해야 한다. • Unknown Application에 대한 분석을 위한 자동 packet capture 적용 기능을 제공해야 한다. • 하나의 Application에 대해서 표준 포트 이외의 서비스 포트 변경시에도 Application 분류 및 차단 기능 확인이 가능해야 한다. • 동일한 IP, Port, 설정된 여러 정책에서 어플리케이션별로 구분하여 정책 설정 및 운영이 가능해야 한다. (Port에 상관없이 Application 구분) • 주요 애플리케이션에 대해 Port 변조 시에도 탐지 및 제어가 가능해야 한다. • 지정된 Application 내부의 파일 Type별 탐지와 탐지된 파일의 업로드/다운로드 방향성에 따른 제어 기능을 제공해야 한다. • 개별 Application의 표준포트만 차단/허용이 가능해야 한다. • 개별 Application의 표준포트가 동적일 경우도 Application 트래픽만 차단/허용 가능해야 한다. • Application 별 QoS 정책 설정이 가능해야 한다. • Application의 카테고리 특성, 리스크 별 정책 설정이 가능해야 한다.	

1. 차세대 방화벽(계속)

구분	기능 및 규격	비고
운영 관리	• 사용자 연동 시 계정 및 그룹 정보에 대해서 한글(2byte)을 지원해야 한다. • IPSEC VPN, SSLVPN 동시지원이 가능해야 한다. • 3DES, AES(128-bit, 192-bit, 256-bit) Encryption을 지원해야 한다. • Split Tunneling 기능을 지원해야 한다. • VPN 사용자 인증시 AD, LDAP, RADIUS, SecurID or Local DB Authentication 지원해야 한다. • Windows(XP SP3 - 10), iOS, Android OS에서 SSL VPN 접속을 지원해야 한다. • URL / URI 기반을 설정을 통한 웹 통제 가능을 제공해야 한다. • 암호화 사용 웹 사이트 차단이 가능하여야 한다. • 관리모듈과 서비스 모듈이 분리되어야 한다. • 운영 중 관리프로세스를 리부팅 하더라도 패킷 손실이 없어야 한다. • 내부의 정책 승인 시스템과 연동할 수 있는 시스템(3rd Party)을 통해 자동 정책 관리가 가능하도록 API 기능을 제공할 수 있어야 한다. • 하나의 화면에서 Application, 사용자, IP, 공격 위협 등을 모니터링 할 수 있는 가시성을 제공하여야 한다. • 기존 port base 정책에서 application 정책으로 변환하기 위한 기능을 제공해야 한다. • 각 정책별 사용된 어플리케이션 내역과 어플리케이션 사용시점 정보(최초, 최종)를 제공하여야 한다. • 정책에 적용된 어플리케이션 중 사용되지 않는 어플리케이션을 확인할 수 있어야 한다. • 장비 설정 컨피그를 저장 / 스냅샷 기능을 통합 백업 및 해당 파일을 통한 복구 기능을 지원해야 한다. • 컨피그 변경작업 후 문제 발생시 rollback 을 위한 자동 컨피그 저장 기능을 제공해야 한다. • 컨피그 롤백 시 장비 리부팅이 발생하지 않아야 한다.	

2. 방화벽 이중화 요건

구분	기능 및 규격	비고
방화벽 이중화	• 방화벽 이중화를 위해 현재 운영중인 장비와 동일한 모델(PA-3260)을 제공해야 한다. • 현재 운영중인 방화벽과 동일한 OS(PAN-OS)를 제공해야 한다. • Active-Standby, Active-Active 이중화를 지원해야 한다. • Configuration 및 Session 동기화를 지원해야 한다. • 전원 이중화를 지원해야 한다.	

Ⅳ 제안서 작성

1. 제안서 작성방법

해당 목차를 참조하여 앞에 제안 요구사항 기술하여 제안하여야 한다.

2. 제안서 목차

1) 제안 개요
2) 제안업체 현황
   - 일반현황
   - 수행실적
3) 장비기술부분
   - 장비 규격 및 성능
   - 구축 방안
4) 사업관리 부분
   - 사업수행조직
   - 추진일정
   - 품질 보증(시험 or 테스트)
   - 기밀보호유지
5) 운영 및 유지보수 부분
   - 운영방안
   - 추후 유지보수 방안
   - 기술이전 방안
   - 교육훈련계획
6) 기타