SỞ Y TẾ THÀNH PHỐ HẢI PHÒNG
BỆNH VIỆN TRẺ EM

Số: 442/TM-BVTE
V/v mời báo giá thiết bị CNTT

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hải Phòng, ngày 16 tháng 4 năm 2025

THƯ MỜI BÁO GIÁ

Kính gửi: Quý Công ty, nhà cung cấp.

Bệnh viện Trẻ em có nhu cầu tiếp nhận báo giá để tham khảo, xây dựng giá gói thầu, làm cơ sở tổ chức lựa chọn nhà thầu cho gói thầu mua sắm thiết bị công nghệ thông tin với nội dung như sau:

I. Thông tin của đơn vị yêu cầu báo giá

1. Đơn vị yêu cầu báo giá: Bệnh viện Trẻ em.

Địa chỉ: Phố Việt Đức, phường Đồng Hoà, quận Kiến An, thành phố Hải Phòng.

2. Thông tin liên hệ của người tiếp nhận báo giá: Ks. Nguyễn Phương Thành; Điện thoại: 0913.042.451.

3. Cách thức tiếp nhận báo giá: nhận trực tiếp tại địa chỉ trên.

4. Thời hạn tiếp nhận báo giá: Từ **08 giờ ngày 16 tháng 4 năm 2025** đến **trước 17 giờ ngày 26 tháng 4 năm 2025.**

(Các báo giá nhận được sau thời điểm nêu trên sẽ không được xem xét)

5. Thời hạn có hiệu lực của báo giá: Tối thiểu 90 ngày kể từ ngày tiếp nhận báo giá.

II. Nội dung yêu cầu báo giá

1. Danh mục thiết bị CNTT cần mua sắm.

Chi tiết về danh mục, số lượng, yêu cầu kỹ thuật tối thiểu tại Phụ lục 01

2. Địa điểm cung cấp: Bệnh viện Trẻ em.

Địa chỉ: Phố Việt Đức, phường Đồng Hoà, quận Kiến An, thành phố Hải Phòng.

3. Thời gian dự kiến giao hàng: Quý II/2025.

4. Các điều khoản thanh toán: Theo thoả thuận.

5. Các thông tin khác: Nêu các yêu cầu về bảo hành, bảo trì, hướng dẫn sử dụng, đào tạo, cung cấp phụ tùng thay thế, các điều kiện thương mại….

Kính đề nghị các Công ty/ Nhà cung cấp/ Đơn vị quan tâm và có khả năng đáp ứng gói thầu nghiên cứu phạm vi và yêu cầu kỹ thuật và gửi Báo giá để Bệnh viện có căn cứ xây dựng dự toán của gói thầu.

Nơi nhận:
- Như kính gửi;
- Lưu: VT, VTYT.

Q. GIÁM ĐỐC

SỞ Y TẾ THÀNH PHỐ HẢI PHÒNG
BỆNH VIỆN TRẺ EM

BSCKII. Trần Minh Cảnh

Phụ lục 01

DANH MỤC, SỐ LƯỢNG, YÊU CẦU KỸ THUẬT TỐI THIỂU

(Kèm theo thư mời số 442/TM-BVTE ngày 16 / 4 /2025)

STT	Tên hàng hóa	Tính năng kỹ thuật cơ bản, tối thiểu	Đơn vị tính	Số lượng
1.	Thiết bị Tường lửa (Firewall)	**Phần Cứng thiết bị** - Có sẵn tối thiểu 16 cổng 10/100/1000 Base-T - Có sẵn tối thiểu 06 cổng 10GE SFP+ - Có sẵn tối thiểu 02 khe cắm mở rộng NIC - Hỗ trợ khe cắm mở rộng NIC loại Interface Card lên đến 2 x 40GE QSFP+ - RAM: 16GB - Storage: 256GB SSD - Nguồn: 2 Nguồn, hỗ trợ thay thế nóng **Năng lực thiết bị** Thông lượng tường lửa (Firewall Throughput) tối thiểu ≥ 30 Gbps Thông lượng IPSec VPN ≥ 3.5 Gbps Hỗ trợ IPS thông lượng ≥ 7Gbps/5Gbps Số session đồng thời (Concurrent Connections) ≥ 4,000,000 Hỗ trợ Threat Prevention thông lượng ≥ 3.6Gbps/3.2Gbps Hỗ trợ Web Application Protection thông lượng ≥ 3.2Gbps/1.5Gbps **Tính năng** Có sẵn tính năng định tuyến Layer 3: RIPv1/v2, RIPNG, OSPFv2/v3, BGP/BGP4+ Hỗ trợ tính sẵn sàng cao: Active-Active, Active-Standby, Hardware Bypass Hỗ trợ Site-to-site IPsec VPN (static IP, dynamic IP, dynamic domain) Hỗ trợ xây dựng lại đường hầm VPN (VPN Tunnel) tự động trong trường hợp lỗi nhịp (heartbeat) hoặc chuyển đổi dự phòng HA Bảo vệ chống tấn công DoS/DDoS cho cả mạng	Bộ	1

		và thiết bị Lọc URL với cơ sở dữ liệu chữ ký URL (URL signature) tích hợp Xóa phần mềm độc hại khỏi các tệp độc hại được phát hiện Quản lý băng thông theo ứng dụng, người dùng/nhóm, địa chỉ IP, lịch trình, quốc gia/khu vực, giao diện phụ, giao diện VLAN, đường hầm VPN Kiểm tra gói tin sâu (Deep Packet Inspection - DPI): Xác định các ứng dụng để cho phép/từ chối truy cập Bảo vệ ứng dụng web chuyên dụng với công cụ phát hiện ngữ nghĩa, không phải với IPS Trình quét lỗ hổng web thời gian thực: Phân tích lỗ hổng ứng dụng web ở chế độ thụ động và tạo báo cáo ở định dạng HTML Bảo vệ chống khai thác lỗ hổng: Bảo vệ chống lại các khai thác lỗ hổng nhắm vào hệ thống, ứng dụng, phần mềm trung gian, cơ sở dữ liệu, explorer, Telnet, DNS, v.v. Bảng điều khiển bảo vệ chống Ransomware: Phát hiện và quản lý các rủi ro liên quan đến Ransomware như mật khẩu yếu, cổng rủi ro, v.v. Giúp quản trị viên tạo chính sách bảo vệ chống Ransomware Hỗ trợ bảo vệ tài khoản: hỗ trợ bảng điều khiển chuyên dụng có thể cung cấp thông tin hợp nhất về việc sử dụng bất thường tài khoản người dùng, bao gồm mật khẩu yếu, tấn công bằng cách dùng vũ lực, đăng nhập đáng ngờ, v.v. **Quản lý thiết bị** Hỗ trợ trình tối ưu hóa chính sách: Chỉ cần một cú nhấp chuột để xác định các bất thường trong chính sách kiểm soát truy cập, bao gồm sự dư thừa, trùng lặp và xung đột Hỗ trợ WebUI, SSH, CLI, serial port, SNMP v1/v2c/v3, SNMP trap hỗ trợ mật khẩu cục bộ (Local Password), máy chủ TACACS và máy chủ RADIUS Cho phép quay trở lại firmware trước		

		Cảnh báo qua email về bất thường của phần cứng, mức sử dụng tài nguyên, sự kiện bảo mật, trạng thái HA, .. Khắc phục sự cố qua giao diện Web (WebUI); Xác định lý do mất gói tin theo chính sách, giao diện, v.v. **License tính năng và hỗ trợ kỹ thuật** Thiết bị kèm theo sẵn hỗ trợ kỹ thuật và license 3 năm với đầy đủ các tính năng: SSL VPN, Site-to-Site IPsec VPN, Stateful Firewall, Bandwidth Management, URL Filtering, Application Control, IPS, Botnet Prevention, Email Security, SOC Lite, Basic Security Reporter		
2.	Triển khai hệ thống	**I. Triển khai cài đặt thiết bị** **1. Khảo sát & chuẩn bị trước triển khai:** Khảo sát thực tế vị trí lắp đặt thiết bị tại tủ rack hoặc khu vực vận hành trung tâm mạng. Kiểm tra điều kiện môi trường phù hợp (nguồn điện, hệ thống làm mát, không gian rack, kết nối mạng). Chuẩn bị các phụ kiện cần thiết: dây nguồn, dây mạng, console, giá đỡ (rail kit nếu có), tài khoản truy cập hệ thống. **2. Cài đặt vật lý:** Gắn thiết bị vào tủ rack. Kết nối nguồn và các cổng mạng WAN/LAN theo sơ đồ mạng yêu cầu. Kết nối cổng console để tiến hành cấu hình ban đầu. **3. Cấu hình phần mềm:** Cấu hình thông số IP tĩnh, thông tin VLAN, route tĩnh hoặc OSPF nếu yêu cầu. Triển khai các tính năng bảo mật chính: tường lửa, IPS, lọc web, VPN, kiểm soát ứng dụng, DLP… Đồng bộ thời gian, cấu hình SNMP, nhật ký hệ thống (log), cảnh báo email. **4. Kiểm tra và nghiệm thu:** Kiểm tra luồng truy cập từ LAN/WAN, kiểm thử VPN (IPSec/SSL), tính năng bảo mật đã kích hoạt.	HT	1

		Ghi lại toàn bộ cấu hình, lưu trữ trên thiết bị và sao lưu offline. Bàn giao biên bản nghiệm thu kèm tài liệu cấu hình cho đơn vị sử dụng. **II. Phương án bảo trì thiết bị** 1. Bảo trì định kỳ (3 tháng/lần hoặc theo yêu cầu Hợp đồng): Kiểm tra nhật ký hoạt động và log sự kiện của hệ thống. Kiểm tra hiệu suất CPU, RAM, dung lượng lưu trữ log, thông số nhiệt độ thiết bị. Cập nhật bản vá (firmware) mới nếu được phép. Kiểm tra kết nối VPN, tính toàn vẹn rule tường lửa, cấu hình lọc. Xác minh kết nối SCC và khả năng phản hồi sự cố từ xa. **2. Bảo trì khẩn cấp (khi có sự cố):** Hỗ trợ từ xa hoặc trực tiếp trong vòng ≤ 8 giờ làm việc kể từ khi tiếp nhận yêu cầu. Phân tích log, truy dấu sự cố (packet trace, debug CLI). Cấu hình lại hoặc khôi phục từ file backup (nếu cần). Đề xuất giải pháp tối ưu hóa sau khắc phục (nếu có). **3. Ghi nhận & báo cáo:** Cung cấp biên bản bảo trì, báo cáo tình trạng thiết bị, khuyến nghị nâng cấp định kỳ. Đề xuất thay đổi cấu hình nếu phát hiện rủi ro bảo mật hoặc không tương thích.		